International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 8 –NOVEMBER 2016.

A STUDY ON OPPORTUNISTIC ROUITING IN WIRELESS AD HOC NETWORKS

P.Balamurugan[#1] and Dr.S.Dhanalakshmi[*2]

[#] *Research Scholar, Periyar University,Salem,India.*

[*] *Vivekanandha College of Arts and Science for Women (Autonomous),Tiruchengode,India.*

***Abstract*— Opportunistic routing has recently attracted much attention as it is considered a promising direction for improving the performance of wireless ad hoc and sensor networks. With opportunistic routing, intermediate nodes collaborate on packet forwarding in a localized and consistent manner. Opportunistic routing greatly increases transmission reliability and network throughput by taking advantage of the broadcast nature of the wireless medium. This paper presents basic concepts of ad hoc networks. And also this paper illustrate the basic idea behind opportunistic routing, and then presents a survey of the most significant opportunistic routing protocols for ad-hoc wireless networks.**

***Index Terms*— Wireless Ad Hoc Network, Opportunistic Routing Protocols, Packets**

I. INTRODUCTION

Ad-hoc wireless networks [1] [2] [3], however, do not require any infrastructure to work. Each node is capable of talking directly to other nodes, so access point controlling medium access is not required. Fig 1 shows two ad-hoc networks with three nodes each. Within an ad-hoc network nodes can only communicate, if they can reach each other physically, i.e., if they are present within radio range of each other or if other nodes forward the message. Nodes from the two networks shown in Figure 1 cannot, therefore, communicate with each other if they are not within the same radio range.

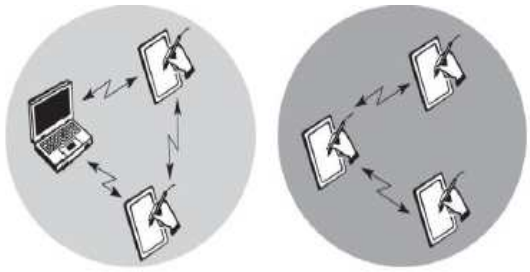

Figure 1: Example of two ad-hoc wireless networks

In ad-hoc networks, the complexity of each node is higher because every node has to implement medium access mechanisms and perhaps priority mechanisms, to handle hidden or exposed terminal problems and to provide a certain quality of service respectively. This type of wireless network shows the greatest possible flexibility in quick replacements of infrastructure or communication scenarios. However, might be a selected nodes with the capabilities of forwarding data is present in an ad-hoc networks and most of the nodes have to connect to such that special node first in order to transmit data if the receiver is out of their range.

- **Single-hop [3]** (All partners max. one hop apart), For Example: Bluetooth piconets, PDAs in a room, gaming devices.

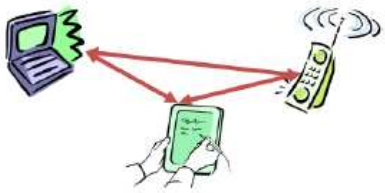

Figure 2: Single-hop

- **Multi-hop [3]** (Cover larger distances, circumvents obstacles), For Example Bluetooth scatter net, TETRA police network, car-to-car networks.

Figure 3: Multi-hop

Out of three WLANs: IEEE 802.11 and HiperLAN2 are usually needs infrastructure, and additionally they support ad-hoc networking. The third WLAN (Bluetooth) is the classical wireless ad-hoc network. Bluetooth focuses on spontaneous ad-hoc networks or on the simple connection of two or more devices without the setup of any infrastructure.

A. Ad Hoc Networks Characteristics

- **Mobility:** Nodes can be quickly repositioned. We can have individual random mobility, group mobility etc. The mobility model can have mainly significant force on the selection of a routing method and can thus influence the performance.
- **Multihopping:** A multihop network is a network where the paths from source to destination pass through numerous nodes. Ad hoc nets frequently reveal multiple hops for obstacle negotiation, spectrum reuse and energy conservation.

