ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

Trust Aware Watchdog Mechanism to Detect Selfish Node in MANET

Resmi C. S[1], Sindhu S[2]

PG Student, Computer Science & Engineering, NSS College of Engineering, Palakkad, India [1]

Associate Professor, Computer Science & Engineering, NSS College of Engineering, Palakkad, India [2]

Abstract: MANET nodes rely on network cooperation schemes to properly work. Node cooperation is important since there is no fixed infrastructure and central authority in MANET. There is the possibility of existence of nodes refuse to cooperate by not forwarding data in order to save its own energy and resources. Presence of selfish node degrades network performance by increasing packet dropping. Collaborative watchdog introduces an efficient approach to reduce the detection time of selfish nodes based on contact dissemination. If one node has previously detected a selfish node using its watchdog it can spread this information to other nodes when a contact occurs. This method does not consider presence of malicious node and detection function to be implemented in every pair of nodes. In this paper, we propose a new framework which uses a trust based scheme and watchdog to detect selfish node.Also alert model is implemented in which node which are not ready to cooperate can send warning messages to adjacent nodes. Trust relationship must be set up between every pair of nodes. Packet forwarding ratio and energy is used to maintain trust between nodes. Watchdog functions are implemented in trusted node only. It reduces the overhead of implementing watchdog in every node.

Keywords: selfish node, reputation, trust, mobile ad hoc networks (MANETs).

I. INTRODUCTION

MANET is one of active research area in wireless network. Since the popularity of wireless network and mobile devices increased significantly, it is now become one of most lively and active field of communication and networking research.

Mobile ad hoc networks (MANETs) are characterized by their autonomous nature and the lack of a central authority. Each device is free to move independently, causes dynamic topology of MANET. Major problem in MANET is to maintain information needed to route traffic efficiently. Mobility of nodes and changing topology make it susceptible to various kinds of attacks such as packet modification, eavesdropping etc. Providing security to such a environment is difficult.

The routing protocols in MANET are proactive routing protocol and reactive routing protocol. In proactive routing, routing table get updated periodically. In reactive routing routing table is updated only when it is needed.
The major security challenges in the wireless ad hoc networks are the lack of a central control and the fact that each node has to forward the packets of other nodes. Consequently, each node in the network is expected to be highly cooperative, in forwarding packets sent from another node. However, since each node has its own constraints such as limited availability of power, which needs to be preserved, encouraging cooperativeness is difficult.

MANET is suitable in areas where it is difficult to set up a fixed infrastructure like natural or human induced disasters, military and rescue applications. In these scenarios, nodes are deployed without the support of pre-existing infrastructures for communication. As a result, nodes in a wireless ad hoc network need to configure themselves through their own communication activities to form a reliable infrastructure during initialization for further operations. However, since the mobile nodes in this network are constrained with limited resources, such as CPU, battery, channel bandwidth some nodes in the network might not be willing to cooperate for the packet transmission, in order to save their resources. Since lack of central authority to manage packet transmission, we cannot guarantee the cooperation between nodes. There will be a chance that some nodes try to maximize its benefit by not forwarding the packet of others but enjoying the service provided by network at same time. Presence of selfish node will degrade the performance of network and it may lead to network partition. So efficient mechanism must be find out to detect selfish node and to ensure cooperation of nodes.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

In MANET trust management between participating nodes is essential. Trust is a relationship exists between two entities; it helps to create relationship between nodes in network. In this paper trust based scheme will classify nodes to trusted node and regular node. The node which joins the network at any time will be in either of these classifications. Packet delivery ratio and energy is used to calculate trust between nodes. Main reason for selfish node behaviour is some node have low energy. So source must route packets through nodes which have sufficient amount of energy. When energy of a node is lower than predefined threshold level, then node does not ready to cooperate with other nodes. The collaborative watchdog function implement only in trusted node. The new mechanism help to save energy consumed by deploying detection function in every node by assigning trusted nodes for detection function. Since watchdog has limitation like ambiguous collision, receiver collision this method helps to ensure cooperation of nodes more efficiently. Packet dropping will be less than collaborative watchdog approach. This paper presents a novel approach to detect selfish node in mobile adhoc network. Simulation result shows that this approach reduces detection load and complexity for other nodes.

