iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** V **Month of publication:** May 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Collaborative Watchdog and Classifier Based Scheme to Detect and Avoid Selfish Nodes in MANET

Aniket Patil[1], Javed Khan[2], Ashish Khandave[3], Abhishek Yadgire[4], Prof.Monika Dangore[5]
[1,2,3,4,5]*Department of Computer Engineering, Dr.D.Y. Patil School Of Engineering, Lohegaon, Pune-411015*

Abstract— Wireless mobile ad hoc networks are self-configuring, dynamic networks in which nodes are free to move. A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires, some-times untrustworthy. From last decade, mobile ad hoc networks have become a very popular research topic. Communication range among mobile nodes in ad-hoc network is limited; hence several hopes are needed in a network to transmit a packet from one node to another node. In mobile ad hoc network, some nodes may selfishly decide only to cooperate partially, or not at all, with other nodes as its a cost intensive activity. This behavior of selfish nodes could then degrade the overall data accessibility which results into performance degradation of overall network. We surveyed some key technique for detecting selfish nodes in MANET.

The proposed system provides a technique used to detect selfish nodes in such network as well as compare them (to study)in order to reduce the effect of selfish nodes in mobile ad hoc networks. The technique is based on classification which generates classes of nodes as partial selfish or fully selfish. To make such classes it uses details of routing such as number of packets sent, received, and dropped. After analyzing every single parameter classes are generated in order to prevent diffusion of false positives in network. By reducing number false positive messages network can be kept stable and functioning for long time.

Keywords— Mobile Ad hoc Networks (MANET), Self-configuring, Cost-intensive, Selfish nodes.

I. INTRODUCTION

Wireless mobile ad hoc networks are self-configuring, dynamic networks in which nodes are free to move. A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Setting up of fixed access points and backbone infrastructure is not always viable Infrastructure may not be present in a disaster area or war zone. Infrastructure may not be practical for short-range radios; Bluetooth (range ~ 10m).

The term ad hoc networking typically refers to a system of network elements that combine to form a network requiring little or no planning. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. Dynamic Source Routing [DSR] and AODV are some algorithms that have been designed to handle such transmission of data [3].

Applications of mobile ad hoc networks have been developed mainly for crisis situations (e.g. natural disasters, military conflicts and emergency medical situations). In these applications, all the nodes of the network belong to a single authority and have a common goal. With the progress of technology, it has now become possible to deploy mobile ad hoc networks for civilian applications as well. Examples include networks of cars parking and provision of communication facilities in remote areas. In such networks nodes do not belong to a single authority and they do not pursue a common goal. In addition, these networks could be larger, have a longer lifetime, and they could be completely *self-organizing*, meaning that the network would be run solely by the operation of the end-users. In such networks, there is no good reason to assume that the nodes cooperate. Indeed, the contrary is true: In order to save resources (e.g., battery power, memory, CPU cycles) the nodes tend to be “selfish”.

Literature studied so far provides two main strategies which helps to deal with selfish behavior: a) motivation or incentive based approaches, and b) detection and exclusion. The first approach, tries to motivate nodes to actively participate in the forwarding activities [17].The detection and exclusion approach is a straight-forward way to cope with selfish nodes and several solutions have been presented [1], [4], [5].

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Impact of node selfishness on MANETs has been studied in [6]–[8]. In [8] it is shown that when no selfishness prevention mechanism is present, the packet delivery rates become seriously degraded, from a rate of 80% when the selfish node ratio is 0, to 30% when the selfish node ratio is 50%. The survey [7] shows similar results: the number of packet losses is increased by 500% when the selfish node ratio increases from 0% to 40%. A more detailed study [6] shows that a moderate concentration of node selfishness (starting from a 20% 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. Therefore, detecting such nodes quickly and accurately is essential for the overall performance of the network.

II. PROPOSED SYSTEM

A mobile ad hoc network (MANET) is an infrastructure-less network. In mobile ad hoc network, some nodes may selfishly decide only to cooperate partially, or not at all, with other nodes in order to save its own resources. This behaviour of selfish nodes could then degrade the overall data accessibility which results into performance degradation of overall network.