- **Self-organization:** The ad hoc network must unconventionally determine its own configuration parameters including addressing, routing, clustering, identification of position, power control etc.
- **Energy conservation:** Most ad hoc nodes (e.g., laptops, PDAs, sensors, etc.) have limited power supply and no capability to generate their own power (e.g., solar panels). Energy efficient protocol design (e.g., MAC, routing, resource discovery, etc) is critical for longevity of the mission.
- **Scalability:** In some applications (e.g., large environmental sensor fabrics, battlefield deployments, urban vehicle grids, etc) the ad hoc network can grow up to numerous thousand nodes.
- **Security:** The ad hoc networks, however, are even more exposed to attacks than the infrastructure counterpart. Both active and passive attacks are possible. In active attack attacker tries to interrupt operations (control and data packets; reintroduces bogus control packets; damages the routing tables beyond repair; unleashes denial of service attacks, etc.). Passive attacks are unique in ad-hoc network and can be more hazardous than the active attack. The active attacker is eventually discovered and physically disabled. The passive attacker is never discovered by the network. It monitors data and control traffic patterns and thus infers the normal operation. Defence from passive attacks requires powerful novel encryption techniques coupled with careful network protocol designs.
- **Connection to the Internet:** As discussed, there is merit in extending the infrastructure wireless networks opportunistically with ad hoc appendices. The integration of ad hoc protocols with infrastructure standards is thus becoming a hot issue.

II. OPPORTUNISTIC ROUTING

The new approach discussed in this paper uses the broadcasting nature of the wireless network for packet forwarding. This approach is named as "Opportunistic Routing (OR)". The key idea behind OR is to use the broadcasting nature of wireless network such that transmission from one node can be overheard by multiple nodes. Instead of choosing the next forwarder node ahead of time, the OR chooses the next node dynamically at the time of transmission. The forwarding is done by the node closest to the destination. It has been shown that OR gives better performance than traditional routing. The key task of the OR is to select the forwarder set and prioritize the nodes in the set. Consider the following example. Here the source node S has four intermediate nodes with packet delivery probability of 15%. Each intermediate node has packet delivery probability of 85% to the destination. Traditional routing will choose only one intermediate node for data forwarding, while OR will consider all these nodes for data forwarding. Thus, OR proves to be more efficient and reliable than traditional routing.

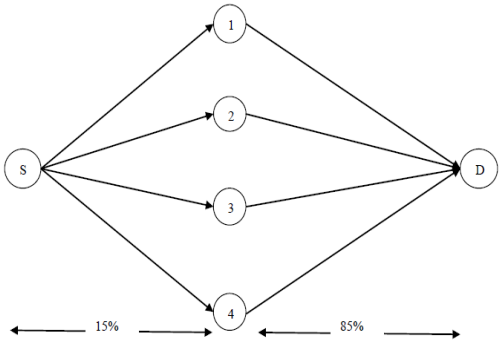

Figure 4: Illustration in which each source node has multiple intermediate nodes along with packet delivery probability for data transmission to the destination node.

A. Opportunistic Routing Characteristics

1) How Opportunistic Routing works?

In opportunistic routing, and differently from traditional routing, the routing schemes are not based on pre-selection. Actually, the forwarding process is dynamic; and characterized by these steps: firstly, the broadcast of the data packet to relay candidates. And secondly, based on a coordination protocol, the selection is done by choosing the best relay candidate (node) to forward the data packet.

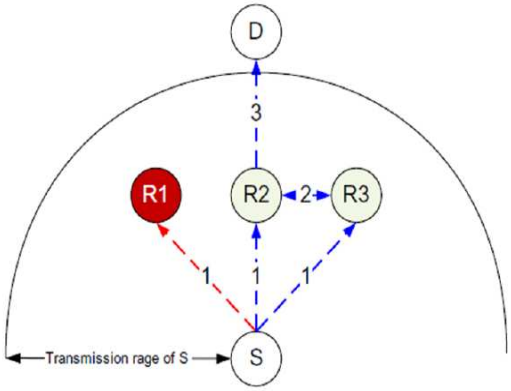

Figure 5.How opportunistic routing works

To illustrate the dynamic forwarding process of opportunistic routing, the figure 5 is considered. As we can see, the source S sends a data packet to the destination D, through three different nodes R1, R2 and R3. The sequence of events is represented by the number mentioned in each edge. The first step of the forwarding process is when S broadcasts a packet. We remark that, both of the nodes R2 and R3 receive successfully the packet. On the contrary, the node R1 failed. Then, after running a coordination protocol, both of R2 and R3 take the decision of making R2 the elected node to forward the data packet to the destination D.

Opportunistic routing is also characterized by two important advantages: Increase reliability and increase transmission range.

