Volume 4, Issue 3, March 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Anonymizing Geographic Routing for Preserving Location Privacy Using Unlinkability and Unobservability

K.G.S. Venkatesan
Associate Professor, Dept. of CSE
Bharath University, Chennai, INDIA

R.Resmi, R.Remya
Department of C.S.E.
Bharath University, Chennai, TamilNadu, India

Abstract —Privacy-preserving routing is crucial for some Ad Hoc networks that require stronger privacy protection. A number of schemes have been proposed to protect privacy in Ad Hoc networks. However, none of these schemes offer complete unlinkability or unobservability property since data packets and control packets are still linkable and distinguishable in these schemes. In this project, Define stronger privacy requirements regarding privacy-preserving routing in mobile Ad Hoc networks. In order to provide location authentication and location privacy simultaneously. In these packets, they are identified by pseudonyms which are generated from random nonces and secret session keys. The nonces are only used once and never reused, and so are the pseudonyms. Except the random nonce and the pseudonym, the remaining part of the message, including the trapdoor information in the route request, is decrypted and encrypted at each hop. Hence even for a global adversary who can eavesdrop every transmission within the network, it is impossible for him to find linkage between messages without knowing any encryption key. Protocol also authenticates the routing paths taken by individual messages. Achieving anonymity is a different problem than achieving data confidentiality. While data can be protected by cryptographic means, the recipient node address (and maybe the sender node address) of a packet cannot be simply encrypted because they are needed by the network to route the packet.

Key Words: Mobile ad hoc Networks, Route Discovery, Routing protocols, Unlinkability & Unobservability Approach.

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring network consisting of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae [1]. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration. The mobile hosts can move arbitrarily and can be turned on or off without notifying other hosts. The mobility and autonomy introduces a dynamic topology of the networks.

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies [2]. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. The mobile ad hoc network has the following typical features :Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants [3]. Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes. Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol. Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

A. Network Model - A mobile ad hoc network (MANET) is a self-configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management [4]. Each node is

equipped with a wireless transmitter and receiver, which allow it to communicate with other nodes in its radio communication range. In order for a node to forward a packet to a node that is out of its radio range, the cooperation of other nodes in the network is needed; this is known as multi-hop communication.

B.. Attacks Against Routing - Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their malicious behaviors. In the mobile ad hoc networks, attacks against routing are generally classified into two categories: attacks on routing protocols and attacks on packet forwarding/delivery.

C. Intrusion Detection Method - Intrusion Detection (ID) systems are relatively new tools that use engines and agents to spot and analyze anomalies in the network, and alert administrators of network attacks [5]. An ID system is a dynamic monitoring complement to the static monitoring abilities of the firewall. ID systems work by listening to all packets on a network in promiscuous mode, very much like a network sniffer does. Network packets are next analyzed for rule violations by a pattern recognition algorithm. When rule violation(s) are detected, the ID system may alert the administrator, and some can even launch retaliatory attacks. ID products available include RealSecure by Internet Security Systems, Intrusion Alert by Unified Access Communications, SecureNet Pro by Intrusion.

II. DISCUSSION

A. ALARM: Anonymous Location-Aided Routing - Require an off-line group manager (GM) that initializes the underlying group signature scheme and enrolls all legitimate MANET nodes as group members [6]. (This is done well before MANET deployment.) In case of a dispute, the GM is responsible for opening the contested group signature and determining the signer. Depending on the specific group signature scheme, the GM may also have to handle future joins for new members as well as revocation of existing members. However, we claim that in most envisaged MANET scenarios, membership is likely to be fixed, i.e., all joins can be done in bulk, a priori. Also, revocation might not be feasible since it would require propagating – in realtime – updated revocation information to all legitimate MANET nodes. (However, if dynamic membership is necessary, our scheme is capable of supporting it, with minor additional assumptions.)

B. Malicious Node Detection in Geographical Secure Path Routing - Malicious node detection is based on the broadcast nature of wireless communication and is modeled after the watchdog protocol. Nodes listen to the transmissions of their neighbors in order to detect malicious nodes. Malicious nodes are not used for routing. Honest nodes witnessing malicious activity will warn neighboring nodes through the periodic beacon. Watchdog protocols are vulnerable to blacklisting attacks.

