© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Efficient technique to Detect Blackhole Attack in Mobile Ad Hoc Networks

R. Deenadhayalan, S. Anandamurugan
Kongu Engineering College, Perundurai, Erode, Tamilnadu, India

ABSTRACT

An ad hoc routing protocol is a pattern, or standard, that controls to route packets between mobile devices in a mobile ad hoc network. A new node announces its presence and listens for announcements broadcast by its neighbours. To communicate one node to another one, each node can act as both host as well as router at the same time and perform all the routing and state maintenance operations. Source routing allows a sender of a packet to partially or completely specify the route the packet takes through the network. Source routing allows easier troubleshooting, improved traceroute, and enables a node to discover all the possible routes to a host. Opportunistic data forwarding has not been widely utilized in MANETs, because the lack of an efficient lightweight proactive source routing capability. A lightweight Table Driven Source Routing (TDSR) protocol can maintain more network topology information than Distance Vector (DV). To facilitate source routing and also smaller overhead than DV-based protocols, Link State (LS) and reactive source routing protocols. The threats to users of wireless technology have increased as the service has become more popular. Because of the dynamically changing topology, open environment and lack of security infrastructure, a mobile ad hoc network (MANET) is susceptible to the presence of malicious nodes and to ad hoc routing attacks. The variety of routing attacks that target the weakness of MANETs. In proposed scheme, efforts on mobile ad hoc network's routing weakness and analyses the network performance under black hole attack that can easily be employed against the mobile ad hoc network (MANET). The resistive schemes against these attacks were proposed for Table Driven Source Routing (TDSR) protocol and the effectiveness of the schemes is validated using NS2 simulations.

Keywords: MANET(Mobile Ad hoc Network), source routing, and proactive routing protocol

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a wireless communication network, where nodes that are not within the direct transmission range of each other require other nodes to forward data. The determination of which nodes forward data is made dynamically based on the network connectivity. MANET is in contrast to older network technologies in which some designated nodes, usually with custom hardware and variously known as routers, switches, hubs, and firewalls, perform the task of forwarding the data. Nodes should be able to relay traffic since communicating nodes might be out of range. They can provide access to information and services regardless of their geographical position. MANET is, ease of deployment and decreased dependence on infrastructure. To support opportunistic data forwarding in a mobile wireless network as in ExOR[2], an IP packet needs to be enhanced such that it lists the addresses of the nodes that lead to the packet's destination.

II. METHODS AND MATERIAL

A. Routing Protocols For MANETs

Routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network. In ad hoc networks, nodes are not familiar with the topology of their networks. Instead, they have to discover it. A new node

announces its presence and listens for announcements broadcast by its neighbors. Each node discovers about other nearby nodes and how to reach them.
The following is a list of ad hoc network routing protocols:

- Table-driven (proactive) routing protocols
- On-demand (reactive) routing protocols
- Hybrid (both proactive and reactive) routing protocols

i. Table-driven (proactive) routing protocols

In proactive routing scheme every node continuously maintains complete routing information of the network. It is achieved by flooding network periodically with network status information to find out any possible change in network topology. Current routing protocol like Link State Routing (LSR) protocol (Open Shortest Path First) and the Distance Vector Routing Protocol (Bellman-Ford algorithm) are not suitable to be used in mobile environment. Destination Sequenced Distance VectorRoutingprotocol (DSDV) and Wireless Routing Protocols (WRP) were proposed to eliminate counting to infinity and looping problems of the distributed Bellman-Ford Algorithm.

ii.On-demand (reactive) routing protocols

Every node in On-demand routing protocol maintains information of only active paths to the destination nodes. A route search is needed for every new destination therefore the communication overhead is reduced and the route search is making delay to send the packets. Rapidly changing wireless network topology may break active route and cause subsequent route search.
Examples of reactive protocols are:

- Ad hoc On-demand Distance Vector Routing (AODV).
- Dynamic Source Routing (DSR).

iii. Hybrid (both proactive and reactive) routing protocols

Hybrid routing protocol combines the advantages of proactive and reactive routing. The routing is initially established with proactive prospected routes and serves the demand from additionally activated nodes through reactive flooding. Proactive protocols have large overhead and less latency while reactive protocols have less overhead and more latency. So a Hybrid protocol is presented to overcome the shortcomings of both proactive and reactive routing protocols.
Examples of hybrid routing protocols:

- Zone Routing Protocol (ZRP).
- Enhanced Interior Gateway Routing Protocol (EIGRP), developed by Cisco.

