International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.1, Jan-Feb 2012 pp-499-503 ISSN: 2249-6645

# Addressing Asymmetric Link in Wireless Mesh Networks

**Ashok Kumar. S*, Krishnammal. N****

*II M.E CSE, Sri Shakthi Institute Of Engineering and Technology, Anna University,Coimbatore.
**Asst.prof CSE, Sri Shakthi Institute of Engineering and Technology, Coimbatore.

## Abstract
In a mesh network, each node acts as a router/repeater for other nodes in the network. These nodes can be fixed pieces of network infrastructure and/or can be the mobile devices themselves. In such networks, because of the heterogeneous transmission range of the clients and routers, link asymmetry problem exists. Link asymmetry poses several challenges such as the unidirectional link problem, the heterogeneous hidden problem and the heterogeneous exposed problem. These challenges degrade the network performance. The proposed approach addresses these challenges and eliminates the unidirectional link in the network layer.

***Index Terms***—heterogeneous hidden/ exposed problems, link asymmetry, unidirectional link, mesh networks.

## I. INTRODUCTION
A wireless mesh network (WMN) is a mesh network created through the connection of wireless access points installed at each network user's locale. Each network user is also a provider, forwarding data to the next node. The networking infrastructure is decentralized and simplified because each node need only transmit as far as the next node. Wireless mesh networks (WMNs) are dynamically self-organized and self-configured, with the nodes in the network automatically establishing an ad hoc network and maintaining the mesh connectivity. WMNs are comprised of two types of nodes: mesh routers and mesh clients. Other than the routing capability for gateway/bridge functions as in a conventional wireless router, a mesh router contains additional routing functions to support mesh networking.

Through multi-hop communications, the same coverage can be achieved by a mesh router with much lower transmission power. To further improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. In spite of all these differences, mesh and conventional wireless routers are usually built based on a similar hardware platform. Mesh routers have minimal mobility and form the backbone for mesh clients. Thus, although mesh clients can also work as a router for mesh networking, the hardware platform and software for them can be much simpler than those for mesh routers.

Mesh networking (also called "multi-hop" networking) is a flexible architecture for moving data efficiently between devices. In a traditional wireless LAN, multiple clients access the network through a direct wireless link to an access point (AP); this is a "single-hop" network. In a multi-hop network, any device with a radio link can serve as a router or AP. If the nearest AP is congested, data is routed to the closest low-traffic node. Data continues to "hop" from one node to the next in this manner, until it reaches its final destination. The transmission range of the mesh router is usually larger than the transmission range of the mesh client. This indicates that link asymmetry exists in the mesh access network.

Link asymmetry causes numerous challenges such as the unidirectional link problem, the heterogeneous hidden problem and the heterogeneous exposed problem which degrade the network performance. In the network layer, an algorithm is developed to establish the local route spanning tree for each mesh client to solve the unidirectional link problem. With the spanning tree, the mesh router and mesh clients can be connected via multihop communication. To address the hidden terminal problem a new control frame delay to send (DTS) is introduced. DTS is used to avoid collision on demand by cancelling the transmission of a heterogeneous hidden terminal. The rest of this paper is organized as follows: In Section II, we present the overview of the problems. In Section III, we present our approach in detail. In Section IV, the link asymmetry problem is addressed. The simulation results are shown in section V. In Section IV, we conclude this paper and outline our future research direction.

## II. PROBLEMS OVERVIEW
The transmission range of the mesh router is usually larger than the transmission range of the mesh client. Hence, link asymmetry exists between the mesh router and the mesh client. The link asymmetry raises the following three problems: 1) unidirectional link problem; 2) heterogeneous hidden problem; and 3) heterogeneous exposed problem.

### *1) Unidirectional link problem*
A unidirectional link arises between a pair of nodes in a network when only one of the two nodes can directly communicate with the other node. The clients with small transmission range cannot respond to routers after receiving requests from routers. Consider Fig.1. A unidirectional link exists between the router R and client G. The router R initially sends Request To Send (RTS) signal to client G. Due to the small transmission range of client G, it cannot send Clear To Send (CTS) signal to respond router R. This problem leads to

incorrect topological information and misbehavior of routing protocols, which commonly assume that the links of the network are bidirectional.

