A Novel Approach to Secure Mysterious Location Based Routing For Manet

Swetha M. S, Thungamani M

Abstract: ***MANET consists of mobile devices that interact impulsively over the air. The network is changing frequently because of the itinerant nature of its nodes. Security problem arises mainly due to nodes maintaining its capabilities and configuring by itself. In MANET biggest problem is keeping the node secure which cannot be identified easily while routing. Many proposals are made to encounter this problem but no proposal is fully able to resolve this problem. The proposed method have a strong secure mysterious location based routing (S^2MLBR) protocol for MANET using optimal partitioning and trust inference model. In S^2MLBR protocol, first partitions a network into sectors using optimal tug of war partition (OTW) algorithm. Then, compute the trustiness of every mobile node using the constraints received signal strength, mobility, and path loss and cooperation rate. The process of trust computation is optimized by the optimal decided trust inference (ODTI) model, which provides the trustiness of each mobile. Then selects the highest trust owned node in each sector as intermediate nodes used for data transmission, which form a non-noticeable mysterious route***

Index Terms: ***Mobile ad-hoc network, Optimal Tug of War (OTW), Optimal Decided Trust Inference (QDTI) Strong Secure Mysterious Location Based Routing (S^2MLBR).***

I. INTRODUCTION

MANET consists of mobile devices that interact impulsively over the air. The network is changing frequently because of the itinerant nature of its nodes. Security problem arises mainly due to nodes maintaining its capabilities and configuring by itself. In MANET biggest problem is keeping the node secure which cannot be identified easily while routing. A major requirement on the MANET is the ability to provide mysterious for mobile nodes and their traffic. Designing defeating protocols for such argumentative environments is an challenging task in MANETs due to misbehaving of nodes [2] we need a fault tolerant and secure routing protocols to identify and to address routing in argumentative environments, specifically in the presence of defective nodes, by exploring network redundancies [3,4].

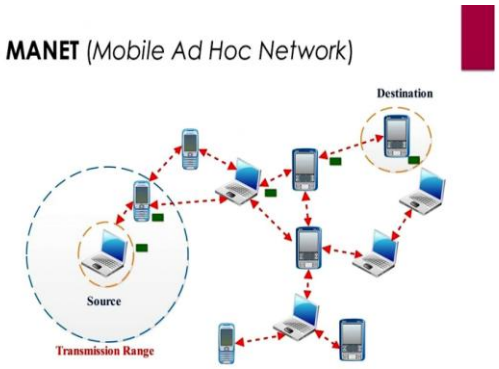

Fig.1: Simple structure of Manet

MANETS nodes are easily attacked so all the proposals made in secure ad hoc routing must pass on the basic user requirement for example authentication, confidentiality and integrity, so that the node from Source to Destination must function regularly even when there is an malicious attack. [5]. In MANETs, most important part is hiding the nodes during communication. This can be achieved when nodes satisfy two conditions 1) Unidentifiability wherein source nodes and destination node should not exposes itself other nodes. 2) Unlinkability wherein the movement of nodes and the route they move from source to destination should be unable to be linked [9].

Security is a very important in Argumentative Environments. But nodes inside the network cannot be always trusted, since a valid node may be captured by malevolent and becomes malevolent node. As a result, mysterious communications (secure routing) will hide the node identifications and routes. The node identity is replaced by random numbers or pseudonym number for protection purposes. There have been many mysterious routing protocols proposed in the past decade. A direct method is mysterious routing uses on-demand ad-hoc routing protocols, such as AODV and DSR [10]. Mysterious routing protocol transfers the information very securely while compared with other techniques.

II. MOTIVATION

For security issue one solution is to use mysterious routing in the network that cannot be identified by any other nodes or attacker or observer [7][11][13][15]. High security and privacy in MANET has been a major issue, while it comes in the field of defense and other such routing. Most of the communication system provides security in routing and data content. Mysterious communications should focus on anonymity in identity, location and route of the participating nodes.

Revised Manuscript Received on May 06, 2019

Swetha M S, Department of Computer Science and Engineering, Visvesvaraya Technological University (VTU), Bengaluru, India.

Dr. Thungamani M, Department of Computer Science and Engineering, Visvesvaraya Technological University (VTU), Bengaluru, India.

Mysterious communication between the MANET nodes are challenging as the nodes are free to move anywhere..

