Volume 9, Issue 1
February 2020

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X



# Detection And Isolation Of Sinkhole Attack In Manet

**[1] Rajwinder singh, [2] Dr. Paramjeet Singh and [3] Dr. Shveta Rani**

[1]Department of Computer Science And Engineering, Mtech Student GZSCET, Bathinda

[2]Department of Computer Science And Engineering, Professor GZSCET, Bathinda

[3]Department of Computer Science And Engineering, Professor GZSCET, Bathinda

E-mail: [1] rajwindersinghhusnar@gmail.com, [2]param2009@yahoo.com, [3]garg_shavy@yahoo.com

## ABSTRACT

Wireless MANET (Mobile AdHoc Network) is category of radio network where collection of radio nodes can join and leave the network at any time without any permission. These nodes are capable of communicating to nodes which are in the communication range of each other and other nodes by means of their contiguous nodes in their radio range. As MANET automatically configurable network hence the topology of the network changes time to time depending on the behavior of nodes. Density of the network depends upon the practice where network is used. MANET is more exposed to various types of security threats from the affected nodes in the network such as Sinkhole attack, blackhole attack, warmhole attack, greyhole attack etc. Sinkhole is attack where affected node showcases him having latest or the soonest route to the target and get all data towards it. In this paper we have specify a more efficient way to detect the sinkhole attack and also the simulation results which shows that the proposed scheme is more reliable and efficient.

## 1. INTRODUCTION

A wireless AdHoc network called as MANET is collection of tiny radio nodes which can exchange the packets of information using the radio link between them. Because MANET has no base architecture, decentralized control and nodes cooperation functionality it is prone to many types of security attack. Attacks can be classified to Main category:-

- **Passive attack:-**In this category of attack the compromised node snoops the data packets transmitted between the sender and receiver without disturbing the normal process of the network and it does not modify the data packets so only break the confidenality of the network. Due their silent nature these category of attack are difficult to detect and can make road map to other type of attacks.

1. Eavesdropping: - Eavesdropper can fetch the packet information like routing.
2. Data, public key, key design pattern which can be further used to do a unintentional act to compromised the security of the network.
3. Snooping:-Snooping is just like the eavesdropping but different in the sense that it does not necessary to collect the data while it is travelling over the network but one can also make use of programs that can send the data back to remote user or it can make use of the user screen to steal the information.
4. Traffic analysis:-In this type of attack, attacker analyze the traffic to know about the sender and receiver, network size, packet size and their frequency.

- **Active attack:-** These attack are more dangerous because attacker try to disturb the routine functioning of the network .Attacker can get the packets change the information, make fake routing packet.

1. Sinkhole attack:-Sinkhole attacker node pretend to itself having shortest route or latest route to the destination s as to attract network traffic towards it.
2. Sybil attack:-Sybil attack where a nodes can show multiple fake identities so highly dangerous. For example in Automated VAN traffic network it can used to show multiple fake identities in the road and divert the traffic.
3. Flooding attack:-In this type attack the compromised node try to waste the network resource by transmitting fake packets and make nodes busy hence consume their energy and reduce the network bandwidth.
4. Greyhole attack:- This is routing misbehavior type attack where one node publicize it having legitimate route to the destination and then start dropping the data packets when the packet comes to it.
5. Link spoofing:-The attacker node advertise itself as it has links to non neighbor nodes and in the network hence provide fake routing information.
6. Jellyfish Attack:-In this attack the attacker node first try to gain access to the network and if it gains access it try to receive the packet and forward after some delay so as to introduces high end to end delay in the network.
7. Byzantine attack:- A Compromise node or set of compromise intermediate nodes work together to carry out a attack as creating routing cycles, forwarding data through long paths, so it radiuses the network performance.[1][2][3]

Volume 9, Issue 1
February 2020

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X



## 2. STUDY OF SINKHOLE ATTACK

In order to implement sinkhole attack in AODV attacker can make use hop count and packet sequence no so as to falsely claim himself as shortest route to the destination or having latest route to target destination. Main intention of the attacker is to draw traffic towards him so as to cry out malicious activity such dropping the data packet, reading the data packet, modifying the data packet, analysis of network traffic ,implementing denial of service attack by receiving the packet and not forwarding to next node in the path or to the destination.