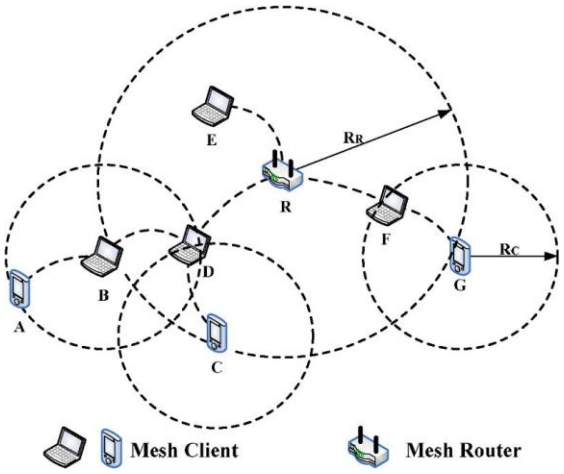


**Fig.1** Wireless Mesh Network

***2) Heterogeneous hidden problem.***

For many wireless technologies in typical ad hoc networking environments, the interference range is larger than the associated coverage range. In such an environment, a node A that does not receive an CTS message from a node B may transmit a packet that will collide with the reception at node B. The reason is that node B may be within the interference range of node A, while node A is outside the transmission range of node B. This problem is called as the hidden part of the interference-range hidden/exposed terminal problem. This refers to collisions raised by accessing the channel from B-node, which cannot be silenced by the G-node CTS frame. Consider Fig. 1. The router R is a heterogeneous hidden terminal of client B. To send data to client B, the router R sends RTS to client B initially. Due to the heterogeneous transmission range the router R cannot receive CTS from client B. Hence, a collision occurs if router R accesses the channel when client B receives data from client A. The heterogeneous hidden terminal increases the possibilities of data collision across nodes and hence the network performance and throughput is affected.

***3) Heterogeneous exposed problem.***

This refers to the decline of spatial reuse of wireless channel that is caused by clients, which are forced to remain silent by the router's CTS. However, their data transmission will not interfere with the data transmission of the router that sent the CTS. As shown in Fig. 1, both clients C and D are heterogeneous exposed terminals for router R, because clients B and C are within the transmission range of router R and they remain silent by receiving router R's CTS. However, if router R is receiving data from client F or client G, the communication between client B and client C will not affect router R.

## III. RELATED WORK

In this section, the proposed approach is described in detail.

***1) Basic Handshake and Channel Reservation Operations:***

Two new control frames DTS and N-ACK are introduced in our approach. Hence, there are three basic handshake operations in our approach. *RTS/CTS/DATA* is used to handle normal data transmission. When a node needs to send DATA, it first checks the data channel and the control channel. When both channels are idle and the idle time lasts longer than the period of time that is equal to short interframe space, RTS can be transmitted through the control channel. By receiving RTS, if the channel condition allows it to receive DATA, the destination node now replies to RTS by CTS. After receiving CTS from the destination node, the DATA is sent through the data channel. *RTS/DTS/Backoff/ .../retransmit* is used when the channel condition of the destination does not meet the requirements for receiving DATA. After receiving DTS from the destination, the source node will delay its data transmission and retry after backoff. This way, the chance of collision can be largely reduced. The *RTS/CTS/DATA/N −ACK/Backoff/.../Retransmit* is used to provide the reliability for DATA transmission. In case of any collision on the data channel, the destination will send N-ACK to the source. After the backoff procedure, retransmission will recover the collided DATA frame. In addition to these basic handshake operations, channel reservation operations are also performed in this approach. To implement the channel reservation, the network allocation vector (NAV) is used to determine how long the channel will be occupied. Each node maintains three NAVs. In particular, NAVC is used to monitor the control channel. Transmitting a control frame is forbidden when NAVC is positive. NAVS and NAVR are used to manage sending and receiving operations on the data channel. When NAVS is positive, RTS is not allowed to transmit and when NAVR is positive data receiving is forbidden. A Duration field is appended to each control frame to support channel reservation. Based on handshake operations, when handshake is conducted on the control channel, the duration information appended in each control frame can be used to update three NAVs (i.e., NAVC, NAVS, and NAVR) for channel reservation.

