Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 7, July -2017

Selfish node detection in packet routing for MANET using global watchdog

[1]Priyanka A. Deokar (Student)

[2]Deepali B. Gothawal (Assistant Prof)

[1,2]*Department of Computer Engineering, D.Y.Patil College of Engineering,Pune-44*

Abstract: *WSN is the most frequently used network for better scalability and reduce of resources.WSN is also named as MANET and contains a infrastructure less network structure. Every network contains some type of attack that affects the network. One among these attacks is the selfish node attack that reduce the performance of MANET half the total performance. To overcome this performance, new algorithm used to provide safe routing in the presence of selfish node that not only prevents time needed to recover system from attack but also helps route the packet to destination fast.*

I. INTRODUCTION

Wireless Ad-hoc networks can be used without any presence of pre-existing infrastructure network . Therefore, this helps in reducing the need of physical resources needed to generate the network. The only difference between a MANET and the Ad-hoc network is the presence of some central device for controlling the nodes present in the network. The MANET does not need any central base station for controlling the nodes present in the network. The nodes are the mobile nodes that keep moving around and therefore the MANET is called the self organising network.

A. MANET Network:

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.[3] Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.[4]

MANETs are a kind of wireless ad hoc network (WANET) that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz)

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale, etc.

B. Routing Principles

Routing protocol plays a crucial role for effective communication between mobile nodes and operates on the basic assumption that nodes are fully cooperative. An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network.

In ad hoc networks, nodes are not familiar with the topology of their networks. Instead, they have to discover it typically, a new node announces its presence and listens for announcements broadcast by its neighbours. Each node learns about others nearby and how to reach them, and may announce that it too can reach them.
The types of routing are the table-driven ,on-demand routing and hybrid routing .The introduced algorithm falls under the hybrid routing.

C. Selfish nodes and its affect in MANET:

Mobile Adhoc Network (MANET) is highly vulnerable to malicious attacks due to infrastructure less network environment, be deficient in centralized authorization. The fact that security is a critical problem when implementing mobile ad hoc networks (MANETs) is widely acknowledged. One of the different kinds of misbehavior a node may exhibit is selfishness. Routing protocol plays a crucial role for effective communication between mobile nodes and operates on the basic assumption that nodes are fully cooperative. Because of open structure and limited battery-based energy some nodes may not cooperate correctly [1]. There can be two types of selfish attacks :

- selfish node attack (saving own resources) and
- sleep deprivation (exhaust others' resources.

II. RELATED WORK

The system generated consist of nodes and a watchdog system where the nodes are the mobile nodes(wireless devices like laptops, mobiles, etc..) that are free to move in and around network.
Watchdog is the mechanism that can be used to monitor the system actions. There are various watchdog monitored devices like fire alarm, refrigerator. The simple concept behind using watchdog is to monitor the change in action that are predefined. For example consider the fire alarm where the alarm beeps when sensor senses some smoke .This sensing of smoke is called change in action which watchdog detects.
Similar to this works the proposed system where the change in the routing pattern detects selfish node and an indication is given to the sender to resend the packets through other node that has not been detected as selfish node. This rerouting of the packets done with the help of algorithm which first performs checksum over the message and later breaks the message into packets and sends it to receiver one by one . At the receiver end the packets are first collected all and later the checksum is calculated again to cross check the accuracy. The checksum is not just calculated but applied with encryption and decryption algorithm to protect the checksum that is used for the verification of the packets.
In this paper, we propose a new approach Selfish mobile node detection based on watchdog and re-routing of non-forwarded packets. This system uses the watchdog as the monitoring agent that keeps the track of the packets routing in the network that is sent from the nodes whose records are kept with watchdog monitor.

D. Routing of packets

The routing of the packets done with the use of dijkstra's algorithm which is used for finding the shortest path for routing the packets. Every packet is encrypted and identified with a unique key that is attached with the packet while routing it.
The unique key is generated from the checksum that is calculated on the sender side . Later this unique is cross checked by the receiver to cross check the received packet.

E. Watchdog Module

The watchdog is a monitor that keeps tracks of actions that it is assigned to. In this paper the watchdog is used to monitor the packet routing. If the receiver is not forwarding the packet within the time it is,the node is marked as selfish node and the notification is sent to the sender node to resend packet skipping the selfish node.

The mobile node that fails to route the packet forward is given three chances in just to confirm if the node is not facing any other hardware or software problem. This prevents the non- selfish nodes from stooping to participate in the routing functions of the network.

F. System Architecture:

System Architecture is the overview of the entire system and its functionality. The system will operate as shown in the figure below. The system architecture in this paper will work on the mechanism of watchdog collaborative system.

