Cluster based Detection and Reduction Techniques to Identify Wormhole Attacks in Underwater Wireless Sensor Networks

Tejaswini R Murgod[1]
Research Scholar, Department of Computer Science and Engineering, GSSSIETW, Mysuru
Affiliated to VTU Belagavi, India

Dr. S Meenakshi Sundaram[2]
Professor and Head, Department of Computer Science and Engineering, GSSSIETW,Mysuru
Affiliated to VTU Belagavi, India

***Abstract*—Underwater Wireless Sensor Networks (UWSN) is widely used in variety of applications but none of the applications have taken network security into considerations. Deployment of underwater network is a challenging task and because of the hash underwater environment, the network is vulnerable to large class of security attacks. Recent research on underwater communication focuses mainly on energy efficiency, network connectivity and maximum communication range. The nature of underwater sensor network makes it more attractive for the attackers. One of the most serious problems in underwater networks is wormhole attack. In this research work we concentrate on providing security to the underwater network against wormhole attacks. We introduce the wormhole attack in the network and propose a solution to detect this attack in underwater wireless networks. Energy Efficient Hybrid Optical - Acoustic Cluster Based Routing Protocol (EEHRCP) is incorporated and using the round trip time and other characteristics of wormhole attack, the presence of the wormhole attack in the network is identified. The simulation results depicts that the proposed wormhole detection mechanism increases throughput by 26%, reduces energy consumption by 3%, reduces end to end delay by 13% and increases packet delivery ratio by 3%.**

***Keywords*—Underwater communication; wormhole attack; round trip time; EEHRCP**

I. INTRODUCTION

UWSN are used for variety of applications like military, pollution monitoring, disaster maintaining etc. Because of the hash underwater environment, fast node mobility, water pressure, temperature, salinity, lack of topology make them vulnerable to large range of security attacks. Traditional security mechanism cannot be applied to underwater network because they are heavy and require large number of computations. Underwater nodes are less energy efficient and the energy level of the nodes get drained due to movement, so nodes cannot waste their energy level in large computation to provide security against attacks [1-2].

Underwater channel have some special characteristics that makes it different from other sensor networks. These characteristics are listed below.

- Nodes battery level, memory space is limited, and nodes batteries cannot be easily recharged.
- UWSN are self-configuring and self-organizing as the node mobility is high and they drift with water.
- The topology changes rapidly.
- The control of sensor nodes is centralized which is located near the shore so that it can be easily located using GPS and it can be easily replaced in case of occurrences of any faults.

UWSN are vulnerable to large kind of attacks. These attacks can be classified as data security attacks, Denial of Service (DOS) attack, replication attack and physical attacks [3]. Among these DOS attack is a serious threat as this attack is a passive attack. It does not make any changes to the data but simply degrades the network and both throughput and performance are reduced. The various DoS attacks are listed below.[4].

- Jamming: It is a type of DoS attack where the intruder disturbs communication by corrupting valid packets or by simply sending excess packets in order to drain the energy level of the nodes.
- Wormhole attack: In this type of attack the intruder creates a virtual path that creates an illusion to the neighbouring node that it is the shortest and efficient route. When the nodes transfer the packets through the tunnel it simply drops or corrupt the packets. Here the attackers need not the cryptographic concepts, encryption methods. It just simply needs to monitor the data transfer and just corrupt the packets.
- Spoofing attack: In this type of attack the attacker gets the ID of the legitimate node and then floods the network with broadcast and acknowledgement packets with the spoofed ID. This type of attack difficult to detect quickly as the attacker uses the legitimate node ID for spoofing [5].
- Sybil attack: In this type to attack the attacked node appears at different locations at a particular time instance. This attack degrades the routing technique used in the network.
- Selective forwarding attack: It is an attack where the attacker targets the important anchor node or central

authority node and tries to flood the node with large number of request packets. Due to which the anchor node energy level degrades quickly and node fails. This results in reduced throughput because all other sensor nodes take help of anchor node for communication [6-8].

Fig. 1 depicts the different DoS attacks in UWSN.

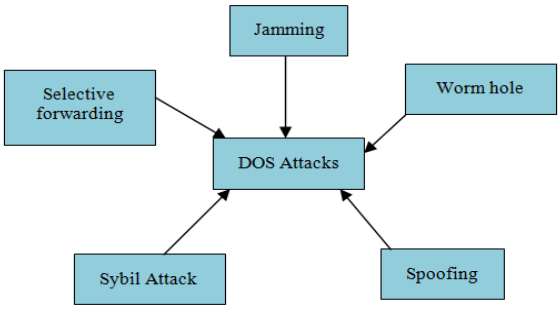

Fig. 1. Types of DOS Attacks.

