IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-12 E-ISSN: 2347-2693

An Improved Dynamic Source Routing Protocol for Detection and Removal of Black Hole Attack in Mobile Ad-Hoc Network

S.Anusuya[1*] and S.Meenakshi[2]
[1*,2] *Department of Computer Science, Bharathiar University, India*

www.ijcseonline.org

Received: 26/Nov/2015 Revised:09/Dec/2015 Accepted:22/Dec/2015 Published: 31/Dec/21015

Abstract— A mobile ad-hoc network (MANET) is a group of wireless mobile devices or nodes that communicate with each other without any help of a pre-installed infrastructure and centralized access points. Security is the most important concern for the functionality of network in MANET. MANET is unsecure from various attacks in the routing path and understanding the form of attacks is always the primary step towards the secured communication between mobile nodes. A number of attacks affect the safe exchange of information in MANET and among them the occurrence of black hole attack causes several limitations such as fault tolerance, packet loss, denial of service and jamming of network while transmitting data between nodes in the route. In order to preserve the security of MANET from attacks, routing protocols are important to ensure proper functioning of the path from source to destination nodes. In this research paper an improved dynamic source routing (IDSR) technique has been proposed to detect and remove the black hole attack nodes in the routing path and ensures reliable communication between nodes by constructing the black hole attack free route in MANET.

Keywords— MANET, black hole attack, routing protocols, dynamic source routing technique.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a group of wireless mobile devices or nodes that communicate with each other without any help of a pre-installed infrastructure and centralized access points. In a MANET independent mobile nodes can communicate to each other via radio waves. MANET offer several advantages over traditional networks include reduced infrastructure costs, ease of establishment and fault tolerance. Security is the most important concern for the functionality of network in MANET. MANET often suffer from security attacks because of its features like open medium, dynamic topology, lack of central monitoring and management.

MANET is unsecure from various attacks in the routing path and understanding the form of attacks is always the primary step towards the secured communication between mobile nodes in the route. A number of attacks affect the safe exchange of information which causes the communication interrupt or information steal in MANET.

The occurrence of attacks results in performance degradation in the network and also disturbs routing process between nodes in MANET. In order to preserve the security of MANET from attacks, routing protocols are important to ensure proper functioning of the path from source to destination nodes [2]. A routing protocol is a standard that controls flow of data packets in the network and also decide that which path should be followed by the packets to the reach the particular destination. A routing protocol must fulfill certain requirements to ensure proper functioning of the path from source to destination in presence malicious nodes are [1]: i) authorized nodes should perform route computation ii) minimal exposure of network topology iii) detection of spoofed routing messages iv) detection of fabricated routing messages v) detection of altered routing messages vi) avoiding formation of routing loops vii) prevent redirection of routes from shortest paths. A number of attacks affect the safe exchange of information in MANET and among them the occurrence of black hole attack causes severe limitations such as fault tolerance, packet loss, denial of service and jamming of network while transmitting data between nodes [6].

Hence detecting and removal of black hole attack at router level is an important research work in MANET. In this research paper an improved dynamic source routing (IDSR) technique has been proposed to detect and remove the black hole attack nodes in the routing path and ensures reliable communication between nodes by constructing the black hole attack free route in MANET.

The remaining sections of this paper are organized as follows. Section II describes the literature review of existing work for the detection and removal of black hole attack. Section III presents the design and algorithm of the proposed system to detect and removal of black hole attack on network layer in MANET. Section IV specifies the performance analysis and experimental results of the proposed IDSR algorithm and Section V presents the conclusion of this research paper.

Corresponding Author: *S.Anusuya, anusuresh628@gmail.com*
Department of Computer Science, Bharathiar University, India

II. LITERATURE REVIEW

Black hole attack is a kind of denial of service attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. Black hole attack may occur due to a malicious node which is deliberately. The various proposed techniques for the detection and removal of black hole attack in the literature are described as follows:

Shalini Jain [14] has proposed for detecting and removing the malicious nodes launching black hole attack. In this work malicious nodes are detected and removed in between the transmission of two blocks by ensuring an end-to-end checking. Source node sends a prelude message to the destination node before start of the sending any block to alert it about the incoming data block. Flow of the traffic is monitored by the neighbours of the each node in the route. After the end of the transmission destination node sends an acknowledgement via a postlude message containing the no of data packets received by destination node. In this work the process of detecting and removing malicious node by aggregating the response from the monitoring nodes and the network.

