ISSN:0975-9646

K.Sumithra devi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7804-7806

Increasing Throughput Capacity of Multihop Wireless Networks

K.Sumithra devi, .R.Sivakani and M.Pabitha
Dept of CSE, Apollo Engineering College, Chennai, Tamilnadu

***Abstract*--Many-to-one communication is a common communication mode. The performance challenges of multi-hop networks have long been recognized and have led to a lot of research on the medium access control, routing, and transport layers of the networking stack.The many-to-one throughput capacity and by same way, one-to-many throughput capacity of IEEE 802.11 wireless networks, in which many sources send data to a sink.**

Keywords- Multi-hop,Hidden nodes, Canonical Networks,AODV Routing

1.INTRODUCTION

Allocate some link capacity a Ls at the sink to the one-hop source nodes and then determine the throughput for the source nodes that are two or more hops apart based on the remaining capacity.

The throughput of the one-hop nodes will be around a Ls. Remaining capacity L can be used efficiently by the source traffic that is two or more hops away. Consider the notion of "canonical networks," a general class of regularly structured networks that allow us to investigate the system throughput by varying the distances between nodes and other operating parameters.

When all links have equal length, show that 2/3 of upper bound for general networks, including random topologies and canonical networks.

When the links are allowed to have different lengths, show that the throughput capacity of canonical networks has an analytical upper bound of 3/4.

2.LITERATURE SURVEY

2.1MOBILE ADHOC NETWORKS

A mobile ad-hoc network (MANET) is a collection of nodes, which have the possibility to connect on a wireless medium and form an arbitrary and dynamic network with wireless links[3]. It means that links between the nodes can change during time, new nodes can join the network, and other nodes can leave it. A MANET is expected to be of larger size than the radio range of the wireless antennas, because of this fact it could be necessary to route the traffic through a multi-hop path to give two nodes the ability to communicate. There are neither fixed routers nor fixed locations for the routers as in cellular networks also known as infrastructure networks. Cellular networks consist of a wired backbone which connects the base-stations. The mobile nodes can only communicate over a one-hop wireless link to the base-station. Multi-hop wireless links are not possible. By contrast, a MANET has no permanent infrastructure at all. All mobile nodes act as mobile routers. A MANET is depicted in Fig 2.1

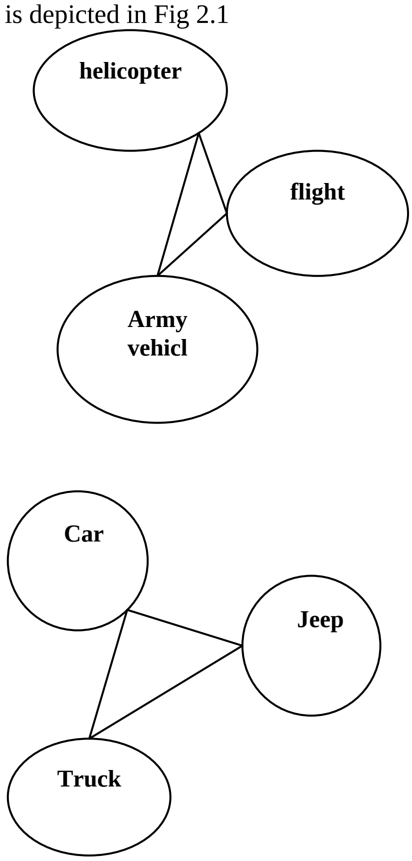

Fig 2.1 MANET

2.2 ADHOC ON-DEMAND DISTANCE VECTOR (AODV)

The Ad hoc On-Demand Distance Vector (AODV) protocol enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network[6]. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication.

AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network)[1]. One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program.

2.2.1 AODV OPERATION

This section describes the scenarios under which nodes generate Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages for unicast communication towards a destination, and how the message data are handled. In order to process the messages correctly, certain state information has to be maintained in the route table entries for the destinations of interest. All AODV messages are sent to port 654 using UDP.

A fundamental issue in multi-hop wireless networks is that performance degrades sharply as the number of hops traversed increase [5]. For example, in a network of nodes with identical and omnidirectional radio ranges, going from a single hop to 2 hops halves the throughput of a flow because wireless interference dictates that only one of the 2 hops can be active at a time.

Two well known problems that can cause performance degradations in IEEE 802.11 wireless networks are the exposed-node (EN) and hidden-node (HN) problems in wireless networks, the exposed node problem occurs when a node is prevented from sending packets to other nodes due to a neighboring transmitter. The standard 802.11 technology is not scalable because, due to EN, more Access Points (APs) do not yield higher total throughput. By removing EN, these schemes make it possible to achieve scalable throughput. Consider an example of 4 nodes labeled R1, S1, S2, and R2, where the two receivers are out of range of each other, yet the two transmitters in the middle are in range of each other. Here, if a transmission between S1 and R1 is taking place, node S2 is prevented from transmitting to R2 as it concludes after carrier sense that it will interfere with the transmission by its neighbor S1. However R2 could still receive the transmission of S2 without interference because it is out of range from S1.

