International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 02 – Issue 09 || September 2017 || PP. 40-46

# Intra Group Key Management Scheme for Secure Data Exchange in Mobile Ad-Hoc Networks

[1]Dr. B. Gopalakrishnan,
*Associate Professor, Dept of IT, Bannari Amman Institute of Technology*

[2]Dr. M. Gunasekaran,
*Associate Professor, Dept of IT, Bannari Amman Institute of Technology*

[3]Mr. P. Purusothaman,
*Assistant Professor, Dept of IT, Bannari Amman Institute of Technology*

**Abstract:** Many emergency communications is based on mobile Adhoc networks. It suffers from restricted communication and hardware capabilities of mobile nodes. Dynamic key management is an important factor for all security goals in MANETs. In this paper we propose a scheme to generate the public and private keys through Euclid's theorem. The forward and backward secrecy in creating the group key is done through Breadth First Search (BFS) and Depth First Search (DFS) traversals respectively. The group key evolved during this process ensures secured data transfer among the group nodes by encryption/decryption using group key. The proposed scheme enhances the computational complexity of the group key generation algorithm to provide effective and secure communication among the group nodes. The proposed scheme was simulated in NS2 to analyze the computational and communicational capabilities in group key management. This scheme proves more secured than other key management protocols in mobile Ad-hoc networks.

**Keywords:** Euclid's Theorem, Intra-Group Communication, Mobile Adhoc Networks, Forward and Backward Secrecy.

## 1. Introduction

An ad hoc network is a collection of independent nodes which communicate with each other, most obviously by using a multi-hop wireless network. A mobile ad hoc network, or simply MANET, is collection of wireless mobile hosts that that shape a transitory system without the guide of any incorporated organization or support.

Conceivable utilizations of MANETs include: fighters transferring data on critical situational on the war zone; business partners sharing data during a meeting; participants utilizing PCs take part in an intelligent gathering; crisis catastrophe help faculty that are planning endeavors at destinations of flames, sea tempests, or seismic tremors. Providing secure communication in the above said application are more vulnerable to attacks that target underlying secrecy of the system, and also due to their resource constraints, generation of common secrets or key scheduling problem becomes a more fundamental issue in wireless communication. Security services include the functionality that is required to provide a secure networking environment. It comprises authentication, access control, confidentiality, integrity, non-repudiation, and availability. Group key management is a central building block in securing group communications in MANETs. For instance [9] [12][16], GDH and LKH have been extended into the MANETs. Recently, some researches [12] applied a new light-weight cryptographic technique ID-based signcryption for ID-based and threshold key management in MANET. Zhang L and Yang H [17] focus on light-weight cryptographic technique a new ID-based signcryption scheme from bilinear pairings while respecting the constraints of MANET.

A key administration proposition for secure gathering correspondence in MANETs was depicted by Vimala et al. in [14]. They examine a progressive key administration plot (HKMS) for secure gathering interchanges in MANETs. For security, they encrypted a packet twice. They likewise speak about gathering support in their paper so as to manage changes in the topology of a MANET. A Simple and Efficient Group Key (SERGK) management plot is proposed for Region based MANETs. In order to preserve the security, the region-based group key management protocols deal with outsider attacks in MANETs. The experimental results compare the computation cost and time for the existing and proposed approach and the results that outperforms the existing method with lesser computation cost and time. In [10], a low cost solution to the key scheduling problem based on ARQ (Automatic Repeat reQuest) transmission mechanism in wireless communication is proposed which used universal Hashing. ARQ communication protocol was also utilized for the purpose of secret key sharing and reliable communication.

The remaining portion of the paper is organized as section I describes the research works that are proposed early to improve the security requirements in group communication. Section II deals with the group formation through Dynamic core based Multicast routing protocol to establish the path between the group nodes like a graph. The group key involves Euclid's algorithm to compute private and public keys of the node and through forward and backward secrecy the group key is generated. Section III simulation and results that analyze the communicational and computational capabilities in group key generation.