There are generally two ways launch a Sinkhole attack:-

1. **Augmented Sequence number: -** Sequence number in AODV represents the life of a packet. Each time when packet flow from one node another it is increased by one. Higher the sequence number more time it will stay in the network. Attacker with malicious intention will enhance the sequence no (multiply it with a certain no) and broadcast the route request packet to its neighbor nodes, neighbor will identify that the sequence number of these packet is higher than other route request packet so they will assume it is latest route or the fresh route request and respond to route packet sent by the attacker.

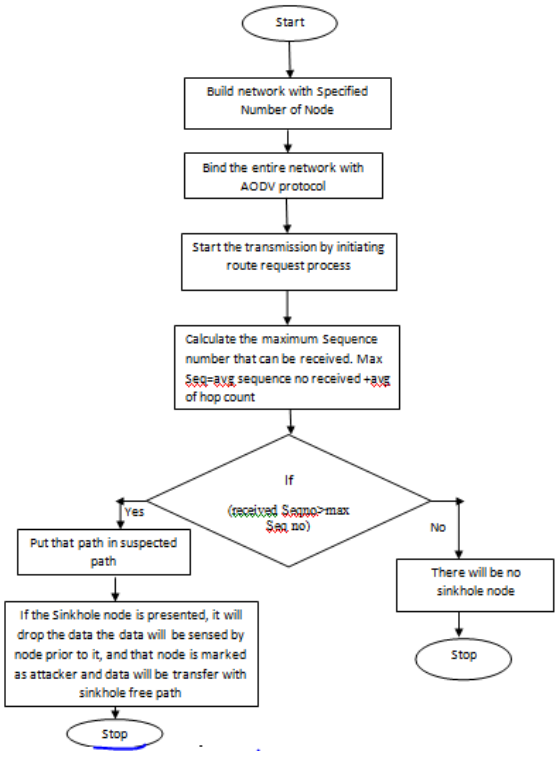
2. **Least Hop count: -** Decreasing the hop count is another way to attract network traffic on receiving the route packet the attacker node will decrease the hop count value instead of increasing it by one .it falsely claim that it will have shortest route to the destination.

## 3. RELATED WORK

Lakshmi Agarwal et. al [2] presented a sinkhole detection scheme .They suggested that when the source node receives the route replies, it will analyze the nodes in the path claiming the route to destination node. It says that if the next hop of the node (that claims it has route to destination) is destination node, then the node is malicious. Khushboo Tunwal,Priyanka Singh Dabi and Pankaj Sharma[5] "an individual trust management technique for mitigating sinkhole attack in MANET" presents a trust based scheme based on their behavior in the network. Nodes make use of their power of promiscuous mode to check whether the nodes are moving the packet forward, dropping and etc. Nisarg Gandhewar and Rahila Patel[6] "detection & prevention of sinkhole attack on aodv protocol in mobile AdHoc network" make use of difference between the current route request sequence no and previous route request sequence no if the difference is too large or more than a threshold value than the intermediate source of this route request is considered as malicious. Rajakumar P, Prasanna venkatesan T and Pitchaikkannu A[7] provide a survey paper on the various passive and active security attacks in MANET and network layer where these attacks are implemented. This paper also discusses the detection scheme for various types of attack. Priyanka Sharma, H.P. Sinha, Ph.D, and Abhay Bindal[8] proposed a cryptography based technique to exchange a secret key to encrypt the packet at each level and decrypting the packet and matching the secured secret key in AODV environment.

## 4. PROPOSED ALGORITIHM

The source node will follow the traditional AODV to find route to destination node. It will broadcast the RREQ packets to find route to destination node. All the nodes that receive the RREQ packet will rebroadcast it, until it reaches the destination node. When the destination node receives the route request, it will send route replies to the source node. Along the route replies, any node which is sink hole can augment the sequence number abruptly such that received sequence number at the source node is higher than other nodes in other paths. When the route reply reaches the source node, it will compute the maximum sequence number which it should receive. It should be equal or less than to the average sequence number at the destination node added with the average number of hops of the paths. Because at each node in the path, the sequence number is incremented by 1. If for any path, the source node finds that the received sequence number is greater than desired sequence number, then the source node will put the entire path in the suspected list. To detect sinkhole node in that particular path, the source node would now send few data packets over this path. If there will be sink hole node on this path, the node will drop the received packets. The node (which is prior to the sink hole node) in the path can sense the dropped packets in the promiscuous and reply back to the source node about the same. The source node can then send data to the destination over the another path that does not contains any sink hole node.




