International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Analysis of Various Malicious Node Detection Techniques: A Review

Priyanka[1], Mukesh Dalal[2]

[1]Master of Technology, Department of Computer Science and Engineering, MITM, Hisar, Haryana, India

[2]Assistant Professor, Department of Computer Science and Engineering, MITM, Hisar, Haryana, India

Abstract: ***Mobile Ad-hoc Network (MANET) is self configured network and collection of autonomous nodes that communicate with each other by forming a multi-hop radio network and maintaining connections in decentralized manner. Security is major concern in MANET due to its various features such as open medium, limited power supply and lack of clear lines of defense.*** **It is vulnerable to various types of DoS attacks like black hole, grey hole, worm hole, impersonation etc.** ***In black hole attack, attacker claims to have shortest route to destination by injecting a fake reply message. This document introduces a comparative study of various malicious or DoS nodes detection schemes and analyze their performance based on various parameters viz node mobility, Quality of service, false alarm detection etc.***

Keywords**:** Mobile Ad-hoc Networks (MANET), Ad-hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Denial of Service (DoS), Black hole attack, malicious node

1. Introduction

A MANET [1] is self configured and decentralised network that can be easily deployed and needs no infrastructure. It consists of mobile nodes which communicate with each other to forward packets from source to destination by forming multi-hop radio network. It is widely applicable [2] in many areas such as in military and battlefield applications, disaster area networks etc. MANET posses many characteristics [3] such as mobility, multi hop communication, dynamic topology, bandwidth constraint and variable link capacity etc. It is vulnerable to various types of attacks due to many security issues such as dynamic nature, limited computation, and lack of clear lines of defence. It is mainly influenced by Denial Of Service (DoS) [4] attacks such as black hole, grey hole, worm hole, impersonation, eavesdropping and replay attacks.

A malicious node can easily join the network and starts its malicious behaviour by dropping packets, advertising wrong routing information. A malicious node can silently drops all or some of the packets even when no congestion occurs. This situation becomes more sever when a group of malicious nodes co-operate each other. So, Security in MANET is an essential component for basic network functionalities like packet forwarding, routing and network management performed by all nodes instead of dedicated ones. Network operation can be easily jeopardized if security countermeasures are not embedded into basic network functions at the early stages of their design.

The advantages [5] of MANET are as follows:

- Fast Installation
- Dynamic Topologies
- Fault Tolerance
- Mobility
- Spectrum Reuse Possibility

In order to prevent the adverse effects of routing misbehaviour, the malicious nodes must be detected and removed from the network. In this paper we will discuss various techniques for the same but before that we will discuss various security attacks that can occur in MANET and disrupt its normal working operation.

1.1 Classification of Attacks In MANET

Security of communication in MANET is important for secure transmission of information. Attacks on networks come in many varieties and they can be grouped based on different characteristics. There are many ways to diversify attacks:

- Location or source based attacks
- Behavior based attacks
- Malicious and selfish node attacks

1.1.1 Location based attacks**:** Based on location of attacker, attacks can be categorized into two types:

a) *External attacks***:** External attacks are mainly carried out by node that does not belong or outside the network. They get access to the network by some means and once they get access to the network they start sending bogus packets, wrong routing information and cause denial of service in order to disrupt the performance of the whole network.

b) Internal attacks: In internal attack [6], the attacker has normal access to the network as well as participates in the normal activities of the network. The attacker enters in the network as new node either by compromising a current node in the network or by malicious impersonation and starts its malicious behavior.

Internal attacks are more dangerous than the external attacks: because the compromised nodes are originally the benign users of the ad-hoc network, they pass the authentication mechanism easily and get protection from the security mechanisms.

1.1.2. Behavior based Attacks: Based on behavior of the node, attacks are classified further into two types:

a) *Active attacks:* In active attack the attacker disrupts the performance of the network by stealing important information and destroying the data during the exchange in the network [1]. Active attacks can be an internal or an external attack.

b) *Passive attacks:* In passive attacks [1], attackers do not disrupt the normal operations of the network but listen to network in order to get important information, what is happening in the network, how the nodes are communicating with each other and how they are located in the network.

c) *Malicious and Selfish Node attacks:* Malicious nodes can disrupt the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information and by impersonating other nodes.