In this research work we propose a methodology for identifying the wormhole attack in UWSN. The major contribution of our work can be summarized as below.

- To identify the intruder node that performs wormhole attack in the network.
- We propose a cluster based approach to detect wormhole attack.
- Simulation of the proposed algorithm is performed and compared with the existing methodologies.

The organization of the paper is as follows: Section 2 reviews the related work. Section 3 describes the wormhole detection algorithm. Section 4 presents the simulation evaluation of the proposed methodology. Conclusion and summary of research work are presented in Section 5.

II. Related Work

Wormhole attack is the route constructed by the intruder between the source and destination with less delay and high bandwidth than any other routes. Fig. 2 depicts the wormhole attack. Here a malicious node constructs the wormhole link and inform the nodes that it is the fastest and shortest link. The nodes believe that the wormhole link is shortest and thus transfer the data packets through the wormhole link. The malicious node need to just monitor the link for the packets and it then drops the packets or discards the packets as and when node transfers them [9].

Distributed wormhole attack detection is proposed by Yurong Xu, where the node calculates the hop count to its neighboring nodes. It than finds the shortest path to construct the local map. Distortion in local map is identified to detect the wormhole attack. The diameter feature is used identify wormhole link. A threshold is defined for the diameter when the node identifies that the diameter of the network cross the threshold than it immediately identifies the presence of the wormhole attack. The simulation results depicts that the proposed methodology can detection rate is around 80% and has low false alarm rate [10].

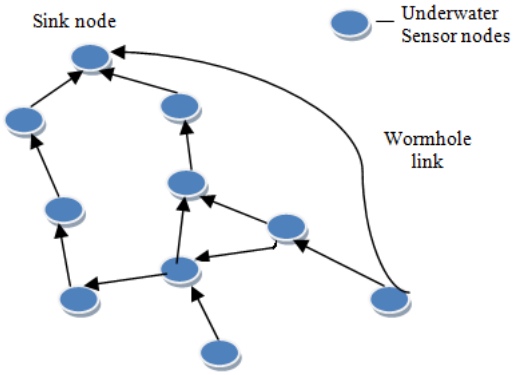

Fig. 2. Scenario for Wormhole Attack.

Rupinder Singh presents a watch dog concept based hybrid wormhole detection model where packet drop and delay at each hop is considered for detecting wormhole attack. At the time of route discovery the probability of wormhole presence is also calculated, using which packet loss probability of a node is calculated and then packet loss probability for the entire route is calculated. These probability values are used to take a decision regarding existence of wormhole attack [11].

Parmar Amish et al. proposes a solution to wormhole attack where each node maintains the routing table which consists of information about all the neighboring nodes. Before sending a packet the node checks the routing table for route information, if route information is not found than it sends a request packet and waits for reply. The destination node on receiving request packet sends back the reply packet through the same route from where it received request packet. The sender if it receives more than one reply packets it identifies that there are more than one route. Sender node than calculates the round trip time and compares it with the defined threshold, if RTT is less than threshold it identifies the wormhole attack and drops such routes [12].

Mousam A. Patel et al. proposes a wormhole detection methodology using promiscuous method and Packet Leashes methods. In promiscuous method a watchdog node continuously monitor the network it verifies the packet sent by sender and then forward it to over the route and silently watch the movement of packet. Packet leashes use the geographical location of the node and require the awareness of the location of the nodes. The methodology also uses the RTT to suspect the presence of the wormhole tunnel than the trusted neighbor nodes helps the source node to detect wormhole within the network [13].

He Ronghui et al. proposes a wormhole detection mechanism using beacon nodes. A distributed algorithm is proposed where the beacon nodes play the role of the detector. The job of the sensor nodes is to maintain the hop count with the neighboring nodes. The beacon node continuously sends an alarm message to the base station. The base station responsibility is to start the detection method and take necessary actions when attack is detected. The simulation is run by considering around 250 nodes. The proposed methodology does not require additional hardware or manual setup. It can also locate the wormhole location with minimum localization error [14].