Deng, Li and Agrawal [5] have proposed black hole attack which protect against on AODV routing protocol. In this work a route reply packet is received from one of the intermediate node in the path, another route request is sent from the source node to the neighbour node of the intermediate node in the path. This research work eliminates the black hole attack by a single attacker, but it fails also in case of the gray hole attack.

JaydipSen and Harish Reddy [7] have proposed a solution for detection of the black hole attack. The authors proposed four different modules such as neighborhoods data collection module, local anomaly detection module, cooperative anomaly detection module and global alarm raising module to detect black hole attack. This work not only detects the black hole attack but also detect the grey hole attack. However, this work cannot stimulate nodes to forward other nodes packets.

Mohamed Elisalih and Xuemin Shen [10] have introduced as scheme TRIPO (Telephony Routing over Internet Protocol) to detect and remove black hole attack. This approach uses the credits to stimulate the rational packet droppers to relay packets and uses a reputation system to identify and evict the irrational packet droppers in black hole attack. In this work, nodes are stimulated to relay packets and use the trusted third party nodes. The trusted third party measures node's packet dropping frequency based on the receipts rather than the medium overhearing technique. TRIPO ensures fairness, as it can compensate the nodes that relay more packets by rewarding them with credits. Since packets pay for relaying their own packets, it discourages launching a resource exhaustion attack by sending spurious packets to exhaust the resources of the intermediate nodes.

Chang Wu Yu et al., [4] have proposed an approach DCM (distributed and cooperative mechanism) to solve the black hole attack. In this work an estimation table is constructed and maintained by each node in the network. Each node evaluates the information of overhearing packets to determine whether there is any malicious node. If there is one suspicious node, the detect node initiates the local detection phase to recognize whether there is possible black hole. The initial detection node sends a check packet to ask the cooperative node. If the inspection value is positive, the questionable node is regarded as a normal node. Otherwise the initial detection node starts the cooperative detection procedure, and deals with broadcasting and notifying all one-hop neighbors to participate in the decision making.

Hesiri Weerasinghe [7] has proposed a collaborative black hole attack based on solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate black hole attacks. This work introduces a data routing information (DRI) table and cross checking using further request and further reply scheme.

Tamilselvan [15] has proposed a CAD (channel aware detection) approach has been proposed that adopts two strategies, hop-by-hop loss observation and traffic overhearing. Each intermediate node in the forwarding path observes the behaviour of its previous-hop and next-hop neighbours to detect the misbehaving nodes. These nodes judge the behaviour of its neighbours by comparing the observations against two detection thresholds known as monitoring and loss rate threshold. In this approach, every node in the forwarding path has to observe both its upstream and downstream neighbours by promiscuous overhearing which results in more energy loss at individual nodes. Whereas this approach does not employ any promiscuous monitoring by upstream nodes in the source route and the nodes in forwarding path observe other nodes behaviour by means of query request and query reply packets.

Most of the black hole attack removal techniques reviewed in this section detects and remove black hole attacks based on the techniques such as channel aware detection and trust based approach. The proposed above techniques are prone

to various issues include fault tolerance, packet loss, denial of service and jamming of network. Thus the limitations of the existing black hole attack techniques may serve as directions to extend or improve the area of routing techniques further. Hence the focus of this research paper is to detect and removal of black hole attack in routing path for secured data transmission between nodes at router on network layer in MANET.

III. PROPOSED METHODOLOGY

The black hole attack in a network is likely to occur when the number of packets arriving at suspicious value of a node exceeds its threshold value. In this research paper an improved dynamic source routing (IDSR) technique has been proposed for detection and removal of black hole attack at routing path based on the intrusion detection system (IDS) technique. The proposed IDSR algorithm has been used to find the attack free path for data transmission and it also ensures reliable communication between nodes in MANET with several advantages such as low packet drop ratio, low routing overhead and low end-to-end delay.