III. LITERATURE SURVEY

Zhang et al. [11] Proposed protocol working on ACO and PAO and introduced B-TRP. Initially Perceptive ants were introduced using cross-layer perception into ACO, These perceptive ants would find route table in each zone and would find route to destination While BHTRP would utilize PAO to find best route from the existing different routes for multi –zone communication. Thus by utilizing ACO & PAO improved performance but they was high energy consumption when compared with DHT routing method.

Biswas et al. [12] has proposed a system wherein performance of secure routing better resource utilization and good throughput were gained but lacked in performance. According to his system packet transmission with great security with better resource utilization of mobile were involved along with neglecting black hole attacks. He ensured trust in every node based on most reliable route during transmission in the network which had stability based on mobility & pause time, remaining battery power.

Abid et al. [13] proposes a system which works on DHT-based routing. As per this routing nodes uses 3D structure to find relationship of node which again exploits 3D logical space by taking physical intra-neighbor relationship of a node. These nodes have algorithm assigned to it which runs to find its nearest logical identifier in the #D logical space. Since it uses 3D structure which has multi-paths to destination node which helps it to measure and bounce back to its original path in case of node/link failure. Even though this proposed system has some great advantage when compared with other DHT routing protocol such as routing overhead, end-to-end delay, path-stretch values and packet-delivery ratio. It is not suitable for high density network because network lifetime is very low.

Uddin et al. [14] proposes AD HOC system based on multipath distance vector protocol with Fitness function (FF-AOMDV). According to these nodes find best possible path to reach from source to destination in multipath routing so as to reduce energy consumption. Even though this system is better than AOMDV & AOMR-LM in many of the network performance metrics and parameters but has a major problem within its internal module during malicious attacks during data transmission.

Ejmaa et al. [15] have proposed a protocol which is far better when compared with NCPR and AODV when made comparison with end to end delay, energy consumption network connectivity packet delivery ration and normal routing overhead. His protocol uses neighbor node connection dynamically and is named as DCFP-Dynamically Connectivity Factor routing Protocol. This routing protocol fetches data dynamically with neighbor nodes without the help of system administrator.

Smith et al. [16] in recent years many have used MANET due to its mobility and flexibility. In order to protect these networks security protocols have been developed. But these security protocols either protect Routing or Communication. But full protection has to be for both Routing and Communication. Keeping this as basis SUPERMAN framework was proposed. According to this framework protocols were allowed to do its function keeping control over access, anonymity of node and secure communication. Simultaneously SUPERMAN frame work is compared with others to develop wireless communication security.

Shen et al. [17] designed a routing which partitions the network field dynamically into zones and then randomly chooses next node to pass on the information. In this routing nodes are non-traceable and anonymity of routing is secured. His routing is based on Anonymous Location based and Efficient Routing Protocol (ALERT). ALERT has capability to hide the data initiator which in turn strengthens the Source providing anonymity of Source node. This routing is also tough when it comes to timing attacks and intersection. At the end when data is transmitted to destination zone it provides complete K-anonymity.

Defrawy et al. [18] designed an routing which can be used in Military and law system wherein high security, privacy and un-traceability is require. He proposed Anonymous Location-Aided Routing in Suspicious MANETs wherein nodes uses current location to safely know and construct topology snapshot to forward data. With the help of advanced cryptographic technique this routing is best in terms of protection against active/passive and insider/outsider attacks. This is the first routing which provides security, privacy, and performance tradeoffs in the context of link-state MANET routing.

IV. PROPOSED SYSTEM

The proposal is for a strong secure mysterious location based routing (S^2MLBR) protocol for MANET using optimal partitioning and trust inference model.

In S^2MLBR protocol, first partitions a network into sectors using **optimal tug of war partition (OTW) algorithm**. Then, compute the trustiness of every mobile node using the constraints received signal strength (RSS), mobility, path loss and cooperation rate. RSS is cost-effective metric used to estimates the distance between the mobile nodes for localization objectives. RSS is the most widely used benchmark because it is easy to measure and is directly related to the provision excellence

The process of trust computation is optimized by the Optimal Decided Trust Inference (ODTI) model, which provides the trustiness of each mobile. Then selects the highest trust owned node in each sector as intermediate nodes used for data transmission.