B. Challenges in MANETs:

Some of the challenges in MANETs:

- Unicast routing
- Multicast routing
- Dynamic network topology
- Speed
- Frequency of updates or Network overhead
- Scalability
- Mobile agent based routing
- Quality of Service
- Energy efficient/Power aware routing
- Secure routing

The key challenges faced at different layers of MANET are shown in Figure 1 It represents layered structure[3] and approach to ad hoc networks.

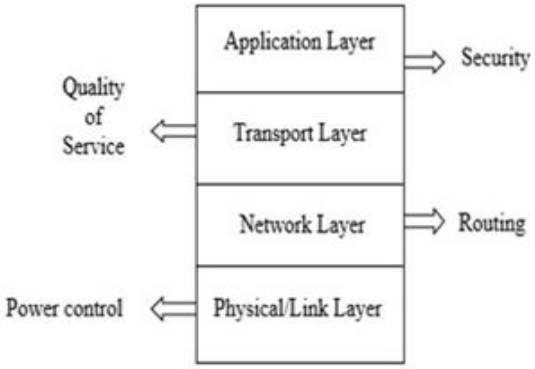

Figure 1: Layered structure of MANETs.

C. QoS in Mobile Ad Hoc Networks:

Quality of Service (QoS) is particularly important for the transport of traffic with special requirements. In particular, the technology has been developed to allow computer networks to become as useful as telephone networks for audio conversations, as well as supporting new applications with even service demands.

Quality of traffic:

- Throughput: The average rate of successful message delivery over a communication channel.
- Packet Delivery Ratio: The number of data packets delivered to multicast receivers over the number of data packets supposed to be delivered to the multicast receivers.
- Delay: When a packet travels from source node to destination node, it may suffer from different kinds of delays such as nodal processing delay, transmission delay and propagation delay. It degrades the performance of the network.

D. Related Work:

Perkins. C. E (1994) proposed Destination-Sequenced Distance-Vector Routing (DSDV) protocol for Mobile ad hoc networks. An adhoc network is the cooperative engagement of a collection of Mobile Hosts without the required intervention of any centralized Access Point. Each Mobile Host act as a specialized router, which periodically advertises its view of the interconnection topology [10] with other Mobile Hosts within the network. The Bellman-Ford routing mechanisms are suitable for a dynamic and self-starting network mechanism as is required by users to utilize ad hoc networks. The Bellman-Ford routing mechanisms is overcome the problem of looping properties of such algorithms in the face of broken links and the resulting time dependent nature of the interconnection topology describing the links between the Mobile Hosts. In DSDV the basic network-layer routing can be modified to provide MAC-layer support for ad-hocnetworks.

Murthy.S (1996) proposed the wireless routing protocol [7] (WRP). WRP reduces the number of cases in which a temporary routing loop can occur.WRP makes use of the routing table at each node in the record to complete the routing, and require each node to operate a record four tables, namely Distance table, Routing table, Link-cost table, Message retransmission list (MRL) table. WRP use the update message between adjacent nodes in each pass is used to determine whether the adjacent nodes to maintain their link relationship, and Message retransmission list is used to update records which need to re-transmission, and which update needs acknowledgement. WRP use of distance and the second-to-last hop information to find the path, such an approach can effectively improve the distance-vector routing possible count-to-infinity problem.

Clausen. T (2003) proposed an optimized link state routing protocol, named OLSR, for mobile wireless networks. The protocol is based on the link state algorithm and it is proactive in nature. It employs periodic exchange of messages to maintain topology information of the network at each node [10]. OLSR uses multipoint relaying technique to efficiently and economically flood its control messages. It provides optimal routes in terms of number of hops, which are immediately available when needed. The proposed protocol is best suitable for large ad hoc networks.

Perkins.C. E (2003) proposed Ad hoc on demand Distance Vector (AODV) routing algorithm for the ad hoc networks. Each Mobile Host operates as a specialized router and routes are obtained as needed (i.e., on demand) with little or no reliance on periodic advertisements. AODV is quite suitable for a dynamic self-starting network as required by users to utilize ad hoc networks. AODV provides loop-free routes even while repairing broken links.