A. System design

The primary path discovery process is given the number of input packets in network layer on MANET. The proposed improved dynamic source routing algorithm has been used to detect and remove black hole attack using intrusion detection technique. The intrusion technique has been used to detect the occurrence of black hole attack at any intermediate node and after the detection it sends warning message to all other intermediate nodes on the network. The proposed IDSR algorithm is used to find the attack free path for data transmission.

The proposed system design is shown in Figure-3.1. The performance of the proposed system has been analyzed using the metrics such as low packet drop ratio, low routing overhead and low end-to-end delay.

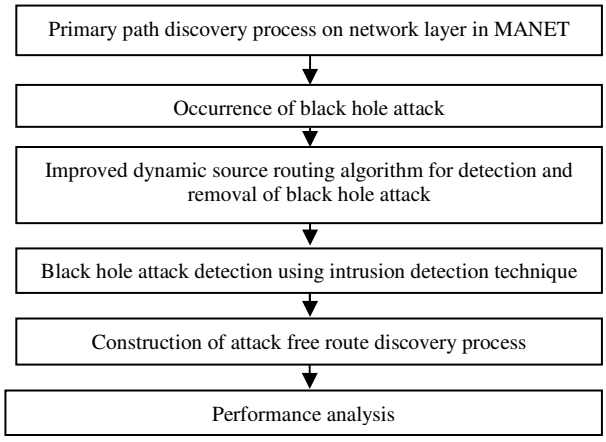

Figure-3.1 System design

B. Dynamic black hole attack detection and removal algorithm

Dynamic black hole attack removal algorithm find the source node broadcasts route request packet to find the path to reach the destination. The proposed system uses the node thresholds to detect the black hole nodes in the routing path. If probability of packet greater than threshold value then the destination node detects the black hole node is present in the route. Otherwise intrusion detection system can be sending a warning message to all other neighbouring node. If the destination node is in its two-hop list, then the data packet is transmitted by intermediate node. Otherwise the source node broadcasts the route request to the network. Then receives this route request packet, it also checks its two-hop list. If the destination node is in its two-hop list, then route request directly forward to the destination node. The destination node responds to the first received route request and sends back a route reply packet. The route reply packet has travel back in the same path and adds a new entry in its routing table. The attack free path now becomes the primary route between the source and the destination. The destination node path sends the route reply to the source node in response.

The black hole nodes also participate in route discovery process and claim for the shortest route to the destination. If the route is chosen through the black-hole node, then it can drop the data packets. In this approach the source node has to send route request packet to find a path to reach the requested destination. The requested destination, or any intermediate node having the path, can send back the reply to the source node. The malicious nodes which perform black hole attack participate correctly in the route discovery process. The proposed improved dynamic source routing algorithm for detecting and removing of black hole attack between the source node and the destination nodes is shown in Figure-3.2.

Step 1: If source node S

Send to the destination node D, forwarded to the number of data packets

Send the data packets through path in black hole attack discovery process

Else if

Destination node data packets received and compare the data packets initiate to the source node.

Step 2: Calculate the probability of packets received by destination node as P_D.

Step 3: If $P_D > T$

Detecting the malicious nodes present in the route

Else

Intrusion detection system sent a warning message

to all other neibhouring node.

Step 4: Each node update the malicious node status Information in its routing table.

Step 5: Source node generate route request to the destination node.

Step 6: The destination node send route reply packet to source node.

Figure-3.2 Dynamic black hole attack detection and removal algorithm

The proposed IDSR technique has been developed with two components such as: (i) detection and removal of black hole attack using intrusion detection system (ii) black hole attack free route discovery process for ensuring reliable communication between nodes in MANET with several advantages such as low packet drop ratio, low end-to-end delay and low routing overhead.

- *Detection and removal of black hole attack using intrusion detection system*

Intrusion detection system used for the destination node intimates the suspected nodes in the source route to its nearby IDS nodes through an MNREQ (malicious node request) packet. The MNREQ packet is forwarded to all the IDS nodes. The MNREQ packet is forwarded only by an IDS node to its neighbour nodes. The IDS node near neighbour is the source node sends an ALARM packet to the source node to intimate the presence of attacker in the data forwarding path and to send the next block of data. When the source node sends the next block of data, the IDS nodes that are neighbours to the suspected nodes turn into promiscuous mode and listen whether the data packets are forwarded or dropped by the suspected nodes. If any of the suspected nodes is found to be dropping data packets intentionally, it can be moved to the malicious node list.