Flowchart of Proposed scheme

Volume 9, Issue 1
February 2020

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X



## 5. SIMULATION RESULTS

Implemented in network simulator 2.35. This is an open source simulator which can be used for the simulation of wireless ad hoc networks, vehicular ad hoc networks and wired networks as well. The network was also tested under the effect of sink hole attack with 60 and 70 nodes respectively. The parameters which were considered for the simulation of the network are shown in the table below:

| Parameter & values | Parameters & Values |
|---|---|
| Channel-Wireless | Initial Energy-60 Joules |
| Mac-802.11 | Network area-1200*1200 sq meters |
| Propagation-Two ray ground | Routing Protocol-AODV |
| Antenna-Omni directional | Number of nodes-60,70 |

**Network Performance Matrices (In 70 nodes scenario):-**

**Throughput: -** Throughput is the no of packet received by destination in per unit of time.
Throughput= no packet received/unit time. Throughput is calculated as received throughput in bit per second at the traffic destination

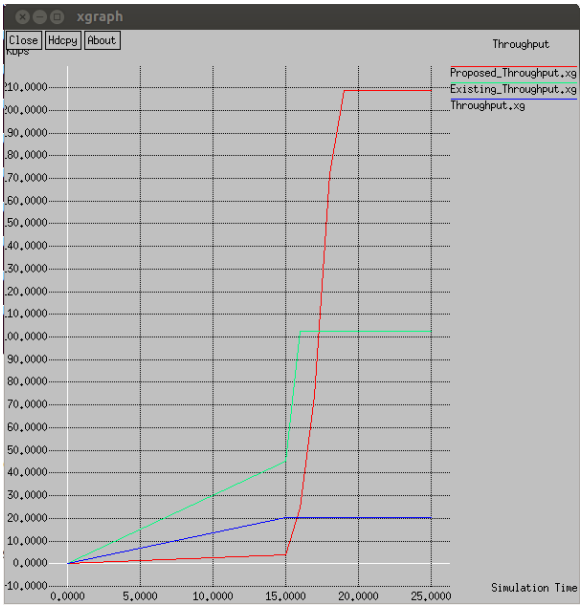



Figure no- 1 Throughput (70 nodes)

The above figure shows the comparison of the throughput for three scenarios. The throughput for the proposed scheme was found to be 208 Kbps and for the existing scheme was 102 Kbps. However, under the attack the value of throughput was 20 Kbps.

**End to End delay: - start time –receive time**

**Start time: -** it is time when the packet is send by the sender.
**Receive time: -** it is the time when the packet is received by intermediate or final receiver.

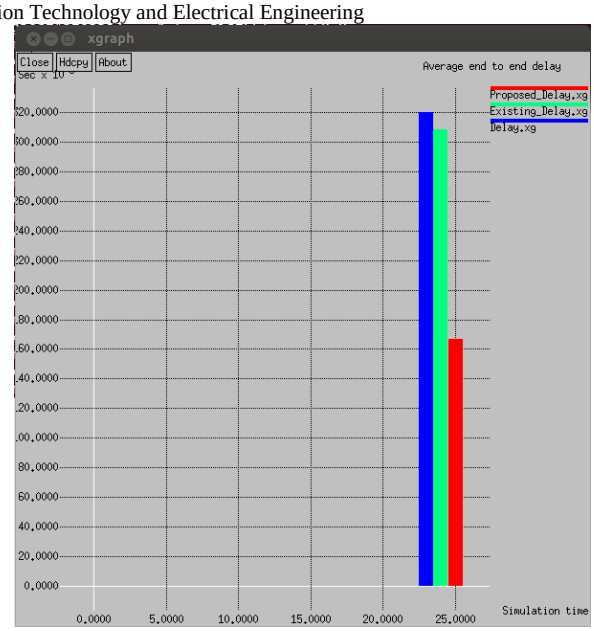



Figure no-2 End to End delay (70 nodes)

The above figure shows the comparison of the delay for three scenarios. The delay for the proposed scheme was found to be 0.16 seconds and for the existing scheme was 0.30 seconds. However, under the attack the value of delay was 0.32 seconds.