Johnson. D. B (2007) proposed Dynamic Source Routingprotocol (DSR) specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network. The source routing allows packet routing to be loop-free, avoids the need for up-to-date routing information in the intermediate nodes through which packets are forwarded.

E. Existing Methodology:

Design of Table Driven Source Routing Protocol:

Breadth-first search is a way to find all the vertices reachable from the given source vertex, s. Like depth first search, BFS traverse a connected component of a given graph and defines a spanning tree. Intuitively, the basic idea of the breath-first search is this: send a wave

out from source s. The wave hits all vertices 1 edge from s. From there, the wave hits all vertices 2 edges from s.

Table Driven Source Routing (TDSR) provides every node with a Breadth-First Spanning Tree [12] (BFST) of the entire network rooted at itself. Nodes periodically broadcast the tree structure to their best knowledge in each iteration. Based on the information collected from neighbours during the most recent iteration, a node can expand and refresh its knowledge about the network topology by constructing a more recent BFST. When a neighbour node is lost, a procedure is triggered to remove its relevant information from the topology repository maintained by the detecting node [11].

The network is undirected graph

$$\mathbf{G} = (\mathbf{V}, \mathbf{E}) \qquad \mathbf{(1)}$$

Where V is the set of nodes (or vertices) in the network and E is the set of wireless links (or edges).

Two nodes u and v are connected by edge

$$\mathbf{e} = (\mathbf{u}, \mathbf{v}) \in \mathbf{E} \qquad \mathbf{(2)}$$

If they are (u, v) close to each other and can directly communicate.

For the node v, use N(v) to denote its open neighbourhood, i.e.,

$$N(v) = \{u \in V \mid (u, v) \in E\} \qquad (3)$$

i. Route Update

The operation of TDSR is iterative and distributed among all nodes in the network because of the proactive nature. At the beginning, node v is only aware of the existence of itself, there is only a single node in its BFST, which is root node v. By exchanging the BFSTs with the neighbours, it is able to construct a BFST within N[v], i.e., the star graph centered at v, which is denoted Sv. In each subsequent iteration, nodes exchange their spanning trees with their neighbours. From the view of node v, toward the end of each operation interval, it has received a set of routing messages from its neighbours packaging the BFSTs.Node v contains the most recent information from each neighbour to update its own BFST. It broadcasts the tree to its neighbours at the end of the period. Formally, v has received the BFSTs from its neighbours. Including those from whom v has received updates in recent previous iterations, node v has a BFST, which is denoted Tu, cached for each neighbouru ∈N(v).

Node v constructs a union graph, i.e.,

$$Gv = Sv \cup \bigcup_{u \in N(v)} (Tu - v) \quad (4)$$

T − x to denote the operation of removing the subtree of T rooted at node x. As special cases, T − x = T if x is not in T, and T − x = ∅if x is the root of T. Then, node v calculate a BFST of Gv, which is denoted Tv, and places Tvin a routing packet to broadcast to its neighbours. Tvis modified every time when a new tree is received from a neighbour. This does not increase the communication overhead at all because one routing message is always sent per update interval.

ii. Neighborhood Trimming

When a neighbour is deemed lost, its contribution to the network connectivity should be removed, this process is called neighbour trimming. Consider node v.

The neighbour trimming procedure is triggered at v about neighbour u either by the following cases:

- No routing update or data packet has been received from this neighbor for a given period of time.
- A data transmission to node u has failed, as reported by the link layer.

Node v responds by:

- First, updating N(v) with N(v) − {u};
- Then, constructing the union graph with the information of u removed, i.e.,

$$Gv = Sv \cup \bigcup_{w \in N(v)} (Tw - v) \qquad (5)$$

- Finally, computing BFST Tv.

Tvis not broadcast immediately to avoid excessive messaging. With this updated BFST at v, it is able to avoid sending data packets via lost neighbours.

Therefore, multiple neighbour trimming procedures may be triggered within one period.

iii. Compact Tree Representation

The compact tree representation in full-dump and differential update messages to divide the size of the messages. To broadcast the BFST information stored at a node to its neighbours in a short packet. Convert the general rooted tree into a binary tree of the same size, e.g., s nodes, using left-child sibling representation.