On the other side, **selfish nodes** can severely degrade network performances and eventually partition the network by simply not participating in the network operation [5]. These nodes do not participate in network activities to save their battery power.

1.2 Attacks Types

Among numerous possible threats and attacks, MANETs are particularly susceptible to DoS attacks. Some known DoS attacks developed against MANETs are examined.

1) *Denial of Service (DoS) attack:* The first type of attack is denial of service, in which the attacker aims to crab the availability of certain node or even the services of the entire ad-hoc networks. However, as seen so far, they are basically the results of most of the kinds of tampering with network integrity, redundancy and availability. In the traditional wired networks, the DoS attacks are mainly caused by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and the services provided by the target become unavailable.

2) *Black hole Attack:* Black hole attack is **D**enial **of S**ervice (DoS) attack on routing traffic. Black hole attack has two properties: First, the node advertises itself as having a shortest and fresh route containing larger sequence number and smallest hop count number to a destination node and exploits the mobile ad hoc routing protocol such as AODV, even though the route is not valid, with the intention of intercepting or dropping packets. Second, the attacker drops most of the packets without any forwarding. A black hole can be caused either by a single node or by several nodes in collusion.
   In case of a **single node black hole attack**, the node drops the entire packet instead of forwarding to destination.
   In case of **multi-node collusion [7] or cooperative black hole attack**, BH forwards all the data to BH' and BH' drops them instead of forwarding to the destination. Black hole attacks have serious impact on routing algorithms.

3) *Gray hole Attack*: A Gray hole attack [8] is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later.

4) *Wormhole Attack***:** In a wormhole attack, a malicious node uses a path which is outside the network to route messages to another compromised node at some other location in the network. This attack is hard to detect because the path that is used to pass on information is usually not part of the actual network.

5) *Eavesdropping attack [9]:* This is a passive attack. The malicious node simply listens to the network and observes the confidential information. Later, it uses this information to carry out attacks.

6) *Impersonation attack***:** The attacker assumes the identity of another node in the network and receives messages directed to the node it fakes. Usually this would be one of the first steps to intrude a network with the aim of carrying out further attacks to disrupt operation. Depending on the access level of the impersonated node, the attacker is able to reconfigure the network so that other attackers can (more) easily join or he could remove security measures to allow subsequent attempts of invasion.

7) *Sleep deprivation torture***:** The idea behind this attack as described in [9] is to request the services a certain node offers, over and over again, so it cannot go into an idle or power preserving state, thus depriving it of its sleep.

The rest of the paper is organized as follows: Section II discusses various proposals carried out earlier by researchers along with a comparison table as discussed in section III and finally Section IV concludes the paper.

2. Literature Work On Malicious Node Detection Techniques

With the increasing interest in MANETs, there has been a great focus on the subject of securing such networks. MANETs must have a secure way for transmission and communication which is challenging and vital issue. Out of the many discussions and research groups discussing the different security issues in the field of mobile ad-hoc networks, a variety of secure routing protocols have been proposed by researchers that defend against malicious nodes' attacks that MANETs face. Some of the contributions are described here:

In [10], Bansal and Baker proposed an **O**bservation-based **C**ooperation **E**nforcement in **A**d-hoc **N**etworks (OCEAN) scheme for malicious node detection that is based on direct observations. The rating of a node is increased if the observed behavior is positive whereas if the observed behavior is negative the rating is decreased by more value than that is used for increment. If the rating of a node decreases beyond faulty threshold then it is added in faulty list. This faulty list is appended in route request by each node broadcasting it to be used as the list of nodes to be avoided. A route is rated good or bad depending on whether the next hop is on faulty list or not. It is rated bad if next hop is in faulty list and traffic from that route is rejected. A second chance mechanism employs timeout after an idle period. After a timeout, the node is removed from the faulty list with its rating remaining unchanged.

