IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791(Impact Factor: 1.479)
www.ijreat.org

An Efficient Location Based Anonymous Routing Protocol For ADHOC Networks

J.Kirubhakaran[1], Dr.G.K.D.PrasannaVenkatesan[2], R.Muthusuganya[3]
Assistant Professor[1], Vice Principal, Professor and Head[2] ,Post Graduate student- ME in Communication Systems[3]
Department of E.C.E., PGP College of Engineering and technology, Namakkal, Tamilnadu,India

***Abstract*—Mobile ad hoc networks (MANETs) are infrastructure-less networks used in areas where rapid network configuration is needed, such as communication in a battle field. The lack of a trusted centralized authority, limited resources and the broadcast nature of wireless links make these networks susceptible to security threats. The existing routing protocol for anonymity needs hop-by-hop encryption or redundant traffic at high cost and there is no full anonymity protection to data source, destination and routes. To give high anonymity protection, we propose an Anonymous Location-based and Efficient Routing proTocol (ALERT). In this, with the help of GPSR algorithm the network field is dynamically partition into many zones and the nodes are choosen randomly as intermediate relay nodes. It forms a non-traceable anonymous route. It prevents timing attacks and intersection attacks. This approach provides nodes the advantage of having a broader view of the quality of other node by received signal strength. This prevents Sybil attacks. It also improves the use of hidden servers.**

***Keywords*- zone partition, encryption, anonymity, hidden server, signal strength**

I. INTRODUCTION

A mobile adhoc networks is a collection of mobile users that communicate through a bandwidth constrained wireless links. It forms continuously without a need for an infrastructure or centralized controller, since the nodes are mobile. It is a decentralized network, in which all network activities including finding the topology and delivering messages should be done by the nodes. The routing functionality is included into mobile nodes. The applications for mobile adhoc networks is diverse, ranging from small to large scale, static networks that are constrained by power sources, mobile, highly dynamic networks. However, MANET also need a efficient distributed algorithms to determine the organization of the network, link scheduling, and routing.

However, in determining the paths for the networks and delivering messages in an adhoc environment, in which the fluctuations in network topology is not a problem. The shortest path which was based on cost function from source to a destination in static network is always an optimal route; this idea is not easily extended to MANETs. Some factors become relevant issues such as variable wireless link quality, fading, propagation path loss, multiuser interference, power expended and topological changes. The network must be able to alter the routing paths adaptively to control any these effects. Military environment needs a preservation of intentional jamming, security, latency, reliability, and recovery from failure are significant concerns. Minimum configuration and rapid deployment makes ad hoc networks suitable for emergency situations like military conflicts, natural disasters, human disasters, induced, emergency medical situations etc. Due to this, nodes mostly prefer to radiate as little power as needed and transmit as infrequently as possible. This will decrease the probability of interception or detection. Any disturbance in these requirements may degrade the dependability and performance of the network.

A MANET is a self-maintained, self-forming, and self-healing which gives network flexibility of mobile devices connected by wireless. Ad hoc is Latin and means “for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. The goals of passive attacks is to collect network information such as traffic flows , node identities, network topology, node locations etc., The process repeats until it traces, locates, and then physically destroys the malicious node. Many security protocols are proposed to protect wireless communications, but they do not consider anonymity protection and leave identity information freely available to nearby passive eavesdroppers. The passive enemy will avoid aggressive actions as performed in routing security attacks, such as route disruption or “denial-of-service” attacks, in order to keep themselves to be as “invisible”.

Many anonymous routing schemes have been proposed for MANET recently. Most of them use the on-demand routing approach following the MANET on-demand routing paradigm. The operations of an on-demand protocol are triggered by the communication demand at sources. Typically, an on demand routing protocol has two components: route discovery and route maintenance. The proposed anonymous on-demand routing protocols use various cryptographic operations to anonymize both the transmission events and stored data. However, for battery and CPU power limited mobile devices, how the incurred cryptographic operation

overhead affects the performance in general is an important issue that needs to be studied to gain a better understanding on the protocol design and applicability.