## IV. ADDRESSING LINK ASYMMETRY

***1) Addressing the Unidirectional Link Problem:***

To address the unidirectional link it is essential to establish multihop routing reserve paths for mesh routers and mesh clients. Establishing reverse paths between mesh routers and mesh clients is a critical task in this approach. For each mesh client Ci, it is not essential to set up paths connecting it to all routers in the network. Instead, each client Ci only needs to establish paths to connect routers within a range of RR. We define these routers as a set names as R(ci). As shown in Fig. 2, client C1 establishes a path consisting of routers R2, R3, and R4 within the range of RR via clients C4, C2, and C3. We can see that C1 does not establish a path with router R5, because R5 is not within C1's range of RR. Obviously, the local route spanning tree LRST(c1) consists of C1 as its root and routers in R(C1), i.e., (R1, R2, R3, and R4) as its leafs.

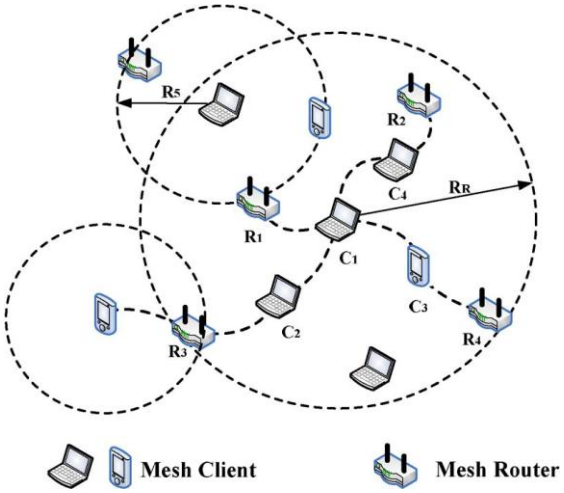


**Fig. 2.** Example of local route spanning tree.

There are three steps for establishing LRST and addressing the unidirectional link problem. In the first step, a bidirectional table is built for each node to determine whether a unidirectional link exists between a pair of router and client. In the second step, mesh clients are connected to mesh routers by discovering multihop paths. In this step, LRST can be formed in each mesh client. In the third step, the topological information of LRST is used to address the unidirectional link problem. The detailed procedures are presented below.

**Step 1:** Establishing the bidirectional neighbor table. The bidirectional neighbor table is used to determine whether a unidirectional link exists between the router and the client. The router and the client may periodically need to broadcast Hello packets. In the following, we define *Hello*(*ci*) or *Hello*(*ri*) as the Hello packet sent by client *ci* and router *ri*, respectively. This way, when a mesh router receives *Hello*(*ci*) or *Hello*(*ri*), it knows that *ci* or *ri* are its bidirectional neighbors. By receiving *Hello*(*ci*), a mesh client can also ensure that *ci* is its bidirectional neighbor.

However, when a *Hello*(*ri*) is received by a mesh client, it cannot determine whether these routers are its bidirectional neighbors or not. To address this problem, *Hello*(*ri*) should append the bidirectional neighbour table of *ri*. According to the neighbor list appended in *Hello*(*ri*), a mesh client can determine whether routers are its bidirectional neighbor or not. Hence, the bidirectional neighbor table is formed. In addition, a sequence number is also appended in *Hello*(*ri*). It is used to indicate the freshness of information. Once the router generates a Hello packet, the sequence number will increase. When a *Hello*(*ri*) is received by *ci* and *ri* is the bidirectional neighbor of this client, a sequence number that is larger than the sequence number maintained for *ri* will trigger an update for the record of *ri* in the bidirectional neighbour table.

**Step 2:** Establishing a reverse path to connect the router and the client. When a new bidirectional link between client *ci* and router *ri* is detected by receiving *Hello*(*ri*) or an update is triggered for *ri* due to a fresh sequence number, a connection from *ci* to *ri* is established. In this case, *ci* notifies its bidirectional neighbors that the path from *ci* to *ri* has been established by broadcasting a *RSCP*(*ci*, *ri*). After receiving *RSCP*(*ci*, *ri*), the bidirectional neighbours of *ci* will obtain the information that *ri* could be connected via *ci*. Therefore, those bidirectional neighbors continue to broadcast *RSCP*(*x*, *ri*), where *x* belongs to the bidirectional neighbors of *ci*. Hence, the bidirectional neighbours of *ci* can connect to router *ri*. By repeating this process, a distributed LRST will be formed, and routers are connected via multihop paths connected through mesh clients.

