Random Routing Algorithm for Secured Data Collection Accessed in Wireless Sensor Networks

Dr. S. Tamilarasan
Dept. of CSE, LITAM, Sattenapalli, Guntur, AP, India

Abstract
we can send secured data from sender to destination; it is possible through Wireless Sensor Networks with network monitoring data on a host, they can used to detect compromised node and denial-of-service is two key attacks. In this article, we studied and present four "Multi-path randomized routing Algorithm" a method to send the data multiple ways to classify the data in to normal and attacks in wireless sensor networks. The Pure Random Propagation shares are propagated based on one-hop neighborhood information, sink TTL initial value N in each share and remaining algorithms improve the efficiency of shares based on using two-hop neighborhood information. Our work studies the best algorithm by detecting the comprised nodes with black holes and denial of service in the packet information with Multipath routing algorithms that has not been used before. We analyses the algorithm that have the best efficiency and describes the proposed system.

Keywords
Wireless Sensor Networks, Security, Attacks and Routing.

I. Introduction

Wireless sensor networks are emerging networks which consists of a large number of low-cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communication capabilities. These sensor nodes communicate over short distance via a wireless medium and collaborate to accomplish a common task, for example, environment monitoring, military surveillance, and industrial process control. The basic philosophy behind WSNs is that, while the capability of each individual sensor node is limited, the aggregate power of the entire network is sufficient for the required mission [1].

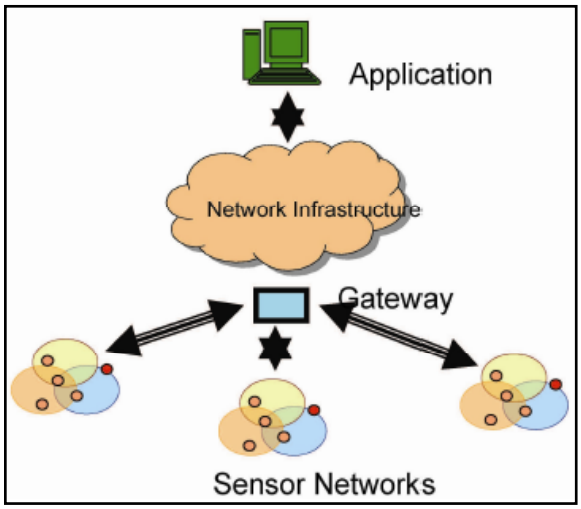
In many WSN applications, the deployment of sensor nodes is performed in an ad hoc fashion without careful planning and engineering. Once deployed, the sensor nodes must be able to autonomously organize themselves into a wireless communication network. Sensor nodes are battery-powered and are expected to operate without attendance for a relatively long period of time. In most cases it is very difficult and even impossible to change or recharge batteries for the sensor nodes [1-2].

WSNs are characterized with denser levels of sensor node deployment, higher unreliability of sensor nodes, and sever power, computation, and memory constraints. Thus, the unique characteristics and constraints present many new challenges for the development and application of WSNs.

Wireless Sensor Network (WSN) is a heterogeneous system contains a combination of millions of petite, inexpensive sensor nodes with several distinctive characteristics. It is low processing power and radio ranges, permitting very low energy consumption in the sensor nodes, and performing limited and specific sensing and monitoring functions. Nevertheless, WSNs form a particular class of ad hoc networks that operate with little infrastructure and have attracted researchers for its development and many potential civilian and military applications such as environmental monitoring, battlefield surveillance, and homeland security. However, designing security protocols is a challenging task for a WSN because of the following unique characteristics: Wireless channels are open to everyone and has a radio interface configured at the same frequency band. Thus, anyone can monitor or participate in the communication in a wireless channel. This provides a convenient way for attackers to break into a network [2].

A stronger security protocol costs more resources in sensor nodes, which can lead to the performance degradation of applications. In most cases, a trade-off has to be made between security and performance. However, weak security protocols may be easily broken by attackers.

A WSN is usually deployed in aggressive areas without any fixed infrastructure. It is difficult to perform continuous observation after network deployment. Therefore, it may face various potential attacks [1,5-6].



