Proficient Data Broadcast Technique in Wireless ad hoc Network

[1]Anita Dhirte , [2]Rohit Kumar Miri
[1, 2] *Department of Computer Science & Engineering*
Dr. C.V. Raman Institute of Science & Technology, Bilaspur

[1]anita.dhirte15@gmail.com
[2]rohitmiri@gmail.com

***Abstract*— in the last few years, we have seen the fast development of wireless communication technologies and a wireless network play a major role of the wireless communication Wireless network is a collection of wireless nodes without any existing network communications or centralized organization. A wireless network is particularly defenseless to denial of service (DoS) attacks. Existing DoS attack trace back approaches are not suitable for tracing the flooding attacks in Wireless network. The challenges root in several facts, such as he node mobility and the presence of address spoofing. We propose an attack separation scheme to improve the attack impact on the network. A wireless network is particularly vulnerable to flooding attacks. To avoid being identified, attackers generally recruit multiple accomplices to dilute attack traffic thickness of each attack source, and use the address spoofing procedure to challenge the attack tracing. In this paper, we present a detailed investigation of the secure data broadcasting technique for Wireless network.**

Keywords *— **Denial of service (DoS), Mobile Ad Hoc Network (MANET), Wireless Sensor Network (WSN), Security**.*

I. INTRODUCTION

In the last few years, we have seen the rapid development of wireless communication technologies. Today wireless technologies are widely used across the globe to support the communication needs of a huge number of end users. Wireless Networks have become a hot topic in research. Their capabilities for monitoring large areas, accessing remote places, real-time reacting, and relative ease of use has brought scientists a whole new horizon of possibilities. In wireless networks, mobile nodes transmit the information using electromagnetic propagation in the air. The information transmitted by the node can only be received by the nodes that are within the transmission range of the transmitting node. Wireless Networks are a new paradigm of wireless communication for mobile hosts [15]. All nodes in a wireless network act as a router and host as well as the network topology is in energetically, because the connection between the nodes may vary with time due to some of the node departures and new node arrivals. The special features of wireless Network bring this technology huge prospect mutually with severe challenges [2]. Wireless Network also has nodes whose power storage space is very restricted. Often, they are sequence prepared, with very limited to no recharging or alternately promising. Conserving power while demanding to run normal operations is a huge issue in the propose and accomplishment on a Wireless Network. Another limited resource in Wireless Network is bandwidth.

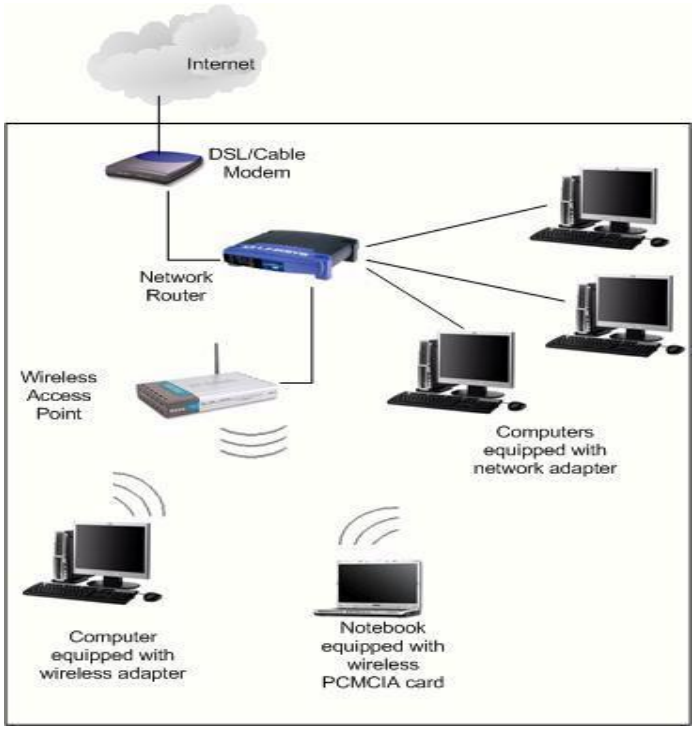

Figure 1: Wireless Network Architecture.