Then a block message is sent to all the nearby nodes by the IDS nodes which monitored them. The IDS node that receives the block message will broadcast to its neighbours and hence the malicious node is isolated from the network. The block message is forwarded only by the IDS nodes to the network. Any node that receives the block message has learned the malicious node information and then drops the message without forwarding. Once the malicious node is identified, all nodes remove the routing information in node.

- *Black hole attack free route discovery process*

The destination node discovers that the actual number of data packets it receives from its previous hop node is significantly less than the number of data packets the source node sends and it starts the black hole node discovery process. First it sends a query request packet to the node in the source route (data forwarding path) at a 2-hop distance from it. If S, a_0, a_1, a_2, .. , a_{n_3}, a_{n_2}, a_{n_1}, an, D represents the source route, then node D sends a query request packet to node a_{n_1}which is at 2-hop distance to node D. The query request is used for finding the number of data packets forwarded by that node, to its next hop node. The node a_{n_1}sends back a query reply packet to the destination node D. The query reply contains the number of data packets a node forwarded to its next hop neighbour in the source route. The query reply it receives, the destination node verifies whether its previous hop neighbour is correctly forwarding all the data packets it receives from its previous node. If not correct, the destination node moves both nodes $a_{n_1}$and a_n to the suspected list. If correct, it means that those two nodes are participating correctly in data forwarding. So the destination again sends a new query request to the node a_{n_3}which is at 2-hop distance from the node a_{n_1} in the source route. The query reply it receives, the destination node verifies whether two nodes $a_{n_3}$and a_{n_2} are forwarding all the data packets they received. This process continues until the query request reaches the node which does not have a previous hop node at 2-hop distance in the source node.

Using the query reply packets the verification of data forwarding behaviour of the intermediate nodes in the source route will be carried out by the destination. If the difference in number of packets forwarded between any two intermediate node crosses the monitoring threshold value, the destination node marks both the intermediate nodes as suspected nodes.

IV. SIMULATION RESULTS

The various parameters have been used for testing the proposed IDSR technique has been described and is shown in table-4.1. The network consist area of 1000 * 1000 meter, 40 nodes executing the IDSR protocol. The transmission range is 250 meters with bandwidth 2 Mbps. The network layer is based on IEEE 802.11 distributed coordination function. The mobility model used was the random way point model. The data flow used constant bit rate (CBR), which varies from 3 packets to 30 packets, and the load flow varies from 10 to 40. The maximum speed of the node is 20 m/s and the simulation time is 900 seconds.

Table-4.1: Simulation parameters

Routing protocol	DSR
Coverage area	1000*1000 m
Number of nodes	40
Simulation time	900 seconds
Transmission range	250 meters
Mobility model	Random way point model
Traffic type	UDP-CBR
Load	5 kb UDP packets

Mobility speed	20 milli seconds
Pause time	0,5,10 and 15 seconds
IDS nodes	8 nodes(fixed)

A. Performance metrics and results

The primary path discovery process is given the number of input packets in network layer on MANET. The proposed ISDR algorithm has been used to detect and remove black hole attack using intrusion detection technique. The performance of the proposed IDSR technique has been compared with existing dynamic source routing (DSR) algorithm by using the metrics such as packet drop ratio, end-to-end delay and control packet overhead. The simulation results are based on number of nodes and time.

- *Packet drop ratio*

Packet drop ratio defined as the total number of data packets dropped by the malicious nodes and also to the total number of data packets sent. Packet drop ratio of the network is shown in the graph. In the X-axis number of nodes mobility is taken and in the Y-axis the total packet loss is taken. The graph shows that if the number of node is decreased and the total packet loss is also decreased. The proposed improved dynamic source routing algorithm achieves lower packet loss compared with existing dynamic source routing estimation technique and is shown in Figure-4.1.