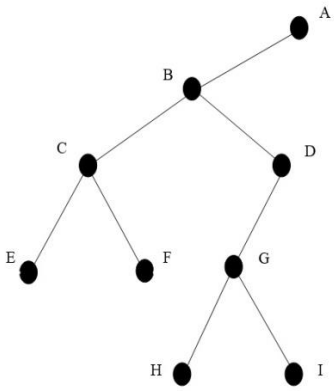

Figure 2 : Compact tree representation

The binary tree is represented as A10B11C11D10E00F00G11H00I00 for the nodes mentioned in Figure 2.

The binary tree using a bit sequence of 34 × s bits, assuming that IPv4 is used. Scan the binary tree layer by layer. When processing a node, it include the IP address in the sequence. In addition, we append two more bits to indicate the left and/or right child.

The size of the update message is a bit over half compared with the traditionalapproach, the message contains a discrete set of edges.The difference between two BFSTs can be represented by the set of nodes that have changed parents, which areessentially a set of edges connecting to the new parents. By observe that these edges are often clustered in groups. Similar to the case of full dump, rather than using a set of loose edges, we use a tree to package the edges connected to each other. As a result, a differential update message usually contains a few small trees, and its size is shorter.

F. Proposed Methodology

i. Black Hole Attack

A black hole attack is a type of denial of service attack accomplished by dropping packets. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocols based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node;hence a malicious and forged route is created. When this route is established, now the attacker node may drop all the packets or forward it to the unknown address. To succeed in the black hole attack, the attacker must generate its RREP with destination sequence number greater than the destination sequence number of the destination node. It is possible for the attacker to find out destination sequence number of the destination node from the RREQ packet. In general, the attacker can set the value of its RREP's destination sequence number based on the received RREQ's destination sequence number.

- Malicious node iadvertise itself for having theshortest path to the destination noded
- Route is established from source node s to destination node d through malicious node i
- The attacker nodei drop all the packets

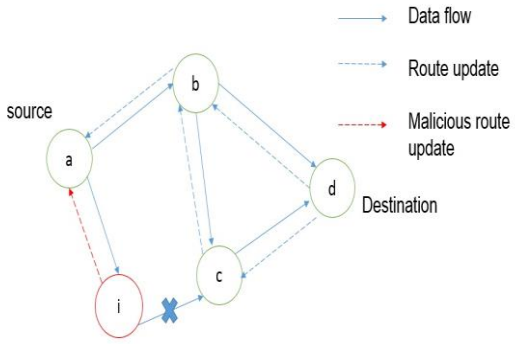

Figure 3 : black whole attack

Algorithm For Blackhole Attack

Agent Definition

- Node id = index (variable)
- If index = malicious
- Get the destination seq no from neighbours
- Seq no = Destination seq no++
- If (seq no % 2) - (for storing even numbers in the table to avoid the loops in routing)
- seq no ++

Malicious Node Send The Reply To Source Node

- Malicious node id
- Source node id
- Hop count to the destination = 1 (fixed)
- seq no (it is greater than existing)

ii. Defense Against Attack (DAA)

To resist the black hole attack, we propose a defence mechanism which could be potentially exploited by malicious nodes. A Neighbourhood Route Monitoring Table (NRMT) is maintained by each node in the network. The NRMT maintains packet routing information of its neighbour nodes. It contains the source ID, destination ID, source sequence number, destination sequence number, and a threshold value of sequence number which is dynamically updated, the time at which RREQ packet enters the node (RREQ-IN-TIME), the time at which RREQ packet leaves the node (RREQOUT-TIME), the time at which RREP packet enters the node (RREP-IN-TIME) and the time at which RREP packet leaves the node (RREP-OUT-TIME). If the node is the normal node, once it receives the RREQ packet, it checks its routing table to identify whether it is the destination or not. According to TDSR protocol, if it is the destination node, it will send the RREP packet to the source node through its route or it will forward the RREQ to its one hop neighbour. Checking the routing information from the table requires a minimum time period known as MINTIME. If the node is the black hole node, it will send a RREP message without checking the table. The NRMT maintains the record of the time of Reply. The first step of the detection process is based on the timing information of NRMT. Every node in the network when it receives the RREP from its neighbour, finds DIFF-TIME which is the difference between the RREQ-OUT-TIME and RREP-IN-TIME and compares this with INTIME. If the RREP is from the black hole node DIFF-TIME will be less than the MIN-TIME. Thenode is identified as a suspicious node. It is well known that the black hole node assigns a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. As the second step of detection mechanism, RREPs sequence number is compared with the threshold value of sequence number. In this protocol, the threshold value is dynamically updated at every time interval. If the current sequence number is greater than the threshold value the node is confirmed as black hole and it is eliminated fromthe routing table. Once a node is detected to be really malicious, the scheme has a notification mechanism for sending messages to all the nodes that are not yet suspected to be malicious, so that the malicious node can be isolated and not allowed to use any network resources.