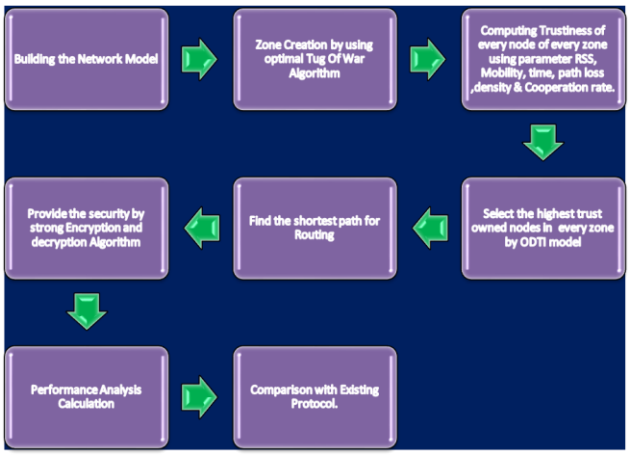

Fig 2: Structure of Network Model

The proposed research focuses on the following objectives:

- To provide mistrustful for mobile nodes.
- To reduce parameters delay, latency, routing overhead, loss ratio & vitality ingesting of mobile nodes.
- To progress or maximize the throughput, system lifetime & delivery ratio of the routing protocols.

V. METHODOLOGY

The proposed work carries the following steps
A) Creation of grid model.
B) Optimal Tug of War Partition.
C) Creation of Sectors by nodes.
D) Selection of Trustiness node in each sector.
E) Routing Scheme.
F) Performance Analysis.

A. Creation of Grid Model.

MANETs consists group of mobile nodes that can communicate through shared wireless medium. The implementation is done through the network simulator ns2 or ns3. In the beginning step will create a 50 nodes as per the screen resolution. The node will be placed by reading the X and Y axis quadrants. In the similar way we can create a network of 100 nodes 200 nodes and for 500 nodes and to maintain the density of the node will use optimal tug of war process (OTW).

B. Optimal Tug of War Partition.

Partition using Tug-of-war optimization algorithm

1 Begin
2 Initialize number of mobile nodes, variables and range of variables
3 Generate population of variable by random solutions
4 While do
5 Compute the objective function
6 Define the weights of groups
7 Sort the solutions and save best one
8 For each group i
9 For each group j
10 If ($W_i < W_j$)
11 Move group I towards group j
12 Close if
13 Close for
14 Compute total displacement of group i
15 Compute total displacement of group j
16 Use the side constraints handling technique
17 Compute the new objective functions
18 Close if
19 Close while
20 Close
Return: optimal partitioning

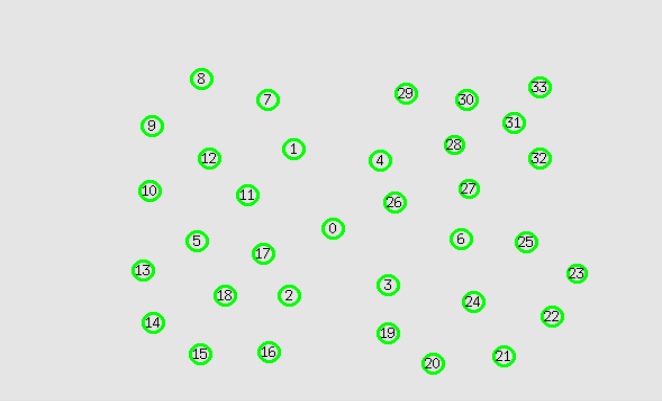

Fig 3: Network Model

C. Creation of Sectors by nodes.

In the proposed model entire system is gathered to form sectors. Sectors are nothing but grouping of nodes based on its positioning. Once Sectors are being created they calculate distance between current node and source node which then starts grouping based on nearest distance. In the sectors node trustiness is computed by every node is calculated by the parameter like received signal strength (RSS), mobility, path loss and cooperation rate and that process is going to called as Optimal Decided Trust Inference (ODTI) method or model, which provides the trustiness of each mobile. Then selects the highest trust degree owned node in each sector as intermediate node for data transmission, which form a non-traceable mysterious route.