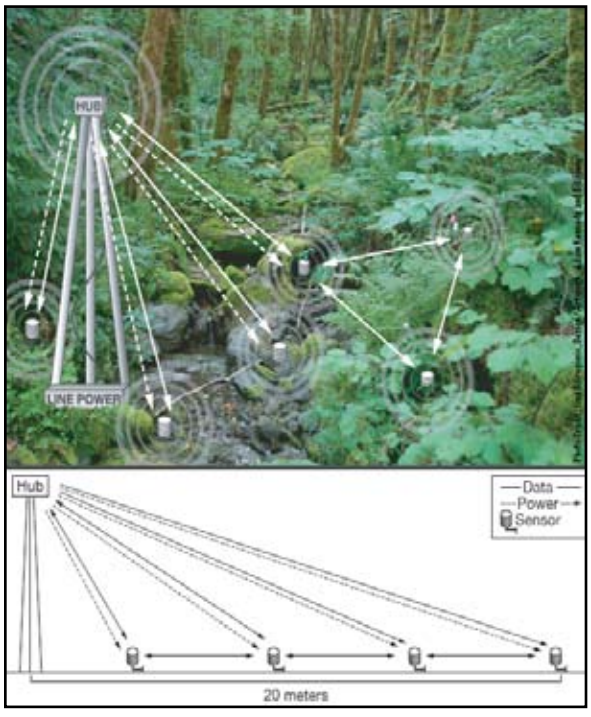


Fig. 1: Examples of Wireless Sensor Networks

II. Routing Protocols in WSN

Routing in wireless sensor networks is very challenging due to several characteristics that distinguish them from fashionable communication and wireless ad hoc networks. It varies from the conventional routing in fixed networks in various behaviors. There is no infrastructure, wireless links are unreliable, sensor nodes may fail, and routing protocols have to meet firm energy saving requirements. All major routing protocols proposed for WSNs may be divided into seven categories.

A. Location-Based Protocols

In location-based protocols, sensor nodes are addressed by means of their locations. Location information for sensor nodes is required for sensor networks by most of the routing protocols to calculate the distance between two particular nodes so that energy consumption can be estimated.

B. Data Centric Protocols

Data-centric protocols differ from traditional address-centric protocols. In Data-Centric Protocols, the data is sent from source sensors to the sink. In address-centric protocols, each source sensor that has the appropriate data responds by sending its data to the sink independently of all other sensors. However, in data-centric protocols, when the source sensors send their data to the sink, intermediate sensors can perform some form of aggregation on the data originating from multiple source sensors and send the aggregated data toward the sink. This process can result in energy savings because of less transmission required to send the data from the sources to the sink.

C. Hierarchical Protocols

Clustering is an energy-efficient communication protocol that can be used by the sensors to report their sensed data to the sink. We describe a sample of layered protocols in which a network is composed of several clusters of sensors. Each cluster is managed by a special node, called cluster head, which is responsible for coordinating the data transmission activities of all sensors in its clump. As shown in fig. 2, a hierarchical approach breaks the network into clustered layers [5].

Nodes are grouped into clusters with a cluster head that has the responsibility of routing from the cluster to the other cluster heads or base stations. Data travel from a lower clustered layer to a higher one. Although, it hops from one node to another, but as it hops from one layer to another it covers larger distances. This moves the data faster to the base station. Clustering provides inherent optimization capabilities at the cluster heads.

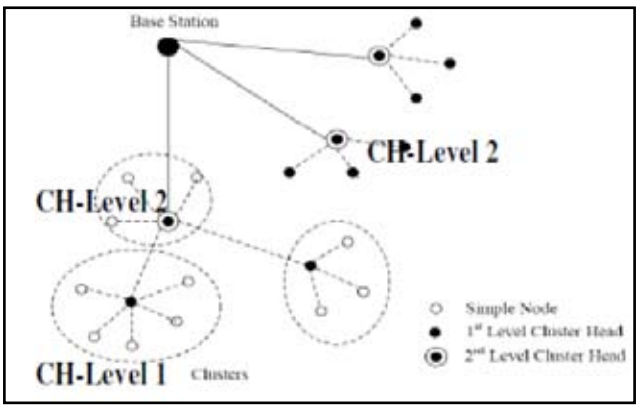


Fig. 2: Cluster-Based Hierarchical Model

D. Mobility-Based Protocols

Mobility brings new challenges to routing protocols in WSNs. Sink mobility requires energy efficient protocols to guarantee data delivery originated from source sensors toward mobile sinks.