2) Increase reliability

When it comes to increase reliability, the opportunistic routing is doing well. In fact, it has additional backup links

due to the dynamic nature of transmission, which is based on forwarding a data packet through any possible link rather than one specified link. As consequence, the probability of transmission failure is reduced.

3) Increase transmission range

With opportunistic routing, the performance can be improved due to the possibility of direct transmission to the farthest relay node. What makes this possible is the use of all possible links when forwarding a data packet.

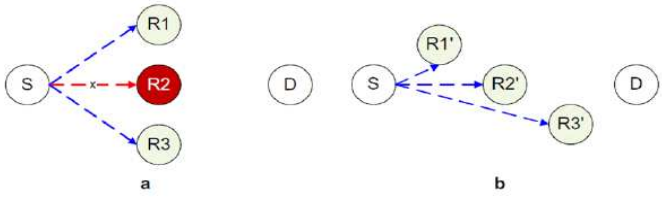

Figure 6: How overhead packets could be utilized.
(a) Enhancing transmission reliability.(b) Maximizing transmission range

B) Basic Operation of Opportunistic Routing in Ad Hoc

Opportunistic routing is based on the broadcast transmissions of the data packets. This type of transmission is used in order to increase the probability that at least one potential relaying node receives the packet. Next figure illustrates the advantage of broadcast transmissions.

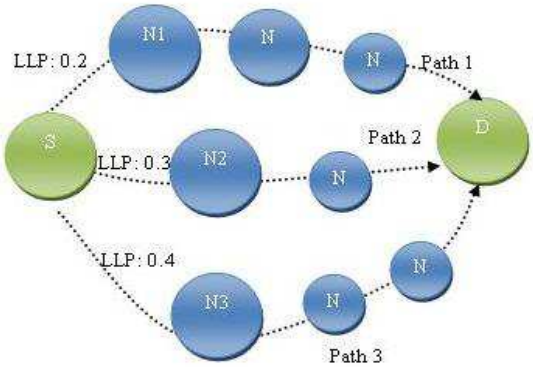

Figure 7: Connections in a wireless network to illustrate the benefits of opportunistic routing.

The source (*S*) needs to send packets to the destination (*D*). It knows that its neighbors *N1*, N2 and *N3* provide different paths to the destination (*path1*, *path2* and *path3*). It has also estimated the loss probability in each link (LLP) to its neighbor. Specifically, the link to *N1* has a loss probability of 0.2 while to *N2* and to *N3* the loss probability is 0.3 and 0.4 respectively.

Using traditional routing, the Source *S* should select one of these potential forwarders as the next hop. Then, it will send the packet to this neighbor by a unicast transmission. Taking into account the loss probability, the source will select *N1* as the next hop and the probability that the packet is not retransmitted is 0.2. Alternatively, opportunistic routing will emit the packet in broadcast so the three neighbors (and some others too) will be able to receive it and to retransmit it. The probability that the packet will not be retransmitted is equivalent to the probability that no neighbors will receive the packet. This probability is 0.2•0.3•0.4, that is, 0.024. As we can see, the loss probability obtained with the opportunistic strategy is much lower than the resulting from the traditional routing.

B. Phases of Opportunistic Routing

In order to better understand how opportunistic routing works, we will pay attention to the sequential phases that form part of an opportunistic routing protocol. These phases are:

- **Candidate Selection:** The protocol in the Layer-Three in the IP stack selects a set of nodes that allow the transmission of the packet from the source to the destination. This set of candidate relays is known as the forwarding candidates, the candidate forwarder set or the relay set. The nodes in the list may be ordered according to some criteria in the second phase. The source informs about its relay set including the IDs of the candidates belonging to the forwarding list in the packet header. In order to reduce the space required to store all the addresses of the relay set in the packet headers, a Bloom filter is suggested in [4].
- **Candidate Priority Assignment:** When the source informs about the forwarding candidates, it orders them according to their convenience to act as relaying nodes. The appropriateness of a node is based on some metrics. For instance, the metrics could be derived at the MAC layer such as the loss probability. Nodes should periodically measure these parameters. The relay set plays an important role in opportunistic routing protocols. The candidate selection and its order are usually performed periodically so that the two first phases are not always executed in the emission of every data packet.
- **Data transmission:** The original opportunistic routing protocols are supported by the transmission of broadcast packets so that they can be received by multiple neighboring nodes. However, there are some opportunistic routing protocols [5] where the data packets are unicast. In particular, the best forwarding node is specified in the next hop field of the packet. The other candidates receive the packet by eavesdropping.
- **Receiver coordination:** Among the forwarding candidates that receive the data packet, just one of them should be the relaying node for the current packet. The elected node will be also responsible for confirming the data reception at the MAC layer. The election is carried out by incorporating a distributed procedure in the nodes. The goal of the procedure is that the selected node should be the highest-priority relay that has successfully received the packet. In this sense, some proposals opt for modifying the MAC layer. For instance, [6] includes a list of four fields in the RTS (Ready to Send) messages. The list represents the forwarding set. The candidates reply with one CTS (Clear to Send) message sequentially. Then, the source decides about which node is going to act as the forwarding node and it sends the data to the elected node.