**Step 3:** Eliminating unidirectional link.

The purpose of establishing LRST is to enable control information exchange between the router and the client on unidirectional links for the MAC protocol. By the interactions between the network and link layers in our approach, the MAC protocol can use LRST to route control frames via multihop paths through clients. Fig. 2 shows one simple example. We can observe that the link between router *R*3 and client *C*1 is the unidirectional link. When router *R*3 wants to transmit DATA to client *C*1, it first sends RTS to client *C*1. After receiving RTS from router *R*3, client *C*1 finds that *R*3 is not its bidirectional neighbor according to LRST. Hence, it replies to *R*3's RTS by CTS via multihop paths through clients. CTS is first delivered to intermediate client *C*2, which then forwards CTS to *R*3. Finally, router *R*3 sends DATA to client *C*1. As we can see, the unidirectional link problem is solved by our proposed mechanisms.

***2) Addressing Heterogeneous Hidden Problem:***

The main idea to solve the heterogeneous hidden problem is to route control frames, which can either block or delay the router's transmission. One scheme to achieve this goal is to increase the coverage of CTS sent by client . Another scheme is to delay the transmission of router on demand. This scheme is based on the fact that collision may only occur when the heterogeneous hidden terminals access the channel and the client receives DATA. Obviously, the on demanded scheme incurs much less overhead. We adopt the second scheme in our approach.

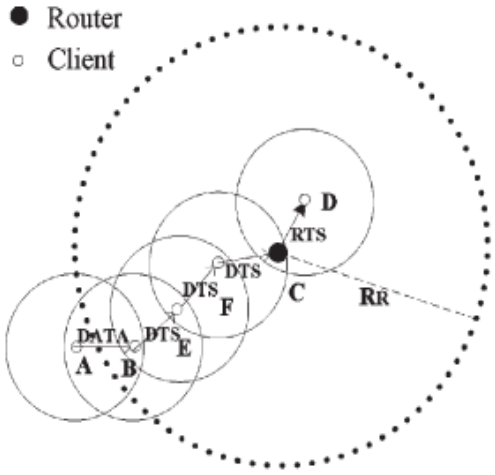


**Fig. 3(a).** Addressing heterogeneous hidden problem.

In particular, each client senses potential collision by listening to the control channel. If RTS from the router is received by the client on the control channel when it is receiving DATA, the client can ensure that the DATA transmission from that router will collide with the DATA to be received. In this case, DTS is forwarded via a multihop path through mesh clients to the heterogeneous hidden terminal, i.e., the router, to cancel its current data transmission.

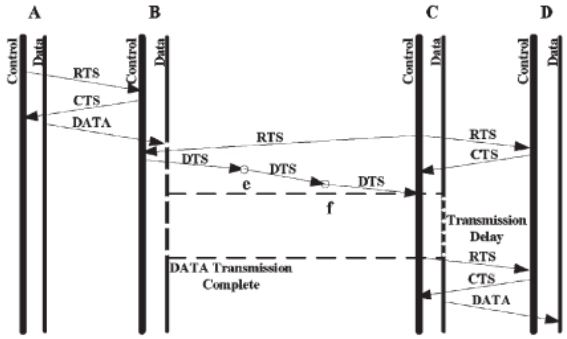


Fig. 3(b). Solution for the heterogeneous hidden problem.

**Fig. 3(a)** shows a simple example, where client B is receiving DATA from A after RTS/CTS handshake. At this moment, router C tends to send DATA to client D; it sends RTS on the control channel to D, and D replies to CTS. Nevertheless, router C will not immediately transmit DATA on the data channel, but it will wait a period of time to see if there is any DTS that has arrived. When receiving RTS from router C, client B finds that DATA transmission will collide with the DATA to be received. Meanwhile, client B finds that the link between router C is unidirectional according to its LRST; hence, it transmits DTS to client E, and client E forwards the DTS frame. Finally, router C receives DTS, cancels its transmission, and retries according to the Duration field in the DTS frame. Hence, the heterogeneous hidden problem is solved by the proposed mechanisms.

