Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENERGY EFFICIENT TRAFFIC CAPACITY IMPROVEMENT IN WIRELESS NETWORKS

[1]D.SYLVIA, [2]JEEVAA KATIRAVAN, [3]D.SRINIVASA RAO

[1]Resarch Scholar, Department of ECE, Jawaharlal Technological University, Hyderabad

[2]Associate Professor, Department of Information Technology, Velammal Engineering College, Chennai

[3]Professor and Head, Department of ECE, Jawaharlal Technological University, Hyderabad

E-mail: [1]sylvia.sanjana@gmail.com

ABSTRACT

Wireless communication has seen rapid technological advancements in recent years. Wireless mesh network and ad-hoc network are types of wireless networks. Both are multihop networks: in wireless ad hoc networks the mobility of the relay nodes is very high when compared to the low mobility of the relay nodes in wireless mesh networks. These multihop networks depend on the relay nodes for packet transmission and therefore the network lifetime time is an important consideration in these networks. The residual energy of the nodes should be high enough, such that the network life time is extended and therefore improve the traffic carrying capacity of the network. Data from malicious nodes also tend to use the network energy and due consideration is to prevent the malicious nodes from using the energy and bandwidth of the network. In this paper, an energy efficient secure routing is proposed with the primary objective of improving the traffic carrying capacity of the network .The efficiency of the proposed algorithm is shown using extensive simulations.

Keywords: Wireless Networks, Cooperative Communication, Energy Efficiency, Capacity improvement

1. INTRODUCTION

Wireless mesh networks are a type of Ad Hoc networks, which are characterized to be self-healing and self-configuring network. These networks provide multiple paths and the nodes co-operate among themselves in routing the packets. In such networks, the communication from a source node to a destination node maybe achieved by direct communication, if the destination node is within the transmission radius of the source node. But due to the mobile nature of the networks, the networks depend on intermediate nodes to act as relay nodes. The neighboring nodes within the transmission radius of the source node are able to overhear the communication towards the destination node, due to the broadcast nature of the wireless channel. Communication between a single source and destination without the help of relay nodes is called direct communication or single-hop communication, as shown in Figure 1.

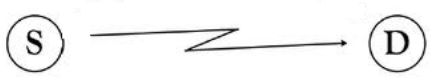

Figure.1 Direct Communication

Whenever there is a possibility of using a neighbour node for communication, it is called multi-hop communication as shown in Figure 2 , in which the nodes collaborate with each other to provide a robust communication of the transmitted packets.

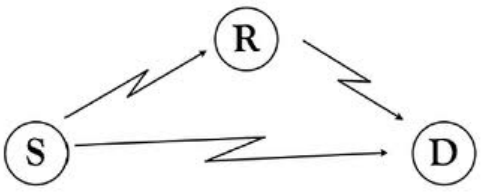

Figure. 2 Cooperative Communication

Using the cooperative communication model, it becomes possible to achieve spatial diversity without the use of multiple antennas. Cooperative communication has several advantages which include, improvement in network capacity, improvement in power and spectrum efficiency, reduced delay and enhancement in performance. This cooperation maybe realized wither by using relay nodes to assist in the communications between source and destination or by allowing the intermediate nodes to aid in reaching the corresponding destination.

The characteristics of the wireless channels, such as fading and interference have a detrimental effect on

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the propagation of the signals. Spatial diversity can overcome these disadvantages and can be achieved either by the use of multiple antennas or by using cooperative communication. Cooperative communication has been a research topic of interest in recent years and has been used to address several issues in wireless networks. Providing security in wireless ad hoc networks is a very challenging task. Attacks maybe broadly classified as Active and passive attacks. Active attackers just snoof the communication, whereas active attackers alter the data being transmitted. One of the major passive attack is the resource consumption attack, in which the attacker tries to waste the resources such as battery power and bandwidth of the legitimate nodes in the network, by continuously forwarding packets to them. This paper addresses this issue by suitable consideration of bandwidth and available power, while also considering the time to live of the node.

The remainder of the paper is organized as follows. The related works is discussed in Section 2. Section 3 describes the proposed algorithm. Section 4 discusses the simulation environment. Section 5 compares the performance of AOMDV and PAMR. Conclusions are presented in Section 6.