III. Proposed System

In this section the proposed wormhole detection algorithm is discussed. The Energy Efficient Hybrid Optical - Acoustic Cluster Based Routing Protocol (EEHRCP) [15] is used as the underlying network topology. The Cluster Head (CH) plays an important role within the network. To reduce the load of the CH node a two layered approach is used. The sensor nodes are placed randomly deep inside the sea. The job of the sensor nodes is to sense the data and transform it to the CH. The CH collects all the data aggregates it and then forwards it to the surface buoys. The surface buoy communicates with the base stations where the processing of the sensed data takes place. The CH selection procedure is same as in EEHRCP. The layered approach of the network is shown in Fig. 3.

To monitor the malicious activity in the network an additional Guard Node (GN) is considered. The main purpose of utilizing the GN is to monitor the clusters and report the CH if any malicious activity found within the network. The GN is used to reduce the burden of the CH as it has to monitor the sensor nodes. When the GN informs the CH about the malicious activity, the CH has to take certain action against the intruders. The nodes underwater are critical and the energy level of the nodes should be maintained as it is very difficult to recharge the batteries of the nodes underwater. In order to save the energy level of the CH the outer layer CH2 is used to take actions against malicious activity. It is the responsibility of the CH2 to inform all the inner level nodes about the malicious activity in the cluster.

A. Wormhole Detection Methodology

In the proposed system each node maintains the following information

- Round Trip Time (RTT) which is the time from the source sending the packet till it receives an acknowledgement.
- Based on the hop count between source and destination the expected time of delivery ETD is estimated.
- A threshold value is set (Th) in order to tolerate the lost packets.
- Number of packets sent and received from source S to destination D is also maintained as PSent and PReceived.

Fig. 4 depicts the detection method.

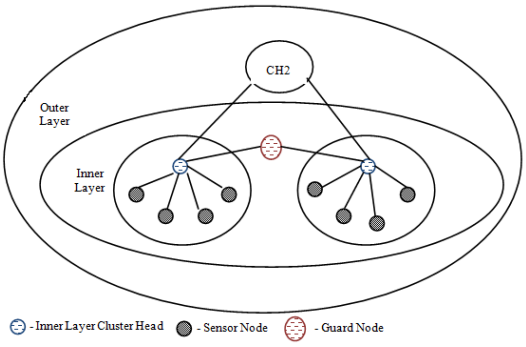

Fig. 3. Layered Approach of the Network.

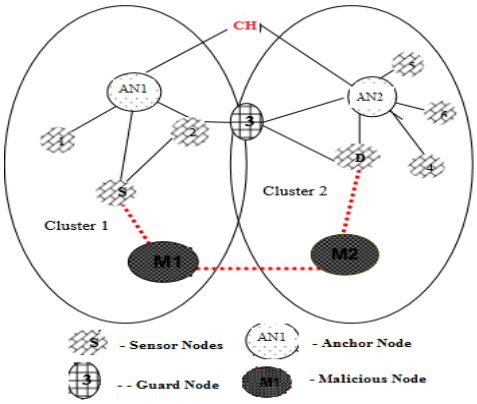

Fig. 4. Cluster based Detection Method.

In Fig. 4 source S from cluster1 wants to send data packet to Destination D in cluster2. It fetches the route from its routing able via node 2 and 3. As node 3 is closer to both the cluster it is chosen as the guard node. The malicious node M1 hears the communication from S and immediately informs other malicious node M2 from cluster2. As node 3 is chosen as guard node it keeps on monitoring the communication, when it suspects some malicious activity it immediately informs the CH. The detailed algorithm is discussed below.

B. Wormhole Detection Algorithm

Wormhole Detection Algorithm

Step 1: Nodes are deployed, CH is selected and the node that is nearest to both the cluster is chosen as guard node.

Step 2: S node sends a HELLO packet to D and initiates its timer t1.

Step 3: PSent = PSent +1.

Step 4: S stops timer at t2 when it receives ack from D and Calculate ETD = t2 - t1

Step 5: once connection is established S starts sending data packets and initiated timer td1 and stops at td2 when ack is received.

Step 6: Calculates RTT = td2 – td1

Step 7: if RTT < ETD

Step 8: then guard node calculates

P = PSent (S, D) – PReceived (S, D)

Step 9: Threshold (Th) = Average RTT / No . of hops

Step 10: if P > Th then

Step 11: inform CH2 regarding malicious activity.

Step 11: CH2 informs S to discard the route through M1 and follow other outer to reach D

Step 12: End

IV. Simulation and Result Discussions

In this section the simulation results for various network parameters like throughput, energy consumption, end to end delay and packet delivery ratio. The network settings and performance evaluation are also discussed.