## 2. Related Works

Chung Kei Wong[3], et al. a novel answer for the versatility issue of group/multicast key administration. We formalize the thought of a protected group as a triple (U V A) where means an arrangement of clients, an arrangement of keys held by the clients, and a client key connection. We at that point acquaint key diagrams with indicate secure gatherings. For a unique class of key diagrams, we introduce three methodologies for safely appropriating rekey messages after a join/leave and determine conventions for joining and leaving a safe gathering. The rekeying techniques and join/leave protocols are executed in a model key server we have manufactured. The normal guaranteed handling time per join/leave increments directly with the logarithm of gathering size. Dijiang Huang [4], Deep Medhi multi-level security show, which takes after a changed Bell-La Padula security demonstrate that is appropriate in a progressive versatile impromptu systems administration condition, and a decentralized gathering key administration foundation to accomplish such a multi-level security display. Lessen the key administration overhead and enhance flexibility to any single point disappointment issue. Also, they have built up a roaming protocol that can give secure gathering communication including bunch individuals from various gatherings without requiring new keys; positives of this convention is that it can give persistent group correspondence notwithstanding when the group manager fails.

Peter Hyun-Jeen Lee[10], et al. proposes a proficient Certificateless Encryption plot which is streamlined for Optimized Link State Routing based Mobile Ad Hoc Network condition. Further, they couple Resurrecting Duckling with the plan to accomplish effective key foundation. We likewise demonstrate the security of the plan in arbitrary oracle model show accepting k-Bilinear Diffie-Hellman Inversion issue is hard. Jikai Teng and Chuankun Wu [6] shows a security demonstrate for a certificate less group key management convention and proposes a consistent round group key understanding convention in view of CL-PKC. The proposed convention does not include any significant scheme, which builds the productivity of the convention. It is formally demonstrated that the proposed protocol gives solid AKE-security and endures up to n−2 malicious insiders for powerless MA-security. The convention likewise opposes key control assault under a feeble corruption models.

Chu-Hsing Lin and Chen-Yu Lee[2], proposes a key administration scheme utilizing Shamir's secret sharing plan to develop an Autonomous Key Management (AKM) progressive system structure. Nonetheless, Shamir's mystery partaking in AKM to control key chain of importance needs bigger message transmission costs. In this paper, they alter the secret sharing plan and apply it to AKM for diminishing correspondence and calculation cost. Said Gharout,[13] et al. proposes a solution for bunch key administration with a portability support. Our protocol concentrates on the over three difficulties. It is exceedingly adaptable to dynamic gatherings and treats the hubs' versatility with an null re-keying expense and maintains privacy in reverse and forward secrecies. Our simulation demonstrate that our protocol improves execution contrasted with different conventions while diminishing the general overhead and the quantity of re-keying messages and has no security disappointments.

In Piao[11] et al. group key administration plot, two sorts of polynomials are connected. The ¯rst polynomial (signified by P) is utilized to infer the intra-group key, and the second polynomial is utilized to inter-group key. In what tails we concentrate on the intra-group key administration plot which plans to enable individuals in assemble Gk to share the intra-group key GKk safely and productively. Min-Ho Park,[7]et al. propose new GKM scheme for numerous multicast proposals, called the Master key-encryption-based multiple group key Management (MKE-MGKM) plot. The MKE-MGKM scheme uses different keys, i.e., an master key and various slave keys, which are produced from the proposed Master key encryption (MKE) calculation and is utilized for effective circulation of the group key. It alleviates the rekeying overhead by utilizing the asymmetry of the Master and slave keys, i.e., regardless of the possibility that one of the slave keys is refreshed, the remaining ones can at present be unaltered by changing just the Master key. Through numerical examination and simulations, it is demonstrated that the MKE-MGKM plan can decrease the capacity overhead of a key distribution center (KDC) by 75 percent and the capacity overhead of a client by up to 85 percent, and 60 percent of the correspondence overhead at most, contrasted with the current plans. Wan A Xiong et al[15] . In this article, briefly explains the past works with respect to key administration of MANETs, and afterward essentially present the security scheme introduced by Wang and Fang [8]. They additionally display our plan in view of the security plan's inadequacy in regard of every nodes validation and secure channel for MANETs. At last, we assess the execution of the above scheme in detail. Our answer might be tolerant to t-1 adjusted node and guarantee accessibility of system administrations, for example, key generation and key distribution scheme. The pairing technology furnishes verification and secrecy with reduced communication overhead and computational cost. Our scheme which consolidated the identity based and threshold cryptography can fulfill the safe requirements of MANET.