A. Uses of wireless Ad hoc Networks:

An Ad hoc Network is suitable for a wide range of applications. An application of Ad hoc network includes [1, 9]:

1) Sensor Networks: A Wireless Sensor Network (WSN) consists of spatially circulated autonomous sensors to observe physical or ecological circumstances. A wireless sensor network (WSN) has imperative applications such as remote ecological monitoring and objective tracking. [7]. Wireless sensor network increases its uses in development field as well as in customers application very speedily. Its development increases day by day.

2) Military Tactical operations: A MANET could be deployed speedily for military communications in the battleground.

3) Emergency Services: As the internet significance growing quickly, A MANET could be effortlessly organized where the network connectivity has missing due to ordinary failure.

4) Meeting room applications: A Wireless Network could also be deployed speedily in scenarios such a classroom, meeting room, a city shipping wireless network and so on.

5) Dissimilar a permanent wireless network, wireless ad-hoc or on-the-fly networks are differentiated by the lack of infrastructure. Nodes in a mobile ad-hoc network are free to travel and arrange themselves in a random manner. Each user is free to travel concerning while communicating among others.

B. Uniqueness of Ad hoc Networks:

Mobile Ad hoc networks are inherently different from well known wired networks. The characteristics of ad hoc networks are as follows [4]:

1) Multi-hop routing: Non defaulting router accessible, each node acts as a router and forwards each and every packet of other's to facilitate in order to distribution of information among mobile nodes.

2) Dynamic changing network topology: The nodes in wireless networks are liberated to shift at any path at any time. So the network topology of the wireless networks changes quickly and randomly at any instance of time.

3) Multi-hop broadcasting relay: When a source node and the destination node for a message is out of the broadcasting range, the Wireless ad hoc network is accomplished by multi-hop routing.

4) Bandwidth constraints: Wireless links have radically minor bandwidth than well known wired networks.

5) Node cooperation: Wireless Networks maintain and support cooperative algorithms. In Wireless ad hoc network each node is responsible for the routing and forwarding information to maintain and make best use of the total network throughput.

C. Security issues in MANET:

Wireless Networks are much more vulnerable to attacks; there are various security threats and issues that disturb the development of it. The security services of wireless ad hoc networks are not overall different than those of other network communication paradigms. The goal is to defend the information and the resources from attacks and threats [3, 10].

1) Availability: To ensure that the preferred network services are accessible every time when they are estimated, in spitefulness of attacks. Systems that make sure accessibility seek to conflict denial of service and energy starvation attacks.

2) Mobility models: The capability of wireless ad hoc network protocols to appropriately perform in a self-motivated situation, where the device's location may incessantly change in the network and it is a major issue in wireless ad hoc network.

3) Threats: threats include hackers, disgruntled employees, industrial espionage, national intelligence services, and criminal organizations. We consider three main categories of threats [5]:

- **Amateur adversary:** Amateur adversaries can launch unsophisticated attacks such as wireless sniffing or denial of service. Examples are script kiddies or hobbyist hackers.

- **Professional adversary:** A professional adversary can launch more sophisticated attacks such as layer hijacking, man-in-the-middle attack, data modification and many more. Examples are Crime syndicates or terrorist organizations.

- **Well-funded adversary:** A well-funded adversary does not have any constraints on money. Such an adversary can launch very sophisticated attacks such as rushing attacks, wormhole attacks as well as capture devices that are part of the network. Examples are foreign intelligence services.

4) Attacks: The attack may modify, discharge, or reject data. Designing security mechanisms require a deep knowledge of attack models. Attacks on wireless ad hoc networks are categories [15]:

- **Denial-of-service:** A node is disallowed from receiving and sending data packets to its destinations. In this type of attack, an attacker tries to avoid genuine and certified users of the services accessible from the network

- **Jamming**: On jamming, the attacker primarily keeps monitoring the wireless medium in order to determine the regularity at which the destination node is receiving signals from the sender. It then transmits signals on that regularity so that error-free reception of the receiver is delayed.

- **Packet Dropping:** A node drops data packets that it is supposed to forward.

- **Spoofing:** Inject data or control packets with modified source addresses.

- **Wormhole:** A tunnel is shaped between two nodes that can be utilized to surreptitiously broadcast packets. In wormhole attack, a spiteful node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network

- **Data Flooding:** Deliver unusually large amount of data or control packets to the whole network or some target nodes.

5) Privacy: Privacy is a major security issue for ad hoc networks which assure that information is not accessed by unauthorized persons [10].