A. Environment Settings

The environment settings used for simulation are provided in Table I.

Initially the normal EEHRCP Algorithm results are considered and the wormhole node is added in the network. The results are noted after injection of the malicious node. The proposed methodology is applied to the malicious network and the results are compared for all the three scenarios.

Table II depicts values of network throughput. Fig. 5 shows the comparison of network throughput with all the three protocols. The wormhole attack decreases the network throughput as the malicious node continuously drops the packets and degrades the throughput of the network by 48%. By applying the wormhole detection algorithm the throughput is further increased by 26%.

TABLE I. Parameters used in EEHRCP

Parameters	Value
Network Area	1000*2000 m3
Routing Protocol	EEHRCP
No of nodes	500
Min distance between nodes	80 m
Number of sectors	16
Sensor node initial energy	10 kJ
Transmission power	2.8 w
Channel bandwidth	10 kHz
Depth	2.0 km
Mobility Model	Fixed

TABLE II. No. of Nodes vs. Network Throughput

No. of Nodes	Network Throughput (kbps)		
	Normal EEHRCP	Wormhole EEHRCP	Proposed EEHRCP
50	60	20	30
100	110	50	80
150	150	90	110
200	160	95	130
250	198	90	135
300	295	100	150
350	350	150	250
400	400	190	325
450	410	225	340
500	430	240	392

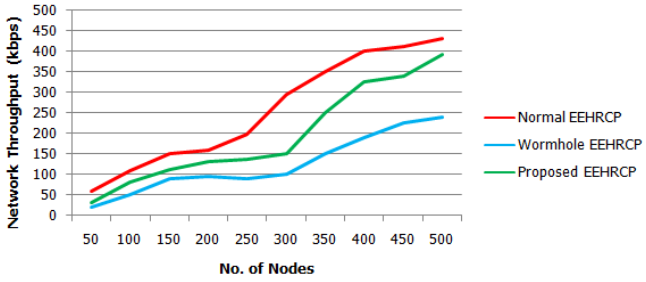

Fig. 5. Comparison of Network Throughput.

Fig. 6 shows the comparison of energy consumption and the values are depicted is Table III. As the nodes underwater are crucial and it is very difficult the recharge the battery of the sensor nodes, the energy level of the nodes should be efficiently utilized. The inclusion of the wormhole node within the network decreases the energy level of the node by 15%. Proposed wormhole EEHRCP detection algorithm further decreases the energy consumption of the node by 3% when compared with wormhole EEHRCP.

End to end delay is the time taken by the packets to reach the destination. Table IV depicts the end to end delay values and, Fig. 7 shows the comparison of end to end delay of all the three methodologies. When the wormhole attack is applied on the network the delay is increased as the malicious node corrupt or drops the packets because of which the packets do not reach the destination node. There is an increase by 16% in the delay when the network is affected by wormhole. The proposed methodology detects the wormhole attack and further reduces the delay by 13%.

The ratio of packets generated by packets delivered is packet delivery ratio, Table V depicts the paket delivery ratio and, Fig. 8 depicts the comparison of packet delivery ratio. The wormhole attacked system decreases the delivery ratio by 11% as the main intension of the malicious node is to ensure that the packets are not reached to the destination node. Further the proposed methodology identifies the attack and further increases the delivery ratio by 4% when compared to the attacked system.

TABLE III. No. of Nodes vs. Energy Consumption

No. of Nodes	Average Energy Consumption (Joules)		
	Normal EEHRCP	Wormhole EEHRCP	Proposed EEHRCP
50	100	300	150
100	120	382	200
150	220	430	350
200	300	490	420
250	320	485	460
300	400	610	500
350	590	740	652
400	710	895	752
450	700	925	772
500	650	950	790

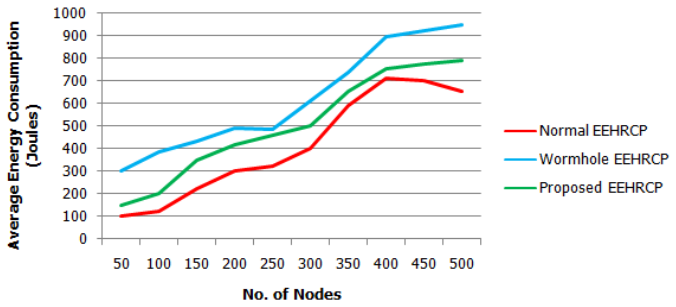

Fig. 6. Comparison of Energy Consumption.