Bing Wu and Yuhong Dong [1] present a group key administration approach. The basic idea of the approach is that a multicast tree is framed in MANETs for productive dissemination of messages, including keys. They utilize the same multicast tree structure and propose new group key management protocols. Two multicast trees are developed and kept up in parallel to accomplish adaptation to failure conditions. Group members become a group facilitator to register and multicast the blinded keys to all individuals through the dynamic tree links. Each group member computes the group key locally by collecting necessary keys from the group coordinator. The operation can be made in rounds and the coordinator is selected.

Wu B and Wu J[16] et al, outlined the formation of double multicast trees and membership dynamics, and focus on the group key agreement protocol. Yining Liu [18] et al. propose an revised authentication key exchange protocol in view of Shamir's mystery sharing. The proposed protocol accomplishes key classification because of security of Shamir's mystery sharing, and gives key validation by broadcasting a authentication message to all individuals. Moreover, the proposed resist against both insider and outsider assaults.

## 3. Proposed System

The proposed framework encloses following procedure to have Euclid's Secure Intra-Group communication (ESGC) in Mobile Adhoc Network.

- ✓ Node Initialization by characterizing the information structures
- ✓ Group Formation through DCMP Protocol.
- ✓ Computing private and Public key applying Euclid's Algorithm
- ✓ Group key Generation applying graph traversing calculations by utilizing contributory
- ✓ Public keys for the nodes.
- ✓ Group Maintenance (rekeying is required because of node join/leave the group)

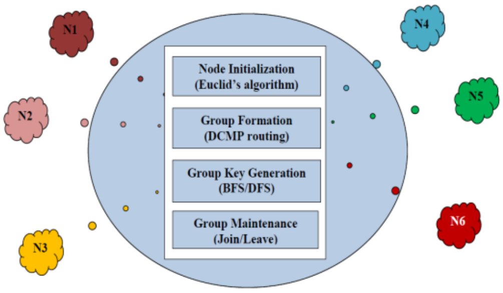
N1
N2
N3
N4
N5
N6
Node Initialization (Euclid's algorithm)
Group Formation (DCMP routing)
Group Key Generation (BFS/DFS)
Group Maintenance (Join/Leave)

Fig 1. Proposed Model ESGC

### A. Node Initialization

The mobile nodes are connected through mesh topology to enable group communication through wireless channel. The nodes are formed with the following Node Structure.

**Node Structure**

| Attribute | Description | Memory |
|---|---|---|
| Nodeid | Node identity | 8-bit |
| xN | Unique integer | 8-bit |
| yN | Unique integer | 8-bit |
| Pr key | Private Key | 8-bit |
| Pu key | Public key | 8-bit |
| Gr key | Group key | 8-bit |
| Hop Count | No of Reachable nodes | 8-bit |

| | | |
|---|---|---|
| St | Ack, NAck | 8-bit |
| Btrper | Battery Percentage | 8-bit |
| Next Hop | Array of nodes | 8-bit |

Table 1. Node Structure

**B. Group Formation**

The nodes are made with node structure and plotted scatter in the system. The multicast routing is applied to establish communication among the nodes in the MANETs. In this, we have considered an effective Dynamic Core Multicast Routing Protocol to identify the patht exist between every nodes in the network. We have two stages in the DCMP protocol - Route Discovery and Route Maintenance Phase

The following steps are proposed to establish the group during route discovery phase:

Step 1: Each Active Node in the system send JReq (Ni, Hcount, BL); message to every one of the neighbors of that hub.

Step 2: The Receiving nodes that are Active will send the JAck (Ni, Status, yi) message to the comparing hub that sent the JReq.

Step 3: The Active Nodes that receives Jack( ), checks Jack, if Status == ACK then update the nexthop cluster of that node.

Step 4: Nodes send "y" value to register the Public key and Private key from x, y of that hub by applying Euclid's calculation to locate the Greatest Common Divisor of the qualities Euclid's calculation .In the event that Ni send JReq to Nj and Nj send JAck to Ni then Public (Pukey) and Private Key (Prkey) of Ni and Nj are computed as follows,

Prkeyi <- Euclid (xi, yi);

Pukey <- ∑ Euclid (yi, yj); for every one hub neighbors of that hub.