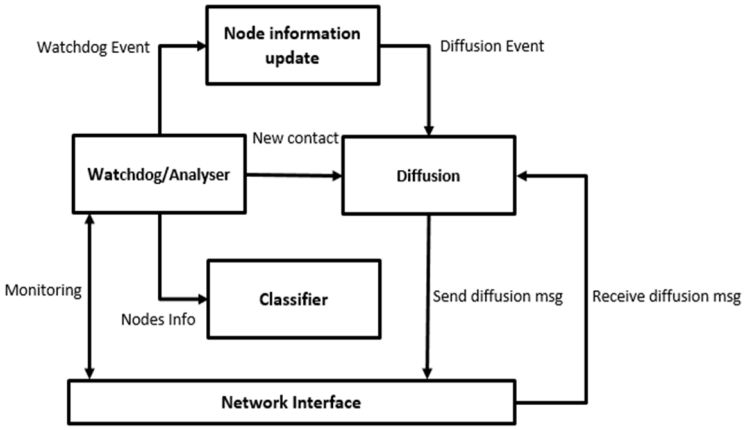


Fig. 1 System Architecture of proposed model

In proposed system nodes have three states:

A. Initial state

1) Initially node does not have any information about any selfish node

B. Selfish contact (Positive)

1) It is a state when a node detects a selfish node using its watchdog and historical record

C. Collaborative contact

1) It is a state when contacts between pairs of nodes occurs to transmit there detection information.

D. Partial Selfish contact (Positive)

1) It is a state when a node detects a partial selfish node using its watchdog and historical record

In proposed method by using the local watchdog can generate a positive (or negative) detection in case the node is acting selfishly (or not) and this decision is based on the ratio between packets received to packets being re-transmitted It is based on the combination of a local watchdog and the diffusion of information when contacts between pairs of nodes occurs. A contact is defined as an opportunity of transmission between a pair of nodes (that is, two nodes have enough time to communicate between them). Assuming that there is only one selfish node, the figure shows how initially no node has information about the selfish node. When a node detects a selfish node using its watchdog, it is marked as a positive, and if it is detected as a non selfish node, it is marked as a negative. Later on, when this node contacts another node, it can transmit this information to it; so, from that moment on, both nodes store information about these positive (or negative) detections. Therefore, a node can become aware about selfish nodes directly (using its watchdog) or indirectly, through the collaborative transmission of information that is provided by other nodes.

E. Classifier

For classifier we have used following mathematical approach:

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Let S be the event that a node has selfishness, S' be the event that the node does not have selfishness, Pos be the event that the node test is positive for the selfishness, and Neg be the event that the node test is negative for the selfishness; that is what is **Test(S | Pos)** ?

Using SVM we first analyze nodes by learning historical data of particular nodes. Then gather the current data of each node and analyze current behavior of each node. On the basis of current data and historical data SVM classifies nodes as selfish or partial selfish.

Here we are using Linear SVM

Given some training data D, a set of n node points of the form

$$\boldsymbol{D = \{(xi, yi)|xi\ \epsilon\ p, yi\ \epsilon\{-t, t\}\}_{i=1}^{n}}$$

Where the *yi* is either t or −t, indicating the class to which the point *xi* belongs. Each *xi* is a *P* dimensional real vector (here *xi* is nothing but the set of packet dropped by each node). We want to find the maximum-margin hyper plane that divides the points having *yi* = *t* from those having *yi* = *-t*. (Where t = positive threshold and –t =negative threshold). Any hyper plane can be written as the set of points *x* satisfying maximum-margin hyper plane and margins for an SVM trained with samples from two classes. Samples on the margin are called the support vectors.

In simpler way we are classifying the nodes have positive threshold and negative threshold. Positive threshold means which satisfies the packet dropped limit, and negative threshold means which is under the packet dropped limit.