TABLE IV. NO. OF NODES VS. END TO END DELAY

No. of Nodes	End-to-End Delay (seconds)		
	Normal EEHRCP	Wormhole EEHRCP	Proposed EEHRCP
50	10	15	13
100	8.5	12.8	11
150	6.2	10.6	8.7
200	4.8	8.2	7.6
250	4	7.4	6.3
300	3.6	6.2	4.3
350	3.8	6	5.6
400	3.4	5.8	4.3
450	3	5.6	4.2
500	2.5	5.8	4

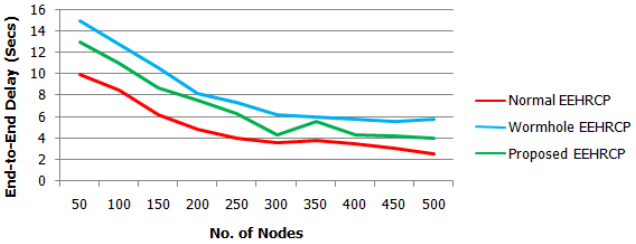

Fig. 7. Comparison of End to End Delay.

TABLE V. NO. OF NODES VS. PACKET DELIVERY RATIO

No. of Nodes	Packet Delivery Ratio		
	Normal EEHRCP	Wormhole EEHRCP	Proposed EEHRCP
50	8.2	5.2	6.5
100	8.9	5.4	6
150	9	5.8	7.5
200	9.8	6.3	8.3
250	10	7.2	8.5
300	10.4	7.3	8.9
350	10.8	7.6	9.2
400	11.3	7.6	9.3
450	12	7.9	9.6
500	12.3	8.5	9.7

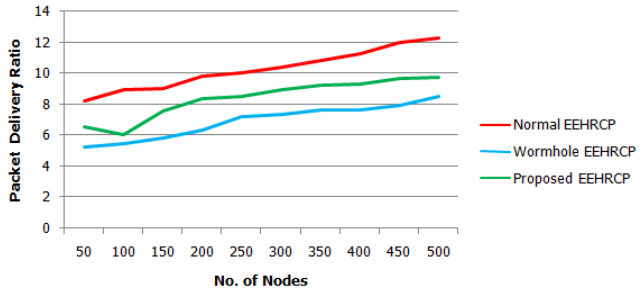

Fig. 8. Comparison of Packet Delivery Ratio.

V. CONCLUSION

One of the applications of underwater communication is military where the secret information is sent through underwater nodes, so security is the important feature that needs to be considered. Providing security to the underwater nodes is a challenging task because of the harsh underwater environment. As the nodes continuously drift with the water the network topologies continuously changes and energy of the node degrade quickly due do which managing nodes becomes challenging.

In this research work we propose a solution to the wormhole attack in the underwater communication system. Wormhole is a passive attack where the attacker need not know the encryption keys information. All that the attacker does is simply sit and listen the network for communication and then make feel the sender that the route through malicious node is a shortest path to reach the destination. As the source always chooses the shortest distance to reach the destination and forwards the packets to the malicious node. The malicious nodes simply drop or corrupt the packets send by the sender which degrades the overall performance of the network.

The wormhole attack is applied to EEHRCP algorithm and the simulation results show the comparison of Normal EEHRCP, wormhole attacked EEHRCP and proposed EEHRCP. According the simulation results the throughput is increased by 26%, energy consumption is reduced by 3%, end to end delay is reduced by 13% and packet delivery ratio is increased by 3% when compared with the wormhole affected EEHRCP algorithm.

REFERENCES

[1] P. V. Venkateswara Rao, N. Mohan Krishna Varma and R. Sudhakar, "A Systematic Survey on Software-Defined Networks, Routing Protocols and Security Infrastructure for Underwater Wireless Sensor Networks (UWSNs)", Springer Nature Singapore Pte Ltd. 2020, 551-559.

[2] Tooska Dargahi, Hamid H. S. Javadi, Hosein Shafiei, "Securing Underwater Sensor Networks Against Routing Attacks", Wireless Press Communications, 2017, 1-18.

[3] Guang Yanga, Lie Daia, Guannan Sia, Shuxin Wanga, Shouqiang Wanga, "Challenges and Security Issues in Underwater Wireless Sensor Networks", International Conference on Identification, Information and Knowledge in the Internet of Things, IIKI, 2018, 210-216.