In [11,] a generic mechanism known as **Co**llaborative **R**eputation mechanism (CORE) was proposed by Michiardi P, Molva R. to enforce node cooperation in MANET. It can be integrated with any network function like forwarding of packets, route discovery, network management and location management and is mainly an extension to the DSR protocol. Core stimulates node cooperation by using a collaborative monitoring technique and a reputation mechanism. In CORE, reputation is a measure of someone's contribution to network operations and three types of reputations are defined: subjective reputation, functional reputation and indirect reputation. CORE works on watchdog mechanism in which watchdog listens next node transmissions. Each node computes a reputation value for every neighbor using a sophisticated reputation mechanism that differentiates between the three types of reputations. Members that have a good reputation can use the resources while members with a bad reputation are gradually excluded from the community.

CONFIDANT (**C**ooperation **o**f **N**odes: **F**airness **in** **D**ynamic **A**d-hoc **N**etwork) [12], a reputation-based protocol was presented by Buchegger and Boudec. It aims at detecting and isolating uncooperative nodes so that to make it unattractive for nodes to deny cooperation. Nodes rely on passive observation of all packets within a one-hop neighborhood. With Confidant, each node has the following four components: monitor, trust manager, reputation system and path manager. These components interact with each other to provide and process protocol information.

Each node monitors the behavior of its neighbors by monitor component. If a suspicious event is detected, the information is given to the reputation system. If the monitored event is significant for the node, it is checked for its occurrence for more than a predefined threshold that is high enough to distinguish deliberate malicious behavior from simple coincidences such as collisions. If a certain threshold exceeds, the reputation system updates the rating of the node that caused the event. If the rating turns out to be intolerable, the information is sent to the path manager, which deletes all routes containing the misbehaving node.

In [7], a protocol BAAP is described by Saurabh Gupta et. al. for avoiding malicious nodes in the routing path by using legitimacy table which is maintained by each node in the network. In BAAP, **A**d-hoc **O**n-demand **M**ultipath **D**istance **V**ector (AOMDV) is used to form link disjoint multi-path during path discovery. When intermediate node replies to source node, few nodes in the routing path may have more than one path to the destination but it chooses only one path to destination node. In BAAP, a legitimacy table is maintained by each node to choose the most legitimate node to source node and next hop to destination node while sending RREP back to source node. The fields contained by legitimacy table are: Node ID, Path count and Sent count. Node ID field stores the IP address of the node whose legitimacy value is being recorded. Path count field indicates the number of times the node has been chosen in the path and the Sent count field describes the number of times connections have been successful through the Node ID to destination node. These two count fields are used to define the Legitimacy Ratio (Sent count/ (Path count +1)) of a Node ID which indicates the confidence of node in performing its function of correct routing. A higher legitimacy ratio has higher possibility of a node being non-malicious.

In [13], Vishnu K et al. presents a scheme based on backbone network to detect and remove black hole nodes from network. Backbone network consists of group of nodes those are powerful in terms of battery power and range and are permitted to allocate the Restricted IP address to the newly arrived nodes. When a source node wants to initiate route discovery it asks the backbone network to allocate any unused RIP address. After the backbone network assigns the RIP address, the source node sends RREQ not only to search for destination but also for allocated RIP. If the RREP for the RREQ comes from the destination then network is safe but if RREP comes from RIP then it is assumed that there is black hole node in the network. The source node sends a monitor message to neighbor nodes to go into promiscuous mode and listen to the network. If the neighbor nodes monitors that the node drops the packet more than normal case it sends reply message to source node that there is black hole node in the network.

SAODV (Secure Ad-hoc On Demand Distance Vector) [14] is a security extension to the AODV routing protocol. This protocol provides security features like data integrity, non-repudiation and authentication. It uses two concepts: digital signature and hash functions. Digital signatures are used to protect non mutable fields of messages and hash functions are used to protect hop count information. It uses extension messages. In these extension messages there is digital signature of AODV packet signed with private key of sender. The source node sends this packet, all the intermediate node verifies the signature and makes the route if the signatures are verified. The same also happens in the reverse direction.

In [15], Qu He Presents a **S**ecure **O**bjective **R**eputation based **I**ncentive (SORI) scheme to encourage packet forwarding and discipline selfish nodes. This scheme consists of three components. First, neighbor monitoring which monitors the neighbor nodes for their packet forwarding behavior and a neighbor node list (NNL) which consists of details for all the neighbors of a node is maintained by each node. Based on this list, a record of reputation is build for each neighbor by reputation propagation component. This reputation is shared by all the neighbor nodes to identify the selfish node. Finally a punishment scheme is used by punishment component to penalize selfish nodes. The unique feature of this scheme is that reputation is secured by one-way hash based authentication scheme and communication overhead is less since reputation is propagated to neighbor nodes only.