III. RESULT AND ANALYSIS

A. *Simulation Setup*

Parameters	Value
Number of nodes	20
Routing Protocol	AODV
Packet Size	256,512,768,1024 bytes
Traffic model of sources	Constant bit rate
Simulation time	100,200,300,400 sec

Table 1

Initially it is assumed that there is only one selfish node. At this stage, no node has information about the selfish node. When a node detects a selfish node using its watchdog, analyzer sends information about that node to classifier and then it is marked as a positive, and if it is detected as a non-selfish node, it is marked as a negative. Later on, when this node contacts another node, it can transmit this information to it. So, from this stage, both nodes store information about this positive (or negative) detection. Therefore, a node can become aware about selfish nodes directly (using its watchdog) or indirectly, through the collaborative transmission of information that is provided by other nodes. This collaborative approach reduces the time and increases the precision when detecting selfish nodes.

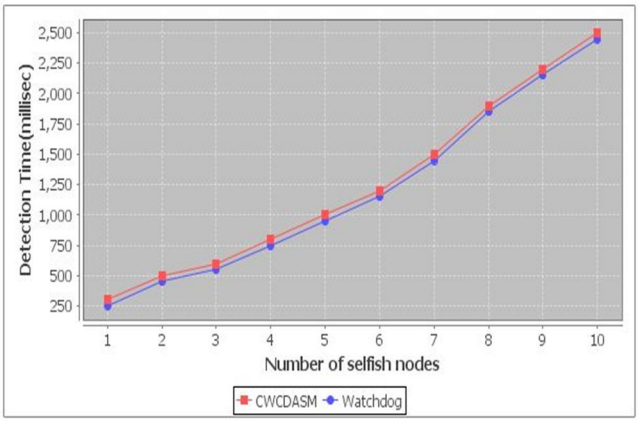


Fig.1 Detection time

Fig 1.illustrates the graphical representation of the detection time of collaborative watchdog method and collaborative watchdog with classifier method. It is clear that watchdog and classifier method takes much less time to detect the same selfish nodes.

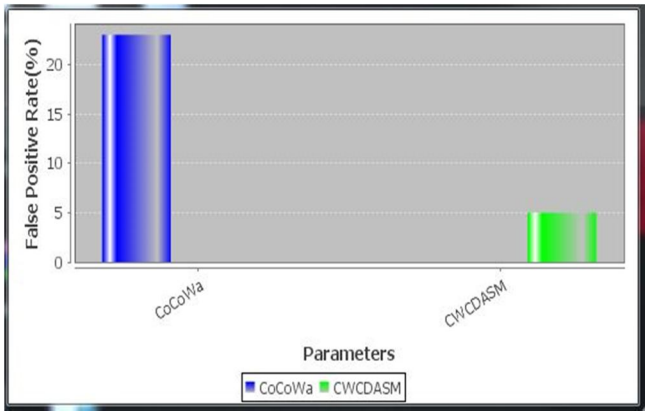


Fig. 2 FDR

IV. CONCLUSION

As we know how the selfish or malicious nodes in ad hoc networks are detected, but it's a complex task. This survey paper considers number of different techniques that can detect selfish nodes .From this survey, we conclude that the reputation based scheme i.e. Collaborative Watchdog is the most efficient technique for detecting selfish nodes. Analytical and experimental results show that it can reduce the overall detection time with respect to the original detection time when no collaboration scheme is used, with a reduced overhead (message cost).