[4] Yanping Cong, Guang Yang, Zhiqiang Wei, Wei Zhou, "Security in Underwater Sensor Network", International Conference on Communications and Mobile Computing, 2010, 162-168.

[5] S. Misra, S.Dash, M Khatua, A V Vasilakos, M S Obaidat, "Jamming in underwater sensor networks: detection and mitigation", IET Communications, vol 6, issue 14, 2012, 2178-2188.

[6] Guang Yang, Zhiqiang Wei, Yanping Cong, Dongning Jia, "Analysis of Security and Threat of Underwater Wireless Sensor Network Topology", Fourth International Conference on Digital Image Processing, 2012, SPIE vol 8334, 1-4.

[7] Guangjie Han, Jinfang Jiang, Ning Sun, and Lei Shu, "Secure Communication for Underwater Acoustic Sensor Networks", IEEE Communication Magazine, 2015, 54-60.

[8] Haifeng Jiang, Yi Xu, "Research advances on Security Problems of Underwater Sensor Networks", Advanced Materials Research, Vol 317-319, 2011, 1002-1006.

[9] Mari Carmen Domingo, Barcelona Tech University, "Securing Underwater Wireless Communication Networks", IEEE Wireless Communications, 2011, 22-28.

[10] Yurong Xu, Guanling Chen, James Ford and Fillia Makedon, "Detecting Wormhole Attacks In Wireless Sensor Networks", International Federation for Information Processing, Volume 253, 2008, 267-279.

[11] Rupinder Singh,Jatinder Singh,and Ravinder Singh, "WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks", Hindawi Publishing Corporation Mobile Information Systems Volume 2016, Article ID 8354930, 1-13.

[12] Parmar Amisha ,V.B.Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol", 7th International Conference on Communication, Computing and Virtualization 2016, 700-707.

[13] Mousam A. Patel, Manish M. Patel, "Wormhole Attack Detection in Wireless Sensor Network", International Conference on Inventive Research in Computing Applications, 2018, 269 – 274.

[14] He Ronghui, Ma Guoqing, Wang Chunlei, and Fang Lan, "Detecting and Locating Wormhole Attacks in Wireless Sensor Networks Using Beacon Nodes", International Journal of Computer and Information Engineering Vol:3, No:7, 2009, 1714 – 1745.

[15] Tejaswini R Murgod, S Meenakshi Sundaram, "Design of an Optimal Distributed Energy Efficient Hybrid Optical – Acoustic Cluster Based Routing Protocol (EEHCRP) to Minimize the Energy Consumption in Underwater Wireless Sensor Networks", International Journal of Recent Technology and Engineering, Volume-8 Issue-5, January 2020, 873-880.

AUTHORS' PROFILE

Tejaswini R Murgod received B.E. Degree in Computer Science and Engineering from Visvesvarya Technological University ,Belagavi, India in June 2008. She acquired her Master's Degree in from Visvesvarya Technological University, Belagavi, India in Jan 2015. At present she is working as Assistant Professor at GSSS Institute of Technology for Women, Mysuru. Currently she is pursuing Ph. D at Visvesvaraya Technological University, Belagavi and completed Comprehensive Viva. Her research focus includes Underwater Communication, Optical Networks and Wireless Networks.

Dr. S. Meenakshi Sundaram is currently working as Professor and Head in the Department of Computer Science and Engineering at GSSS Institute of Engineering and Technology for Women, Mysuru. He obtained his Bachelor Degree in Computer Science & Engineering from Bharathidasan University, Tiruchirappalli in 1989, M.Tech from National Institute of Technology, Tiruchirappalli in 2006 and Ph.D. in Science & Engineering from Anna University Chennai in 2014.He has published 53 papers in refereed International Journals, presented 3 papers in International Conferences and has delivered more than 40 seminars. He is a reviewer of Springer – Soft Computing Journal, International Journal of Ah Hoc Network Systems, Journal of Engineering Science and Technology, Taylor's University, Malaysia and International Journal of Computational Science & Engineering, Inderscience Publishers, UK. He has organized more than 40 seminars / Workshops / FDPs. He has attended more than 45 Workshops / Seminars. His area of interest includes Computer Networks, Wireless Communication, Software Engineering, Optical Networks and Data Mining. He is a Life Member of Indian Society for Technical Education (ISTE) and a member of Computer Society of India (CSI). He has 30 Years of teaching experience and 10 years of research experience. Currently 7 research scholars are pursuing Ph.D. in VTU Belagavi, India under his guidance.