III. OPPORTUNISTIC ROUTING PROTOCOLS

One of the main features of the opportunistic routing protocols is how to determine the forwarding set and how to assign the priority to the nodes in the set. In order to quantify the convenience of a node to belong to this set, that is, to determine its priority, a metric is used. Depending on the kind of metric, the opportunistic routing protocols are classified as below:

Extreme Opportunistic Routing: Extreme Opportunistic Routing (ExOR) [7] is a state-of-the-art OR protocol for wireless multihop networks and has been implemented on the RoofNet testbed at Massachusetts Institute of Technology (MIT). ExOR integrates routing and MAC protocols. It improves routing performance by utilizing long-range but lossy links. ExOR is designed for batch forwarding. The source node includes a forwarder list in each packet, prioritized by ETX distance to the destination: the shorter the distance, the higher the priority. Only those nodes that are closer to the destination than the source are included in the forwarder set. Each packet has a BITMAP option, which marks those packets that have been received by the sending node or nodes with higher priorities. All packets are broadcast. A forwarder transmits a packet only if no forwarder with higher priority has explicitly acknowledged receipt of it, as indicated in the BITMAP position for this packet. ExOR has good routing performance. However, it also has the following drawbacks. First, it reduces spatial reuse because it enforces global coordination among forwarders. Second, forwarders connected with low-quality links or no links can make inconsistent decisions on packet forwarding because a forwarder may not hear the acknowledgment from other forwarders with higher priorities, which causes duplicate transmissions.

Integration of Aomdv And Anycast : Jain and Das developed an anycast MAC protocol to perform channel-state-based next hop selection among multiple next hop candidates [8]. The designed protocol is an extension of the IEEE 802.11 MAC layer. A sender first multicasts an RTS to the multiple next hop candidates, which contains the addresses of all the receivers. CTS transmissions are staggered in time in order of the priorities of the receivers, which can be based on hop count or queue length at the receivers. Upon receipt of CTS, the sender transmits DATA to the sender of the CTS after a short interframe space (SIFS) interval, which notifies the remaining receivers to stop sending their CTSs. In [8], this anycast MAC protocol is further integrated with a multipath extension to the Ad Hoc On Demand Vector (AODV) routing protocol, referred to as AOMDV. Experimental and simulation results show that the integrated protocol can improve network performance in time-varying radio environments.

OPRAH: OPRAH [4] builds a braid multipath set between source and destination via on-demand routing to support opportunistic forwarding. For this purpose, OPRAH allows intermediate nodes to record more sub paths back to the source and also those sub paths downstream to the destination via received Route Requests and Route Replies. OPRAH can increase end-to-end forwarding reliability. In OPRAH the destination may receive duplicate data packets because a built route set may contain spatially disjoint paths or partially disjoint paths from an intermediate node down to the destination.

Robust and Scalable Geographic Multicast Protocol (RSGM): RSGM can scale up to a large group size and network size. It provides robust packet transmission in a dynamic MANET. Protocol uses several virtual architectures for more robust and scalable membership management and packet forwarding in unstable wireless network. Membership management is done using virtual zone based structure. Data and control packets will be transmitted along efficient tree like path. This protocol is different from other tree based protocol. In this protocol there is no need to create and maintain tree structure. Stateless virtual tree based structure reduces tree management overhead and supports efficient packet transmission. Geographic forwarding is used to increase the scalability and robustness. The efficient source tracking mechanism is used to avoid the periodic flooding of the source information in the network. RSGM can scale to large group and network size over existing protocol ODMRP. It also increase the delivery ratio under all circumstances such as node speed, node density etc. This protocol is having minimum control overhead and joining delay.