Tamilsevan in [16] presents a method for enhancement of AODV by introducing fidelity table. The RREP coming from destination nodes or intermediate nodes are collected in response table and fidelity level of each RREP is checked and the one having highest level is selected. On receiving the data packets, the destination node sends back an acknowledgement. The fidelity level of intermediate node is increased upon receiving the acknowledgement considering it safe and decreased when no acknowledgement is received. When the fidelity level of a node reaches beyond the threshold then it is detected as black hole node.

Arijit Ukil and Jaydip Sen et. al. [17] described the mechanism which modifies the AODV protocol by introducing two concepts, (i) **D**ata **R**outing **I**nformation (DRI) table (ii) cross checking. DRI table has two bits information respond to the RREQ message of a source node. The source node broadcasts a RREQ message to discover a secure route to the destination node. The intermediate node generating the RREP has to provide information regarding its next hop node and its DRI entry for that next hop. After receiving the RREP message from intermediate node (IN), source node (SN) will check its own DRI table to see whether IN is its reliable node. If IN is used by SN before for routing data packets, then IN is a reliable node and SN starts routing data through IN. Otherwise, IN is unreliable and SN sends further-route-request(FRQ) message to **N**ext-**H**op-**N**ode (NHN) to check the identity of the IN, and asks NHN about the following information: (i) if IN has routed data packets through NHN, (ii) who is the current NHN's next hop to destination, and (iii) has the current NHN routed data through its own next hop. The NHN then responds with further-route-reply (FRP) message including the following responses: (i) DRI entry for IN, (ii) the information about its (NHN's) next hop node, Based on the FRP message from NHN, SN checks whether NHN is reliable or not. If NHN is used by SN before to route data, NHN is reliable; otherwise, NHN is unreliable.

Khalil et al. [18] introduces **L**ightweight counter measures for **W**ormhole attack (LITEWORP) that provides detection of attack by using secure two hop neighbor discovery followed by isolation of malicious nodes by local monitoring. The concept of guard node is used. The guard node is a common neighbor of two nodes to detect a legitimate link between them. Guard nodes increment the counter by one if malicious action is detected. After the counter reaches beyond threshold value, the node is identified as malicious. It is suitable for resource constrained multihop wireless networks

Xin Jin et.al. [19] Proposed a method for tracing DoS attackers in MANETs. The ZSBT algorithm consists of three processes: initialization process, a zone sampling process, and a path reconstruction process. ZSBT algorithm uses the zone information of each node sampled by the packets to reconstruct the path between the attacker and the victim. In this algorithm, when a node forwards packets, the node writes its zone ID into the packets with a probability. Upon receiving these packets, the victim reconstructs the path between the attacker and itself. However, there is a shortcoming of ZSBT algorithm. This scheme sacrifices the accuracy of the path for tracing DoS attackers.

Jian-Ming Chang et. al. [20] proposed CBDS (**C**ooperative **B**ait **D**etection **S**cheme) which is able to detect and prevent malicious nodes launching cooperative black hole attacks. It integrates with the proactive and reactive defense architectures and the source node randomly cooperates with a stochastic adjacent node. When source node initializes Route Discovery, it sends out the bait RREQ' and then source node receives RREP. If RREP is from not existed destination node or intermediate node then trace which node sends back the RREP according to RREP packet's Record address field. The location of black hole is recognized and detected by source node when receiving the fake RREP. Then the detected black hole node is listed in the black hole list and noticed all other nodes to revoke the certificates of black hole by propagating Alarm packets through the network. Further any responses from black hole are discarded.

In [21] Dokurer proposed a solution that is based on ignoring the first established route to reduce the adverse effects of black hole attack. He assumed that first RREP message would normally come from a malicious node. Unfortunately, this solution has some limitations. For example, the second RREP message received may also come from malicious node if the real destination node is nearer to the source node than the malicious node. This method also does not address how to detect and isolate malicious node from the network.