Because the GSPR protocol uses temporary pseudonyms, a blacklisting attack can only have a temporary effect. Avoiding temporary blacklisting is not a goal of the protocol, and is not considered further. Malicious nodes are detected both by checking for inconsistencies in the periodic beacons and by checking the correctness of geographically routed messages and their reverse source routed responses.

III. EXISTING SYSTEM

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic .Most of the current 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. In addition, many approaches cannot provide all of the aforementioned anonymity protections. For example, ALARM cannot protect the location anonymity of source and destination, SDDR cannot provide route anonymity, and ZAP only focuses on destination anonymity [7]. Many anonymity routing algorithms are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing (GPSR) that greedily forwards a packet to the node closest to the destination. However, the protocol's strict relay node selection makes it easy to reveal the source and destination and to analyze traffic.

An On-Demand Anonymous Routing protocol for wireless ad hoc networks to enable complete anonymity of nodes, links and source-routing paths/trees using Bloom filters . From Bloom filter is a space-efficient probabilistic bit vector data structure for starting the elements of a set, and testing whether or not any given element is a member of the set. The drawback –it provide only identity anonymity but not unlinkability for MANET. From ALARM uses nodes' current locations to securely disseminate and construct topology snapshots and forward data. With the aid of advanced cryptographic techniques for an example group signature, ALARM provides both security and privacy features, including: node authentication, data integrity, anonymity and untraceability tracking resistance. It also offers protection against passive and active insider and outsider attacks. It leaks quite a lot sensitive privacy information-network topology, location of every node is the major drawback. From Anonymity is an important part of the overall security architecture for mobile ad hoc networks as it allows users to hide their activities. This enables private communications between users while making it harder for adversaries to focus their attacks. A solution that provides stronger anonymity properties while also solving some of the efficiency problems. The main drawback of this method is during the route discovery process, each intermediate node creates a one-time public/private key pair to encrypt/decrypt the routing onion, so as to break the link between source and destination [8].

- Un-traceability and Un-locatability is difficult.

- The setup of MASK is very expensive.

A. The ALERT Routing Algorithm

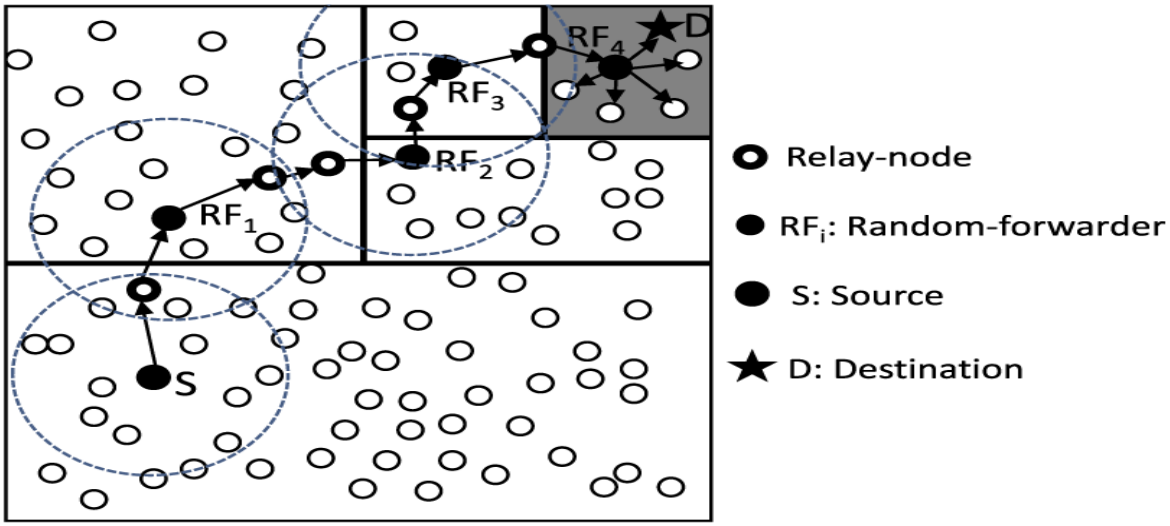

Fig.1: Routing in ALERT

Information of the bottom-right and upper left boundary of the network area is configured into each node when it joins in the system. This information enables a node to locate the positions of nodes in the entire area for zone partitions in ALERT. For encryption, the symmetric encryption algorithm is AES and the public key encryption is RSA. Data are generated randomly according to the packet size specified in the paper. Packets are encrypted whenever needed. Recall that anonymous routing protocols can be classified into hop-by-hop encryption and redundant traffic. To evaluation the routing performance in terms of effectiveness on anonymity protection and efficiency. The number of actual participating nodes. These nodes include RFs and relay nodes that actually participate in routing. This metric demonstrates the ability of ALERT's randomized routing to avoid routing pattern detection [9].