6) Truthfulness: denotes the genuineness of data sent from one node to another. That is, it ensures that a message sent from node one to node other was not customized by a spiteful node throughout the data transmission [10].

7) Misuse or signature detection systems: The system keeps signatures of known attacks and uses them to evaluate with the captured data [4].

II. EVOLUTION

Joseph P. Macker, Justin Dean and William Chao proposed a model of implemented a working IP multicast forwarding prototype for use in mobile ad hoc networks (MANETs) based upon flooding mechanisms. They present the design of a working experimental prototype and some initial performance results using the NRL mobile network emulation system and various optional flooding approaches within the design framework. In addition, They present supplemental analytical examination of several implemented flooding algorithms for MANET environments and discuss related performance tradeoffs. They conclude by presenting further technical considerations and future work issues [11].

In 2000, Wei Peng and Xi-Cheng Lu developed a model On the Reduction of Broadcast Redundancy in Mobile Ad Hoc Networks. Flooding in mobile ad hoc networks has poor scalability as it leads to serious redundancy, contention and collision. In this paper, we propose an efficient approach to reduce the broadcast redundancy. In their approach, local topology information and the statistical information about the duplicate broadcasts are utilized to avoid unnecessary rebroadcasts. Simulation is conducted to compare the performance of our approach and flooding. The simulation results demonstrate the advantages of our approach. It can greatly reduce the redundant messages, thus saving much network bandwidth and energy. It can also enhance the reliability of broadcasting. It can be used in static or mobile wireless networks to implement scalable broadcast or multicast communications [12].

In 2001, Christine e. Jones et al. Studied A Survey of Energy Efficient Network Protocols for Wireless Networks. Wireless networking has witnessed an explosion of interest from consumers in recent years for its applications in mobile and personal communications. As wireless networks become an integral component of the modern communication infrastructure, energy efficiency will be an important design consideration due to the limited battery life of mobile terminals. Power conservation techniques are commonly used in the hardware design of such systems. Since the network interface is a significant consumer of power, considerable research has been devoted to low-power design of the entire network protocol stack of wireless networks in an effort to enhance energy efficiency [13].

In 2001, PENG Wei and LU Xicheng develop an efficient Broadcast Protocol for Mobile Ad Hoc Networks in which Broadcast is an important operation in many network protocols. It is utilized to discover routes to unknown nodes in mobile ad hoc networks (MANETs) and is the key factor in scaling on-demand routing protocols for larger networks. They present the Ad Hoc Broadcast Protocol (AHBP) and its performance. In the protocol, messages are only rebroadcast by broadcast relay gateways that constitute a connected dominating set of the network. AHBP can efficiently reduce the redundant messages which make flooding like protocols perform badly in large dense networks. Simulations are conducted to determine the performance characteristics of the protocol. The simulation results have shown excellent reduction of broadcast redundancy with AHBP. It also contributes to a reduced level of broadcast collision and congestion [14].

In 2002, Yu-Chee Tseng, Sze-Yao Ni, Yuh-Shyan Chen and Jang-Ping Sheu proposed The Broadcast Storm Problem in a Mobile Ad Hoc Network. In which Broadcasting is a common operation in a network to resolve many issues. In a mobile ad hoc network (MANET) in particular, due to host mobility, such operations are expected to be executed more frequently (such as finding a route to a particular host, paging a particular host, and sending an alarm signal). Because radio signals are likely to overlap with others in a geographical area, a straightforward broadcasting by flooding is usually very costly and will result in serious redundancy, contention, and collision, to which they call the broadcast storm problem. In this paper, they identify this problem by showing how serious it is through analyses and simulations. They propose several schemes to reduce redundant rebroadcasts and differentiate the timing of rebroadcasts to alleviate this problem. Simulation results are presented, which show different levels of improvement over the basic flooding approach [8].

In 2003, Yu-Chee Tseng, Sze-Yao Ni and En-Yu Shih developed an Adaptive Approaches to Relieving Broadcast Storms in a Wireless Multihop Mobile Ad Hoc Network. In which a multihop mobile ad hoc network, broadcasting is an elementary operation to support many applications. It is shown that naively broadcasting by flooding may cause serious redundancy, contention, and collision in the network, which they refer to as the broadcast storm problem. Several threshold-based schemes are shown to perform better than flooding in that work. However, how to choose thresholds also poses a dilemma between reach ability and efficiency under different host densities. In this paper, there propose several adaptive schemes, which can dynamically adjust thresholds based on local connectivity information [6].