E. Multipath-Based Protocols

Considering data transmission between source sensors and the sink, there are two routing paradigms: single-path routing and multipath routing. In single-path routing, each source sensor sends its data to the sink via the shortest path. In multipath routing, each source sensor finds the first k shortest paths to the sink and divides its load evenly among these paths.

F. Heterogeneity-Based Protocols

In heterogeneity sensor network architecture, there are two types of sensors namely line-powered sensors which have no energy constraint, and the battery-powered sensors having limited lifetime, and hence should use their available energy efficiently by minimizing their potential of data communication and computation.

G. QoS-Based Protocols

In addition to minimizing energy consumption, it is also important to consider Quality Of Service (QoS) requirements in terms of delay, reliability, and fault tolerance in routing in WSNs.

III. Security Issues and Requirements

A. Attack and Attacker

An attack can be defined as an attempt to gain unauthorized access to a service, a resource or information, or the attempt to compromise integrity, availability, or confidentiality of a system. Attackers, intruders or the adversaries are the originator of an attack. The weakness in a system security design, implementation, configuration or limitations that could be exploited by attackers is known as vulnerability or flaw. Any circumstance or event (such as the existence of an attacker and vulnerabilities) with the potential to adversely impact a system through a security breach is called threat and the probability that an attacker will exploit a particular vulnerability, causing harm to a system asset is known as risk.

B. Security Requirements

Sensor Network is a special type of wireless Ad-hoc Networks. WSN shares some essential property of wireless ad-hoc networks such as computer networks, some routing protocols characteristics such as mobility, packet delivery ratio, path setup between any devices around the network, etc. Routing in WSN meet several challenges due to its spontaneous characteristics like infrastructure less, etc... The objective of the security service in WSN is to protect information or messages from attacks and misbehavior of the nodes. The security requirements of a wireless sensor network can be classified as follows:

1. Availability

This ensures that the desired network services are available even in the presence of denial-of-service attacks [5].

2. Authorization

This ensures that only authorized sensors can be involved in providing information to network services [5].

3. Authentication
which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node [5].

4. Confidentiality
Ensures that a given message cannot be understood by anyone other than the desired recipients [5].

5. Integrity
Ensures that a message sent from one node to another is not modified by malicious intermediate nodes

6. Nonrepudiation
Which denotes that a node cannot deny sending a message it has previously sent

7. Freshness
which implies that the data is recent and ensures that no adversary can replay old messages Moreover, as new sensors are deployed and old sensors fail, we suggest that forward and backward secrecy should also be considered:

8. Forward Secrecy
A sensor should not be able to read any future messages after it leaves the network [3].

9. Backward Secrecy
A joining sensor should not be able to read any previously transmitted message [7].

IV. Problem Definition

A. Proposed System
Our proposed random routing algorithm set up a randomized multi-path routing between nodes that can overcome the black holes formed by Compromised-node and denial-of-service attacks. Instead of selecting paths from a pre-computed set of routes, our aim is to compute multiple paths in a randomized way each time an information packet needs to be sent, such that the set of routes taken by various shares of different packets keep changing over time. To intercept different packets, the intruder has to compromise or jam all possible routes from the source to the destination, which is practically infeasible.

1. Advantages
- Provides highly dispersive random routes at low energy cost without generating extra copies of secrete shares.
- If the routing algorithm becomes known to the adversary, the adversary still cannot pinpoint the routes traversed by each packet.
- Energy efficient.

B. Randomized Multipath Delivery
We consider a three-phase approach for secure information delivery in a WSN as illustrated in fig. 3:
1. Secret sharing of information,
2. Randomized propagation of each information share, and
3. Normal routing (e.g., min-hop routing) toward the sink.