The number of random forwarders. This is the number of actual RFs in a S-D routing path. It shows routing anonymity and efficiency. The number of remaining nodes in a destination zone. This is the number of original nodes remaining in a destination zone after a time period. A larger number provides higher anonymity protection to a destination and to counter the intersection attack. We measure this metric over time to show effectiveness on the destination anonymity protection. The number of hops per packet. This is measured as the accumulated routing hop counts divided by the number of packets sent, which shows the efficiency of routing algorithms. Latency per packet. This is the average time elapsed after a packet is sent and before it is received.

IV. PROPOSED SYSTEM

ALERT strengthens the privacy protection for S(source) and D(destination) by the unlinkability of the transmission endpoints and the transmitted data . That is, S and D cannot be associated with the packets in their communication by adversaries. The route anonymity due to random relay node selection in ALERT prevents an intruder from intercepting packets or compromising vulnerable nodes en route to issue DoS attacks. In ALERT, the routes between two communicating nodes are constantly changing, so it is difficult for adversaries to predict the route of the next packet for packet interception. Privacy protection of mobile ad hoc networks is more demanding than that of wired networks due to the open nature and mobility of wireless media [10 – 12]. In wired networks, one has to gain access to wired cables so as to eavesdrop communications. Messages are routed through secure routing paths. The destination node receives the secure routing path.

A) Anonymity - He senders, receivers, and intermediate nodes are not identifiable within the whole network, the largest anonymity set.

B) Unlinkability - The linkage between any two or more IOIs from the senders, the receivers, the intermediate nodes, and the messages is protected from outsiders. Note linkage between any two messages, e.g., whether they are from the same source node, are also protected.

C) Unobservability - Any meaningful packet in the routing scheme is indistinguishable from other packets to an outside attacker. Not only the content of the packet but also the packet header like packet type are protected from eavesdroppers. And any node involved in route discovery or packet forwarding, including the source node [13], destination node, and any intermediate node, is not aware of the identity of other involved nodes (also including the

source node, the destination node, or any other intermediate nodes). these requirements unobservability is the strongest one in that it implies not only anonymity but also unlinkability.