**3)** ***Addressing the Heterogeneous Exposed Problem:***

Because of the large transmission range of the router, the CTS frame from the router may block data transmission from clients. Hence, the problem becomes how to decrease the coverage of the CTS frame. Our idea is to limit the effective coverage of the CTS frame from the router. Based on the LRST established in the network layer, each client can determine whether the router is its bidirectional neighbor or not. Hence, when the client receives CTS from the router, it can process CTS in different ways than those listed here. When the router is not its bidirectional neighbor, CTS will be ignored. If the router is the bidirectional neighbor, the CTS frame will be processed. Fig. 4(a) shows one simple example. We can see that clients *D* and *E* are heterogeneous exposed terminals when router *B* replies CTS to client *A*.

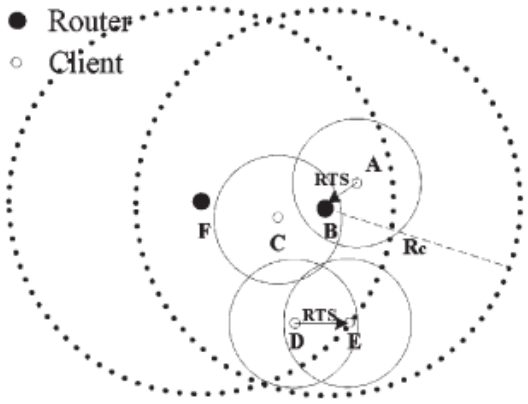


**Fig. 4(a).** Addressing heterogeneous exposed problem.

Using our mechanism, client *C* and router *F* will be blocked after receiving CTS from router *B*, because they are bidirectional neighbors based on LRST. However, clients *D* and *E* find that router *B* is not their bidirectional neighbor based on LRST. Hence, they simply ignore CTS and initialize RTS for data transmission. Hence, the heterogeneous exposed problem is solved by the proposed mechanisms.

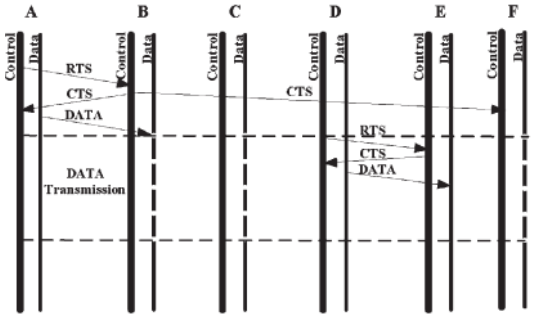


**Fig. 4(b).** Solution for the heterogeneous exposed problem.

## V. PERFORMANCE EVALAUTION

The network capacity and impact of collision are the main aspects considered for the network. To evaluate network capacity, we consider the metric *aggregated one-hop throughput*, which is defined as the total number of packets delivered to the destinations. To measure the impact of collision, we consider the metric *efficiency of data delivery ratio*, which is defined as the ratio of the aggregate one-hop throughput to the number of transmitted packets.

The constant bit rate (CBR) traffic model is used in this simulation as it is a very popular traffic model and has been widely used in the simulation of the MAC protocol. Fig. 5 and 6 shows the simulation results in terms of throughput for CLSM and IEEE 802.11. The throughput of CLSM steadily increases, whereas the throughput of the IEEE 802.11 protocol rapidly decreases when the traffic load increases.