Each MANET node is anonymous that is it occurrences at different locations cannot be linked. More generally, we anticipate that the MANET type considered in this paper would be encountered in a law enforcement disaster recovery or military environment. Such critical settings have some characteristics in common. First, node location is very important –knowledge of the physical (as opposed to logical or relative) topology makes it possible to avoid wasteful communication and to focus on areas (nodes) that are positioned within, or at, a specific area. (Thus, the emphasis is not on the long-term node identity but rather on current node location.) Second, critical environments are susceptible to security and privacy attack. Attacks on security aim to distribute false routing information or impede propagation of genuine routing information. Whereas, attacks on privacy aim to track nodes as they move.

I. ANONYMOUS ROUTING PROTOCOLS IN MANET

In existing systems, MANET has two types of methods for anonymity routing

1. Hop-by-hop encryption and 2.Redundant traffic.

A. HOP BY HOP ENCRYPTION

In this each node has to decrypt each received message, then correspondingly aggregate the message according to the aggregation function and, finally, encrypt the aggregation result before forwarding it. The nodes in between the transmitter and receiver are known as intermediate nodes. The function of the hop is to transmit the packets from one hop to other hop is known as single hop transmission. In multi hop transmission the packets are transmitted through two hops, which means that two intermediate nodes in between the transmitter and receivers. The encryption and the decryption process will takes place in the transmitter and in the receiver section respectively.

B. REDUNDANT TRAFFIC

The AO2P (Ad hoc On demand Position based and Private routing) and ALARM (Anonymous Location Aided Routing in MANETs) take the shortest path in routing. The latency of AO2P is a little higher than ALARM because AO2P has a contention phase and may generate a slightly longer path length. In ALARM and AO2P, the latency caused by the public key cryptography outweighs the benefit of short latency using the shortest path. Therefore, even though ALERT generates more routing hops than AO2P and ALARM, the latency of ALERT is still significantly lower than ALARM and AO2P. Our existing concept requires the high cost to protect the data in the network. The source and destination nodes information's are not hiding in this concept. For provide this security is consumes the high cost and also it does not provide the full anonymity to the nodes.

The public key encryption and the high traffic require the high cost to protect the data. The ALARM concept does not provide the location based anonymity for source and destination nodes and also the routes which means the path used for the packet transmission between the source and destination nodes. Ariande.A Secure On demand Routing Protocol for Ad hoc Network it is a new secure on-demand ad hoc network routing protocol .Ariadne prevents attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents many types of Denial-of-Service attacks. In addition, Ariadne is efficient, using only highly efficient symmetric cryptographic primitives. Itprovides only route anonymity.

The main limitation of this hop by hop encryption and redundant traffic stated as follows: Most of the existing approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high cost.

II. EFFICIENT GREEDY PERIMETER STATELESS ROUTING (PROPOSED SYSTEM)

In proposed system EGPSR algorithm is used. It is very efficient to provide the alert routing for the networks. In this work, the attackers may be battery powered nodes that receive network packets passively. According to the analytical results from their hacked packets they can also inject packets to the network. ALERT is also prevents intersection attacks, Sybil attacks and timing attacks.. ALERT gives anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/ receivers. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. It can also achieve comparable routing efficiency to the base-line GPSR algorithm.

This ALERT concept uses the EGPSR algorithm to find the closet node in the network. For transmitting a packet in the network first we have to find the closet nodes which mean that source node, destination node and then the forwarded node. With the help of the forwarded node we send the packet to the destination in secure manner. After that we start the packet transmission. The timing and intersection attack can be identified and controlled in our proposed concept.

In our proposed concept use the EGPSR routing algorithm to find the best path in our network. The node between the source and destination is known as a relay node. The relay node is the forwarding node that forwards the original packet to the destination node and then transmits the dummy packets to the remaining nodes in the network. The principle for this

routing depends on the information about the geographic position . Greedy forwarding helps to bring the message nearer to the destination in each step using only local information.