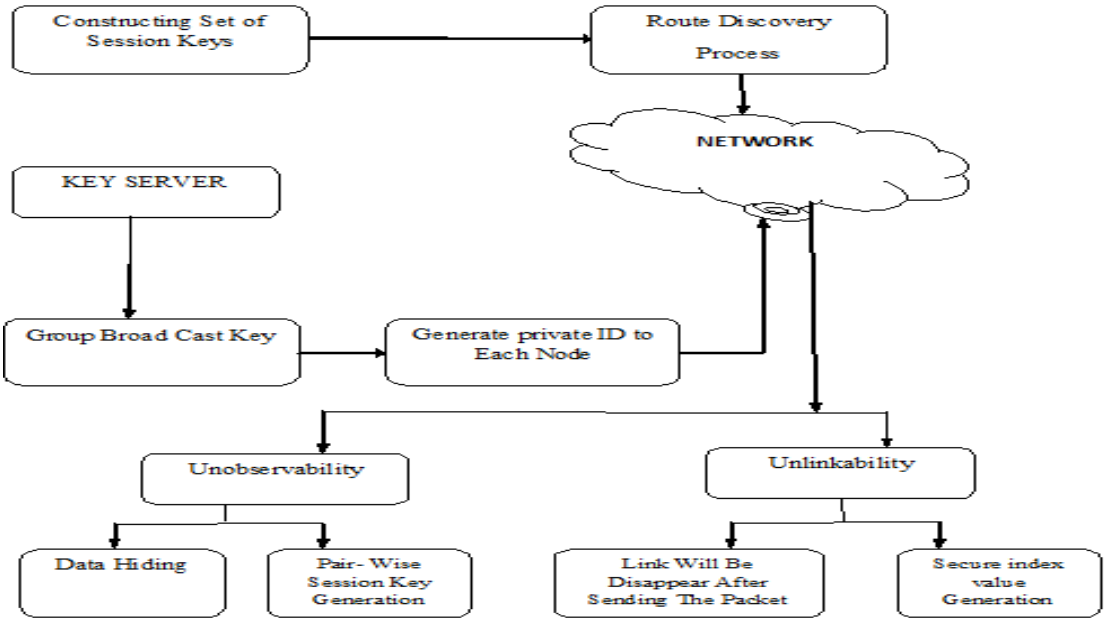

Fig.2 : System Architecture

Hence we further refine unobservability into two types 1) *Content Unobservability* - referring to no useful information can be extracted from content of any message.

E) *Traffic Pattern Unobservability* - referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic. This paper will focus on content unobservability, which is orthogonal to traffic pattern unobservability, and it can be combined with mechanisms offering traffic pattern unobservability to achieve truly unobservable communication [14].

Our geographical secure path routing (GSPR) protects adhoc routing against malicious nodes and passive adversaries. The protocol has the following goals:

i) Route messages to desired geographic locations in the presence of malicious nodes. Detect and avoid bad geographic regions containing malicious or faulty nodes.

ii) Authenticate self-generated public keys and geographic locations of nodes on the routing path.

Similarly, the communication of two nodes in ALERT cannot be completely stopped by compromising certain nodes because the number of possible participating nodes in each packet transmission is very large due to the dynamic route changes. In contrast, these attacks are easy to perform in geographic routing, since the route between a given S-D pair is unlikely to change for different packet transmissions, and thus, the number of involved nodes is much smaller than in ALERT. To achieve unobservability, a routing scheme should provide unobservability for both content and traffic pattern. Hence we further refine unobservability into two types one is content Unobservability, referring to no useful information can be extracted from content of any message and another one is Traffic Pattern Unobservability, referring to no useful information can be obtained from frequency, length, and source-destination patterns of message traffic.

1. Route Discovery - When source node sends a packet to the destination node, it first searches its route cache for suitable route to destination. If no route from source to destination exists in source's route cache, Source initiates Route Discovery and sends out a ROUTE REQUEST message to find the route [15]. The source node is referred to as initiator and destination node as the target. When a node receives a ROUTE REQUEST message it examine the target ID to determine if it is the target of message. If not, then nodes own id is appended to the address list and the RReq is broadcasted. If the node is the target it returns a ROUTE REPLY message to the initiator.

2. Intrusion Detection - Intrusion detection can be defined as a process of monitoring activities in a system, which can be a computer or network system. An IDS collects activity information and then analyzes it to determine whether there are any activities that violate the security rules [16]. Once an IDS determines that an unusual activity or an activity that is known to be an attack occurs, it then generates an alarm to alert the security administrator. In addition, IDS can also initiate a proper response to the malicious activity.

3. Broadcast Key Distribution - The broadcast key has been established among the nodes in the network. The key generated from the public key generated for the group. This broadcast key act like a security issue where each node

should get authenticated before it enters into the network for communication. The BK will be shared among the neighbors in the zone. In this each node has to create a group signature signing key and an ID-based private key from an offline key server, an anonymous key establishment process is performed to construct secret session keys.

4. Anonymous Network - In this phase the anonymous network has been generated by obtaining unobservability and unlinkability. Unobservability is the strongest one in that it implies not only anonymity but also unlinkability. To achieve unobservability, a routing scheme should provide unobservability for both content and traffic pattern.

5. Data Hiding Mechanism - Content unobservability, which is orthogonal to traffic pattern unobservability, and it can be combined with mechanisms offering traffic pattern unobservability to achieve truly unobservable communication. The major mechanisms to achieve traffic pattern unobservability include MIXes and traffic padding mechanism to attain the data hiding process [17].

6.Performance Evaluation - The number of eavesdropping nodes in the network and compute the sender anonymity of RREQ packets. The sender anonymity is the obtained by calculating entropy of probability distribution of possible sender of RREQ packets. The performance has been rated by comparing the results from MASK. The error rate has been reduced. The evaluation will be shown in the form of graph.

