E STAR for Secure and Reliable Data Transmission in Heterogeneous Multi hop Wireless Networks

[1]Swathy Satheesh, [2] T Chandhini
[1] Final Year Student, ME Communication Systems, [2.]Assistant Professor
EASA College of Engineering & Technology, Navakkarai-641115

***Abstract* – In the proposed system, E STAR integrates the payment and trust systems with the routing protocol with the goal of enhancing the route reliability and stability. The trust system determines the nodes competence and reliability of the nodes in terms of multi-dimensional trust values. The trust values are attached to the nodes public key certificates to be used in making routing decisions. To strengthen the trust evaluation, recommendation from each node is included in trust calculation by Trusted Party. E STAR can secure trust system without any false accusations. While observing the simulation results, routes stability and packet deliver ratio improved.**

Index Terms – Heterogeneous multi hop wireless networks, Establishing Stable and Reliable Routing Protocol, Payment system, trust system, and secure routing protocols.

I. INTRODUCTION

The multi hop wireless network implemented in many useful applications such as data sharing and multimedia data transmission. When a mobile node needs to communicate with the remote destination, it relies on the other nodes to relay the packets. The nodes' behavior is unpredictable in some civilian applications for many reasons. Because of the uncertainty in the nodes' behavior, the intermediate nodes will degrade the routes stability. This proposed system overcomes the drawbacks by the techniques, trust and payment system.

Shortest Reliable Route and Best Available Route are the two trust-based and energy-aware routing protocols.
When the selfish node takes advantage from the cooperative nodes without contributing to them, the cooperative nodes are unfairly overloaded.

The payment system uses credits to charge the nodes which send the packets and reward those relaying packets. The trust system is essential to assess the nodes' trustworthiness and reliability in relaying packets. A node's trust value is the degree of belief about the node's behavior. The trust value is calculated from the nodes' past behaviors and is used to predict their future behavior.

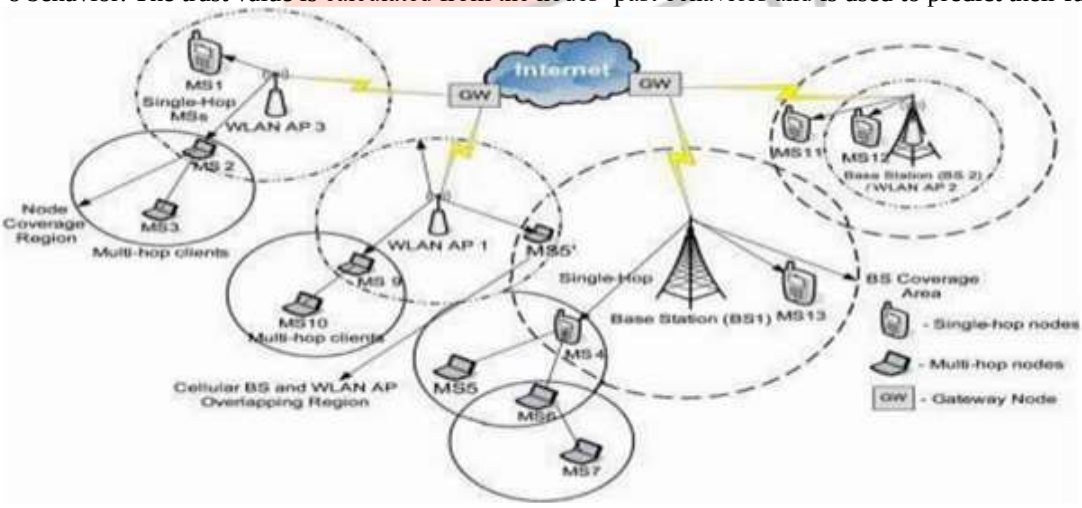

Figure 1: Multi hop Wireless Network Architecture

The main contributions of this paper are:

i) Trust based and energy aware routing protocols to establish stable routes.
ii) E STAR stimulates the nodes to relay others packets even if they have many credits and to stabilize the routes and report the energy capability truthfully to increase their chance to participate in future routes.
iii) E STAR integrates the payment system and the trust systems with the routing protocol with a goal of enhancing the route reliability and the stability.