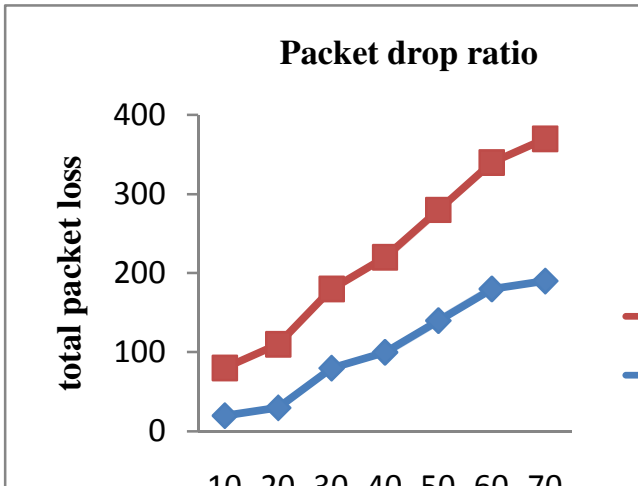

Figure-4.1 Comparison of packet drop ratio

- *End- to- end delay*

End-to-end delay refers to the time elapsed between time when the source node is triggered off to the time the destination node receives. In the graph number of nodes mobility is taken in the X-axis and time is taken in milliseconds in the Y-axis. The graph shows that if the number of nodes increases the end-to-end delay of the network is decreased.

The proposed IDSR achieves lower end-to-end delay compared with existing DSR technique and is shown in Figure-4.2.

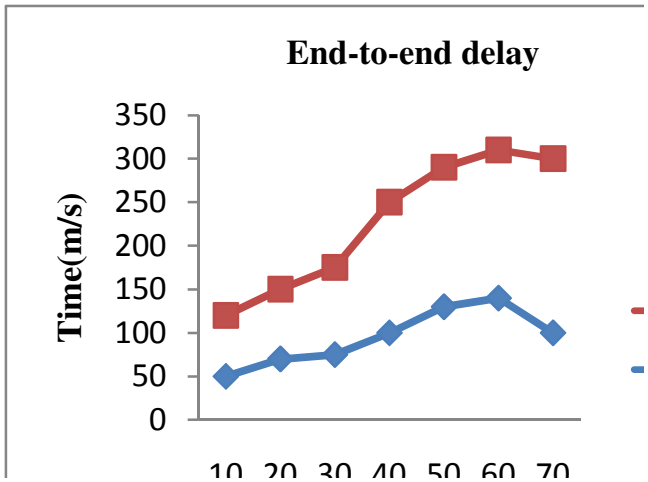

Figure- 4.2 Comparison of end-to-end delay

- *Control packet overhead*

Control packet overhead denotes the amount of traffic added in order to cope with packets droppers. The control packet overhead of the network is shown in this graph. In the X-axis number of nodes is taken and in the Y-axis control packet of the network is taken. This graph clearly shows that if the number of node is decreases the control packet overhead is decreased. The proposed improved dynamic source routing algorithm achieves lower control packet overhead compared with existing dynamic source routing estimation technique and is shown in Figure-4.3.