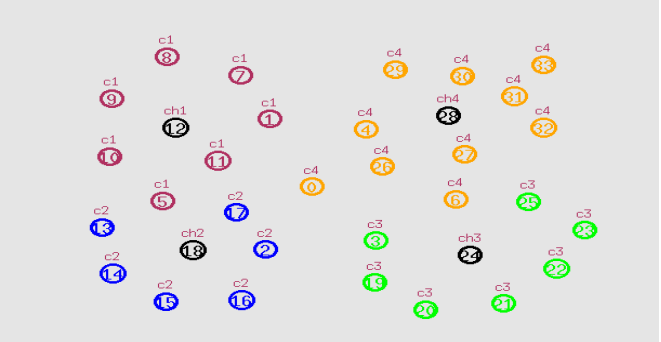

Fig 4: Creation of Sector.

D. Selection of Trustiness node in each sector.

The selection of Trustiness node in each sector done by ODTI model, we propose two OTIPS algorithm variants for the two strategies and analyze the computation complexity.

Trust computation using ODTI model
1 Begin
2 Initialize number of mobile nodes, number of constraints and threshold
3 While do
4 Compute the RSS (K1)
5 Compute the mobility (K2)
6 Compute the path loss (K3)

```
7       Compute the path cooperation rate (K4)
8       Compute the fitness function
9       Define best and worst solutions
10      For each node i
11        Trust degree = K1+K2+K3+K4
12        Threshold = Min (K1+K2+K3) U Max (K4)
13          If (Trust degree > Threshold)
14             Trust degree = optimal solution
15          Close if
16        Close for
17    Close while
18   Close
Return: optimal trust value
```

E. Routing Scheme

The routing of the network done by the selecting the header node in each sector and the selected sector header node responsible to move the data in a network. The selected header node will select the node inside his area and moves the data between the nodes till its gets a proper connection with the next zone

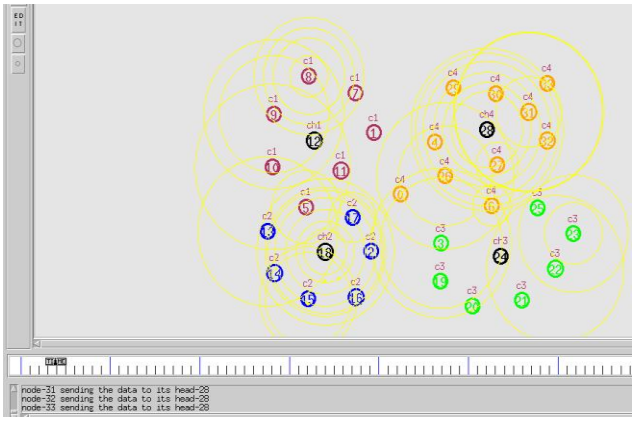

Fig 5: Routing in Proposed model

F. Performance Analysis

Finally, the performance of the proposed strong secure mysterious location based routing (S^2ALBR) protocol is evaluated based on these performance metrics- packet drop, throughput, remaining energy and packet delivery ratio.

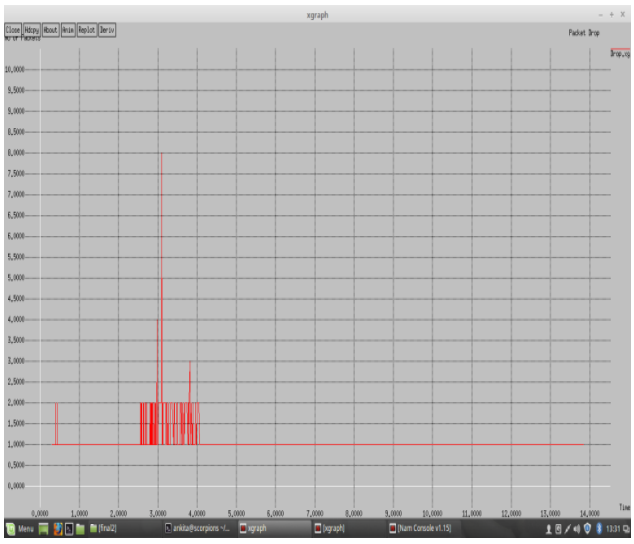

Fig 6: Packet drop graph.