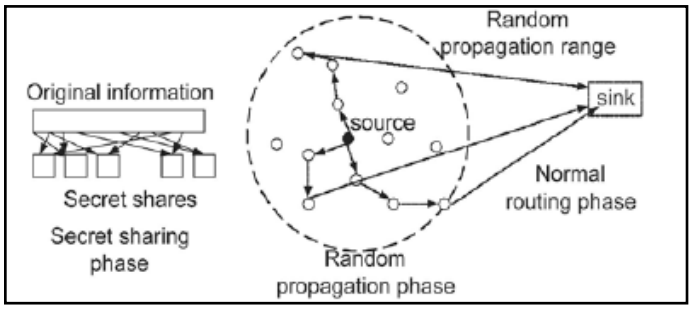


Fig. 3: Randomized Routing in WSN's

More specifically, when a sensor node wants to send a packet to the sink, it first breaks the packet into M shares, according to a (T, M) -threshold secret sharing algorithm. Each share is then transmitted to some randomly selected neighbor. That neighbor will continue to relay the share it has received to other randomly selected neighbors, and so on. In each share, there is a TTL field, whose initial value is set by the source node to control the total number of random relays. After each relay, the TTL field is reduced by 1. When the TTL value reaches 0, the last node to receive this share begins to route it toward the sink using min-hop routing. Once the sink collects at least T shares, it can reconstruct the original packet. No information can be recovered from less than T shares.

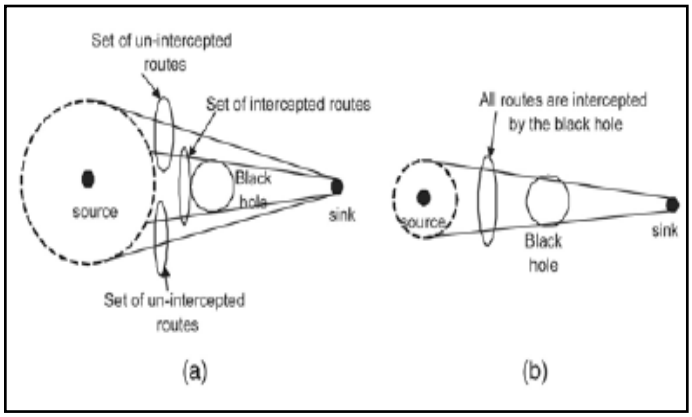


Fig. 4: Implication of Route Depressiveness on Bypassing the Black Hole, (a). Routes of higher depressiveness. (b). Routes of lower dispersiveness

The effect of route depressiveness on bypassing black holes is illustrated in fig. 4. A larger dotted circle implies that the resulting routes are geographically more dispersive. Comparing the two cases in fig. 3, it is clear that the routes of higher depressiveness are more capable of avoiding the black hole. Clearly, the random propagation phase is the key component that dictates the security and energy performance of the entire mechanism [16].

C. Random Propagation of Information Shares
To diversify routes, an ideal random propagation mechanism or algorithm that would propagate shares depressively as much as possible. Typically, this means propagating the shares farther from their source and towards the sink. At the same time, it is highly desirable to have an energy-efficient propagation, which calls for limiting the number of randomly propagated hops. Now the challenge here lies in the random and distributed nature of the propagation i.e. a share may be sent one hop farther from its source in a given step, but may be sent back closer to the source in the next step, wasting both steps from a security point of view. To tackle this issue, some control needs to be imposed on the random

propagation process. Generally we have four types of schemes:

1. Purely Random Propagation (Baseline Scheme)

Pure Random Propagation (PRP), shares are propagated based on one-hop neighborhood information. More specifically, a sensor node maintains a neighbor list, which contains the ids of all nodes within its transmission range. When a source node wants to send data to destination, it includes a TTL of initial value N in each share. It then randomly selects a neighbor for each share, and unicasts the share to that neighbor. After receiving the share, the neighbor first decrements the TTL, if the new TTL is greater than 0, the neighbor randomly picks a node from its neighbor list (this node cannot be the source node) and relays the share to it, and so on. When the TTL reaches 0, the final node receiving this share stops the random propagation of this share, and starts routing it toward the sink using normal min-hop routing.

2. Non- Repetitive Random Propagation

Improves propagation efficiency by recording the nodes traversed so far:

- Adds node-in-route (NIR) field to the share header
- Initially NIR is empty at the source node
- When a share is propagated, the ID of the upstream node is added to the NIR field
- Nodes in NIR fields are excluded from random pick at the next hop
- Thus share is relayed to a different node in each step, leading to better propagation efficiency.

