DETECT AND OVERCOME THE SELFISH PROBLEM IN WIFI NETWORK USING ENERGY SHARING

Preethi.S[1], Srigitha S. Nath[2], Bhargavi.S[3]

1PG Scholar, Department of ECE, Saveetha Engineering College, Tamil Nadu, India
2Head of Department, Department of ECE, Saveetha Engineering College, Tamil Nadu, India
3PG Scholar, Department of ECE, Saveetha Engineering College, Tamil Nadu, India

Abstract

Wireless Sensor networks and Wireless Ad Hoc networks are upcoming fields that demonstrate merit in the research domain due to their versatile nature. Our goal is to detect the misbehaviour in wireless LAN and to overcome this problem. Nodes tend to misbehave when their energy level is below a particular level and this scenario is labelled as selfish behaviour. The main idea of this paper is to detect this misbehaviour in the shortest time possible and to overcome this problem using Energy sharing.

Keywords- *Node misbehaviour, energy sharing, Wi-Fi protocol*

----------***----------

1. INTRODUCTION

Ad hoc networks and wireless sensor networks (WSNs) are different branches of technology that demonstrate remarkable potential. These systems are comprised of multiple sensor nodes called motes. These motes can be likened to miniature data miners. These can be deployed in different environmental conditions, such as temperature sensing, humidity sensing, velocity sensing, etc.

The motes can be deployed in vast areas where human intervention is difficult. Areas like wildlife sanctuaries or having rough terrain and erratic climatic conditions are regions where these sensor nodes are deployed maximum.

Being battery operated, these nodes tend to lose their energy easily. As they are deployed in regions where humans cannot intervene often, recharging the nodes is highly impossible .Therefore it is highly essential to make proper use of every node's energy. When the energy of a node falls below a given level it restricts itself from entering into any packet transmission. This is called selfish behaviour. Certain nodes might be involved in a large number of transmissions due to their location in the network. This leads to high energy depletion of the node within a very short time span. These nodes lose their energy at a very high level and soon get shut down. When such nodes shut down, the packet transmission in the network becomes more difficult since the node was present in the central locality. At such times, another node takes the previous node's place and the transmission continues.

Energy depletion and high packet loss are two main problems that persist in wireless mobile networks. Due to their mobility and wireless nature they tend to lose energy in a faster manner than normal nodes. Since they are battery operated, they cannot be recharged either. Once these nodes exhibit selfish behaviour, these nodes can no more be involved in the transmission. The nodes restrict themselves only to conserve their remaining energy. This might even lead to Denial of Service (DoS) problems since the node might occupy a particular bandwidth but never use it. The packet transmission is blocked in this area and the only solution is re-routing the packets through a different route, even though it might not be the shortest one. This solution again leads to energy waste due to re-transmission.

2. RELATED WORK

The misbehaviour of node is mainly due to the low energy level available in the node. CCA threshold is a parameter used to measure the amount of packets that can be received or sent successfully by a packet. This CCA threshold measures if that particular node is capable of sending the packets properly. But it is also essential that CCA threshold is maintained within a particular level so as to avoid any collision introduced by the MAC layer [1]. When the CCA threshold exceeds a particular level, this leads to new kinds of malicious activities. Here the energy of the node does not deplete but there is high collision rate.

Wireless interference takes place in networks which depend upon the node's interference for packet transmission. Sniffer nodes are placed at different locations in order to track the traffic between nodes. This helps in identifying where packet drop takes place and where there is high traffic. The sniffer nodes do not transmit any packet but only monitors the entire link [3]. This helps in better packet assessment and identifying the network's performance. The sniffers used here are passive

in nature, i.e., they are always in on-state. The drawback here is the deployment of such sniffer nodes, which needs power thereby making the energy requirement of the network greater.

The sniffers may be active in nature also[4]. Here again they are used for the same purpose of monitoring the network. The only difference is that they are in sleep mode when they do not have anything to sense. This conserves energy to a large extent. The nodes wake up only when they sense some activity in the link and when they have to sense the traffic. The rest of the time the sniffer nodes are in sleep mode.

3. PROPOSED WORK

In this paper, the selfish behaviour of nodes is identified. The selfish behaviour of the node is identified by packet drop. Nodes that have lesser energy than actually necessary for packet transmission restrict themselves from transmissions. Therefore the packets that the node receives are dropped without any consideration. This is the packet drop that has to be identified by the network. The main reason behind this packet drop is that, the nodes try to converse their remaining energy in order to stay alive. Sniffer nodes are available in between nodes at multiple locations that monitor the traffic between nodes. Every packet drop by selfish nodes and normal nodes are monitored by these nodes. Using this packet drop information only, the selfish behaviour is detected. The selfish node can be detected only after a few rounds of data transmission. Packet drop is measured at every round and by the fourth round the node is characterised as selfish node.

Energy Sharing is used here, which provide energy to the selfish node, and make the node participate in packet transmission. In any network environment, one transmitter is configured as selfish; the other transmitter is regular and acts as the sole witness. A sniffer node, located in close proximity of each transmitter, monitors the traffic on corresponding link. A node achieves selfishness by not sensing carrier before transmitting. In such a situation the node reserves its energy for its functioning than actual packet transmission. In such situations we can use the energy sharing method, in order to make the node get involved in transmissions.