**PDR Packet delivery ratio:-**

PDR=No of packet sent /no of packet received.


Figure no.3 Packet Delivery Ratio (70 nodes)

The above figure shows the comparison of the packet delivery ratio for three scenarios. The packet delivery ratiofor the proposed scheme was found to be 0.77 and for the existing scheme was 0.62. However, under the attack the value of packet delivery ratio was 0.57. The packet delivery ratio values for all the scenarios have shown a slight decrease towards the end. For the scenario under attack, the sinkhole node drops the packets leading to decrease in the value of packet delivery ratio. The existing scheme as it gets some time

Volume 9, Issue 1
February 2020

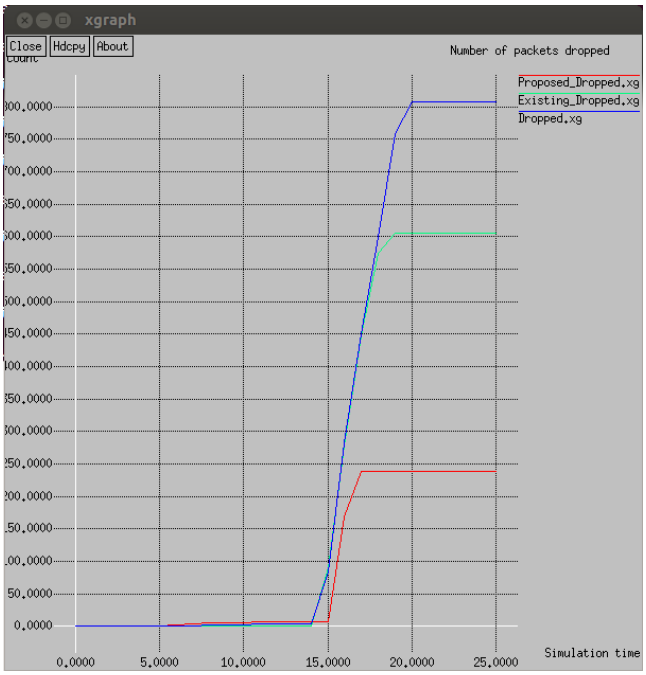
ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X



to detect the attacker. The proposed scheme, the test packets are sent over the suspected paths containing the attacker node. Therefore, drop in the test packets leads to fall in the graph for packet delivery ratio. But after detection when data is sent over the new path packet delivery ratio increases.

**Packet Dropped:-**




Figuer no.5 Packet Dropped(70 nodes)

The above figure shows the comparison of the number of packets dropped for three scenarios. The number of packets dropped for the proposed scheme was found to be 239 and for the existing scheme were 605. However, under the attack the value of number of packets dropped was 808.

**Network Performance Matrices (60nodes):-**

**Throughput:-**

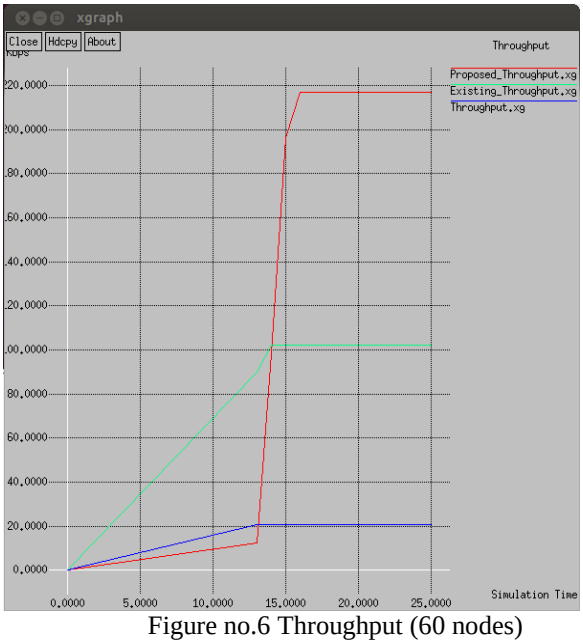



Figure no.6 Throughput (60 nodes)

The above figure shows the comparison of the throughput for three scenarios in network for 60 nodes. The throughput for the proposed scheme was found to be 217 Kbps and for the existing scheme was 102 Kbps. However, under the attack the value of Throughput was 20.48 Kbps.