3. Directed Random Propagation

Improves Propagation Efficiency with Two Hop Neighborhood Information

- Adds last-hop-neighbor list (LHNL) field to the header of each share
- Propagating node updates the LHNL field before sending the share
- Receiving node compares this LHNL against its own LHNL & randomly picks a node that is not in LHNL of both nodes
- TTL value decremented, LHNL is updated, share relayed
- If the LHNL fully overlaps the relaying node LHNL, a random neighbor is selected, just like PRP.

Benefits

- Reduces the chance of propagating a share back and forth
- Better propagation efficiency as the share is pushed outwards

4. Multicast Tree-Assisted Random Propagation

Traditional location based routing algorithms

- Require location information at both the source and the destination and sometimes intermediate nodes (GPS at each node)
- Low accuracy of localization and high cost
- MTRP involves directionality in its propagation without needing location information

The random routes generated by the four algorithms are not necessarily node disjoint. Note that the security analysis for the CN and DOS attacks is similar because both of them involve calculating the packet interception probability [15]. For brevity, we only focus on the CN attack model. The same treatment can be applied to the DOS attack with a straightforward modification. Basically this paper involves three important steps for implementing secure data transmission in WSN's using some programming language like java and database like ORACLE is as follows which include three modules:

A. Topology Creation

In this module, we construct a topology structure. Here we use mesh topology because of its unstructured nature. Topology is constructed by getting the names of the nodes and the connections among the nodes as input from the user. While getting each of the nodes, their associated port and IP address is also obtained. For successive nodes, the node to which it should be connected is also accepted from the user. While adding nodes, comparison will be done so that there would be no node duplication. Then we identify the source and the destinations.

Fig. 5: Topology Creation

B. Randomized Multipath Routing

We achieve randomized multipath routing that can conquer the Compromised Node attack & Denial of Service attack. Here several paths are computed in a randomized pattern each time an information packet needs to be sent. In this context a large number of routes can be potentially produce for each source and destination as shown in figure 6. To capture different packets, the offender need to compromise and squash all possible routes from the source to the destination, which is practically not possible.

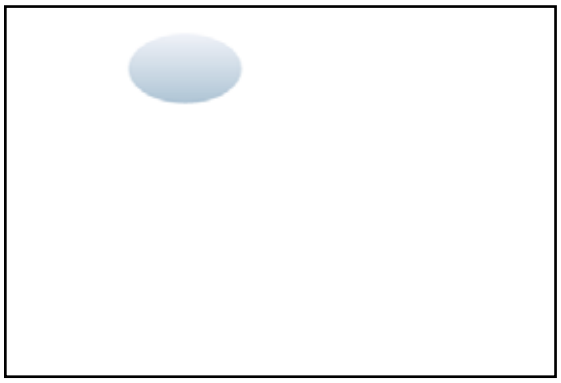


Fig. 6: Randomized Multipath Routing

C. Message Transmission

1. Pure Random Propagation (PRP)

Shares are propagated based on one-hop neighborhood information. More specifically, a sensor node maintains a neighbor list, which contains the ids of all nodes within its transmission range. When a source node wants to send data to destination, it includes a TTL of initial value N in each share. It then randomly selects a neighbor for each share, and unicasts the share to that neighbor, after receiving the share, the neighbor first decrements the TTL. If the new TTL is greater than 0, the neighbor randomly picks a node from its neighbor list (this node cannot be the source node)

and relays the share to it, and so on. When the TTL reaches 0, the final node receiving this share stops the random propagation of this share, and starts routing it toward the sink using normal min-hop routing.

2. Secured Delivery of Packets

In this module we can maintain the routing table; here we add one more column to maintain the packet delivery ratio. In this way we can maintain how many packets are transmitted over each path. It will be useful to identify any path and can packets handle packets number. We can stop transmission for some amount of time period over that path, so that the hacker cannot identify in which path the message is transmitted and also we can easily transmit the data securely.