Energy from the source node or from a nearby node that is uninvolved in the packet transmission is shared with the selfish node. Whenever the selfish nodes drop packets, the previous node re-routes it, thereby leading to more energy loss. In order to avoid this confusion this energy sharing method can be used. Once the energy is shared with the selfish node, it takes active participation in the packet transmission.

There is also the chance that, in case of re-routing the packets, the route it travels might not be an optimum route or shortest path. This again causes excessive energy drain in every node involved in the transmission. The impact of the selfish behaviour can be varied by simply varying the distance between the selfish and witness nodes.

4. SIMULATION & RESULTS

The various degree of selfishness is simulated using Ns2, where the selfish node senses the carrier with only a certain probability.

Once the node has obtained the required share of energy, it starts transmitting the data. There might be data drop due to some other factors. But if once again such selfish behaviour is encountered again the same method is followed to avoid packet drop. This helps in reduction of energy used for route computation, energy spent for packet forwarding and the energy already lost by the nodes involved

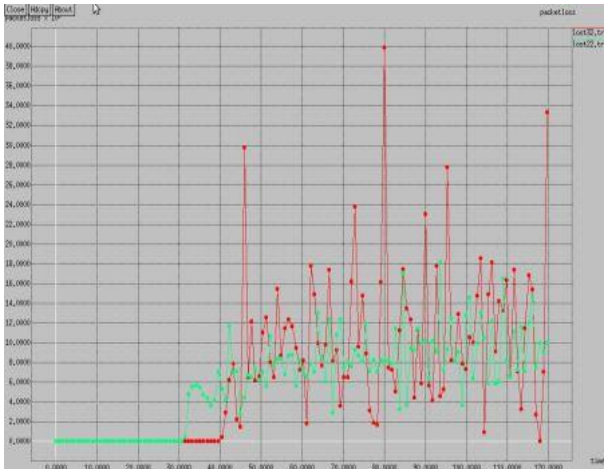

Fig 1 Packet loss

The above figure is the packet loss graph comparing the existing available protocol and the energy sharing method. The energy sharing method proves to have lesser packet loss than the existing protocol.

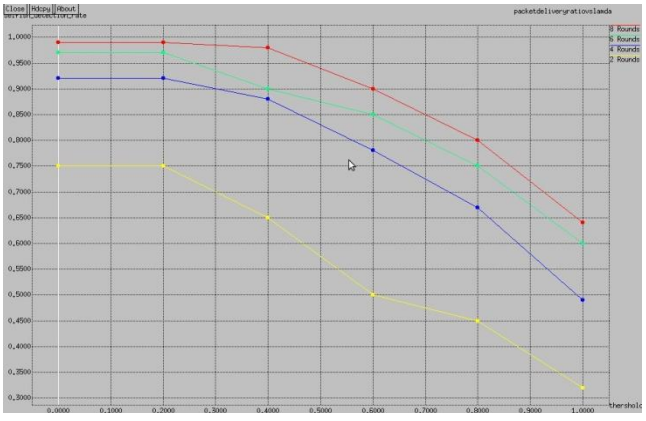

Fig 2 Packet delivery ratio versus lamda (no of rounds)

The above graph explains that as the number of rounds (or times) the data has been sent increases, the packet delivery ratio also increases. The packet drop takes place only until the selfish node has not been identified. At a particular limit the packet drop is completely avoided by sharing energy wirelessly and thereby the packets are delivered successfully.

5. CONCLUSIONS

This paper proposed a solution to overcome the selfish problem in the network, whereby selfish nodes were identified and made into cooperative nodes. This is done by providing additional energy to the selfish nodes from the source node, which is helpful in continuing packet transmission in the same path. This helps in better packet delivery.

REFERENCES

[1]. K. Pelechrinis, G. Yan, S. Eidenbenz, and S.V.Krishnamurthy, "Detecting Selfish Exploitation of Carrier Sensing in 802.11Networks," Proc. IEEE INFOCOM, 2009.
[2]. P. Bahl et al., "DAIR: A Framework for Troubleshooting Enterprise Wireless Networks Using Desktop Infrastructure, "Proc. ACM HotNets-IV, 2005.
[3]. A. Kashyap, U. Paul, and S.R. Das, "Deconstructing Interference Relations in WiFi Networks," Proc. IEEE Seventh Comm.Soc. Conf. Sensor Mesh and Ad Hoc Comm. And Networks(SECON), 2010
[4]. Utpal Paul, Anand Kashyap, Ritesh Maheshwari and Samir R.Das, "Passive Measurement of interference in Wi-Fi networks with application in Misbehavior Detection," IEEE Trans on mobile computing, vol 12, no.3, march 2013.
[5]. P. Bahl et al., "Enhancing the Security of Corporate Wi-Fi Networks Using DAIR," Proc. ACM/USENIX Mobile Systems, Applications, and Services (MobiSys), 2006.

BIOGRAPHIES

Preethi. S pursuing M.E in Computer and Communication She has presented papers in a few conferences.

Srigitha S Nath working as the Head of Department in Saveetha Engineering College She has 16 years of teaching experience and has published 4 papers in international journals.

Bhargavi.S pursuing M.E in Computer and Communication She has presented papers in national and international conferences.