The remainder of this paper is organized as follows. Related work of node cooperation and trust based routing introduced in Section II. The proposed concept is discussed in Section III and concludes this paper in Section IV.

II. RELATED WORK

Two main strategies are there to deal with selfish behaviour of node in MANET. Reputation based and credit based approach. Credit based approach uses virtual currency to stimulate cooperation of nodes. Node forward others traffic will get paid. They use same payment scheme to forward its own packets. Packet trade model [1] and packet purse model are two approaches based on this concept.

Reputation based approach uses reputation values based on behaviour of node. Watchdog and pathrater [2] are used to detect selfish node based on reputation value. It is a scheme for selfish node detection by overhearing other nodes. A buffer is maintained by each node for recently sent packet. Packets within buffer are compared with overhearing packet and match occurs then discard packet from buffer. Then pathrater helps to find reliable route to destination. CONFIDANT [3] detect selfish nodes and alarm messages are sends to other node to inform presence of selfish node.2ACK [4] scheme used to detect misbehaving link and detect misbehaving node which is two hop away from source node. Overhead is high in this approach. CORE [5] is a mechanism based on reputation .It uses network entity, reputation table and watchdog mechanism to find reputation value of other nodes .Contact based collaborative watchdog mechanism [6] uses local watchdog mechanism to detect selfish nodes and diffuse the collected information to network when contact occurs. This method can reduce detection time and reduce false positive and false negative since it uses second hand information to detect selfish node. But complexity will be high since detection function need to be implemented in every node.

T. Ghosh [7] proposed a trust based Ad hoc On-Demand Distance Vector routing protocol. It uses trust to detect malicious nodes. It uses the existence of public key infrastructure. In paper [8] intermediary nodes act as trust gateways and it check trust levels of the nodes for avoiding malicious nodes. Each node monitors its neighbours and maintains a direct trust value for them. Source node uses this trust information to compute the most trustworthy path.

III.PROPOSED SYSTEM

Trust between nodes must be ensured. Packet forwarding ratio is used a metric to calculate trust between nodes. Packet forwarding ratio is less than threshold limit then node is not cooperative in nature. The packet forwarding ratio is the ratio of how many packets the node has received and forwarded successfully.
Suppose node i checking behavior of node j the trust value using packet forwarding ratio is calculated by equation,

$$T_{i,j}(t)=\frac{Fi,j(t)}{Ri,j(t)}$$

$F_{i,j}(t)$represents the number of packets forwarded by node j at time t, $R_{i,j}(t)$ represents the number of packets successfully received by node j at time t.

If packet forwarding ratio is decreased above a particular limit then it indicates that node is not cooperative. The trust value of a node is between 0 and 1 and a threshold value is defined to check if trust value of node is less than threshold the node considers to be not trusted. After regular interval number of packet received and forwarded by each node is used to update trust table. The equation for updating the trust value is,

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

T_{val}=a * T(old) + (1-a) * T(new)

Where a is a weighting factor used to balance current measurement and previous estimation. So in this way the packet forwarding ratio is calculated for every neighbor node and stored in the trust table.

In MANET, the nodes are spending some energy for receiving data packets and amount of energy for forwarding the packet to neighbour nodes. Initially all nodes have maximum battery capacity. Energy consumes only when communication begins. Reason for selfish behaviour of node is less battery power. Node energy utilization will be high for trusted node, since they use network to forward packet of others. But selfish node does not cooperate with other nodes, hence energy consumption will be low. So there is more chance to become a node selfish when its energy is low. So calculation of energy of nodes in network helps to avoid packet dropping since there will be more chances to behave such node as selfish. Energy utilized at node Y due to node X can be calculated by following equation.