Where Euclid's calculation is applied to find the GCD of two numbers

Step5: All the nodes in the network associated by framing undirected diagrams and the Euclid Key Table (EKT) was updated and the values are kept in the EKT for creating the group key

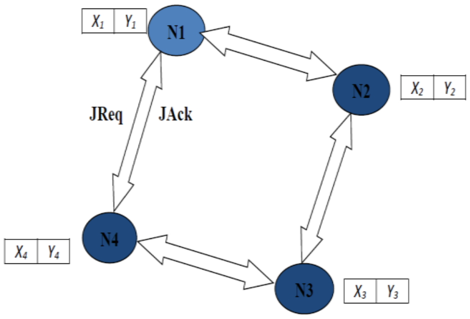

Fig 2 Group Formation

| KEYS | PUBLIC KEY | PRIVATE KEY |
|---|---|---|
| Node N1 | ∑Euclids($Y_1$,$Y_2$),<br>Euclids($Y_1$,$Y_4$) | Euclids($X_1$,$Y_1$) |
| Node N2 | ∑Euclids($Y_2$,$Y_1$),<br>Euclids($Y_2$,$Y_3$) | Euclids($X_2$,$Y_2$) |
| Node N3 | ∑Euclids($Y_3$,$Y_2$),<br>Euclids($Y_3$,$Y_4$) | Euclids($X_3$,$Y_3$) |
| Node N4 | ∑Euclids($Y_4$,$Y_1$),<br>Euclids($Y_1$,$Y_3$) | Euclids($X_4$,$Y_4$) |

**C. Group Key Generation**

The group key is generated by combination of public key values of each node by way of Breadth First Traversal of the nodes that are associated through group arrangement. During the traversal each node calculates the intermediate keys {k1 to kn} where n is the no of dynamic nodes in the group. The Node status been confirmed to check whether node is dynamic or inactive through intermediate keys.

Ki <- Prkeyi pukeyi mod p

The Node id sends the GReq to register the Group Key in the way of the Breadth First Traversal. The GReq message will acknowledge each Active Node in the network and register the group key.

### D. Group Maintenance

A nodes created newly may join or leave the group at any time in the network. A new node created can join the existing group by sending the JReq message and can leave the group with LReq message to its one hop neighbors in the group.

#### D.1 A Node joining the group

Node created will send JReq ( ); message to the one hop neighbors in the network. Node that receives the request, will return JACK( ) status to node to indicate participate in group or not.

The EKT table of the new node and corresponding one hop count neighbors are updated. The Group Key Generation algorithm is invoked. Group Key generation algorithm ensures secure data communication among the nodes by encrypting or decrypting the messages exchanged between the nodes in the group.

#### D.2 A Node leaving the group

A Node that leaves the group will send LReq message to its one hop neighbors that are connected to leaving node. This information is available in the one hop neighbor of that node in the network. The EKT table entries are updated in the One Hop neighbor list of the node. The new group is formed after the modification that happened in the network

The Group Key Generation is invoked with newly formed group.

## 4. Simulation Results and Analysis

The Simulation model has chosen with nodes placement using mesh topology and various protocols are been involved in the process of the evaluation during simulation. The assumption made on the NS2 simulator to analyse the results of the above mentioned algorithms for group key formation with respect to group size, Rekeying operation with respect to group size etc.

### 4.1 Computational Cost of group key with respect to the Group Size

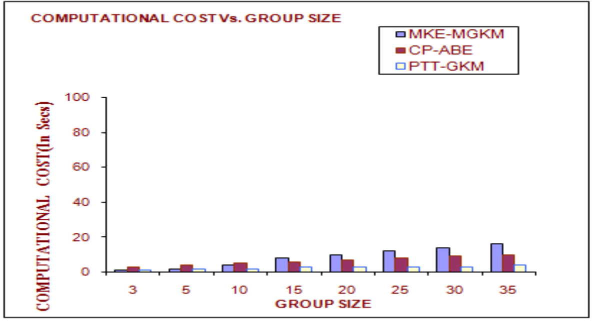

Fig 3 Computational Cost of group key

The computational cost can be evaluated as follows:

Computational Cost = Time taken (to identify node type+ Group Formation + Generating contributory key + to compute pair of keys + to compute group key) * Group Size.