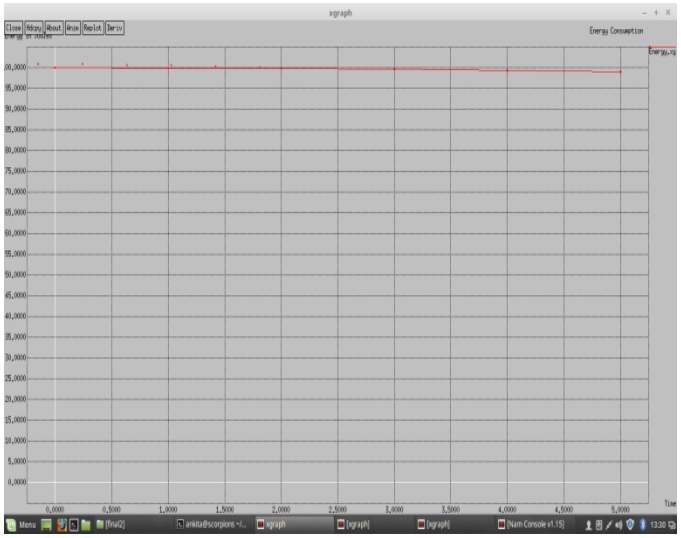

Fig 7. Energy consumption graph

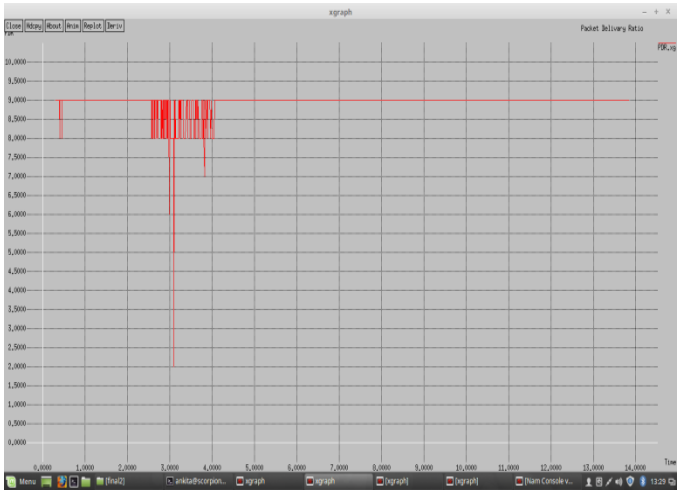

Fig 8. Packet Delivery Ratio graph

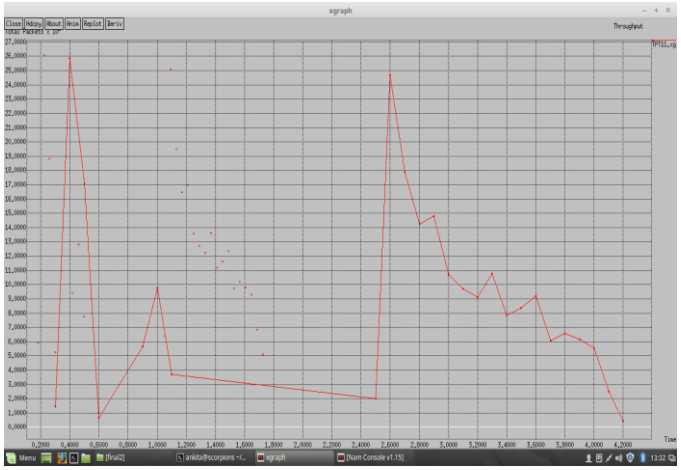

Fig 9.Throughput graph

VI. CONCLUSION AND FUTURE ENHANCEMENT

Mysterious routing protocols are essential in MANETs to provide security between the nodes and communications by hiding node identities and routes from outside observers. The aim of the proposal is provide a strong secure mysterious location based routing (S^2MLBR) protocol which reduces the network parameter like delay, energy consumption, latency, routing overhead, loss ratio; and maximize the throughput, network lifetime, delivery ratio of a network

To prove security of each node the proposed, strong secure mysterious location based routing (S^2MLBR) protocol with compared with the existing protocol like ALERT, ALARM and AASR.

