Literature on Detecting Selfish Nodes in Mobile Ad-Hoc Networks

P.Priya[1] B.Gopinathan[2]
[1]P.G. Scholar [2]Associate Professor
[1,2]Department of Computer Science & Engineering
[1,2]Adhiyamaan College of Engineering, Hosur (India)

Abstract— The aim of this paper is to detect the selfish nodes and improves the network performance in Mobile Ad-hoc network (MANET). MANET is a self-organization network in which the mobile devices are connected by the wireless links. In MANET, nodes can freely move in any direction while communicating with each other. The nodes are participated in packet forwarding should be co-operate with each other. If the nodes does not forward the packets to destination means that will be considered as selfish nodes. There are many techniques are available for detecting selfish nodes. In this paper I have provide the comparative study of different type of methods to increase the selfish node detection and improve the network performance and precision speed and network throughput.

Key words: MANET, Selfishnodes, Network performance

I. INTRODUCTION

Mobile Adhoc Network (MANET) is a self-configuring network in which the mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and it will change its links to other devices frequently. The MANET consists of routing protocols namely table-driven routing (TDR)-proactive, on-demand routing (OR)–reactive, and Hybrid routing.- Proactive/reactive each node in the MANET will forward the data to other node but some nodes will not forward the data packet to other nodes they are called selfish nodes. The selfish node will provide different problems in network. Each node is considered in the network are own resources such as- energy, power, CPU time etc… But selfish nodes does not provide the own resource to nearest nodes it means selfish node will not participate in the routing process. If the selfish nodes exist in the network, then there will be a reduction in delivery of packet (dropping the data packets) and increasing the path loss (forwarding path).So, the selfish node detection process is important in order to increase the network performance. Most of the routing algorithms designed for MANET such as DSR and AODV are based on the assumption that every node forwards every packet. But some of the nodes may act as the selfish nodes. These nodes use the network and its services but they do not cooperate with other nodes. Such selfish nodes do not consume any energy such as CPU power, battery and also bandwidth for retransmitting the data of other nodes and they reserve them only for themselves.

II. RELATED WORK AND ITS METHODS

In this section the detection of selfish nodes and its methods are discussed.

A. Improving Selfish Node Detection using A Collaborative Watchdog in Mobile Ad-Hoc Networks:

In this paper they use watchdog technique for detecting selfish node in network. This watchdog technique is used to improve the accuracy of network performance and it is based on the contact dissemination of detecting selfish nodes. Here they explain the concept of selfish contact and collaborative contact. They consist of two approaches namely isolation and incentivation. The isolation means intended to keep the misbehaving nodes outside the network, excluding them from all kinds of communication. The incentivation means try to convince the selfish nodes to change their behaviour and become collaborative instead of selfish, using a virtual payment scheme. In this system they introduce an analytical model to evaluate the detection time and the cost of this collaborative approach. Numerical results show that our collaborative watchdog can dramatically reduce the overall detection time with a reduced overhead. These results shows that can results with a network not having selfish nodes.

B. Audit-based Misbehaviour Detection in Wireless Ad Hoc Networks:

In this paper they described the AMD it evaluates the node behavior per-packet basis, without employing energy expensive overhearing techniques or intensive acknowledgment schemes. AMD can detect selective dropping attacks even if end-to-end traffic is encrypted and it can be applied to multi-channel networks or networks consisting of nodes with directional antennas. AMD can construct a path consisting of highly trusted nodes, this system consists of the integration of three modules: a reputation module, a route discovery module, and an audit module. These modules closely interact to coordinate the functions of misbehaviour detection, discovery of trustworthy routes, and evaluation of the reputation of peers. In this system, it will integrate three critical functions namely reputation management, route discovery, and identification of misbehaving nodes. It will reduce overall detection time with reduced cost in terms of message overhead.

C. Cross Layer Approach for Selfish Node Detection in MANET:

This paper evaluates the AODV (Ad hoc On-demand Distance Vector routing protocol) routing protocol, there are four control messages used to establish and maintain the information and the transmission paths. These control messages include Hello message, Route Request (RREQ) message, Route Reply(RREP) message and Route Error(RERR) message. These types of control messages will process the communication in proper manner. This methods will describe the degree of detecting misbehaviour nodes in ad-hoc networks. Here we are using higher-layer protocol that requires some information from the lower layer at runtime results in the creation of a new interface from the lower layer to the higher layer. In this method it does not provides better classifier of detecting selfish nodes.

D. Selfish Nodes Detection using Random 2ack in MANET:

In this paper, they introduce 2Ackschemes to detect routing Misbehaviour. This 2ACK scheme is a network layer technique in order to detect selfishness and to mitigate their effects. It can be implemented through DSR (Dynamic Source Routing) routing protocol. The 2Ack schemes are used inorder to detect the misbehaviourrouting through the new type of acknowledgment termed as 2Ack packets. The random 2ACK technique is based on a simple 2-hop acknowledgment packet that is sent back by the receiver to next-hop link. The 2Ack techniques take more time to detect selfish nodes, and also it will take more time to get the acknowledgement message because here there may be a packet drop.

E. The COMMIT Protocol for Truthful and Cost-Efficient Routing in Ad Hoc Networks with Selfish Nodes:

This paper presents a COMMIT, a protocol for route discovery and packet forwarding in ad hoc networks that enjoys the same nice features as Ad Hoc-VCG (energy efficiency and truthfulness). The COMMIT protocols achieve the same goals are individual rationality, Truthfulness, energy efficiency, and limited message overhead. In this protocol identified a quantity that can be considered the intrinsic cost of cooperation and pointed out that topology control can be used to curb this cost. The truthful implementations of the individual tasks are a good starting point for designing a comprehensive truthful solution. Finally, In this COMMIT protocol are considered the energy about the a node, doesn't calculated to detect the selfish nodes.

F. Power-Law Inter-Meeting Time in Mobile Ad-Hoc Networks:

In this paper it describes the key metrics in MANET, and also they use end to end delay forwarding algorithm. This protocol will discuss about the relation between the size of the boundary and timescale of interest, and their effect on the inter-meeting time, that's imply removing the boundary it can quickly change the inter-meeting time distribution from exponential to power-law by studying a simple random walk in an open space. This result shows the performance analysis, and protocol design inorder to survive the the power-law distribution of the inter-meeting time in MANET.

G. Innovated Techniques to Detect Selfish Nodes in MANET:

This paper discusses three techniques namely Reputation based technique, Credit based technique and Acknowledgement based technique. These are the techniques that will used to detect the selfish nodes. The reputation based technique is the indication of the other nodes. The reputation value is high then selfish node is co-operated and the reputation value is low then the node is considered to be selfish by other nodes. Credit based schemes will get the credit for every packet you forward and pay some of the credit to send a message to yourself. Acknowledgment based schemes will uses the ACK packets to ensure its node forwarding. If the node does not receive the ACK for the data packets means it will find one selfish node among all the nodes.

H. Intrusion Detection Methods:

Here, all nodes are cooperating with each other in routing and transmitting the packets inorder to deliver the packets to the specified destination. There is no fixed infrastructure in mobile Ad hoc networks. Intermediate nodes may agree to forward the packets, but in fact they delete or modify them, because they are malicious. Only a few misbehaving nodes (malicious nodes, selfish nodes) can decrease whole system performance. There are several methods and protocols have been proposed to detect and prevent such misbehaving nodes. In this technique identifies misbehaving node by eavesdropping on the transmission of the next hop. When a node forwards packets, Watchdog verifies whether the next node in the route forwards the packets or not. If the next node refuses to forward the packets, then it is known as misbehaviour. The advantages of Watchdog mechanism is that it can identify misbehaving nodes not in forwarding level but also in the level of connection. In other words, it identifies nodes not only in the link layer, but also in the network layer.

I. Cooperation Of Nodes, Fairness in Dynamic Ad hoc Networks (CONFIDANT):

CONFIDANT protocol consists of Monitoring System, Reputation System, Trust Manager and Path Manager. Their tasks are divided into two sections: The process to handle their own observations and the one to handle reports from trusted nodes. For observations, the monitoring node uses a neighbourhood watch within its radio range to discover any malicious behaviour. If a dubitable event is detected, monitoring node then reports it to the reputation system. At that time, the reputation system accomplishes several checks and updates the rating of the reported node in the reputation table. If the rating result is dubitable, it forwards the information to the path manager, which then omits all paths containing the misbehaviour node. Then the trust manager sends an ALARM to warn other nodes that monitoring node receives an ALARM message from trusted nodes, at first the trust manager evaluates the message to see if the source node is trustworthy. If so, the ALARM message with the trust level will be stored in the alarm table.

III. CONCLUSION

A MANET network consists of a group of mobile devices (nodes) communicating through a wireless medium. As the use of Mobile Ad hoc Networks (MANETs) has increased. The MANET security has become more important. So, I am going to introducing collaborative methods. CoCoWa: 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).Our watchdog approach is much more secure than the Existing system.

REFERENCES

[1] Reshma,Prof.P.Pachamuthu"Detecting Selfish Nodes in MANETs using Collaborative Watchdogs "in Proc .IEEE Conf, March 2013.
[2] Karthik m, JyothishJohn,"A Survey of Techniques used to Detect selfish Nodes in MANETs" in Proc.Common Technology,Feb 2013.

[3] G.MurugaBoopathi,N.Insozhan,S.Vinod," Selfish Nodes Detection Using Random 2Ack in MANETs"International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013 .
[4] Radu-Ioan Ciobanu, Ciprian Dobre, Mihai Dascalu, Stefan TrausanMatu, Valentin Cristea"Collaborative Selfish Node Detection with an Incentive Mechanism for Opportunistic Networks" in Proc2013 IFIP"
[5] 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.
[6] Enrique Hernandezorallo, Manuel D.Serrat, Juan-Carlos Cano" A Fast Model for Evaluating the Detectionof selfish Nodes Using a Collaborative Approach in MANETs &2012.
[7] Prof. Rekha Patil, Shilpa Kallimath "Cross Layer Approach for Selfish Node Detection in MANET "International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 1, Issue 3, September 2012 .
[8] C. E. Perkins, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, IETF Network Working Group, 1998.
[9] [9].S.Buchegger and J.-Y. Le Boudee,"Self-policing mobile ad hocnetworks by reputation systems," IEEE Commun. Mag., vol. 43, no.7,pp. 101–107, July 2005.
[10] M.Karaliopoulos, "Assessing the vulnerability of DTN data relaying schemes to node selfishnes,"IEEE Commun. Lett.vol. 13, no. 12, pp.923–925, Dec. 2009.
[11] Y. Li, P. Hui, D. Jin, L. Su, and L. Zeng, "Evaluating the impact of social selfishness on the epidemic routing in delay tolerant networks," IEEE Commun. Lett., vol. 14, no. 11, pp. 1026–1028, Nov. 2010.
[12] Y. Li, G. Su, D. Wu, D. Jin, L. Su, and L. Zeng, "The impact of node selfishness on multicasting in delay tolerant networks," IEEE Trans. Veh. Technol., vol. 60, no. 5, pp. 2224–2238, June 2011.
[13] H. Otrok, M. Debbabi, C. Assi, and P. Bhattacharya, "A cooperative approach for analysing intrusions in mobile ad hoc networks," in Proc. 2007 International Conference on Distributed Computing SystemsWorkshops, p. 86.14.
[14] E. Hern_andez-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.
[15] F. Kargl, A. Klenk, S. Schlott, and M. Weber, "Advanced detection of selfish or malicious nodes in ad hoc networks," in Proc. 1st Eur.Conf. Security Ad-Hoc Sens. Netw. 2004, pp. 152–165.