### 4.2 Group Formation vs Group Size

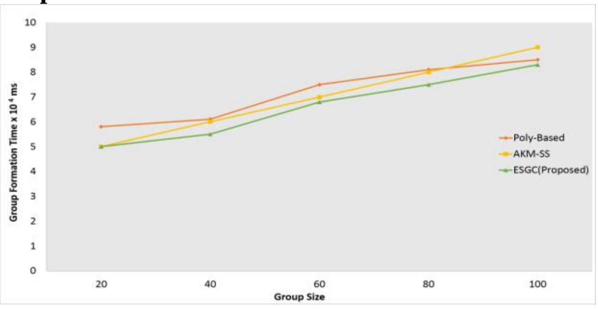

Fig 4 Group Formation Vs Group Size

### 4.3 Rekeying Operation Vs Group Size

| Group Size | MKE-MKGM | PTT_GKM | CP-ABE |
|---|---|---|---|
| 5 | 1125 | 1112 | 1150 |
| 10 | 1200 | 1150 | 1250 |
| 15 | 1250 | 1180 | 1300 |
| 20 | 1300 | 1240 | 1325 |
| 25 | 1288 | 1280 | 1350 |
| 30 | 1350 | 1300 | 1350 |
| 35 | 1290 | 1250 | 1375 |
| 40 | 1300 | 1280 | 1350 |
| 45 | 1250 | 1240 | 1325 |
| 50 | 1340 | 1300 | 1375 |
| 55 | 1300 | 1275 | 1350 |
| 60 | 1280 | 1250 | 1400 |
| 65 | 1350 | 1319 | 1450 |

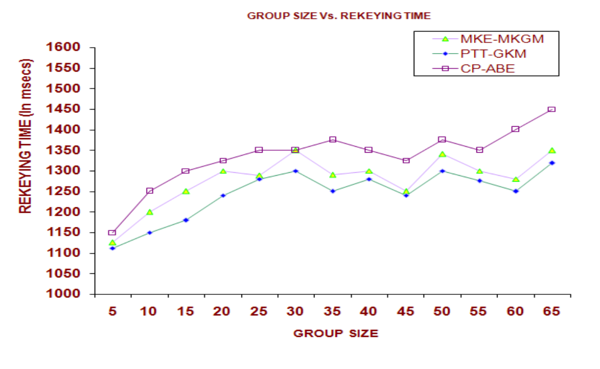

Fig 5 Rekeying Time Vs Group Size

## 5. Conclusion

The secure group communication in Magnets using cryptography has been proposed by many researchers. In this paper we have considered energy factor in Dynamic Core Multicast Routing Protocol (DCMP) to form the group. We have taken Euclid's algorithm to generate private and public of the node and it will be exchanged among the nodes to compute the group key. The group key is used to encrypt/decrypt data or information to have secure communication among the group nodes. The proposed scheme reduces the computational and communicational cost during the node joining or leaving the group. This proposed scheme is also suggested to intergroup communication that brings more scalability in the MANETs.

## References

[1]. Bing Wu and Yuhong Dong (2010) "A Simple Group Key Management Approach for Mobile Ad Hoc Networks", Fifth IEEE International Conference on Networking, Architecture and Storage, PP 73 – 78, 2010.

[2]. Chu-Hsing Lin and Chen-Yu Lee, (2010), "Modified Autonomous Key Management Scheme with Reduced Communication/Computation Costs in MANET", IEEE International Conference on Complex, Intelligent and Software Intensive Systems, PP 818- 821, 2010.

[3]. Chung Kei Wong, Mohamed Gouda and Simon S. Lam (2000) "Secure Group Communications Using Key Graphs" IEEE/ACM Transactions On Networking, PP 16-30 VOL. 8, NO. 1, FEBRUARY 2000.

[4]. Dijiang Huang , Deep Medhi (2007), "A secure group key management scheme for hierarchical mobile ad hoc networks", published in ELSEVIER, Adhoc networks, PP 560 – 577, 2007.

[5]. [5] Jeffrey Lok Tin Woo and Mahesh V. Tripunitara (2013) "Composing Kerberos and Multimedia Internet KEYing (MIKEY) for Authenticated Transport of Group Keys", IEEE Transactions On Parallel And Distributed Systems, 2013.