In 2004, Wenrui Zhao, Mostafa Ammar and Ellen Zegura proposed A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks. In which Mobile Ad Hoc Networks (MANETs) provide rapidly deployable and self-configuring network capacity required in many critical applications, e.g., battlefields, disaster relief and wide area

sensing. In this paper they study the problem of efficient data delivery in sparse MANETs where network partitions can last for a significant period. Previous approaches rely on the use of either long range communication which leads to rapid draining of nodes' limited batteries, or existing node mobility which results in low data delivery rates and large delays. In this paper, they describe a Message Ferrying (MF) approach to address the problem. MF is a mobility-assisted approach which utilizes a set of special mobile nodes called message ferries (or ferries for short) to provide communication service for nodes in the deployment area. The main idea behind the MF approach is to introduce non-randomness in the movement of nodes and exploit such non-randomness to help deliver data. They also studied two variations of MF, depending on whether ferries or nodes initiate proactive movement. The MF design exploits mobility to improve data delivery performance and reduce energy consumption in nodes. They evaluate the performance of MF via extensive NS simulations which confirm the MF approach is efficient in both data delivery and energy consumption under a variety of network conditions [16].

In 2006, Stefan Pleisch, Mahesh Balakrishnan, Ken Birman and Robbert van Renesse developed MISTRAL: Efficient Flooding in Mobile Adhoc Networks. In which Flooding is an important communication primitive in mobile ad-hoc networks and also serves as a building block for more complex protocols such as routing protocols. In this paper, they propose a novel approach to flooding, which relies on proactive compensation packets periodically broadcast by every node. The compensation packets are constructed from dropping data packets, based on techniques borrowed from forward error correction. Since our approach does not rely on proactive neighbor discovery and network overlays it is resilient to mobility. They evaluate the implementation of Mistral through simulation and compare its performance and overhead to purely probabilistic flooding. Their results show that Mistral achieves significantly higher node coverage with comparable overhead [17].

In 2007, Hai Liu, Xiaohua Jia, Peng-Jun Wan, Xinxin Liu, and Frances F. Yao has developed A Distributed and efficient Flooding Scheme is using 1-Hop Information in Mobile Ad Hoc Networks. In which Flooding is one of the most fundamental operations in mobile ad hoc networks. Traditional implementation of flooding suffers from the problems of excessive redundancy of messages, resource contention, and signal collision. This causes high protocol overhead and interference with the existing traffic on the networks. Some efficient flooding algorithms were proposed to avoid these problems. However, these algorithms either perform poorly in reducing redundant transmissions or require each node to maintain 2-hop (or more) neighbors information. In the paper, they studied the sufficient and necessary condition of 100 percent deliverability for flooding schemes that are based on only 1-hop neighbor's information. They further propose an efficient flooding algorithm that achieves the local optimality in two senses: 1) The number of forwarding nodes in each step is minimal and 2) the time complexity for computing forwarding nodes is the lowest, which is O (n log n), where n is the number of neighbors of a node [18].

In 2011, Adnan Agbaria, Muhamad Hugerat and Roy Friedman develop Efficient and Reliable Dissemination in Mobile Ad Hoc Networks by Location Extrapolation. In which Data dissemination is an important service in mobile ad hoc networks (MANETs). The main objective of that paper was to present a dissemination protocol, called locBcast, which utilizes positioning information to obtain efficient dissemination trees with low control overhead. That paper includes an extensive simulation study that compares locBast with selfP, dominantP, fooding, and a couple of probabilistic-/counter-based protocols. It is shown that locBcast behaves similar to or better than those protocols and is especially useful in the following challenging environments: the message sizes are large, the network is dense, and nodes are highly mobile [19].

In 2011, Chaithannia T S and Ashly Thomas T developed Different Enhancements for Flooding Scheme in Mobile Ad hoc Networks. In which Mobile Ad hoc Network (MANET) is a self-organizing, infrastructure less, multi hop network. The flooding scheme, used to discover routes in MANET is shown to cause high retransmissions, packet collisions and media congestion that can significantly degrade the network performance. Flooding must be handled efficiently in order to improve the performance of the protocol. The existing techniques for flooding are not so efficient. So to improve the efficiency of flooding the combination of blind flooding and node caching can be used. In that method cache the nodes which are recently involved in data packet forwarding, and use only them to forward route requests. Dropping route request forwarding from the other nodes considerably reduces routing overhead [20].