Geographic Random Forwarding: Geographic Random Forwarding (GeRaF) [9] is a geographical forwarding protocol. It selects a forwarder set and prioritizes them using location information. In GeRaF each packet carries the locations of the sender and destination. Only those neighboring nodes closer to the destination than the sender can be forwarder candidates. Moreover, these eligible candidates rank themselves based on their geo-distances to the destination. In this way the forwarder set and prioritization can easily be implemented via an RTS-CTS dialog at the MAC layer, which also ensures that a single forwarder can be chosen. GeRaF adopts hop-by-hop forwarder set selection. It is targeted for relatively dense networks. GeRaF is simple to implement. However, the cost for acquiring location information may be too high to implement, at least in the near future.

Coding-Aware Opportunistic Routing : Coding-Aware Opportunistic Routing Mechanism (CORE) [10] is an integration of localized interflow network coding and opportunistic routing. Existing localized network coding mechanisms only adopt best path routing and passively wait for the appearance of coding chances on the path. This leads to inefficient use of network resources. By integrating localized network coding and opportunistic forwarding, CORE enables a packet holder to forward a packet to the next hop that leads to the most coding changes among its forwarder set. Such recursive hop-by-hop operations can greatly improve the end-to-end coding gain in packet delivery with little extra protocol overhead. Table 1 summarizes all the above discussed protocols based on the criteria listed in the previous section.

A Novel Socially-Aware Opportunistic Routing: The author proposes the use of OR for the MANETs using the cost metrics such as social relations and profiles of the nodes. The proposed distributed protocol is Social Relation Opportunistic Routing (SROR) to compute best forwarding node in routing. The protocol mainly considers the social relations, mobility patterns and social profiles for Mobile Adhoc Networks (MANETs). For selection of the forwarding node in the routing SROR following three matching parameters are taken into account viz. social profile matching, social connectivity matching and social interaction. Hence when the node wants to send the packet, due to the algorithm there is high possibility that the best candidates sharing similar interest tend to meet again to forward the data. SROR gives high packet delivery rate and routing efficiency compared to other protocols for MANETs.

IV. ISSUES IN OPPORTUNISTIC ROUTING

Three main issues arise in the design of OR protocols:

- **Candidate selection** all nodes in the network must run an algorithm for selecting and sorting the set of neighboring nodes (candidates) that can better help in the forwarding process to a given destination.
- **OR metric** In order to accurately select and prioritize the CSs, OR algorithms require a metric. First OR algorithms were based on simple metrics inherited from traditional unicast routing, as those used by shortest path first (SPF) algorithms. However, some researchers realized that more accurate metrics were required in OR.
- **Candidate coordination** is the mechanism used by the candidates to discover which one has the highest priority that has received, and thus, must forward the packet. Coordination requires signaling among the nodes, and imperfect coordination may cause duplicate transmission of packets.

With perfect coordination among candidates, the larger is the number of candidates the lower is the expected number of transmissions from the source to the destination. However, increasing the number of candidates increases also the coordination overhead. Therefore, in practice, the maximum number of candidates that can be used is limited.

V. ROUTING METRICS

The general aim of OR is to minimize the expected number of transmission required to carry a packet from the source to the destination. The set of candidate new hop forwarders each node uses and priority order of the candidates has a significant impact on the performance that OR can achieve. Therefore, using a good metric to select and order the candidates is a key factor in designing an OR protocol. Candidates in OR can be prioritized based on hop count, geographic-distance(Geo-Distance), expected number of transmissions (ETX) [11], expected any-path trans- mission (EAX) and so on. Utilization of hop count, ETX or EAX needs an underlying routing protocol (either reactive or proactive) to gather such information. Geo-Distance requires the availability of location information of nodes. The accuracy of a metric depends on the proper measurement of link quality and timely dissemination of such information. Below, we describe the two usual metrics ETX and EAX.