RREQ/ RREP/ NAK		P_S	P_D	L_{ZS}	L_{ZD}	L_{RF}
H	H	K^S_{pub}	$(TTL)_K^{KN}$ pub	$(Bitmap)_K^D$ pub		Data (NULL in NAK)

Fig1. Packet format of ALERT

This algorithm finds the best path in the network using the energy of the node.

Where,
RREQ is route request.
RREP is route reply.
NAK is negative acknowledgement.
h is number of zone so far.
H is maximum number of zones.
TTL is Time To Live.
Ps is Pseudonym of a source.
Pd is Pseudonym of a destination.
Lzs and Lzd are the positions of the H^{th} partitioned source zone and destination zone. Bitmap is used to avoid collision.

The algorithm consists of two methods for forwarding packets. Greedy forwarding, which is used wherever possible, and perimeter forwarding, which is used in the regions greedy forwarding cannot be done.

Under GPSR, packets are marked by their originator with their destinations' locations.As a result, a forwarding node can make a locally optimal, greedy choice in choosing a packet's next hop.Specifically, if a node knows its radio neighbors' positions, the locally optimal choice of next hop is the neighbor geographically closest to the packet's destination.Forwarding in this regime follows successively closer geographic hops, until the destination is reached.

A. GREEDY FORWARDİNG

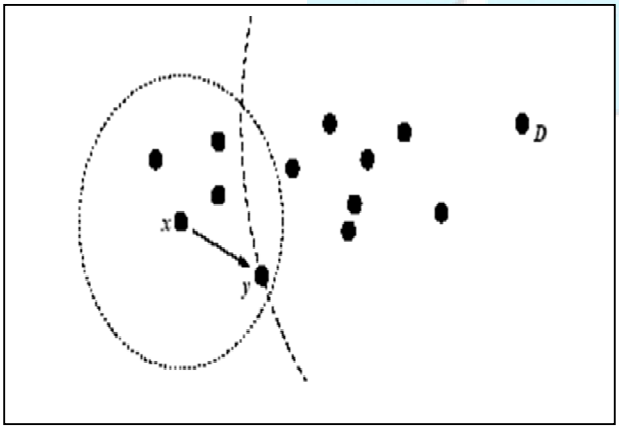

Fig 2.Greedy forwarding example .Y is X's closest neighbour to D.

Greedy forwarding's great advantage is its reliance only on knowledge of the forwarding node's immediate neighbors. The state required is negligible, and dependent on the density of nodes in the wireless network, not the total number of destinations in the network.The power of greedy forwarding to route using only neighbor nodes' positions comes with one attendant drawback. There are topologies in which the only route to a destination requires a packet move temporarily farther in geometric distance from the destination.

B. PERIMETER FORWADING:

Maping perimeters by sending packets on tours of them, using the right-hand rule. The state accumulated in these packets is cached by nodes, which recover from local maxima in greedy forwarding by routing to a node on a cached perimeter closer to the destination.This approach requires a heuristic, the no-crossing heuristic, to force the right-hand rule to find perimeters that enclose voids in regions where edges of the graph cross.

While the no-crossing heuristic empirically finds the vast majority of routes in randomly generated networks, it is unacceptable for a routing algorithm persistently to fail to find a route to a reachable node in a static, unchanging network topology.

GPSR keeps state proportional to the number of its neighbors, while both traffic sources and intermediate DSR routers cache state proportional to the product of the number of routes learned and route length in hops.GPSR's benefits all stem from geographic routing's use of only immediate-neighbor information in forwarding decisions.

The Relative Neighbourhood Graph *(RNG)* and Gabriel Graph *(GG)* are two planar graphs. An algorithm for removing edges from the graph that are not part of the RNG or GG would yield a network with no crossing links. Forour application, the algorithm should be run in a distributed fashionby each node in the network.