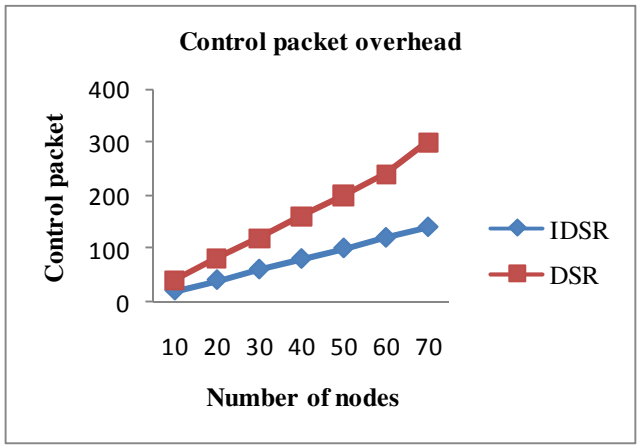

Figure-4.3 Comparisons of control packet overhead

V. CONCLUSION

MANET is unsecure from various attacks and among them the occurrence of black hole attack causes severe limitations. In order to preserve the security of MANET from attacks, a routing protocol must fulfill certain requirements to ensure proper functioning of the path from source to destination nodes in the presence of malicious nodes. In this research paper an improved dynamic source routing (IDSR) technique has been proposed to detect and remove the black hole attack nodes based on the intrusion detection system at router level on network layer and ensures reliable communication between nodes by constructing the black hole attack free route in MANET. The experimental results shows that the proposed IDSR technique provides better performance than the existing dynamic source routing technique for detection and removal of black hole attack, in terms of packet drop ratio, end-to-end delay and control packet overhead.

ACKNOWLEDGMENT

I am grateful to Dr. S.Meenakshi, Associate professor, Department of Computer Science, Gobi Arts & Science College, Tamilnadu, India.

REFERENCES

[1] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi, "A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)", International Journal of Information and Education Technology, Vol. 3, No. 1, February **2013**.

[2] S. Anusuya, Dr. S.Meenakshi, "A Review of Routing Protocols and Attacks in Mobile Ad-hoc Network", International Journal of Advanced Research in Computer Engineering & Technology, Vol. 4, Issue 9, pp.3485-3493, September **2015**.

[3] T.Ashish Bhole, Prachee ,N. Patil "Study Of Black hole Attack In MANET", International Journal of Engineering and Innovative Technology, Vol.2, No. 4, October **2012**.

[4] C-C Chiang, H-K Wu, W .Liu, M.Gerla "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel", In Proceedings of IEEE SICON, pp.197–211, **1997**.

[5] H. Deng, W. Li, and Dharma P. Agrawal, "Routing Security in Ad Hoc Networks," IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol. 40, No. 10, pp. 70-75, October **2002**.

[6] M. Girish Chandra ,S.G.HarishReddy,JaydipSen "A Mechanism for Detection of black hole attack in Manets", In Proceeding of the 6th International Conference on Information, Communication and Signal Processing(ICICS07), Singapore, December **2010**.

[7] HesiriWeerasinghe and Huirong Fu, Member of IEEE, "Preventing Cooperative Black Hole Attacks in Mobile Ad-hoc Networks", Simulation implementation and evaluation, Vol. 2, No.3, July **2008**.

[8] JaydipSen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamurlidhar (Embedded System Research Group, TCS), "Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", IEEE **2007**.

[9] D. B. Johnson, DA.Maltz and J.Broch "Dynamic Source Routing Protocol (DSR)", ACM Digital Library, pp 210-215, October **1996**.

[10] M.Mohanapriya, krishnamurthi "DSR protocol for detection and removal of black hole attack in MANET", ELSEVIER computer and electrical engineering, pp.530-538, **2014**.

[11] V. G. Muralishankar and Dr. E. George Dharma Prakash Raj, "Routing Protocols for MANET: A Literature Survey", International Journal of Computer Science and Mobile Applications, Vol. 2, No.3, March **2014**.

[12] D.B.Roy, R.Chaki and N.Chaki, "A New Cluster-Based black hole Intrusion Detection Algorithm for Mobile Ad Hoc Networks", International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, **2009**.

[13] Shalini, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by dynamic learning method", International Journal of Network Security", Vol.5, No.3, pp. 338-346, 2007.

[14] Tamilselvan, L.Sankaranarayanan, "Prevention of black hole Attack in MANET", International Journal of networks Network Security, Vol.3, No.5, May **2008**.

AUTHORS PROFILE

S.Anusuya is an M.Phil research scholar in Department of Computer Science, Gobi Arts & Science College, Gobichettipalayam. She received her M.Sc., Computer Science from PSG College of Arts and Science in the year 2014. Her area of interest is Advanced Networks.

Dr. S. Meenakshi did her M.C.A from University of Madras and M.Phil, Ph.D in Computer Science from Bharathiar University. She is an Associate Professor in Computer Science at Gobi Arts & Science College, Gobichettipalayam and has 25 years of teaching experience. She has published research papers in International Journals and her areas of interests include Object-Oriented Programming Systems, Advanced Database Systems and Data Mining.