2. RELATED WORKS

Quality of service (QoS) is a performance measure of a network. In ad hoc networks, the lack of central coordination and limited resources in terms of battery and bandwidth tend to have an effect on the QoS that can be achieved. The QoS required varies based on the application. For applications such as multimedia, bandwidth and delay become crucial parameters, whereas in military applications security is the major issue. For search and rescue operations, link life and availability of multiple paths become the key parameters.

QoS aware routing proves to be advantageous, in which parameters such as network throughput, packet delivery fraction, delay, routing overhead and energy consumption are considered while making the routing decisions. Figure 3 shows how traditionally, routing protocols are broadly classified based on the following criteria [1] :

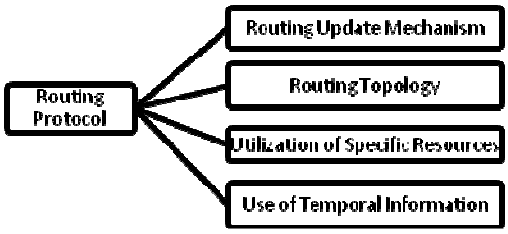

Figure. 3 Classification of Routing Protocol

The wireless network is resource constrained in-terms of bandwidth and power. The popular protocol, Ad Hoc on-demand vector(AODV) [2] routing protocol find routes on an on-demand basis, that is, it finds a route whenever a source node needs to transmit a packet. Another popular protocol, Ad Hoc On-demand Multipath Distance vector (AOMDV) [3] routing protocol, is a multipath extension of AODV which provides loop freedom and effectively copes up with mobility induced route failure.

AODVM [4] deals with node disjoint paths and the effect of node density and node placement are extensively studied. It achieves improved overall reliability of the network, but may suffer from higher overheads.

AODV-BR [5] is yet another enhancement in AODV which utilizes backup routes when the primary route fails, thereby taking care of loss of data packets.

Multipath routing has various advantages in wireless networks, especially since the wireless channel suffers from fading and interference. This has an adverse effect packet delivery due to link failures. Therefore multipath routing helps to provide a high bandwidth, energy efficient, efficient data delivery. The proposed algorithm Power Aware Multipath Routing (PAMR) tries to compute a power efficient optimal route with the major objectives of reducing the power consumption and increasing the capacity of the network. The wireless mesh networks are distributed in nature and the lack of a central coordinator requires better security measures

3. COMMUNICATION MODEL

The wireless channel is characterised by path loss, shadowing and fading between nodes. The signal to noise ratio is an important parameter of concern in an error prone wireless environment. In [6],the authors have described the signal-to-noise ratio

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

required for effective packet transmission to take place, that is, if the sending nose is s and destination node is d, the signal-to-noise ratio is found to be the product of a variable Δ_{sd} and the transmission power of the node P_s

$$SNR_{sd} = P_s . \Delta_{sd} \quad (1)$$

Here the variable Δ_{sd} is used a measure of the path loss and fading that occurs in the transmission path.

$$\Delta_{sd} = \frac{h_{uv}^2}{\sigma_v^2} \quad (2)$$

Under cooperative forwarding, there are two main schemes, the amplify and forward scheme and the decode and forward scheme. In [7], the authors have shown that capacity the relay node that forwards the packet from source node to destination node has a linear dependence on the bandwidth and signal-to-noise ratio. Under direct communication, the maximum achievable rate is given by

$$C_{(s,d)} = B.log_2 (1 + SNR_{sd}) \quad (3)$$

If r is the relay node, it has been shown in [7], that the maximum capacity achievable with a transmission gain I is

$$C_{(sr,d)} = B.I(SNR_{sd} , SNR_{sr} SNR_{rd}) \quad (4)$$

These theoretical observations show that the maximum rate achieved depends on the transmission power of source node and relay node. Thus power adjustments in the path will result in achieving required bandwidth, thereby achieving the required capacity in the network.

The most popular standard for wireless mesh networks is the IEEE802.11b protocol. The capacity of the wireless mesh networks are found to affected by various factors such as network topology, traffic pattern, node density, transmission power level and node mobility.[8]

4. ALGORITHM

Consider a network of n nodes. The proposed PAMR algorithm consists of two modules. In the first module, each node sends a request message with high transmission power. All nodes within the transmission radius are able to hear this broadcast.