III. RESULTS AND DISCUSSION

A. Recommendation of Simulation Environment

The simulation environment is given in the following Table 1. It describes the various parameters used for the simulation. The required simulation tool is Network simulator 2 (NS 2).

Table 1 Simulation Parameters and Values.

PARAMETERS	VALUES
Channel	Wireless channel
Radio Propagation	Two-ray ground
MAC protocol	IEEE 802.11
Routing Protocols	DSR, DSDV, TDSR
No. of Nodes	25, 35, 45
Transmission Range	250
Region	1000x1500 m^2
Movement	Random direction with 30m/s
Data rate	1 Mb/s
Bandwidth	11 Mb/s
Traffic type	FTP
Agent	TCP

In modelling node mobility of the simulated MANETs, the random waypoint model to generate node trajectories. In this model, each node moves toward a series of target positions. The rate of velocity for each move is uniformly selected from [0, vmax]. Once it has reached a target position, it may pause for a specific amount of time before moving toward the next position. This mobility model may eventually lead to an uneven node distribution in the network. That is, the nodes' density in the central area of the network may be higher than that at the network boundary. This uneven node distribution coincides with the real case in our daily life. However, at the beginning of simulations, the nodes' positions are evenly assigned; therefore, the simulation data in the first 30 s, and only the data at a steady state is collected. All networks have 25, 35, 45 nodes in our tests. Two series of scenarios based on the mobility model. The first series of scenarios have a fixed vmax but different network densities by varying the network dimensions. The second series have the same network density but varying vmax.

B. Results - Performance Evaluation

1. Packet Delivery Ratio

In the Figure 4, Packet Delivery Ratio is increased in TDSR protocol with Defence against Attack (DAA*)* when it is compared with TDSR with black hole attack.

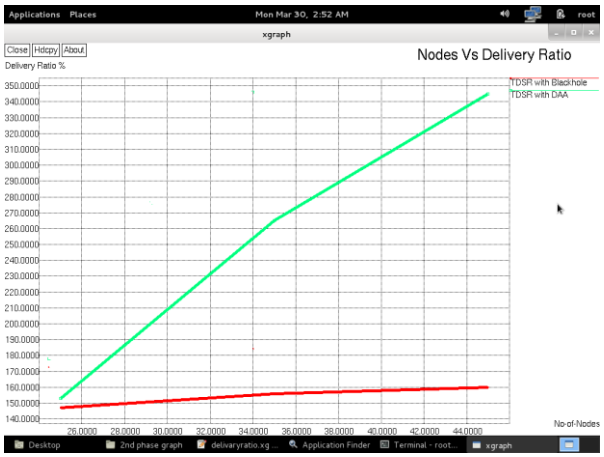

Figure 4. Nodes Vs Packet Delivery Ratio

2. End – to – End Delay

In the Figure 5, End – to End Delay is increased in TDSR protocol with Defence against Attack (DAA*)* when it is compared with TDSR with black hole attack.

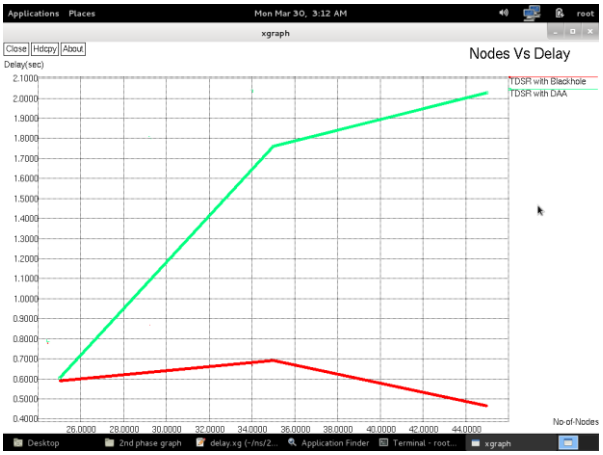

Figure 5: Nodes Vs Delay

IV. REFERENCES

[1] Behrens. J and Garcia-Luna-Aceves J. J, (1994), 'Distributed, scalable routing based on link-state vectors', ACM Conference. SIGCOMM, pp. 136–147.