E STAR aims to identify the good nodes and select them in routing.

II. RELATED WORKS

Reputation-based schemes attempt to identify the malicious nodes that drops the packets with a rate more than a predefined threshold for avoiding them in routing. But it suffers from false accusations, some honest nodes are falsely identified as malicious because the nodes that drop packets temporarily. In order to reduce the false accusations, some tolerant thresholds should be used to guarantee that a node's packet dropping rate can reach the threshold if the node is malicious and this increases the missed detections where some malicious nodes are not identified.
Also, they are not much effective in detecting the grayhole attackers that drop a portion of the packets. Therefore, these schemes are not guaranteeing route stability or reliability in HMWNs.

Payment or incentive schemes use credits to encourage the nodes to relay others' packets. It uses a communication protocol which can transfer messages from the source node to the destination node with limited use of the public key cryptography operations. It is used for only one packet and for next packets, efficient hashing operations are used It is used to prevent the rational packet-dropping attacks. The attackers drop packets because they do not benefit from relaying packets.

The main goal of trust system is to enable the nodes to indirectly build trust relationships using exclusively monitored information. The routing metrics are obtained by combining the requirements on the trustworthiness of the nodes and the quality of service of the links.

While comparing, different from reputation-based schemes that aim to identify the malicious nodes, E-STAR does not suffer from false accusations. It aims to identify the competent nodes in packet relaying and select them in routing. The node will not participate in routing without the need for determining good thresholds. However, E-STAR can evaluate the nodes' trust values more accurately because it can monitor the nodes' behavior. The payment schemes alone are not sufficient for establishing the stable routes. It requires selecting the nodes that behaved well in the past and have sufficient energy.

III. PROPOSED METHOD

The heterogeneous multi hop wireless network HMWN has mobile nodes and offline trusted party whose public key is known to all the nodes. The nodes have different hardware and energy capabilities. With every interaction, there is an expectation of the future reaction. Each and every node has a unique identity and public/private key pair with a limited-time certificate issued by the trusted party. Without any valid certificate, the node cannot communicate nor act as an intermediate node. The trusted party maintains the credit accounts and trust values of the nodes. Each node contacts TP to submit the payment receipts and then TP updates the involved nodes' payment accounts and trust values. This contact can occur via cellular networks or Internet.

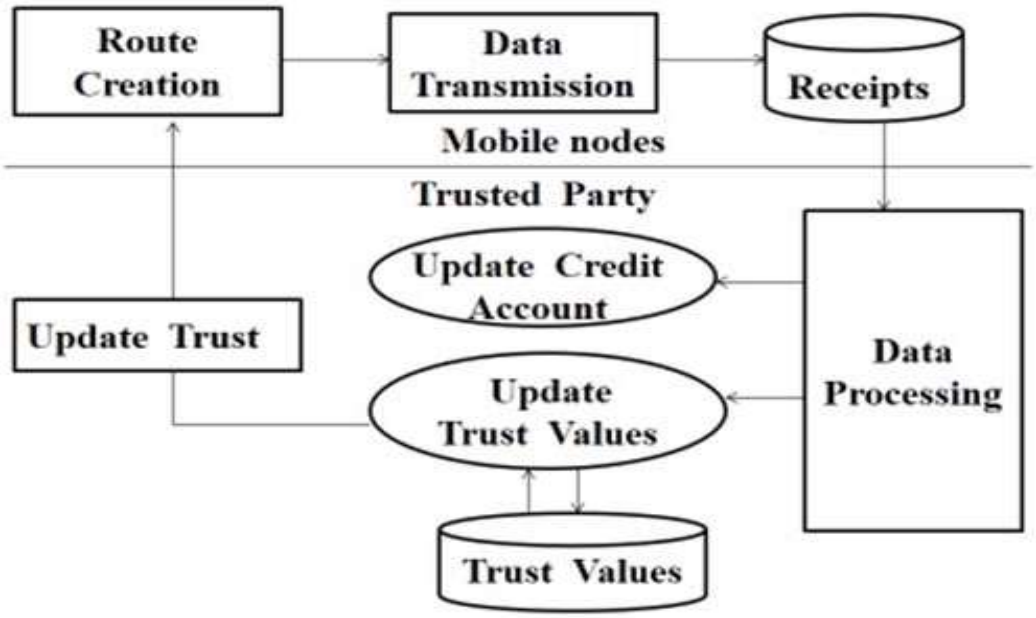

Figure 2: E STAR in multi hop wireless network.