[6]. Jikai Teng and Chuankun Wu (2012) "A Provable Authenticated Certificateless Group Key Agreement with Constant Rounds", Journal of Communications and Networks, PP 104 – 110, VOL. 14, NO. 1, February 2012.

[7]. Min-Ho Park, Young-Hoon Park, Han-You Jeong and Seung-Woo Seo (2013) "Key Management for Multiple Multicast Groups in Wireless Networks", IEEE Transactions On Mobile Computing, PP 1712 – 1723 , VOL. 12, NO. 9, SEPTEMBER 2013.

[8]. Nen-Chung Wang and Shian-Zhang Fang (2007) "A Hierarchical Key Management Scheme For Secure Group Communications In Mobile AD HOC Networks," Journal of Systems and Software, vol. 80, no. 10, pp. 1667-1677, 2007.

[9]. Pandurang Kamat, Arati Baliga, Wade Trappe (2006), "An IdentityBased Security Framework for V ANETS", V ANET'06, USA, ACM 94-95, 2006.

[10]. Peter Hyun-Jeen Lee, Udaya Parampalli and Shivaramakrishnan Narayan (2009), "Secure Communication in Mobile Ad Hoc Network using Efficient Certificateless Encryption" JOURNAL OF NETWORKS, PP 687- 697, VOL. 4, NO. 8, OCTOBER 2009.

[11]. Piao Y, Kim J, Tariq U and M. Hong (2012), "Polynomial-based key management for secure intra-group and inter-group communication," Computers and Mathematics with Applications, 2012.

[12]. Rafaeli S and Hutchison D (2003) "A Survey of Key Management for Secure Group Communication" ACM computing Surveys, vol. 35, no. 3, PP. 309-329, 2003.

[13]. Said Gharout, Abdelmadjid Bouabdallah, Yacine Challal and Mohammed Achemlal,(2012), "Adaptive Group Key Management Protocol for Wireless Communications" published in J.UCS Journal of Universal Computer Science , 874-899, 18, 6 (2012)

[14]. Vimala N, Jayaram B and Dr. R. Balasubramanian (2011) " Efficient Group Key Management Protocol for Region Based MANETs" International Journal of Engineering and Technology, Vol.3, No.1, February 2011.

[15]. Wan An Xiong, Ming Yu Fan and Chun Xiang Xu, "Identity-based and secret share ECC key management scheme for MANET" 2005.

[16]. Wu B, Wu J, Fernandez E, Magliveras S and Ilyas M (2005) "Secure and Efficient Key Management in Mobile Ad Hoc Networks" Proc. of 19th IEEE International Parallel & Distributed Processing Symposium, Denver, PP 234-240, 2005.

[17]. Xiao S, Gong W, and Towsley D (2010) "Secure wireless communication with dynamic secrets," In Proceedings of INFOCOM., PP. 1–9, 2010.

[18]. Yang H, Luo, H., Ye F, Lu S, and Zhang L. (2004) "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, PP. 38- 47, 2004.

[19]. Yining Liu, Chi Cheng, Jianyu Cao and Tao Jiang (2013), "An Improved Authenticated Group Key Transfer Protocol Based on Secret Sharing" IEEE Transactions on Computers, VOL. 4, NO 2. , 2013.

## Bibliography

**Dr B Gopalakrishnan** has completed his M.E. degree in Computer Science and Engineering from Anna University Chennai. He has defended his Ph. D in the area of mobile ad hoc networks and his research interests are wireless networks and security. He is working as Associate Professor in the Department of Information Technology, Bannari Amman Institute of Technology, and Sathyamangalam since 2001. He has published 15 papers in the national and international journals and conferences.

**Dr M Gunasekaran** has completed his M.E. degree in Computer Science and Engineering from Anna University Chennai. He has defended his Ph. D in the area of mobile ad hoc networks and his research interests are mobile ad hoc and sensor networks and network security. He is working as Associate Professor in the Department of Information Technology, Bannari Amman Institute of Technology, and Sathyamangalam since 2001. He has published 20 papers in the national and international journals and conferences.

**Mr. P. Purusothaman** has completed his M.Tech Degree in Information Technology from Anna University, Chennai. He is currently doing his research in Wireless Sensor Networks. He is working as Assistant Professor in Bannari Amman Institute of Technology, Sathyamangalam. He has published 5 Papers in National and International Journals and Conferences.