IEEE 802.11 RTS/CTS mechanism helps to solve this problem only if the nodes are synchronized and packet sizes and data rates are the same for both the transmitting nodes. When a node hears an RTS from a neighboring node, but not the corresponding CTS, that node can deduce that it is an exposed node and is permitted to transmit to other neighboring nodes. If the nodes are not synchronized (or if the packet sizes are different or the data rates are different) the problem may occur that the sender will not hear the CTS or the ACK during the transmission of data of the second sender.

Hidden nodes in a wireless network refer to nodes that are out of range of other nodes or a collection of nodes [7]. Take a physical star topology with an access point with many nodes surrounding it in a circular fashion. Each node is within communication range of the AP, but the nodes cannot communicate with each other, as they do not have a physical connection to each other. In a wireless network, it is likely that the node at the far edge of the access point's range, which is known as A, can see the access point, but it is unlikely that the same node can see a node on the opposite end of the access point's range, B. These nodes are known as hidden. The problem is when nodes A and B start to send packets simultaneously to the access point. Since node A and B cannot sense the carrier, Carrier sense multiple access with collision avoidance (CSMA/CA) does not work, and collisions occur, scrambling data. To overcome this problem, handshaking is implemented in conjunction with the CSMA/CA scheme. The same problem exists in a MANET.Both EN and HN are related to imperfect operation of the carrier-sensing mechanism in 802.11.

Ideal carrier sensing must satisfy two criteria:

1. First, it should prevent simultaneous transmissions by interfering links. Otherwise, one or more of the transmissions will fail, resulting in retransmissions and bandwidth wastage.
2. Second, to exploit spectrum spatial reuse, it should allow simultaneous transmissions by non-interfering links. Prohibiting such simultaneous transmissions lowers the network throughput unnecessarily. Basically, HN arises when carrier sensing fails to satisfy simultaneous transmission.

HFD requires the use of Receiver Restart (RS) Mode and a sufficiently large CSRange.

Consider that 802.11 basic mode and that RTS/CTS are not used. The carrier-sensing mechanism eliminates collisions to the extent that they are negligible, and that collisions are predominantly caused by hidden and exposed nodes. Carrier sensing prevents simultaneous transmissions of nodes within the carrier-sensing range of a node. This imposes a limit on channel spatial-reuse. Potentially, the throughput could be limited by carrier sensing rather than hidden nodes.

3.PROPOSED SYSTEM

In multihop wireless mesh networks there is likely to be little traffic between client stations. Most clients would only want to connect to the core wired Internet via an Internet gateway, using relay nodes if necessary. The client stations and the Internet gateway form a many-to-one relationship. The placement of the relay nodes and the routing of traffic from the clients to the Internet gateway can affect the throughput significantly

For many-to-one networks, the capacity bottleneck is likely to be near the sink node because all traffic travels toward the sink node. Specifically, relay nodes near the sink node are responsible for forwarding more traffic, and these nodes contend for access of the wireless medium because they are close to each other. To obtain an idea on the upper limit of the throughput capacity under 802.11,so consider a class of networks referred to as the canonical networks.

The notion of “canonical networks,” a general class of regularly structured networks that allows us to investigate the throughput capacity systematically by varying the distances between nodes and other operating parameters.

4.IMPLEMENTATION

Here we use Network Simulator (NS2) to simulate the canonical network.

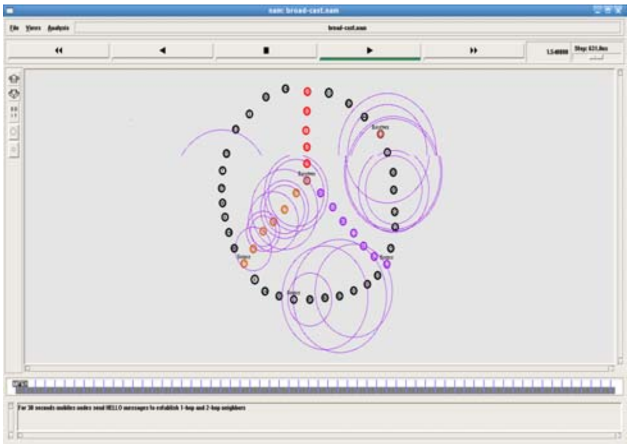

Fig.1.2.Data Transmission from Many-to-One node in a Canonical Network

The above screen shot explains that the data transmission from many source node to single node in the Carrier Sensing Range. This eliminates the hidden nodes by using the Request Restart mode. With RS Mode, a receiver will switch to receive the stronger packet if its power is, 10 dB higher than the power of the current packet.

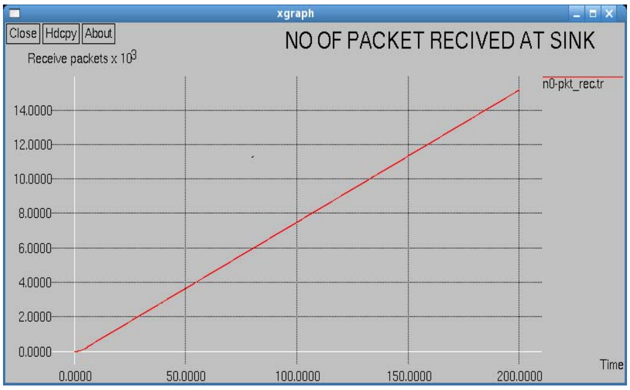

Fig.1.3 Graph for Displaying the No of Packets Received Vs Time

The above graph shows that the no of packets received at the sink in a particular time. As the time increases the number of packets will receive at the sink node also gradually increased.