In [22] Swadas PB proposed a scheme DPRAODV (**D**etection, **P**revention & **R**eactive **AODV**) in which a new control packet called ALARM and concept of dynamic threshold value is used. A dynamic threshold value is taken by calculating the average of dest seq_no between sequence number and RREP packet. Unlike AODV, the RREP seq_no is extra checked whether higher than threshold value or not. If the RREP_seq_no value is higher than the threshold value, the sender is recognized as an attacker and updated it to the black list. The ALARM is sent to its neighbors who include the black list; the RREP from the malicious node is blocked but is not processed. The dynamic threshold value is changed in each slot. By this scheme, the black hole attacks not only be detected but also prevented by updating threshold which responses the realistic network environment and achieves higher packet delivery ratio.

3. Comparison of the Techniques

In this, table 1 represents the multi-aspect qualitative comparison between the detection methods discussed above. The comparison is done on the basis of various parameters such as node mobility, type of protocol used, simulator used etc.

Table1: Comparison of Malicious node Detection Techniques

Detection Technique	*Protocol Name and its type*	*Basic concept*	*Mobility*	*Attack type*	*QoS parameter*	*Change in routing protocol, false detection*	*Simulation tool Used*
Vishnu [13]	AODV, Reactive	Backbone network which allocates Restricted IP address.	Not Considered	Cooperative Black hole	No results	No, Not handled	No Simulation results
SORI [15]	DSR, Reactive	Neighbor monitoring and reputation propagation	Random Way Point Model	Selfish Node	Packet drop rate and throughput	Yes(NNL list is maintained), Not Handled	NS-2
ZSBT [19]	Not specified	Zone sampling based traceback	Random Way Point Model	DoS attacks	Sacrifice accuracy of path	Yes, Not Handled	GloMoSim
DPRAODV [22]	AODV, Reactive	Dynamic threshold value which is changed in each time slot.	Considered	Single Black hole	Packet delivery ratio and delay	No, Not Handled	NS-2
Jaydip Sen [17]	AODV, Reactive	Use Data routing Information table and cross checking	Considered	Cooperative Black hole	Packet loss and delay	Yes(uses DRI and cross checking tables), Handled	NS-2
CBDS[20]	DSR, Reactive	Baiting and reverse tracing.	Considered	Cooperative Black hole	Packet delay and extra overhead	No, Not Handled	Qualnet
LITEWORP [18]	DSR, Reactive	Guard node can detect the wormhole.	Not Considered	Worm hole	Packet loss	No, Handled	NS-2
BAAP [7]	AOMDV, Reactive	Use legitimacy ratio for detection	Considered	Cooperative Black hole	Packet loss increases with mobility	Yes(legitimacy table), Not handled	NS-2
OCEAN [10]	DSR, Reactive	Based on direct observation	Considered	Selfish Node	Throughput	Components system is used, Handled	GloMoSim
CONFIDANT [12]	DSR, Reactive	Based on passively Observed behaviour	Random Way Point Model	Cooperative misbehaving node	Packet Drop rate and throughput	Components system is used, Handled	GloMoSim
Tamilselvan [16]	AODV, Reactive	Use Fidelity table, and detect nodes based on fidelity level	Random Way Point Model	Cooperative black Hole	Packet Delay	Yes, Not Handled	GloMoSim

4. Conclusions

This paper discusses various attacks those can occur in MANETs. With the literature review for the malicious node detection techniques, the problem of secure routing in MANETs and various issues involved in the process are discussed. So, the main focus is on the malicious node detection techniques for MANETs proposed in the literature. A brief overview of such proposals has been experienced, which is summarized in tabular form. Thus, it is concluded that MANETs are more prone to malicious node attacks which causes Denial of Service (DoS). This proves to be a setback in MANETs. Thus malicious node detection and its removal are the two main issues that need to be resolved by maintaining the throughput, detection rate.

This comparison study would be extensively used by the researchers as basic for their research.

References

[1] Joseph Macker and Scott Corson Mobile ad-hoc networks (MANET) http://www.ietf.org/proceedings/01dec/183.htm

[2] Humayun Bakht, "Application of mobile ad hoc networks", http://www.computingunplugged.com/issues/issue200409/00001371001.html.