- **Expected Transmission Count (ETX) [11]:** is the average number of transmissions required to reliably send a packet across a link or route including retransmissions. The ETX of a single path route is the sum of the ETX for each link in the route. With the assumption of the packet transmission between nodes i and j as Bernoulli trials with delivery probability pij, the expected transmission count of the link is:

$ETX(i,j) = 1 / P_{ij}$

In OR, however, it is necessary to consider the fact that there are some candidates who can receive the packet, thus, a packet may travel along any of the potential paths. Authors in have shown that using ETX may give suboptimal selection of candidates and in it was shown that OR in combination with ETX could degrade the performance of the network. Because of that Zhong et al. [12] proposed another metric which has been widely adopted in OR.

- **Expected Any-path Transmission (EAX) [12]:** is an extension of ETX and can capture the expected number of transmissions taking into account the multiple paths that can be used under OR. Alternative methods to compute EAX have been proposed by other authors.

VI. CONCLUSION

Opportunistic routing protocols present a promising scheme to improve the wireless network performance by exploiting the broadcast nature of the medium. The main concern of theses protocols relies on which neighboring nodes should forward the data packets and how to coordinate them to avoid duplicated retransmissions. This paper has reviewed basic concepts of opportunistic routing and their protocols for ad hoc networks to improving the network lifetime and also increases transmission reliability and network throughput by taking advantage of the broadcast nature of the wireless medium.

REFERENCES

[1] C. Siva Ram Murthy & B.S. Manoj, “Ad Hoc Wireless Networks Architectures and Protocols”, Pearson Education, 2nd Edition, 2005.
[2] Chakrabarti, “Quality of Service in Mobile Ad Hoc Networks”, Handbook of Ad Hoc Wireless Networks, CRC press, 2003.
[3] http://en.wikipedia.org/wiki/Wireless_ad_hoc_network.
[4] K. C. Lee, U. Lee, M. Gerla, “Geo-opportunistic routing for vehicular networks”, IEEE Communications Magazine, May. 2010
[5] S. Yang, C. K. Yeo, B. S. Lee, “Robust Geographic Routing with Virtual Destination based Void Handling for MANETs”, in the Proc. of the IEEE 71stVehicular Technology Conference (VTC 2010-Spring), May 2010.
[6] S. Jain, S. Das, “Exploiting Path Diversity in the Link Layer in Wireless Ad Hoc Networks”, in the Proc. Of the 6th IEEE WoWMoM Symposium, 2005.
[7] S. Biswas and R. Morris, “Opportunistic Routing in Multi-hop Wireless Networks,” *Proc. ACM SIGCOMM*, Aug. 2005, pp. 133–44.
[8] S. Jain and S. Das, “Exploiting Path Diversity in the Link Layer in Wireless Ad Hoc Networks,” *Proc. IEEE WoWMoM ‘05*, June 2005, pp. 22–30.

[9] M. Zorzi and R. R. Rao, "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance," *IEEE Trans. Mobile Comp*., vol. 2, no. 4, Oct.–Dec. 2003, pp. 337–48.
[10] Y. Yan *et al*., "Practical Coding-Aware Opportunistic Routing Mechanism for Wireless Mesh Networks," *Proc. IEEE ICC 2008*, May 2008, pp. 2871–76.
[11] Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris. A high throughput path metric for multi-hop wireless routing. Wireless Networks, 11(4):419,434, 2005.
[12] Zifei Zhong, Junling Wang, Srihari Nelakuditi, and Guor-Huar Lu. On selection of candidates for opportunistic anypath forwarding. SIGMOBILE Mob. Comput. Commun. Rev., 10(4):12, 2006.

P. Balamurugan received his M.phil degree from Periyar University, Salem in the year 2008. He has received his M.Sc Computer Science degree from Bharathidasan University, Tiruchirapalli in the year 2003. He is working as an Assistant Professor, Department of Computer Science, Sengunthar Arts and Science College, Tiruchengode, Tamilnadu. He is pursuing his Ph.D degree at Periyar University Salem, Tamilnadu, India. His areas of interest include computer networks, Network security and cryptography.

Dr.S.Dhanalakshmi received her Ph.D Degree from Anna University, Chennai in the year 2011. She has received her M.Phil, Degree from Periyar University, Salem in the year 2004. She has received her M.C.A Degree from Bharathidasan University, Triuchiraapalli in the year 1998.She is working as Assistant Professor, Department of Computer Science, Vivekanandha College of Arts and Science for women,Tiruchengode, Tamilnadu, India. She has 17 years of experience in academic field. She has published 22 International Journal papers and 14 papers in National and International Conferences. Her areas of interest include Computer networks, Network security and Data mining.