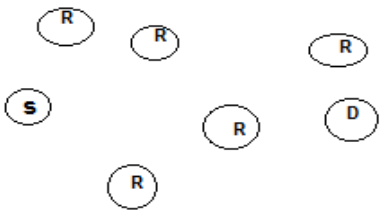

Figure .4 Node deployment

Figure 4 shows a sample topology, in which S is the source node, D is the destination node and R is the set of possible relay nodes. The broadcast message sent by node S is heard by all nodes within the transmission radius. Each relay node, computes the minimum power required to reach the relay, while satisfying the required signal-to-noise ratio to be maintained. On receiving this optimal power information, the sending node selects the relay node with the constraint that it can be reached with minimum power. This relay node is selected as the cooperative relay. Due to this, the path established is the path with minimum power consumption. The route request packet contains the hop count and the transmission power. In the second module, for better security,[10] the neighbour nodes are verified by maintaining a list of neighbour nodes. The malicious nodes are identified by the Node ID and the time of arrival of data. The data transfer from malicious nodes are not forwarded, which saves considerable amount of power.

5. PERFORMANCE EVALAUTION

In the simulations, a wireless multi-hop network is considered in a planar topology. The IEEE802.11b is chosen as the MAC protocol. The Proxim Orinoco PC card by the Lucent technology is optimized specifically for this purpose. It is compatible with the popular IEEE 802.11b wireless MAC standard and supports a variety of data rates of 1, 2, 5.5 and 11 Mbps. It operates in the same 2.4GHz band and its channel bandwidth is 22MHz as in IEEE 802.11b. The card supports variable data rates and the following table gives the Orinoco Gold 802.11b Wireless PC card specifications. [9].The two ray ground model is used as the propagation model and the traffic pattern is constant bit rate.

The simulation was run for random source-destination pairs with constant data rate.
The packet delivery fraction is an important evaluation parameter and maybe defined as the number of packets sent from the application layer of the source nodes and the actual number of packets received at the destination nodes.

The figure 5 shows the Packet delivery Fraction achieved with the proposed and existing protocols.

Journal of Theoretical and Applied Information Technology
20th August 2014. Vol. 66 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

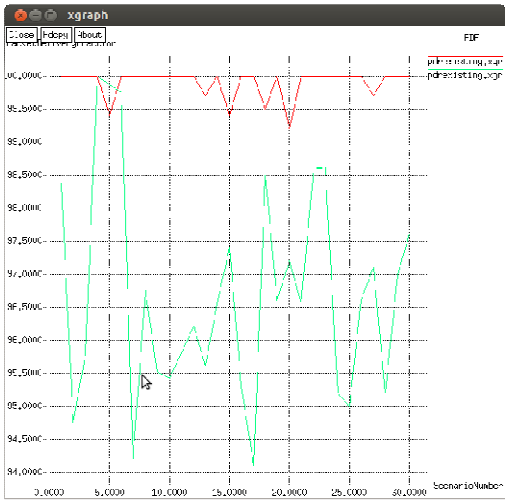

Figure. 5 Packet Delivery Fraction

The proposed PAMR achieves on an average, a packet delivery fraction of 97.11%, whereas the AOMDV achieves an average of 99.61%. In terms of packet delivery fraction, there is only a difference of 2% between the two protocols.

The Figure 6 shows the Average Residual Energy of the network with the proposed and existing protocols.

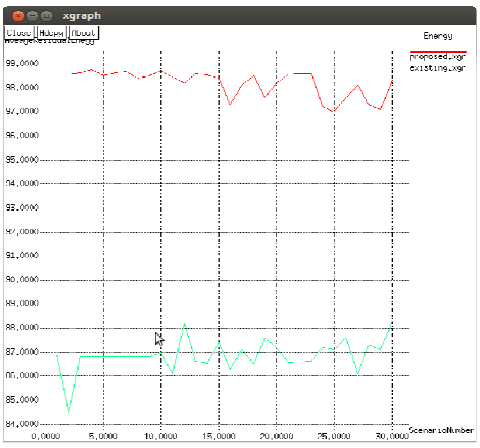

Figure. 6 Average Residual Energy of the Network

The proposed PAMR has an average residual energy per node as 98.56%, whereas the residual energy in the existing method is 86.58%. There is an improvement of nearly 11% of residual energy, which extends the lifetime of the network.