In 2012, S. Nithya Rekha and Dr.C.Chandrasekar developed an improved approach in flooding with packet reach ability in fsr (fisheye state routing) protocol using MANET. In which Packet Reachability and Broadcasting in Mobile Ad Hoc Networks (MANETs) is a fundamental data dissemination mechanism with a number of important applications, e.g., route discovery, address resolution. However broadcasting induces what is known as the ''broadcast storm problem'' which causes a severe degradation in network performance due to excessive redundant re- transmission, collision, and contention. Broadcasting in MANETs has traditionally based on flooding, which simply swamps the network with large number of rebroadcast messages in order to reach all network nodes. Although probabilistic flooding has been one of the earliest suggested schemes to broadcasting, there has not been so far any attempt to analyze its performance behavior in a MANET environment. In an effort to fill this gap, that paper investigates using extensive NS-2 simulations the effects of a number of important system parameters in a typical MANET, including node speed, pause time, and node density on the performance of probabilistic flooding. The results reveal that most of these parameters have a critical impact on the reach ability and the number of saved rebroadcast messages achieved by probabilistic flooding [21].

III. PROPOSED ALGORITHM

A wireless network is most susceptible to flooding attacks. To avoid being identified, the attackers usually recruit multiple accomplices to dilute attack traffic density of each attack source, and use the address spoofing technique to

challenge the attack tracing. We proposed an algorithm which tries to improve the data broadcasting technique for Wireless network.

Notations:

Repeat Path Appeal = False

EXISTINGTIME : time on the system clock

ACKNOWLEDGED TIME : the value of acknowledged Time phase of the node

FURTHER TIME : the value of forward Time period for the node

Total No. of Appeal Acknowledged by the node =False

Drop-Data : 0

INPUT: A Path Appeal Data Packet to node

OUTPUT: Efficient Data Transmission on time of a node.

for all path Appeal Data Packets to Existing node ***do***

if the Existing node a source node and neighbor node is not a Target node
then send path Appeal Data Packet for all neighbors

if duplicate Path Appeal = False **&&** Further Timer =False ***then***

message ***"Appeal Not forward by the node"***

Total No. of Appeal Acknowledged by the node = Total No. of Appeal Acknowledged by the node +1

Drop-data = Drop-data+1

else if duplicate Path Appeal = True **&&** Further Timer =False **then**

message ***"Appeal Not forward by the node"***

Total No. of Appeal Acknowledged by the node = Total No. of Appeal Acknowledged by the node +1

Drop-data = Drop-data+1

else if duplicate Path Appeal = False **&&** Further Timer =True **then**

message ***"Appeal forward Successfully"***
Total No. of Appeal acknowledged by the node = Total No. of Appeal Acknowledged by the node +1

Drop-data = Drop-data

else

message **"reject the replicate path Appeal "**

else

message **"Neighbor is a Target node"**

end for

IV. CONCLUSION AND FURTHER DEVELOPMENT

Today wireless technologies are frequently used transversely the world to hold up the communication needs of a huge number of end users. The significance of wireless technologies in daily life has been discussed. In this paper, we have discussed about the wireless ad hoc networks and we proposed an algorithm for Proficient Data Broadcast Technique which is help full for reducing data replica as well as try to improve the over all performance of the network.

REFERENCES

[1] Yi an Huang and Wenke Lee. "A cooperative intrusion detection system for ad hoc networks" In *SASN*, pp. 135–147, 2003.

[2] G. Anastasi, M. Conti, W. Lapenna, "A power saving network architecture for accessing the internet from mobile computers: design, implementation and measurements" , The Computer Journal 46 (1) (2003) 3–15.

[3] C. Siva Ram Murthy and B. S. Manoj. "Ad Hoc Wireless Networks: Architectures And protocols". Pearson Education India, 2008.

[4] Ningrinla Marchang and Raja Datta. "Collaborative techniques for intrusion detection in mobile ad-hoc networks",*Ad Hoc Networks*, 6(4): pp 508–523, 2008.