V. CONCLUSION

In this paper, we have constructed the framework which supports anonymous location-based routing in certain types of suspicious MANETS. It relies on group signatures to construct one-time pseudonyms used to identify nodes at certain locations. The framework works with any group signature scheme and any location-based forwarding protocol can be used to route data between nodes. Have shown through simulation that node privacy under this framework is preserved even if a portion of the nodes are stationary, or if the speed of movement is not very high. Future work includes developing an analytical model which captures the loss in node privacy due to the dynamics of the speed and the mobility patterns of nodes inside the MANET.

VI. FUTURE WORK

After the source node S successfully finds out a route to the destination source node S successfully finds out a route to the destination node D, S can start unobservable data transmission under the protection of pseudonyms and keys. The proposed method should focus on full and full privacy preserved routing in mobile ad hoc networks. Only security has been improved.

Acknowledgment

The author would like to thank the Vice Chancellor, Dean-Engineering, Director, Secretary, Correspondent, Principal, HOD of Computer Science & Engineering, Dr. K.P. Kaliyamurthie, Bharath University, Chennai for their motivation and constant encouragement. The author would like to specially thank Dr. A.Kumaraval for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the work and the Faculty Members of Department of Computer Science & Engineering. Also, he takes privilege in extending gratitude to his parents and family members who rendered their support throughout this Research work.

REFERENCES

[1] Zhiguo Wan, Kui Ren, and Ming Gu, " *An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks"*

[2] Jiejun Kong, Xiaoyan Ho, *"Anonymous on Demand routing with untraceable Routes for Mobile Ad-hoc Networks"*.

[3] 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.

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

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

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

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

[8] Z. Zhi and Y.K. Choong, *"Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy,"* Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.

[9] 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.

[10] A.R. Beresford and F. Stajano, *"Mix Zones: User Privacy in Location-Aware Services,"* Pervasive Computing and Comm. Workshops (PERCOMW), 2004.

[11] X. Wu, J. Liu, X. Hong, and E. Bertino, *"Anonymous Geo- Forwarding in MANETs through Location Cloaking,"* IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp.1297-1309, Oct. 2008.

[12] K. El-Khatib, L. Korba, R. Song, and G. Yee, *"Anonymous Secure Routing in Mobile Ad-Hoc Networks*," Proc. Int'l Conf. Parallel Processing Workshops (ICPPW), 2003.

[13] S. Ratnasamy, B. Karp, *"Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table,"* , No. 4, pp. 427-442, 2003.

[14] J. Raymond, *"Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems,"* pp. 10-29, 2001.

[15] T. Camp, *"A Mobility Models for Ad Hoc Network Research," Wireless Communications and Mobile Computing",* vol. 2, pp. 483-502, 2002.

[16] X. Hong, M. Gerla, G. Pei, and C.C. Chiang, *"A Group Mobility Model for Ad Hoc Wireless Networks,"* Proc. Second ACM Int'l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.

[17] X. Wu, *"DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles,"* Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373,2006

ABOUT THE AUTHOR

	**R. Resmi** received her B.E degree from Prince Shri Venkateshwara Padmavathy Engg college Chennai. She is currently pursuing her M.Tech., Final Year, II Semester in Computer Science & Engineering from Bharath University, Chennai. She has secured Second Rank Holder in Schools and many Cultural activities Had participated in many college symposiums .
	**K.G.S.Venkatesan** received his B.Tech degree in Computer Science & Engineering from JNT University, Hyderabad and received his M.Tech degree in Computer Science & Engineering from Bharath University, Chennai. He is currently pursuing his Ph.D in Computer Science & Engineering at Bharath University, Chennai. He has 10 years of Teaching experience and has guided many B.Tech and M.Tech projects. He is having Membership in Indian Society of Technical Education (MISTE). He attended **HIGH IMPACT Teaching Skills** Programme conducted by WIPRO MXLA (Mission 10X Learning Approach).
	**R. Remya** received her B.E degree from Prince Shri Venkateshwara Padmavathy Engg college, Chennai. She is currently pursuing her M.Tech., Final Year in Computer Science & Engineering from Bharath University, Chennai. She has participated in many Inter-college cultural. She has secured first class in her under graduate.