The routing overhead involved is higher since the relay node identification and malicious node detection contribute in increasing the routing information.

The chord algorithm is used which verifies the Node Id's and Location Id's , by which the attacker node can be identified. For this purpose the List of the Neighbour Nodes information for each node is used, so that the Intermediate Node can verify the nodes request i.e., unverified and the verified buffer is used. When the attacker is identified, they are further informed to all other nodes and no data passes through that node.

When a delay occurs, the Load balancing algorithm is used which eliminate the collision/delay. The energy level of each node is maintained through which the malicious node is identified and eliminated.

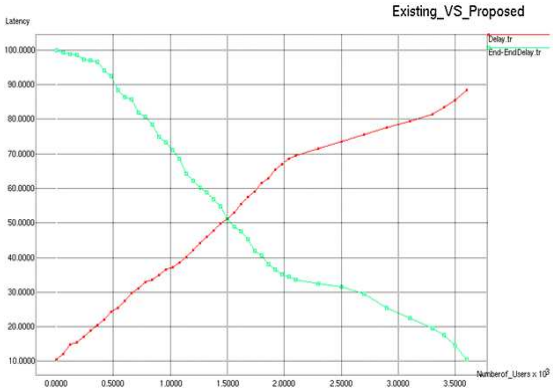

Figure .7 Attacker Detection and end to end delay analysis

The simulations show that for applications that can tolerate a minimal packet loss, but have the capacity of the network to be the primary objective, this algorithm is found to be very effective. And its efficiency has been shown through simulations.

6. CONCLUSION

The proposed PAMR protocol has significantly increased the lifetime of the network and therefore has increased the traffic capacity of the network. In spite of the tolerable reduction in packet delivery fraction, this algorithm is an efficient algorithm in terms of power consumption. In a resource constrained wireless communication, this is a marked advantage. It supports a node-disjoint multipath routing with energy efficiency. Security issues have also been addressed and the compromising nodes transmission is controlled. The work has been carried out in a network with

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

limited mobility and future work would be in networks with high mobility.

REFRENCES:

[1] C.S.R.Murthy, B.S.Manoj, Ad hoc Wireless Networks, Architecture and Protocols, 6th Edition,2004.

[2] Charles E. Perkins and Elizabeth M. Royer. "Ad hoc On-Demand Distance Vector Routing" Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 90-100.

[3] Mahesh K.Marina and Samir Das, ‘"Ad hoc On-Demand Multipath Distance Vector Routing", Wiley Wireless Communications and Mobile Computing (WCMC) Journal, Special Issue on Wireless Ad hoc Networks: Technologies and Challenges, Vol. 6, No. 7, pp. 969-988, Nov 2006.

[4] Ye Z, Krishnamurthy SV, Tripathi SK.”A framework for reliable routing in mobile ad hoc networks”, In Proceedings of IEEE Infocom, 2003.

[5] Lee SJ, Gerla M. “AODV-BR: backup routing in ad hoc networks”, In Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), 2000.

[6] H. L. Xu, L. S. Huang, G. Wang, T. Xu, and G. Liu, “Joint relay assignment and power allocation for cooperative communications,” Wireless Networks, DOI: 10.1007/s11276-010-0254-2, Nov. 2010.

[7] J. N. Laneman, D. N. C. Tse, and G.W.Wornell, Cooperative diversity in wireless networks: efficient protocols and outage behavior,” IEEE Trans.Inf. Theory, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[8] Yan Zhang, J. L. (2007). Wireless Mesh Networking, Architectures, Protocols, and Standards. FL: Auerbach Publications.

[9] ORiNOCO Classic Gold PC Card http://www.proxim.com/

[10] Yongkun Li; Lui, J.C.S., "Epidemic Attacks in Network-Coding-Enabled Wireless Mesh Networks: Detection, Identification, and Evaluation," IEEE Transactions on Mobile Computing, vol.12, no.11, pp.2219,2232, Nov. 2013