[5] Farooq Anjum and Petros Mouchtaris. "Security for Wireless Ad Hoc Networks" . WILEY, 2nd edition, 2007.

[6] Yu-Chee Tseng, Sze-Yao Ni and En-Yu Shih "Adaptive Approaches to Relieving Broadcast Storms in a Wireless Multihop Mobile Ad Hoc Network", IEEE TRANSACTIONS ON COMPUTERS, VOL. 52, NO. 5, Pp: 554-557, MAY 2003

[7] J Yick, B Mukherjee… -"Computer networks", 2008 – Elsevier

[8] Yu-Chee Tseng, Sze-Yao Ni, Yuh-Shyan Chen and Jang-Ping Sheu "The Broadcast Storm Problem in a Mobile Ad Hoc Network", Wireless Networks 8, 153–167, 2002, Kluwer Academic Publishers.

[9] Yongguang Zhang and Wenke Lee. "Intrusion detection in wireless ad-hoc networks". In *MOBICOM*, pp 275–283, 2000.

[10] William Stallings."Cryptography and Network Security principles and practices". Pearson Education Inc, third edition, 2003.

[11] Joseph P. Macker, Justin Dean and William Chao "Simplified Multicast Forwarding in Mobile Ad hoc Networks". Military Communications Conference, 2004. MILCOM 2004. 2004 IEEE (Volume:2).Pp: 744-750.

[12] Wei Peng and Xi-Cheng, "On the Reduction of Broadcast Redundancy in Mobile Ad Hoc Networks", IEEE,2000.

[13] Christine e. Jones, Krishna m. Sivalingam, prathima agrawal and jyh cheng chen "A Survey of Energy Efficient Network Protocols for Wireless Networks", Wireless Networks 7, 343–358, 2001, Kluwer Academic Publishers.

[14] PENG Wei and LU Xicheng "an efficient Broadcast Protocol for Mobile Ad Hoc Networks", Vol.16 No.2 J. Computer Science & Technology, Mar. 2001

[15] Mobile ad hoc network. http ://en:wikipedia:org/wiki/Mobile_ad_hoc_network.

[16] Wenrui Zhao, Mostafa Ammar and Ellen Zegura proposed A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks, MobiHoc'04, May 24–26, 2004, Roppongi, Japan.

[17] Stefan Pleisch, Mahesh Balakrishnan, Ken Birman and Robbert van Renesse developed MISTRAL: Efficient Flooding in Mobile Adhoc Networks, MobiHoc'06, May 22–25, 2006, Florence, Italy.

[18] Hai Liu, Xiaohua Jia, Peng-Jun Wan, Xinxin Liu, and Frances F. Yao "A Distributed and efficient Flooding Scheme using 1-Hop Information in Mobile Ad Hoc Networks" .IEEE transactions on parallel and distributed systems, vol. 18, no. 5, may 2007.

[19] Adnan Agbaria, Muhamad Hugerat and Roy Friedman "Efficient and Reliable Dissemination in Mobile Ad Hoc Networks by Location Extrapolation", Hindawi Publishing Corporation, Journal of Computer Networks and Communications, Volume 2011, Article ID 680936, 11 pages.

[20] Chaithannia T S and Ashly Thomas T "Different Enhancements for Flooding Scheme in Mobile Ad hoc Networks", Conference on Advances in Computational Techniques (CACT) 2011 Proceedings published in International Journal of Computer Applications, Pp : 10-13.

[21] S. Nithya Rekha and Dr.C.Chandrasekar developed an improved approach in flooding with packet reach ability in fsr (fisheye state routing) protocol using MANET, Journal of Theoretical and Applied Information Technology ,15 June 2012. Vol. 40 No.1, Pp: 98-104.

Anita Dhirte, M.Tech.(Pursuing) in Computer Science and engineering from Dr. C.V. Raman Institute of Science & Technology, Kargi Road Kota, Bilaspur.India. , research areas are Wireless ad hoc Network and its enhancement.

Prof. Rohit Kumar Miri , M.Tech Coordinator and Head of CSE department in Dr. C.V. Raman Institute of Science & Technology, Kargi Road Kota, Bilaspur.India. Having seven years long experience in the field of teaching. Research areas are Wireless Computer Network, MANET, Bluetooth Network and its enhancement, His research work has been published in many national and international journals.