V. Conclusion

In this article we describe the effectiveness of the randomized dispersive routing in overcoming the CN and DOS attacks which is energy efficient. The specific approaches of the black hole systems are characterized, we developed pure random propagation method is based on one-hope neighbor information shares. By appropriately setting the secret sharing and propagation parameters, the packet interception probability can be easily reduced by the proposed algorithms to as low as 10-3, which is at least one order of magnitude smaller than approaches that use deterministic node-disjoint multi-path routing. At the same time, we have also verified that this improved security performance comes at a reasonable cost of energy. Our current work does not address this attack. Its resolution requires us to extend, our mechanisms to handle multiple collaborating black holes, which will be studied in our future work.

References

[1] Shio Kumar Singh, M.P. Singh, D.K. Singh,"A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, Vol. 02, Issue 02, pp. 570–580.

[2] Shio Kumar Singh, M.P. Singh, D.K. Singh,"Energy efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN), Aug. 2010, Vol. 2, No. 3, pp. 49-61.

[3] Shio Kumar Singh, M.P. Singh, D.K. Singh,"Applications, Classifications, and Selections of Routing Protocols for Wireless Sensor Networks", International Journal of Advanced Engineering Sciences and Technologies (IJAEST), November 2010, Vol. 1, issue No. 2, pp. 85-95.

[4] Shio Kumar Singh, M.P. Singh, D.K. Singh,"Routing Protocols in Wireless Sensor Networks – A Survey", International Journal of Computer Science and Engineering Survey (IJCSES), November, 2011, Vol. 1, No. 2, pp. 63-83.

[5] Shio Kumar Singh, M.P. Singh, D.K. Singh,"Performance Evaluation and Comparison of Energy-efficient Routing Protocols for Wireless Sensor Network", Global Journal of Computer Application and Technology (GJCAT), Jan. 2011, Vol. 1, No. 1, pp. 57-65.

[6] Shio Kumar Singh, M.P. Singh, D.K. Singh,"Energy Efficient Transmission Error Recovery for Wireless Sensor Network", International Journal of Grid and Distributed Computing (IJGDC), December 2010, Vol. 3, No. 4, pp. 89-104.

[7] S. Misra et al. (eds.),"Guide to Wireless Sensor Networks, Computer Communications and Networks", 2009.

[8] S.K. Singh, M.P. Singh, D.K. Singh,"A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks", International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, Vol. 02, Issue 02, pp. 570–580.

[9] A. S. Wander, N. Gura, H. Eberle, V. Gupta, S. C. Shantz,"Energy analysis of public-key cryptography for wireless sensor networks", in Third IEEE International Conference on Pervasive.

[10] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang,"Security in mobile Ad-Hoc networks: challenges and solutions", IEEE Wireless Communications, Vol. 11, No. 1, pp. 38-47, Feb. 2004.

[11] Adrian Perrig, John Stankovic, David Wagner,"Security in wireless sensor networks", Commun. ACM, 47(6), pp. 53-57, 2004.

[12] D. Carman, B. Matt, D. Balenson, P. Kruus,"A communications security architecture and cryptographic mechanisms for distributed sensor networks", in DARPA Sens IT Workshop. NAI Labs, the Security Research Division Network Associates, Inc., 1999.

[13] H. Chan, A. Perrig, D. Song,"Random key predistribution schemes for sensor networks", in Proceedings of the 2003 IEEE Symposium on Security and Privacy. IEEE Computer Society, 2003.

[14] Shu, T.; Liu, S.; KrunzSecure, M.,"Data collection in wireless sensor networks using randomized dispersive routes", In Proceedings of IEEE INFOCOM Conference, Rio de Janeiro, Brazil, 19–25 August 2009, pp. 2846-2850.

[15] E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)", IEEE Trans. Antennas Propagat., to be published.

[16] J. Wang,"Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)", IEEE J. Quantum Electron., submitted for publication.

Dr. S. Tamilarasan. Ph. D: He received the B.E (CSE) degree from Madras University, Chennai, Tamilnadu, India, M.E (CSE) degree from Anna University, Chennai, India, PhD (CSE) from Mahatma Gandhi Kashi Vidyapeeth University, Varanasi, U.P. currently working as Associate Professor in Information Technology, LITAM, Sattenapalli, A.P.

Specialization: Mobile computing, Advanced Data Structure, Design and analysis of algorithm, Computer networks, His interesting research field is Mobile Ad-Hoc Networks, Computer networks, Wireless Sensor Networks.