**End to End Delay:-**

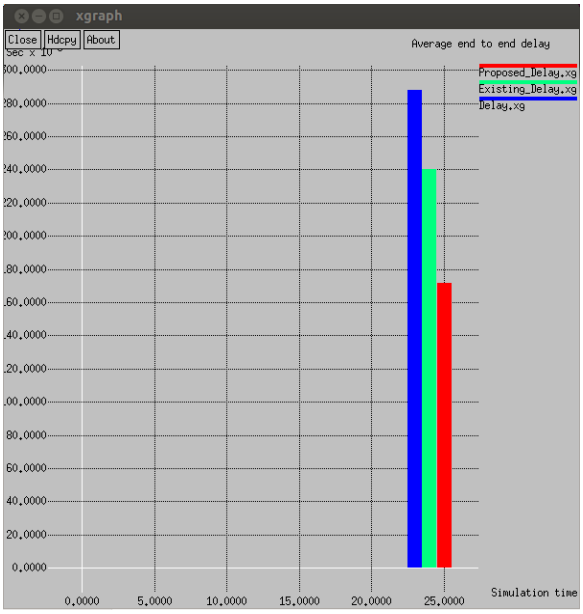



Figure no.7 End to End Delay (60 nodes)

The above figure shows the comparison of the delay for three scenarios in network for 60 nodes. The delay for the proposed scheme was found to be 0.17 seconds and for the existing scheme was 0.24 seconds. However, under the attack the value of delay was 0.29 seconds.

**Packet Delivery Ratio:-**

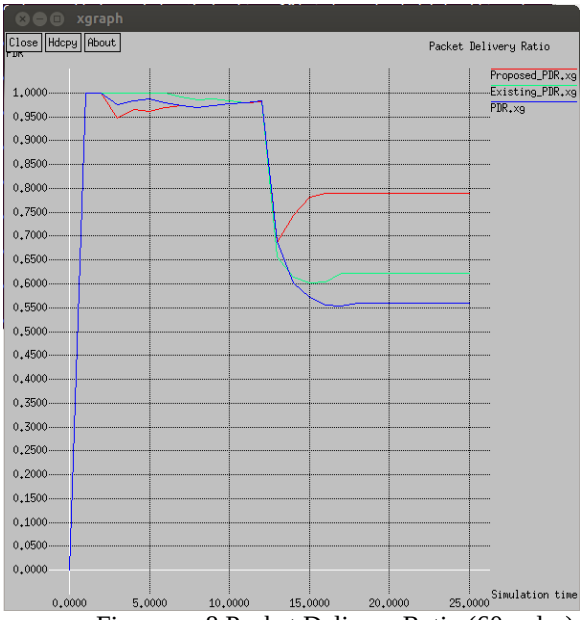



Figure no.8 Packet Delivery Ratio (60nodes)

The above figure shows the comparison of the packet delivery ratio for three scenarios in network for 60 nodes. The packet

Volume 9, Issue 1
February 2020

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X



delivery ratio for the proposed scheme was found to be 0.79 and for the existing scheme was 0.62. However, under the attack the value of packet delivery ratio was 0.56.

**Number of Packet Dropped:-**

The next figure shows the comparison of the number of packets dropped for three scenarios in the network for 60 nodes. The number of packets dropped for the proposed scheme was found to be 141 and for the existing scheme were 578. However, under the attack the value of number of packets dropped was 761.