The figure shows the E-STAR architecture and it has three main phases. In wireless network data transmission is from source to destination and each node has a unique identity and report to the trusted party. The trusted party will evaluate a trust value for each node based on their nodes past behavior. After updating the trust values the routing establishment process are done by SRR and BAR. Whereas SRR will find one shortest and reliable path and it avoids the low trusted nodes. BAR will find out and select the most reliable one.

DATA TRANSMISSION PHASE

The messages are sent from source mode to the destination node through a route with the intermediate nodes. The route is established by the routing protocols. The purpose of the source node's signature is to ensure the authenticity and integrity of the message. Also, secure the payment by enabling TP to ensure that the source has sent messages. Each node in the route composes a receipt and submits it when the node has a connection to the trusted party to claim the payment and update its trust values. Each

intermediate node verifies the source node signature and stores those signatures with hash message for composing the report. A report is the main proof for participating in a route and sending, forwarding and receiving number of messages.

TRUST VALUE PHASE

Once TP receives a receipt, it first checks whether the receipt has been processed before using its unique identifier. Then, it verifies the credibility of the receipt by computing the nodes' signatures and hashing them. If the report is valid, the trust party verifies the destination node's hash message. The trusted party clears the report by rewarding the intermediate nodes and debits the source and destination nodes. The number of sent messages is signed by the source node and the number of delivered messages has been computed from the number of hashing operations. Trust values are calculated from the past behavior for predicting the expected future behavior. The trust system decreases the trust values of the two nodes in a broken link. The nodes that break routes more frequently are accused more and suffer from more trust degradation.

ROUTE ESTABLISHMENT PHASE

1) SRR Protocol

SRR protocol establishes a shortest route which can satisfies the source nodes requirements is trusted enough to act as a relay. This protocol avoids the low-trusted nodes. The source node embeds its requirements in the RREQ packet, and the nodes which satisfy these requirements broadcast the packet. Each intermediate node ensures that it can satisfy the source node's energy requirements, the current time is within a proper range and the number of intermediate nodes is fewer. The verifications are necessary to ensure that the packet is sent and relayed by legitimate nodes and the nodes satisfy the trust requirements because their trust values are signed by TP.

The intermediate node signs the packet's signature and forms a chain of signatures of the nodes that broadcast the packet. This signature proves that the node is the certificate holder and thus the attached trust values belong to the node. At last, the intermediate node broadcasts the packet after adding the signature chain, identity and its certificate. If a node receives the same request packet from different nodes, it processes only the first packet and discards the subsequent packets.

Route selection includes that if there is a route that can satisfy the source node's requirements, only if the destination nodes receive at least one RREQ packet. The destination node composes the RREP packet for the route traversed by the RREQ packet, and sends it to the source node.

2) BAR Routing Protocol

The Best Available Route (BAR) routing protocol enables the destination node to select the best reliable route in the network. The source node first sends the RREQ packet to the intermediate nodes, and then the intermediate node broadcasts those RREQ packets after attaching its identity and certificate. The intermediate nodes are motivated to report the correct energy commitments to avoid breaking up of route and thus degrading their trust values. The RREQ packet flooding generates few routes, because each node broadcasts the packet once, it cannot find the better routes. So the BAR protocol will allow each node to broadcast the RREQ more than once and the route reliability of the recently received packet is much greater than the last broadcasted packet.

After the first RREQ packet was received, the destination node will wait for a while to receive more RREQ packets if there are. Then, it will select the best available route if a set of feasible routes are found. When there are multiple routes with lifetimes, at least to send messages, the destination node selects the most reliable route, or otherwise, it establishes multiple routes for sending the messages in such a way that reduces the routes and maximizes the reliability. Finally, the destination node composes the RREP packet sends that packets to the route.