Multihop operation requires a routing mechanism designed for mobile nodes. It's an Internet access mechanism. The Self configuring networks require an address allocation mechanism. Mechanism to detect and act on, merging of existing networks Security mechanisms .Geographic routing (also known as position-based routing or geometric routing) is a technique to deliver a message to a node in a network over multiple hops by means of position information. Routing decisions are not based on network addresses and routing tables; instead, messages are routed towards a destination location. With knowledge of the neighbors' location, each node can select the next hop neighbor that is closer to the destination, and thus advance towards the destination in each step. The fact that neither routing tables nor route discovery activities are necessary makes geographic routing attractive for dynamic networks such as wireless ad hoc and sensor network. In such networks, acquiring and maintaining routing

information is costly as it involves additional message transmissions that require energy and bandwidth and frequent updates in mobile and dynamic scenarios. In contrast there are geographic routing algorithms that work nearly stateless and can provide high message delivery rates under mobility. The main prerequisite to meet the three assumptions is a positioning system. If this is available, geographic routing provides an efficient and scalable solution for routing in wireless and mobile networks. However, a simple greedy forwarding by minimizing the distance to the destination location in each step cannot guarantee message delivery.

Nodes usually have a limited transmission range and thus there are situations where no neighbor is closer to the destination than the node currently holding the message. Greedy algorithms cannot resolve such dead-end or local minimum situation. Therefore, recovery methods have been developed, the most prominent of which are based on planar graph routing, where the message is guided around the local minimum by traversing the edges of a planar sub graph of the network communication graph. Planar graph routing techniques can provide delivery guarantees under certain assumptions, complement the efficient greedy forwarding. Altogether, greedy forwarding in combination with a recovery can be considered as state of the route in geographic routing.

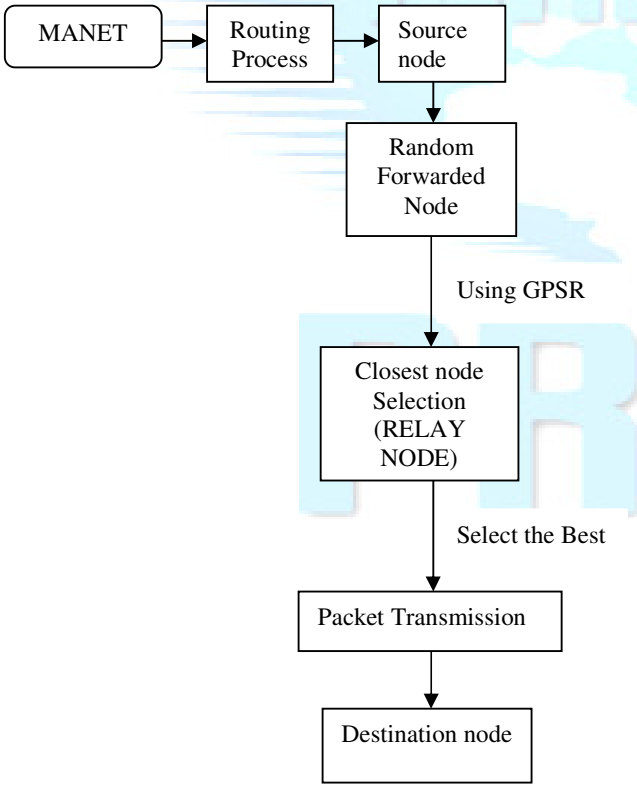

Fig.3. Data Flow diagram

Figure 3. shows the data flow diagram of routing process from source node to the destination node through the random forwarded node using GPSR protocol.

First in MANET the routing process takes place from the source node to the destination node via the intermediate nodes, the main consideration in data transmission is that secure data transmission and data validation. The routing process is takes place from the source node to the designation node through the intermediate random forwarder, the random forwarder uses GPSR protocol to forward the packet or data in secured manner, and chooses the closest path of the routing process by using the protocol. The destination node receives the packet from source to destination in effective way and secured manner.

C. LIGHTWEIGHT SYBIL ATTACK DETECTION IN MANETS

Our approach provides nodes the advantage of having a broader view of the quality of other nodes by using **Opinion Method**.Using this method, a node can be detect whether its malicious or not only by received signal strength.