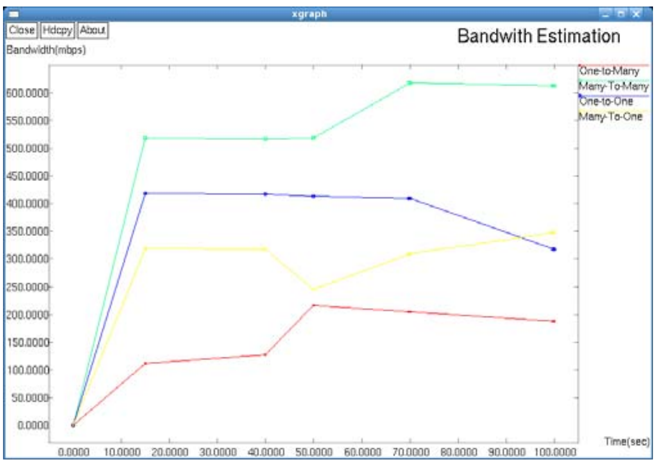

Fig1.3 Bandwidth Estimation For Different Network Structure

The above graph shows the bandwidth evaluation of One to many, Many-to-Many ,One-to-One , Many-to-One node Structure. When comparing all the above node structure Many-to-Many node structure has consume the more bandwidth as the no of packets increases.

5.CONCLUSION

A variant of the 802.11 MAC protocol called Selective Disregard of NAVs (SDN) which achieves network throughput scalability by removing EN entirely. In particular, we can argue that the O(n) scalability based on perfect scheduling is also achievable with CSMA/CA scheduling in infrastructure networks. In addition, we can derive a set of criteria, called Hidden- Node Free Design (HFD) to overcome HN with the less power consumption. This is in contrast to many previous efforts which attempt to deal with the performance problems created by HN rather than get to root of the problem to remove HN directly. In particular, the SDN+HFD, together with power control, can yield scalable and significantly higher throughput than the original 802.11, while minimizing packet collisions due to HN.

REFERENCES

[1] C.P. Chan, S.C. Liew, and A. Chan, “Many-to-One Throughput Capacity of IEEE 802.11 Multi-hop Wireless Networks,” technical report, Department of Information Eng., The Chinese University of Hong Kong, appendix, http://www.ie.cuhk.edu.hk/soung/manytoone, 2008.

[2] D. Marco, E.J. Duarte-Melo, M. Liu, and D.L. Neuhoff, “On theMany-to-One Transport Capacity of a Dense Wireless Sensor Network and the Compressibility of Its Data,” Proc. Second Int’l Workshop Information Processing in Sensor Networks (IPSN ’03),pp. 1-16, Apr. 2003.

[3] E.J.Duarte-Melo and M. Liu, “Data-Gathering Wireless Sensor Networks: Organization and Capacity,” Computer Networks,vol. 43, pp. 519-537, Nov. 2003.

[4] IEEE Std 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE CS LAN MAN Standards Committee, 1997.

[5] K. Jain et al., “Impact of Interference on Multi-Hop Wireless Network Performance,” Proc. ACM MobiCom, Sept. 2003.

[6] L.B. Jiang, “Improving Capacity and Fairness by Elimination of Exposed and Hidden Nodes in 802.11 Networks,” master’s thesis, Chinese Univ. of Hong Kong, June 2005.

[7] L.B. Jiang and S.C. Liew, “Removing Hidden Nodes in IEEE “Hidden-Node Removal and Its Application in Cellular WiFi Networks”,” IEEE Trans. Vehicular Technology, vol. 56, no. 5,pp. 2641-2654, Sept. 2007.

[8] L.B. Jiang and S.C. Liew, “Improving Throughput and Fairness by Reducing Exposed and Hidden Nodes in 802.11 Networks,” IEEE Trans. Mobile Computing, vol. 7, no. 1, pp. 34-49, Jan. 2008.

[9] P. Gupta and P.R. Kumar, “The Capacity of Wireless Networks,” IEEE Trans. Information Theory, vol. 46, Mar. 2000.

[10] P.C. Ng and S.C. Liew, “Throughput Analysis of IEEE 802.11 Multi-Hop Ad Hoc Networks,” IEEE/ACM Trans. Networking, vol. 15, no. 2, pp. 309-322, Apr. 2007.

[11] The Network Simulator NS-2, http://www.isi.edu/nsnam/ns, 2008.

[12] Wikipedia—IEEE 802.11s, http://en.wikipedia.org/wiki/ IEEE_802.11s, 2008.

[13] Wireless Communication Principles and Practice. IEEE Press, 2008.