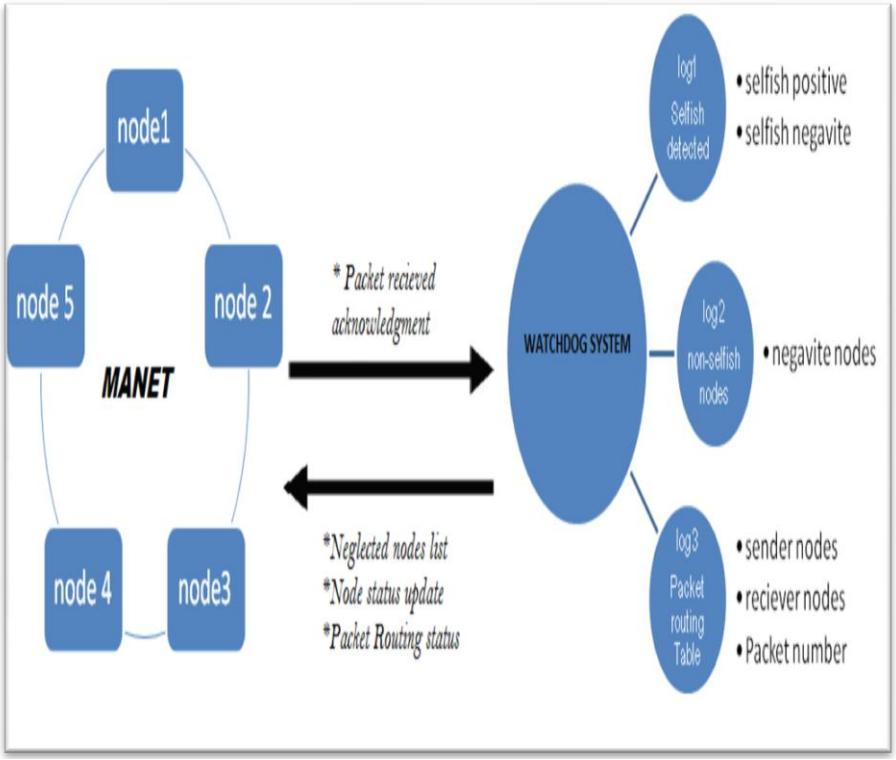

Figure 1

In the Fig 1, above contains a MANET network with more than node. These nodes are connected to the watchdog system that acts as the central controller of the MANET network. The MANET nodes will keep giving the routing information to the watchdog system and packet received acknowledgment. This will help the watchdog keep track over all packets travelling in the MANET.
The watchdog system is responsible for the tracking of all the nodes and packets. On finding that a node has not received a packet that it was supposed to, from the sender node, the sender node will be tested for selfish behaviour and that node will be marked as positive selfish. This positive marking will alert the other nodes and no packet will be further forwarded to this selfish node. Later the lost packet will be re-routed and taken care does not get vanished again.

III. CONCLUSION

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. Selfish node is the node that creates a problem in the MANET. Therefore various mechanisms are worked on to handle the problem of Selfish node. Watchdog is the one mechanism that deals with detection of selfish node. Selfish node detection is important for the consistency and reliability of MANET. Selfish node detection gets better as less time required as compared to other methods.

IV. REFERENCES

1. Ozcan, J. Zizka, and D. Nagamalai (Eds.): WiMo/CoNeCo 2011, CCIS 162, pp. 14–23, 2011. © Springer-Verlag Berlin Heidelberg 2011.
2. Enrique HernandezOrallo, Manuel David Serrat Olmos, Juan Carlos Cano,Carlos T. Calafate, and Pietro Manzoni, "CoCoWa: A Collaborative Contact Based Watchdog for Detecting Selfish Nodes" , IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL.14, NO. 6, JUNE 2015.
3. T.R. Srinivasan and K.G. Chithra, "Detection and Isolation of the Selfish Nodes Using a Collaborative Contact Based Watchdogs" , Middle-East Journal of Scientific Research 24,IDOSI Publications, 2016.
4. Hyun Kyo Oh, Sang-Wook Kim, Sunju Park, and Ming Zhou , "Can You Trust Online Ratings? A Mutual Reinforcement Model for Trustworthy Online Rating Systems" , IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, VOL. 45, NO. 12, DECEMBER 2015.
5. Sumit Mittal, Department MM University Mullana (Ambala) , "Identification Technique for All Passive Selfish Node Attacks In a Mobile Network", International Journal of Advance Research in Computer Science and Management Studies,Volume 3, Issue 4, April 2015.
6. 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.
7. Anamika Pareek and Mayank Sharma, "ARCHITECTURE FOR DETECTION OF SYBIL ATTACK IN MANET USING MAC ADDRESS", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: Issue 6, Volume 2 (June 2015).
8. Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat, "Lightweight Sybil Attack Detection in MANETs," IEEE SYSTEMS JOURNAL, VOL. 7, NO. 2, JUNE 2013.
9. 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.
10. C. K. N. Shailender Gupta and C. Singla, "Impact of selfish node concentration in MANETs", Int. J. Wireless Mobile Network, vol. 3,no. 2, pp. 29–37, Apr. 2011.
11. M. Mahmoud and X. Shen, " ESIP: Secure incentive protocol with limited use of public-key cryptography for multihop wireless networks," IEEE Trans. Mobile Comput., vol. 10, no. 7,pp. 997–1010, Jul. 2011.