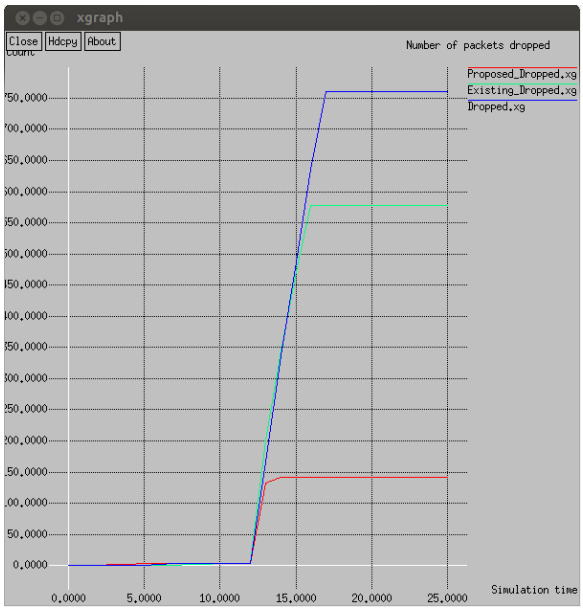



Figure no.8 Packet Dropped (60nodes)

## 6. CONCLUSION

In proposed scheme nodes have to store additional information such as sequence numbers stored with themselves. In future, such values can be stored at some IDS nodes and detection procedure can be carried out by them. Also, other attacks such as wormhole attack or grey hole attack can also be explored in this work in near future

## REFERENCES

[1] Sandeep Kumar1, Col. (Dr) Suresh Kumar "Study of MANET: Characteristics, Challenges, Application, Routing Protocol and Security." In International Journal Of R&D In Engineering, Science And Management, Vol.2, Issue 5, July 2015, Impact Factor-0.439, p.p.266-274, ISSN 2393-865X.

[2] Lakshmi Aggarwal, Rakhi Khandelwal, Pankaj Sharma and Sandeep Sharma, "Analysis of Detection Algorithm of Sinkhole Attack of QoS on AODV for MANET" 2nd International Conference on Next Generation Computing Technologies, 2016.

[3] Ch. Rajya Lakshmi, U. Suresh Kumar "Analyzing the Detection of Active Attacks in MANETs" in international Journal of Electronics Communication and Computer Engineering Volume 4, Issue (6) NCRTCST-2013, ISSN 2249–071X.

[4] Khushboo Tunwal,Priyanka Singh Dabi and Pankaj Sharma "An Individual Trust Management Technique for Mitigating Sinkhole Attack in MANET" in International Journal of Computer Applications (0975 – 8887) Volume 95– No.24, June 2014.

[5] Nisarg Gandhewar and Rahila Patel "detection & of sinkhole attack on aodv protocol in mobile adhoc network" in International Journal of Computer Applications (0975 – 8887) Volume 95– No.24, June 2014.

[6] Rajakumar p, Prasanna venkatesan t and Pitchaikkannu "security attacks and detection schemes in MANET" in International Conference on Electronics and Communication Systems (ICECS) , DOI10.1109/ECS.2014.6892808 feb 2014.

[7] Priyanka Sharma, H.P. Sinha, Ph.D, and Abhay Bindal "Detection and Prevention against Wormhole Attack in AODV for Mobile Ad-Hoc Networks"in International Journal of Computer Applications (0975 – 8887) Volume 95– No. 13, June 2014.

## AUTHOR PROFILES

i. **Rajwinder Singh** received a degree of information technology from IKGPTU, Jalandhar in 2017. He is research student of Computer Science. Currently he completed post graduation from MRSPTU Bathinda in 2019.

ii. **Prof. (Dr) Paramjeet Singh** did B. Tech. in Computer Science and Engineering from SLIET, Longowal, Punjab. He did Masters' and Ph.D. in Computer Science and Engineering from BITS, Pilani, India. He started his professional career as lecturer in the dept. of Computer Science and Engg of GZSCET, Bathinda in 1998. Presently, since 2011, he is working as Professor at GZSCCET MRSPTU, Bathinda. There are 70 research papers to his credit in various International refereed Journals. His research interest includes Computer Networks, Computer Graphics, and Software Engineering. He has guided 7 PhD candidates and 42 M.Tech. Thesis.

iii. **Prof. (Dr) Shaveta Rani** did B. Tech. in Computer Science and Engineering from SLIET, Longowal, Punjab. He did Masters' and Ph.D. in Computer Science and Engineering from BITS, Pilani, India. He started his professional career as lecturer in the dept. of Computer Science and Engg of GZSCET, Bathinda in 1998. Presently, since 2011, he is working as Professor at GZSCCET MRSPTU, Bathinda. There are 67 research papers to his credit in various International refereed Journals.He has guided 7 PhD candidates and 28 M.Tech. Thesis.