IV. PERFORMANCE EVALUATION

The simulation of proposed protocol is performed using Network Simulator (ns-2). To analyze the effectiveness of the proposed protocol it is compared with existing protocol DSR. Performance is analyzed using the following metrics.

A. Packet Delivery Ratio (PDR)

The Packet Delivery Ratio (PER) is the total number of packets received by the destination nodes to the total number of packets sent by a source node. Packet Delivery Ratio of SRR and BAR is higher than that of DSR as they protocol selects the highly trusted nodes and the nodes having sufficient energy to deliver the packets to destination. But DSR protocol randomly selects the intermediate nodes. Therefore it will contains low trust nodes and hence the nodes having low energy deliver the packets to destination.

B. Call Acceptance Ratio

The call acceptance ratio is the ratio of times a route is established after sending a RREQ packet. The Call Acceptance Ratio of SRR and BAR protocol is increased with increase of time. Because in SRR and BAR protocol the data is transferred only through highly trusted nodes and attackers are not involved in this protocol.

C. Route Life Time

The Route Lifetime is the number of packets that sent in one route before it is broken. The normalized route lifetime is the average route lifetime in E STAR compared to that of DSR. It is a good measure for route stability.

The performance of the proposed protocol establishes a much stable route by selecting the reliable intermediate nodes and therefore it delivers packets more successfully comparing to DSR in terms of total number of packets generated, received, forwarded and also packet delivery ratio, call acceptance ratio and route life time.