A legitimate/malicious node must sent a opinion to the neighbor nodes to confirm whether that node is malicious node or not with the neighbor node acknowledgement.
And also the other sector, the transcations in the network should be monitor for a particular time interval. By monitoring the normal transcations using the **Accusation** also can avoid problems form the Sybil attackers/ others.

III. SIMULATION RESULTS

Simulation model is carried out using Network simulator - 2 and the Protocol GPSR is implemented. In simulation model the main process is node creation, zone partition, Relay node selection and closest path routing. The network animator results shows all those process by using NS-2 simulation software. The mobile nodes are created for the transmission and the reception process, mobile nodes are capable of transmit and receive the packets.

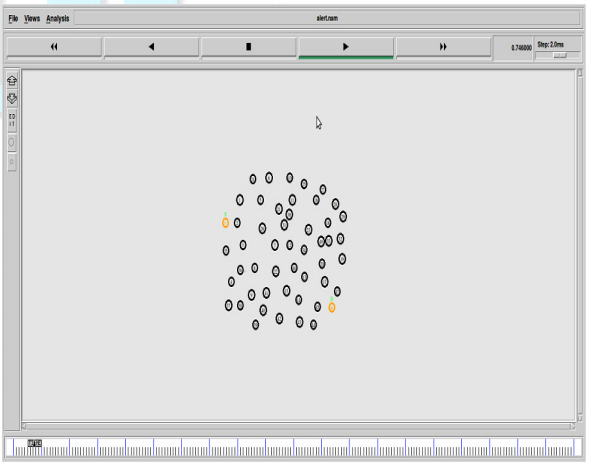

Fig.4. NAM output showing Routing Process

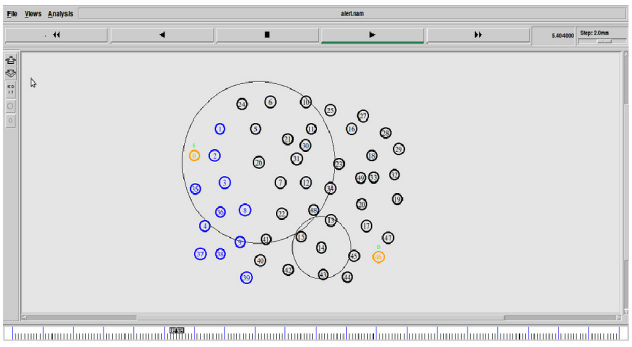

Fig.5 NAM output showing Zone Partition

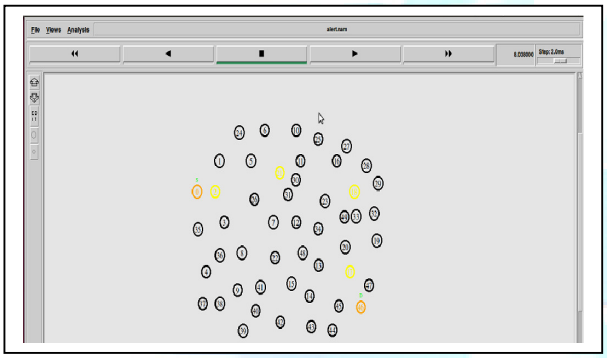

Fig 6.NAM output showing Relay node selection.

Fig.4 shows that routing process in mobile ad hoc network. Several nodes are created for routing, one node is assigned as source and some other node is created as a sink. In between nodes are used to transfer the packet or root the packet form source to the sink node.

Fig 5.Shows that zone partition one group of nodes and other group nodes are separated as zone for easy transmission.

Fig 6. Shows that Relay node selection, this relay nodes are used to forward the packets form source to the designation this relay node act as a forwarder.