[3] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Peit Demeester, "An overview of mobile ad hoc networks: applications and challenges", MAGNET project.

[4] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks", Computer, vol. 35, no. 10, pp. 54-62, 2002.

[5] G. S. Mamatha and Dr. S. C. Sharma "Analyzing the MANET Variations, Challenges, Capacity and Protocol Issues", International Journal of Computer Science & Engineering Survey (IJCSES), vol.1, no.1, August 2010.

[6] Irshad Ullah, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", Master Thesis, Blekinge Institute of Technology, June, 2010.

[7] Saurabh Gupta, Subrat Kar, S Dharmaraja, "BAAP: Black hole Attack Avoidance Protocol for Wireless Network", IEEE proceedings of the International Conference on Computer & Communication Technology (ICCCT), 2011.

[8] Irshad Ullah, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", Master Thesis, Blekinge Institute of Technology, June, 2010.

[9] K. SIVAKUMAR et.al.1366 www.ijcsmr.org. Overview of Various Attacks in Manet and Countermeasures For Attacks.

[10] S. Bansal and M. Baker, “OCEAN: Observation based cooperation enforcement in ad hoc networks”, *Technical Report*, Stanford University,

[11] Michiardi P, Molva R. “Core: a collaborative reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks”, In: Proc. of the sixth IFIP Conf. on Security Communications and Multimedia (CMS), 2002.

[12] S. Buchegger, “The CONFIDANT Protocol”, NCCR MICS Kick - off Meeting, February, 2002.

[13] Amos J Paul ,Vishnu K “Detection and Removal of Cooperative Black/Gray hole attack in Mobile Adhoc Networks”, International Journal of Computer Applications (ISSN NO. 0975 - 8887), vol. 1, no. 22, 2010

[14] Manel Guerrero Zapata, “ Secure ad hoc on-demand distance vector (SAODV) routing”, draft- querrero manet-saodv-03, Mobile Ad Hoc Networking Working Group, 17 March 2005.

[15] Q. He, D. Wu, P. Khosla, “SORI: A secure and objective reputation-based incentive scheme for ad hoc networks”, IEEE Wireless Communications and Networking Conference 2004.

[16] L. Tamilselvan, and V. Sankaranarayanan, “Prevention of Cooperative black hole Attack in MANET”, Journal of Networks, vol. 3 (5), pp.13-20, 2008.

[17] Jaydip Sen , Sripad Koilakonda, Arijit Ukil, “A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks”, IEEE Second International Conference on Intelligent Systems, Modeling and Simulation, 2011.

[18] Issa Khalil, Saurabh Bagchi, Ness B. Shroff “ LITEWORP : A Lightweight Countermeasure for the Wormhole Attack in Multi-hop Wireless Networks”, Proceedings of the International Conference on Dependable Systems and Networks (DSN), 2005

[19] Xin Jin, Yaoxue Zhang,Yi Pan, and Yuezhi Zhou “ZSBT:A Novel Algorithm for Tracing DoS Attackers in MANETs”, Hindawi Publishing Corporation EURASIP Journal on Wireless Communications and Networking vol. 2006.

[20] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao, Jiann-Liang Chen “CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture”, IEEE 2011.

[21] Dokurer, Semih.(2006) ”Simulation of Black hole attack in wireless Ad-hoc networks”. Master's thesis, Atılım University

[22] Raj PN, Swadas PB (2009) DPRAODV: A Dynamic Learning System against Black hole Attack in AODV based MANET. International Journal of Computer Science 2:54–59. doi: abs/0909.2371

Author Profile

Priyanka received her B.Tech degree in Computer Science from Guru Jambheshwar University of Science and Technology (GJU S&T), Hisar and also qualified GATE-2012 exam. She is pursuing her M.Tech in computer science from MITM Engineering College affiliated with GJU S&T. She has published a research paper in IJARCSSE journal.

Mukesh Dalal received her B.Tech degree from JCD, Sirsa and M.Tech degree in Computer Science from Chaudhary Devilal University (CDLU), Sirsa and also honours GATE-2012 exam qualified. She is now assistant professor at MITM engineering college, Hisar. She has published a research paper in IOSR journal and presented two review papers in various conferences.