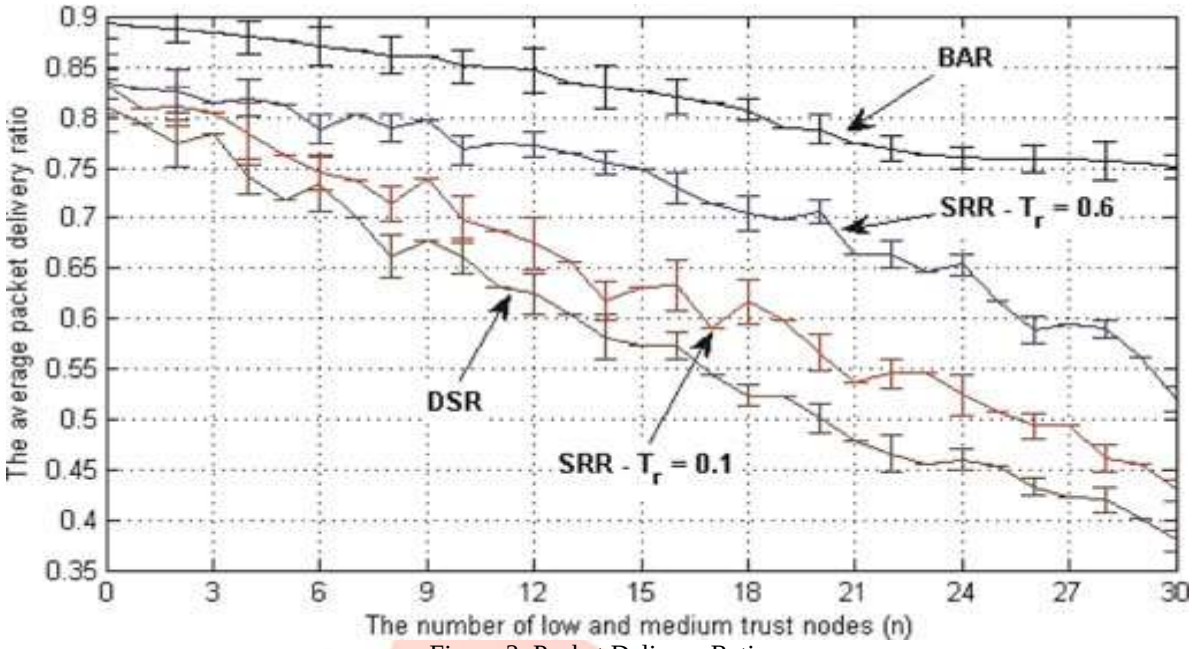

Figure 3: Packet Delivery Ratio

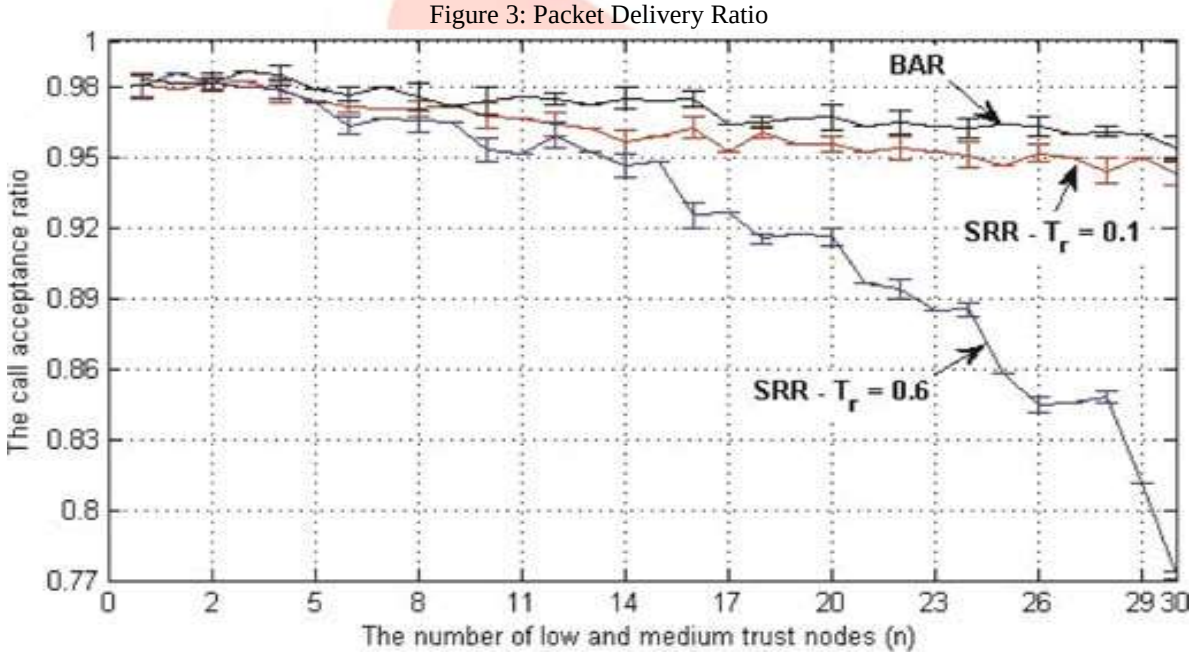

Figure 4: Call Acceptance Ratio

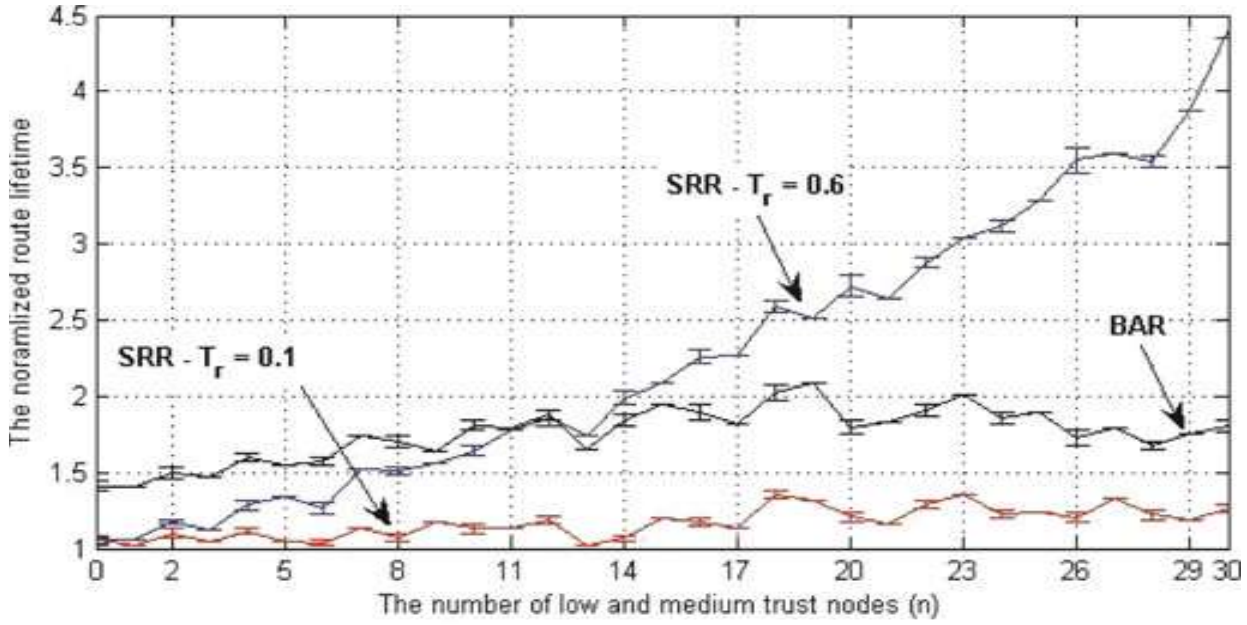

Figure 5: Route Life Time

V. CONCLUSION AND FUTURE WORKS

The proposed E-STAR uses payment and trust systems with trust-based and energy-aware routing protocol to establish stable and reliable routes in wireless networks. E-STAR stimulates the nodes to relay others' packets and also to maintain the route stability. It will punish the nodes that report incorrect energy capability by decreasing their chance of selecting that protocol. The proposed SRR and BAR routing protocols is evaluated the route stability. These protocols can make informed routing decisions by considering many factors, including the route length, the route reliability is based on the nodes' past behavior, and the route lifetime is based on the nodes' energy capability. From the evaluation techniques, the route reliability and packet delivery ratio also improved using this protocol.

REFERENCES

[1] Chou, D. Wei, C. Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, Jan. 2007.
[2] P. Velloso, R. Laufer, D. Cunha, O. Duarte, and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model",IEEE Transactions on Network and Service Management, vol. 7, no. 3, pp.172–185, September 2010.
[3] M. Mahmoud and X. Shen, "ESIP: Secure incentive protocol with limited use Of public-key cryptography for multi-hop wireless networks", IEEE Transactions On Mobile Computing, vol. 10, no. 7, pp. 997-1010, July 2011.
[4] S. Lindsay, Y. Wei, H. Zhu and K. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 305–317, 2006.