REFERENCES

1. Mingchuan Zhang, Meiyi Yang, Qingtao Wu, RuijuanZheng, and Junlong Zhu," Smart Perception and Autonomic Optimization:A Novel Bio-inspired Hybrid Routing Protocol for MANETs"Future Generation Computer Systems ,Volume 81, Pages 505-513, 2018
2. Darren Hurley-Smith, Jodie Wetherall , Andrew Adekunle," SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks" IEEE Transactions on Mobile Computing , Volume: 16, Issue: 10, 2017
3. MueenUddin, AqeelTaha, RaedAlsaqour , TanzilaSaba," Energy Efficient Multipath Routing Protocol for Mobile ad-hoc Network Using the Fitness Function", IEEE Access ,Volume: 5,2017
4. Ali Mohamed E. Ejmaa , ShamalaSubramaniam, Zuriati Ahmad Zukarnain, ZurinaMohdHanapi," Neighbor-based Dynamic Connectivity Factor Routing Protocol for Mobile Ad Hoc Network" IEEE Access , Volume: 4,2016
5. HoudaMoudni , Mohamed Er-rouidi," Secure Routing Protocols for Mobile Ad Hoc Networks", Information Technology for Organizations Development (IT4OD), 2016
6. SalwaOthmen , FaouziZarai, AymenBelghith, LotfiKamoun," Mysterious and Secure On-Demand Routing Protocol for Multihop Cellular Networks", Networks, Computers and Communications (ISNCC), 2016
7. Remya S and Lakshmi K S,"SHARP: Secured Hierarchical Mysterious Routing Protocol for MANETs", Proc. Intl Conf. Computer Communication and Informatics (ICCCI), 2015
8. S.A. Abid, Mazliza Othman, Nadir Shah, Mazhar Ali , A.R. Khan," 3D-RP: A DHT-Based Routing Protocol for MANETs" The Computer Journal , Volume: 58, Issue: 2, 2015
9. SuparnaBiswas, Tanumoy Nag, SarmisthaNeogy," Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET" Applications and Innovations in Mobile Computing (AIMoC), 2014
10. Uma Rathore Bhatt ,NeeleshNema, RakshaUpadhyay," Enhanced DSR: An Efficient Routing Protocol for MANET", Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014
11. W. Liu and M. Yu, "AASR: Authenticated Mysterious Secure Routing for MANETs in Argumentative Environments", IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4585-4593, 2014.
12. Sheng Liu, Yang Yang, Weixing Wang," Research of AODV Routing Protocol for Ad Hoc Networks",AASR IProcedia,Volume 5, Pages 21-31,2013
13. H. Shen and L. Zhao, "ALERT: An Mysterious Location-Based Efficient Routing Protocol in MANETs", IEEE Transactions on Mobile Computing, vol. 12, no. 6, pp. 1079-1093, 2013
14. S. Mohapatra, P.Kanungo," Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator",Procedia Engineering, Volume 30, 2012, Pages 69-76
15. K. El Defrawy and G. Tsudik, "ALARM: Mysterious Location-Aided Routing in Suspicious MANETs", IEEE Transactions on Mobile Computing, vol. 10, no. 9, pp. 1345-1358, 2011
16. B. John Oommen ,SudipMisra," Fault-tolerant routing in argumentative mobile ad hoc networks: an efficient route estimation scheme for non-stationary environments"Telecommunication Systems, Volume 44, Issue 1–2, pp 159–169, 2010.
17. Vikas Kumar, MS Swetha, MS Muneshwara, S Prakash, "Cloud computing: towards case study of data security mechanism," vol-2 issue-4 page no-1-8 2011
18. MS Muneshwara, MS Swetha, M Thungamani, GN Anil, "Digital genomics to build a smart franchise in real time applications," IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT),IEEE page no 1-4 2017 .
19. MS Muneshwara, A Lokesh, MS Swetha, M Thungamani, "Ultrasonic and image mapped path finder for the blind people in the real time system," IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) IEEE, page no 964-969 2017

AUTHORS PROFILE

Swetha M S, completed her B.E from Adichunchanagiri institute of technology (AIT) Chikkamagaluru and M.Tech from RV Institute of Technology (RVCE) Bangalore, in the year 2008 and 2013 respectively. Currently pursuing Ph.D under Visvesvaraya Technological University (VTU), Karnataka, India. Her area of research is Network Security, wireless sensor networks and ad hoc networks and working tools are NS2 & NS3. She has published more than 25 technical papers in various National & International Conferences and more than 9 papers in reputed Journals and she has 12 years of teaching experience.

Dr.Thungamani M has received her Ph. D. in Pattern Recognition from Centre for Manufacturing Research and Technology Utilization (CMRTU) R.V. College of Engineering, Bangalore in the year 2014 and her master from Dr. M G R Educational And Research Institute University, Chennai. She has published more than 40 technical papers in various National & International Conferences and more than 12 papers in reputed Journals and she has 16 years of teaching experience.

.

.