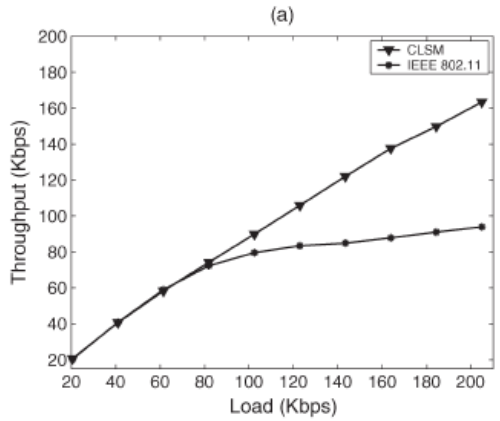


**Fig. 5.** Simulation result: Heterogeneous hidden problem

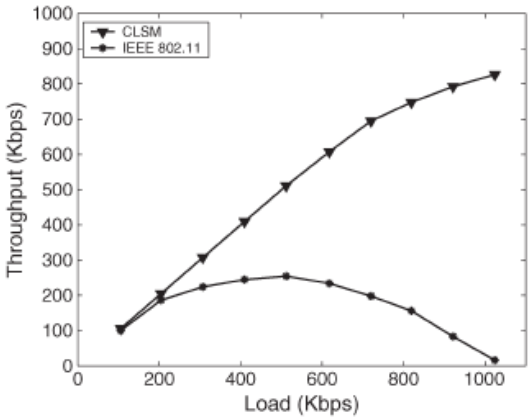


**Fig. 6**. Simulation result: Heterogeneous exposed problem

## VI. CONCLUSION

In this paper, the problems raised by link asymmetry in a wireless mesh network are addressed. The unidirectional link that exists in the network layer is eliminated and the heterogeneous hidden and exposed terminal problems are solved. This approach increases the network performance and throughput which is validated through simulations.

## REFERENCES

[1] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Commun. Mag.*, vol. 43, no. 9, pp. S23–S30, Sep. 2005.

[2] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Comput. Netw.*, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[3] P. Wang and W. Zhuang, "A collision-free MAC scheme for multimedia wireless mesh backbone," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3577–3589, Jul. 2009.

[4] B. S. Manoj, P. Zhou, and R. R. Rao, "Dynamic adaptation of CSMA/CA MAC protocol for wide area wirelessmesh networks," *Comput. Commun.*, vol. 31, no. 8, pp. 1627–1637, May 2008.

[5] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ISO/IEC Std. 8802-11: 1999(E), Aug. 1999.

[6] Y. Y. Su, S. F. Hwang, and C. R. Dow, "An efficient cluster-based routing algorithm in ad hoc networks with unidirectional links," *J. Inf. Sci. Eng.*, vol. 24, no. 5, pp. 1409–1428, 2008.

[7] C. H. Yeh, H. Zhou, P. H. Ho, and H. T. Mouftah, "A variable-radius multichannel MAC protocol for high-throughput low-power heterogeneous ad hoc networking," in *Proc. IEEE GLOBECOM*, Dec. 2003, pp. 1284–1289.

[8] C. H. Yeh, "The heterogeneous hidden/exposed terminal problem for power-controlled ad hoc MAC protocols and its solutions," in *Proc. IEEE 59th VTC*, May 2004, pp. 2548–2554.

[9] N. Poojary, S. V. Krishnamurthy, and S. Dao, "Medium access control in a network of ad hoc mobile nodes with heterogeneous power capabilities," in *Proc. IEEE ICC*, Helsinki, Finland, Jun. 2001, pp. 872–877.

[10] V. Shah, E. Gelal, and S. V. Krishnamurthy, "Handling asymmetry in power heterogeneous ad hoc networks," *Comput. Netw.: Int. J. Comput Telecommun. Netw.*, vol. 51, no. 10, pp. 2594–2615, Jul. 2007.

[11] B. J. David and A. M. David, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, vol. 353, no. 4, pp. 153–181, 1996.

[12] H. Zhai and Y. Fang, "Physical carrier sensing and spatial reuse in multirate and multihop wireless ad hoc networks," in *Proc. IEEE INFOCOM*, Barcelona, Spain, Apr. 2006, pp. 1–12.

[13] P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," *IEEE Trans. Info. Theory*, vol. 46, no. 2, Mar. 2000, pp. 388–404.

[14] X. Du, D. Wu, W. Liu, and Y. Fang, "Multiclass routing and medium access control for heterogeneous mobile ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 55, no. 1, pp. 270–277, Jan. 2006.

## AUTHORS

**Mr. S. Ashok Kumar** received B.E degree in CSE from Anna University, Chennai and Currently pursuing M.E degree in Computer Science and Engineering in Sri Shakthi Institute of Engineering and Technology, under Anna University of Technology, Coimbatore. His research interest includes Networks.

Mrs. N.Krishnammal received B.E degree in ECE from Anna University, Chennai and received M.E degree under Anna University of Technology, Coimbatore and puruing PHD in Networks under Anna University Coimbatore. She is currently working as a assistant professor in Sri Shakthi Institute of Engineering and Technology, Coimbatore. Her area of interest is Networks.