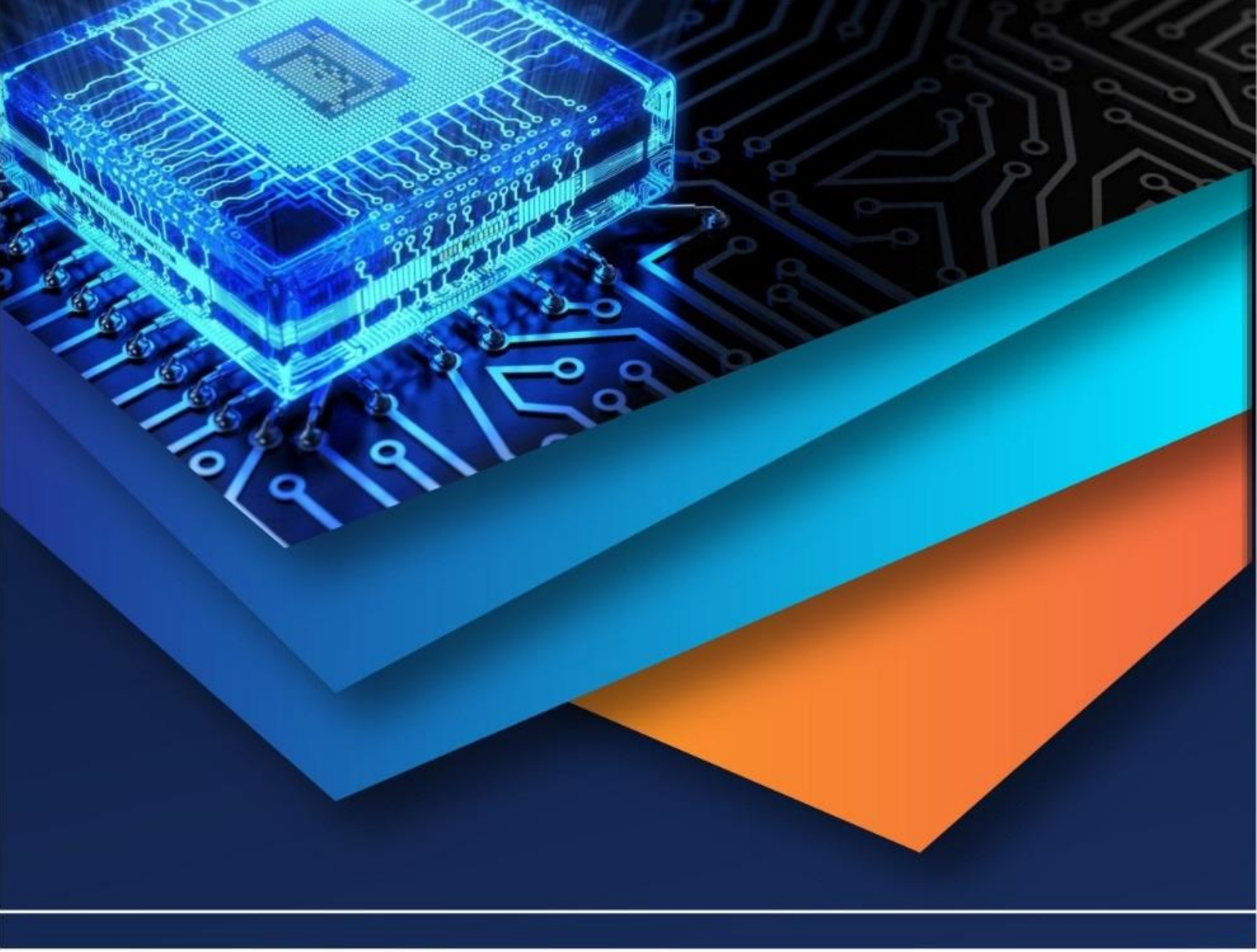
V. FUTURE WORK

One problem that remains with Collaborative Watchdog is that all the thresholds need to be set manually in order to get good detection results. So in the future we will try to find ways how these values can be set and adjusted automatically during operation. We plan to study how we can provide more effective infrastructure-free authentication in ad hoc networks assuming that identities need not be entirely stable at the routing level, but that spoofing of other nodes is unacceptable.