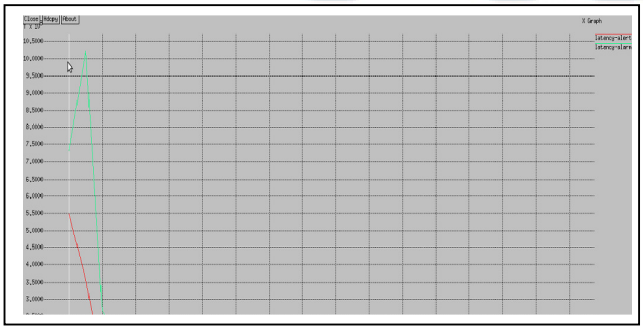

Fig.7. Xgraph compare the latency(time delay) between the ALERT and ALARM. Time delay in ALARM is higher than ALERT routing algorithm.

This Xgraph Fig.7.compares the delay time for ALERT and ALARM. This graph shows that the time delay for ALERT is reduced compared to the ALARM scheme.

IV. CONCLUSION

In mobile ad hoc networks the data's or packets are transferred between the source and destination nodes. In order to provide security and then overcome the problems presented in existing system, we introduce new concept called ALERT (An Anonymous Location based Efficient Routing Protocol). In our proposed concept first selects the node for packet transmission. This means, we select the source node, destination node and forwarded node. After that we select the random forwarded node for packet transmission. In order to provide the security we introduce the GPRS routing protocol to find the best path in our network for packet transmission.The GPSR select the relay for packet transmission. The source first send the data to the random forwarded node, that node sends the packet to the relay in destination zone. This relay node sends the original packet to the destination node and sends the dummy node to the remaining node in the network. This process is continuous until the packet receives the destination node. Finally we construct a graph from the received data and then compared with the theoretical values. This system provides the efficiency and requires low cost for hide the initiator/ receiver identities.

REFERENCES

[1]. A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, "Anonymity,Unlinkability,Unobservability,Pseudonymity , and Identity Managementa Consolidated Proposal for Terminology, Version 0.31,"technical report, 2005.

[2]. Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "AnAnonymous On-Demand Position-Based Routing in MobileAd Hoc Networks," Proc. Int'l Symp. Applications on Internet(SAINT), 2006.

[3]. Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad HocRouting for Preserving Location Privacy," Proc. Third Int'l WorkshopMobile Distributed Computing (ICDCSW), 2005.

[4]. Pathak, D. Yao, and L. Iftode, "Securing Location AwareServices over VANET Using Geographical Secure Path Routing,"Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.

[5]. K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf.Network Protocols (ICNP), 2007.

[6]. K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routingin Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf.Network Protocols (ICNP), 2008.

[7]. Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure OnDemandRouting Protocol for Ad Hoc Networks," WirelessNetworks, vol. 11, pp. 21-38, 2005.

[8]. I.Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for StrongAnonymity in Ad Hoc Networks," Proc. Securecomm and Workshops,2006.

[9]. C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An EfficientAnonymous Communication Protocol for Peer-to-Peer Applicationsover Mobile Ad-Hoc Networks," IEEE J. Selected Areas inComm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[10]. X. Wu, "AO2P: Ad Hoc On-Demand Position-Based PrivateRouting Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4,pp. 335-348, July/Aug. 2005.

[11]. B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng,"Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc.IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN), 2004.

[12]. A.R. Beresford and F. Stajano, "Mix Zones: User Privacy inLocation-Aware Services," Proc. IEEE Second Ann. Conf. PervasiveComputing and Comm. Workshops (PERCOMW), 2004.

AUTHORS PROFILE

1) J. Kirubakaran, Assistant Professor / Electronics and communication and Engineering Department at PGP College of Engineering and Technology, Namakkal, Tamilnadu, India. Presently Research Scholar in Anna University, Chennai, India.

2) Dr.G.K.D.Prasanna Venkatesan, Completed Ph.D from College of Engineering, Anna University, Chennai, India. He is Currently Working as Vice-Principal, Professor & Head of Department of Electronics and Communication Engineering at PGP College of Engineering and Technology. Namakkal, Tamil nadu, India. His research interests includes Wireless Sensor Networks, 4G Wireless Networks, Cloud Computing, Adhoc Network, etc.,

3) R.Muthusuganya, Post Graduate student- ME in Communication Systems at PGP College of Engineering and Technology, Namakkal.