[5] K. Liu, J. Deng, and K. Balakrishnan "An acknowledgement-based approach for the detection of routing misbehavior in MANETs", IEEE Transaction on Mobile Computing, vol. 6, no. 5, pp 536–550, May 2007.
[6] Johnson, D. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks", In C. Perkins, editor, Ad Hoc Networking, chapter 5, pp. 139-172. Addison-Wesley, 2001.
[7] J. Yoon, M. Liu, and B. Nobles, "Sound Mobility Models," Proc. ACM MobiCom, Sept. 2003.
[8] A. Jøsang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.
[9] P. Resnick and R. Zeckhauser, "Trust among Strangers in Internet Transactions: Empirical Analysis of Ebay's Reputation System," Proc. NBER Workshop Empirical Studies of Electronic Commerce, 2000.
[10] G. Indirania and K. Selvakumara, "A Swarm-Based Efficient Distributed Intrusion Detection System for Mobile Ad Hoc Networks (MANET)," Int'l J. Parallel, Emergent and Distributed Systems, vol. 29, pp. 90-103, 2014.
[11] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses," Proc. Third Int'l Symp. Information Processing Sensor Networks (IPSN), 2004.
[12] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom'00, pp. 255-265, Aug. 2000.
[13] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-Hop Relay for Next-Generation Wireless Access Networks," Bell Labs Technical J.,vol. 13, no. 4, pp. 175-193, 2009.

AUTHOR

Swathy Satheesh, received the Btech degree in Electronics & Communication Engineering from Anna University in the year 2008. Later got MBA degree from M G University in the year 2010 and joined for ME Communication Systems in 2014, presently a fourth semester student.