$E_{value}=E_{T\,ack}+E_{T\,pck}+E_{R\,ack}+E_{R\,ack}$
Where,
E_{value}= Energy utilized at node Y due to node X
$E_{T\,ack}$= Energy utilized for one acknowledgement
$E_{T\,pck}$= Energy utilized for transmission of one Data packet
$E_{R\,ack}$= Energy utilized for reception of one ACK Packet
$E_{R\,ack}$= Energy utilized for reception of one Data packet

If the energy value less than a threshold then the node does not consider as a trusted node. Because packet dropping chances are higher when consider these nodes in transmission.

Both energy and packet forwarding ratio is used to calculate trust between nodes. The watchdog mechanism will be implemented on trusted nodes. Watchdog mechanism uses a local watchdog to detect selfish node and every node receives indirect information about selfish node. Initially local watchdog assigns NOINFO and this will get updated when a node find selfish node. Node broadcast information to neighbor.

Different states are,

1. If node find its neighbor as selfish, send POSITIVE
2. If malicious node lie about selfishness send NEGATIVE
3. If a node found nothing then it will send NOINFO

Node reputation=Local watchdog info+ Indirect info

Alternative route is found out to avoid packet dropping by selfish node. Alert model is implemented in which warning messages are sending to the adjacent nodes. When a source need to send data to a destination it uses several intermediate nodes. If a node which are not ready to cooperate can send warning message to adjacent nodes. Then adjacent nodes can select routes which do not contain these nodes.

The main intention of selfish node is to use network resources and save its own resources by not forwarding the packet of others. If there is selfish node exists between source and destination then it must be avoided from route to reduce packet drop. So a new field must be inserted in Hello packet to store selfish status. It will help other nodes to inform that the node is selfish in nature. If node is selfish then necessary actions must be taken to avoid that node from route. Remove it from active routes, send Route Error packet to source to establish new routes. Does not allow it being a member in any route, drop Route Request packet coming from it.

IV. CONCLUSION

In this work a trust aware framework to detect selfish node is proposed which reduces the detection time. Both energy and packet delivery ratio is used to calculate trust between node. It will reduce packet dropping .Watchdog mechanism is implemented in trusted node, reduces overhead. This approach improves network performance and throughput.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

REFERENCES

[1] L. Butty an and J.-P. Hubaux, "Stimulating cooperation in self organizing mobile ad hoc networks," Mobile Netw. Appl., vol. 8,pp. 579–592, 2003.
[2] J. Hortelano, J. C. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs," in Proc.Int. Conf. Commun. Workshop, 2010, pp. 1–5.
[3] 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–
[4] 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.
[5] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proc. 6th Joint Working Conf. Commun. Multimedia 2002,pp.107–121.
[6] Enrique Hernandez-Orallo, Member, IEEE, Manuel David Serrat Olmos, Juan-Carlos Cano,Carlos T. Calafate, and Pietro Manzoni, Member, IEEE "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes," IEEE Transactions on mobile computing, vol. 14, no. 6, June 2015.
[7] T. Ghosh, N. Pissinou, and K. Makki, "Collaborative Trust-based Secure Routing Against Colluding Malicious Nodes in Multi-hop Ad Hoc Networks," in Proc. 29th Annual IEEE International Conference on Local Computer Networks, pp. 224-231, 2004
[8] A. A. Pirzada and C. McDonald, "Deploying trust gateways to reinforce dynamic source routing," in Proc. 3rd International IEEE Conference on Industrial Informatics, IEEE Press, pp. 779-784, 2005.
[9] Saurin J. Choksi,Nikhil N. Gondaliya "A Light-Weight Trust based Mobility Aware Routing Algorithm for Mobile Ad Hoc Networks" International Journal of Computer Applications (0975 – 8887) Volume 97– No.14, July 2014