REFERENCES

[1] S. Buchegger and J.-Y. Le Boudee. Self-policing mobile ad hoc networks by reputation systems. Communications Magazine, IEEE, 43(7):101 – 107, jul. 2005.
[2] S.Bansal and M.Baker, “Observation-based cooperation enforcement in ad hoc networks” Stanford University, Tech. Rep., 2003.
[3] KhairulAzmi Abu Bakar and James Irvine “Contribution Time-based Selfish Nodes Detection Scheme” ISBN: 978-1-902560-24-3 © 2010 PGNet
[4] M. Hollick, J. Schmitt, C. Seipl, and R. Steinmetz. On the effect of node misbehavior in ad hoc networks. In Proceedings of IEEE International Conference on Communications, ICC’04, pages 3759–3763. IEEE, 2004.
[5] M. Karaliopoulos. Assessing the vulnerability of DTN data relaying schemes to node selfishness. Communications Letters, IEEE, 13(12):923–925, december 2009.
[6] C. K. N. Shailender Gupta and C.Singla. Impact of selfish node concentration in MANETs. International Journal of Wireless and MobileNetworks (IJWMN), 3(2):29–37, Apr 2011.
[7] C. Toh, D. Kim, S. Oh, and H. Yoo. The controversy of selfish nodes in ad hoc networks. In Proceedings of Advanced CommunicationTechnology (ICACT), volume 2, pages 1087 –1092, feb. 2010.
[8] Y. Yoo, S. Ahn, and D. Agrawal. A credit-payment scheme for packetforwarding fairness in mobile ad hoc networks. In Proceedings of IEEEICC, volume 5, pages 3005 – 3009 Vol. 5, may 2005.
[9] J. R. Douceur, “The Sybil attack,” presented at the Revised Papers from the First Int. Workshop on Peer-to-Peer Systems, 2002, pp. 251–260.
[10] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat "Lightweight Sybil Attack Detection in MANETs" 1932-8184/$31.00 _c 2012 IEEE
[11] S. Marti, T. Giuli, K. Lai, and M. Bakar, “Mitigating routing misbehaviour in mobile ad hoc networks,” in Proc. 6th Annual Int. Conf. on Mobile Computing and Networking (MobiCom’00), August 2000, pp. 255–265.
[12] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehavior in manets,” in IEEE Transactions on Mobile Computing, 2006, pp. 536–550.
[13] D. Monica, J. Leitao, L. Rodrigues, and C. Ribeiro, “On the use of radio resource tests in wireless ad hoc networks,” in Proc. 3rd WRAITS, 2009, pp. 21–26.
[14] Q. He, D. Wu, and P. Khosla, “Sori: A secure and objective reputationbased incentive scheme for ad-hoc networks,” in WCNC 2004, 2004.
[15] S. Buchegger and J. L. Boudec, “Performance analysis of the confidant protocol: (cooperative of nodes – fairness in dynamic ad hoc networks),” in Proc. IEEE/ACM Workshop on (MobiHoc’02), June 2002, pp. 226–336.
[16] P. Michiardi and R. Molva, “Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” in (CMS’02),

September 2002.
[17] Butty´an, Levente, Hubaux, and Jean-Pierre. Enforcing service availability in mobile ad-hoc WANs. In Proceedings of MobiHoc'00, pages 87–96. IEEE Press, 2000.
[18] N. B. Margolin and B. N. Levine, "Quantifying resistance to the Sybil attack," in Financial Cryptography and Data Security. Berlin, Germany: Sprnger, 2008.
[19] K Balakrishnan, J Deng, and P K Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", Proc. IEEE Wireless Comm. And Networking, pp. 2137- 2142, 2005
[20] Kachirski O, Guha R. (2003). "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks", in Proceeding IEEE, (HICSS'03), pp 57.1.
[21] Nasser N, Chen Y. (2007). Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc network, in Proceeding IEEE (ICC'07), pp 1154-9.
[22] Int. J. Advanced Networking and Applications Volume: Issue: Pages: A Review of Techniques to Mitigate Sybil Attacks Nitish Balachandran Department of Computer Science and Information Systems, BITS Pilani
[23] Informant: Detecting Sybils Using Incen-tives N. Boris Margolin and Brian N. Levine Department of Computer Science, Univ. of Massachusetts, Amherst, MA, USA {margolin,brian}@cs.umass.edu.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY