International Journal of Innovative Research in Information Security (IJIRIS) ISSN: 2349-7009(P)
Issue 05, Volume 04 (May 2017) SPECIAL ISSUE www.ijiris.com ISSN: 2349-7017(O)

Identifying Selfish Nodes Using Contact Based Watchman

Rachitha M V[#1], Amit Singh[#2], Bharath N Gowda[#3], Poornachandra[#4], Yashavanth Yadav[#5]
[1]*Assistant professor,* [2,3,4,5]*Department of computer science and engineering,*
Vemana IT, Bangalore, India

Abstract: ***In MANETs the cooperation between nodes of the network is more important for data transmission to occur in a efficient manner. But, it is not true that all nodes of the network actively participate in data transmission process without affecting network performance. The nodes with selfish behavior reject to cooperate with other neighbor nodes of the network for data transmission activity. Selfish nodes lower the performance of the network by causing data loss or they induce wrong data in the network. The existing local watchdog mechanism is used to identify such nodes, but it is not a good mechanism because it originates wrong positives and wrong negatives. So, in this paper we are introducing a watchman with cooperative characteristic to mark greedy nodes and distribute the same information to other neighbor nodes. With this the energy consumption is saved and the selfish nodes are identified earlier and accurately***

Keywords: ***Manet, Watchman, Watchdog***

1. INTRODUCTION

Network cooperation is becoming a significant emerging design for network layout strategy for wireless mobile networks. The success of network cooperation can lead to cost-effective network services for a specific purpose ambulatory or social networks. The network cooperation is usually based on contact between nodes of the network. The mobile nodes of the network can communicate with one another if contact exists between them, if the communication range provides the nodes the essential infrastructure [1]. The cooperative network usually reduces cost effectiveness i.e., it may lead to cost intensive network particularly with respect to mobile nodes. In the cooperative network design some nodes may behave as selfish nodes. The term selfish node in the context of network means that the node with the selfish property rejects to forward the packet received by it to another node in the same network. So, these selfish nodes must be detected in order to improve the performance of the network along with reducing the energy consumption. Several methods are used to deal with networks containing selfish nodes. We may motivate all the nodes of the network to actively participate in the data transmission, else to detect the malicious selfish nodes and exclude them from the network. The impact of selfish nodes on the performance of network has been studied in various papers. Selfishness nodes degrade the performance of the network from eighty percent to thirty percent, when selfish nodes exist in network. The loss of packets also increases parallel with the increase of selfish nodes. The packet loss is about five hundred percent when the rate of selfish nodes is increased from zero percent to five hundred percent. A selfish node changes the Route Request and Reply packets. It also excludes routing messages. The detection of such selfish nodes that affect the overall performance of the network is highly essential. Hence in our paper we are using a local Watchman in a efficient collaborative manner to detect selfish nodes. In our project we are using positive and negative scheme. If any of the node is indicated as positive, then it is treated as selfish node, else if it is marked as negative, then it shows that node is not a selfish one. This detection mechanism involves use of efficient cooperative Watchman for each of the node participating in data transmission of the network. Some of the characteristics of a selfish node can be mention as follows. It does not participate in data transmission activity of the network. It may drop some packets forwarded to it by its neighbour node. It also delays the RREQ message.

II. EXISTING SYSTEM

The Local Watchdog technique nodes with selfishness behavior are motivated to actively participate else they are excluded from the family of network. The main drawback is that the existing system sometimes produces positive false and negative false for the nodes of the network. The false negative for a node is generated by the Local Watchdog[11] when it is not a selfish node, it generates positive when the node is detected as selfish node. The other main drawback is that some nodes may mislead other nodes by giving false information about other nodes.
The disadvantages of the existing system are:

- *Increases selfish nodes*
- *Increases the packet loss*
- *Reduces throughput value*
- *Increases overhead of the network.*

III. RELATED WORK

The previous research works related to detection of selfish node behaviour tried to motivate the nodes with selfish behaviour to actively participate in network transmission activities or to discard them so that they will not induce wrong functions. A credit based system was given by Zhong called as SPRITE. This SPRITE system found new ways to provoke the network participants to rigorously/energetically associate in data transmission work. This incentive mechanism posed several problems. Requires a basic infrastructure to maintain accounting of nodes. Tamper proof hardware was also used. Game theoretic techniques and COMMIT[12] protocol are made use to achieve truthfulness to lower the knock of selfish nodes on credit payment scheme. Some antecedent activities, it showed that some percentage of cooperation can better the notice selfish nodes. A protocol named confidential was suggested, which integrates a Watchman, System of reputation. A IDS is introduced in another system to detect selfish nodes. A node raises a response by locally identifying intrusion with suitable proofs. If the proof is found to be weak, while detecting a intrusion, it can induct a incursion identifying procedure globally. A familiar mobile intrusion detection system is also used for the same purpose. The mechanism called CORE [collaborative reputation mechanism] is comparable to the distributed IDS[9] technique used by Zhang, a reputation value for each participant of the network is calculated, consolidated and dispensed. The selfish node impact on MANETs[6] is also studied by using SORI protocol, which detects and excludes selfish nodes. By using this agency the trust of a node is calculated by using table maintained for each of the node, which holds first and second hand trust (neighbours) of nodes. The protocol named confidant adjoins trust manage, index reputation to the Local Watchman along with path rater technique. Two lists are used for the purpose to list some nodes which behave sensibly/intelligently are kept in one list. The nodes which act to drop packets received by them to forward to its trusted nodes are put in blacklist. The previous mechanisms identified deployment of Watchman is the most worthy technique to motivate or expunge selfish nodes from the network, In order to increase the performance of the network by reducing the packet loss rate. The impingement of selfish nodes on MANETs has been studied deeply in all of the above coated mechanisms and different counter mechanisms have also been deployed. A selfish node usually denies packet forwarding/drops routing messages. It does not responds to hello requests of the neighbour nodes. It also alters ROUTE REQUEST and ROUTE REPLY messages by modifying TTL values. A mechanism to motivate the participants of the network used nuglet, a virtual currency. This virtual currency is transferred to the intermediate nodes, so that the nodes will actively forward route messages/data packets. Every node of the network is assigned some value of the nuglet. The nuglet is credited to the intermediate nodes to motivate them to forward traffic. This credit is carried out either by source or destination node. If the enough payment (nuglet) is not funded to the relay nodes to forward packets, then the relay nodes intentionally neglects to forward the traffic thrown by the source. The second mechanism of the same protocol to detect or exclude the selfish nodes uses different machinery. The primary trust and secondary trust values are used for the expulsion process of selfish nodes. The nodes investigate about their nearby residents and records values in the primary trust table. The secondary trust hand table contains values related to the values of the neighbour nodes given for other nearby residents of the network.

IV. METHODOLOGY AND SYSTEM ARCHITECTURE

The project uses a new mechanism called contact based Watchman instead of Local Watchdog which was used in existing system to recognize selfish nodes. The main strategy used in the project work is to distribute the information obtained by the Contact based Watchman to neighbor nodes of the network. The information obtained is shared by one node with other when a association takes place with the node. The detection time of the greedy node is reduced and the self-interested nodes are detected accurately. The Local Watchdog has two functions: 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 (for example if the contact time is very low or it does not overhear enough messages). The detection of new contacts is based on neighborhood packet overhearing; thus, when the watchdog 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 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, but sending all known negative detections can be troublesome, producing excessive messaging or the fast diffusion of false negatives.

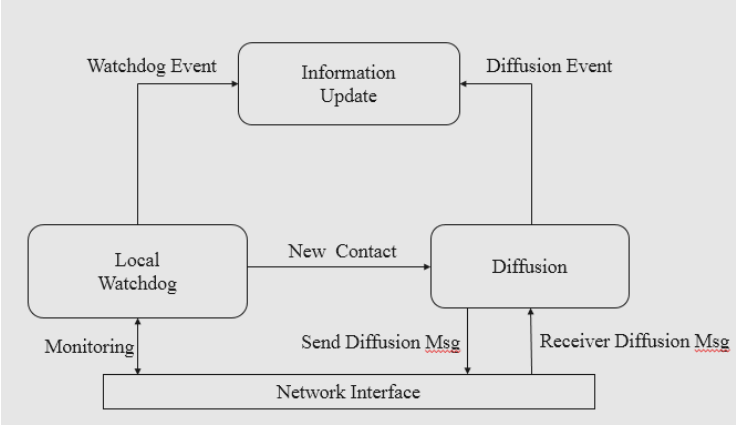

Fig 1. Structure of Watchdog.

Consequently, we introduce a negative diffusion factor g that is the ratio of negative detections that are actually transmitted. This value ranges from 0 (no negative detections are transmitted) to 1 (all negative detections are transmitted). We will show in the evaluation section that a low value for the g factor is enough to neutralize the effect of false positives and false negatives. Finally, when the diffusion module receives a new contact event from the watchdog, it transmits a message including this information to the new neighbor node. When the neighbor node receives a message, it generates an event to the network information module with the list of these positive (and negative) detections. Updating or consolidating the information is another key issue. This is the function of the Information Update module. A node can have the following internal information about other nodes: No Info state, Positive state and Negative state. A No Info state means that it has no information about a node, a Positive state means it believes that a node is selfish, and a Negative state means it believes that a node is not selfish. A node can have direct information (from the local watchdog) and indirect information (from neighbor nodes).

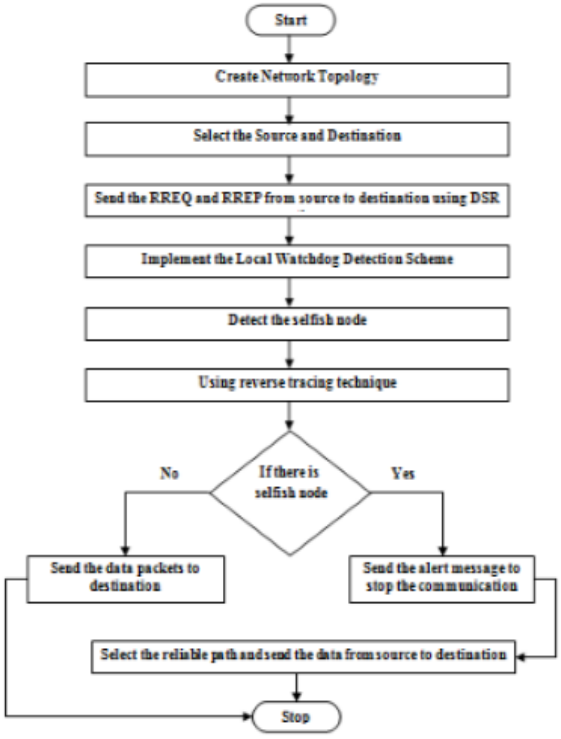

Fig.2 Flow chart for contact based watchman

Fig. 2 shows step by step dataflow summary of the events and actions in the application. The user starts the Application by creating a network topology. Once we have created the network topology we need to select the source and destination. Once the source is created, need to send the RREQ and RREP from source to destination using DSR. After this the Local Watchdog Detection Scheme should be implemented.

The selfish node node is detected and we need to check if there is a selfish node using the reverse tracing technique. If it is true send the alert message to stop the communication and select the reliable path and send the data from source to destination. If it is false send the data packets to destination and the application is halted.

V. CONCLUSION

In this proposed system the energy consumption is lowered by detecting greedy nodes in the MANETs[3] earlier and accurately. For this purpose of detecting selfish nodes in MANETs the contact based watchman is used as a new mechanism, which performs better than the previous Local watchdog used in existing system. The dissipation of information about the selfish nodes is the newly implemented mechanism in the proposed system. The experimental results show that overall detection time of selfish nodes is lowered compared to the detection time of selfish odes in existing system. The overhead of the network is also reduced by the proposed system. The probability of selfish node identification is also increased in this project. The overall effect of selfish nodes in the MANETs is reduced with this contact based watchman detection method

REFERENCES

[1]. S. Buchegger and J.Y. Le Boudee. Self – policing mobile ad hoc networks by reputation systems. Communication Magazine, IEEE, 43 (7): 101 – 107, jul.2005.
[2]. Shailender Guota, C K Nagapal and charu Singla "Impact of selfish node concentration in MANETs", International Journal of Wireless and Mobile Networks (IJWMN) Vol.3, No. 2, April 2011
[3]. Enrique Hernandez-Orallo, Manuel D Serrat, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni "Improving selfish node detection in MANETs using a collaborative watchdog", IEEE COMMUNICATIONS LETTERS, VOL.16, NO.5,MAY 2012.
[4]. Elizebath M Royer, Charles E. Perkis, "An Implementation study of AODV Routing Protocol".
[5]. D. Johnson, D. A. Maltz, Dynamic source routing in ad hoc wireless networks," in Mobile computing systems and applications, (T. Imielinksi and H. Korth, eds.), Kluwer Acad.Publ., 1996.
[6]. C. K. N. Shailender Gupta and C. Singla, "Impact of selfish node concentration in MANETs," Int. J. Wireless Mobile Netw., vol. 3, no. 2, pp. 29–37, Apr. 2011.
[7]. C. Toh, D. Kim, S. Oh, and H. Yoo, "The controversy of selfish nodes in ad hoc networks," in Proc. Adv. Commun. Technol., Feb. 2010, vol. 2, pp. 1087–1092.
[8]. Y. Yoo, S. Ahn, and D. Agrawal, "A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks," in Proc. IEEE Int. Conf. Commun., May 2005, vol. 5, pp. 3005–3009.
[9]. X. Zhang, G. Neglia, J. Kurose, and D. Towsley, "Performance modeling of epidemic routing," Comput. Netw., vol. 51, no. 10, pp. 2867–2891, 2007.
[10]. Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbehavior detection in wireless ad hoc networks," IEEE Trans. Mobile Comput., vol. PP, no. 99, 2012, http://doi.ieeecomputersociety. org/10.1109/TMC.2012.257
[11]. Y. Zhang, W. Lee, and Y.-A. Huang, "Intrusion detection techniques for mobile wireless networks," Wireless Netw., vol. 9, no. 5, pp. 545–556, Sep. 2003.
[12]. S. Zhong, J. Chen, and Y. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in Proc. IEEE Conf. Comput. Commun., Mar. 2003, vol. 3, pp. 1987–1997