[2] Biswas. S and Morris. R, (2005), 'ExOR: Opportunistic multi-hop routing for wireless networks', ACM Conference. SIGCOMM, Philadelphia, PA, USA, pp. 133–144.

[3] Chlamtac. I, Conti. M and Liu J.-N, (2003), 'Mobile ad hoc networking: Imperatives and challenges', Ad Hoc Networks., Vol. 1, no. 1, pp. 13–64.

[4] Clausen. T and Jacquet. P, (2003) 'Optimized Link State Routing Protocol (OLSR)', RFC 3626.

[5] Johnson. D. B and Maltz. D. A, (2007), 'On The Dynamic Source Routing Protocol (DSR) for mobile ad hoc networks for IPv4', RFC 4728.

[6] Murthy. S, (1996), 'Routing in packet-switched networks using path-finding algorithms', Ph.D. dissertation, Computer Engineering., University of California, USA.

[7] Murthy. S. and Garcia-Luna-Aceves. J. J, (1996), 'An efficient routing protocol for wireless networks', Mobile Networks Application., Vol. 1, no. 2, pp. 183–197.

[8] Perkins. C. E and Bhagwat. P, (1994), 'Highly dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for mobile computers', Computer Communication., Vol. 24, pp. 234–244.

[9] Perkins. C. E and Royer E. M, (2003), 'Ad hoc On-Demand Distance Vector (AODV) routing', RFC 3561.

[10] Rajaraman. R, (2002), 'Topology control and routing in ad hoc networks: A survey', ACM SIGACT News, Vol. 33, no. 2, pp. 60–73.

[11] West. D, (2000), 'Introduction to Graph Theory', 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall.

[12] Zehua Wang,Yuanzhu Chen, and Cheng Li, (2014), 'PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks', IEEE Transactions On Vehicular Technology., Vol. 63, no. 2, pp. 859 – 868.

[13] ArunmozhiAnnamalai, VenkataramaniYegnanarayanan, September 2012,'Secured System against DDoS Attack in

Mobile Adhoc Network' Issue 9, Volume 11E-ISSN: 2224-2864.

[14] M .Nasir Iqbal, JunaidA.Khan, (2013), 'Security Enhancement of Pro-active Protocols in Mobile Ad-hoc Networks', J. Basic. Appl. Sci. Res., 3(3)101-107.

V. AUTHOR PROFILE

R.Deenadhayalan obtained his Bachelor's degree in Computer Science from "Maharaja Engineering College-Avinashi" under Anna University and Master Degree in Computer Science and Engineering from "Anna University". He has 5 years of teaching experience and 2 years of industry Experience.Currently he is working as an Assistant Professor in the department of Information Technology in Kongu Engineering College, Perundurai. He is a life member of IAENG, andCSI. He has Published many papers in International and National Journals and National Conferences. His area of interest includes Sensor Networks and Internet of Thing(IoT) and Internet Programming.He has attended Seminars, FDP's, and Workshops organized by various Engineering colleges.

Dr. S.ANANDAMURUGAN obtained his Bachelor's degree in Electrical and Electronics Engineering from "Maharaja Engineering College - Avinashi" under Bharathiyar University and Masters Degree in Computer Science and Engineering from "ArulmiguKalasalingam College of Engineering – Krishnan Koil" under Madurai Kamaraj University. He completed his Ph.D in Wireless Sensor 0Networks from Anna University, Chennai. He has 13 years of teaching experience. Currently he is working as an Assistant Professor (Selection Grade) in the department of Information Technology in Kongu Engineering College, Perundurai. He is a life member of ISTE, CSI& ACEEE. He has received "**Best Staff"** award for the year 2007-08. He has authored more than 70 books. He has Published 20 papers in International and National Journals and 10 Papers in International and National Conferences. His area of interest includes Sensor Networks and Green Computing. He is an Editorial Board Member of the International Journal of Computing Academic Research (IJCAR). He has organized 1CSIR sponsored seminar for the benefit of faculty members and students. He has attended about 40 Seminars, FDP's, and Workshops organized by various Engineering colleges.