# PDBTM-IOV: Probability Distribution Based Trust Model for Internet of Vehicles

Indu Bhardwaj[1,*], Ajay Bhardwaj[2] and Sibaram Khara[3]

[1]*Galgotias University, Greater Noida, Uttar Pradesh, India*
[2]*Delhi Technological University, Delhi, India*
[3]*Sharda University, Greater Noida, Uttar Pradesh, India*
*E-mail: indubhardwaj2011@gmail.com; ajaybhardwaj1999@gmail.com; sianba@rediffmail.com*
[*]*Corresponding Author*

Received 08 January 2025; Accepted 01 May 2025

## Abstract

In Internet of vehicle network, security of data transmitted by nodes is of Prime concern. This paper presents an algorithm for effectively classifying the trustworthy and non-trust worthy nodes for secure communication of vehicles. The categorization is done based on probability distribution curve drawn using statistics of nodes. The nodes will be considered as normal when the PDF of the nodes lies in the range of mean +/-2 standard deviation of the curve. Simulation is performed for three trust threshold ($\theta$ = 0.65,0.7,0.75) and two metrics i.e. trust value and Packet delivery ratio. The proposed model is compared with rater and ratee based model in terms of transaction number growth. From the results, it can be found that average trust maximizes with time for trusted nodes and becomes zero non trusted nodes. Results also depicts that the Packet Delivery Ratio is 0.065 for normal nodes and 0.015 for abnormal nodes. The proposed model distinguishes between trusted and malicious nodes efficiently, providing a better, scalable and lightweight trust

*Journal of Mobile Multimedia, Vol. 21_3&4,* 379–392.
doi: 10.13052/jmm1550-4646.21342

mechanism for IoV environments without relying on cryptographic methods. Future work will focus on improving the model's adaptability to real-world network conditions and incorporating dynamic trust thresholds for greater accuracy in various vehicular scenarios.

**Keywords:** Internet of Vehicles, IoV, security, trust, trust model, joint probability distribution.

## 1 Introduction

Internet of Vehicles (IoV) is defined as distributed network used for wireless exchange of information between vehicles, infrastructure, pedestrians and internet, based on communication protocols and standards [1]. It is combination of vehicular network (VANET) [2] and internet of things IoT [3]. Internet of vehicles has significantly boosted intelligent traffic management [4]. It also overcomes limitations of traditional VANETs, like lack of coordination between distant vehicles, communication with remote RSU's, scalability, information insufficiency etc. The Internet connectivity widens the network globally. However, internet connectivity makes the network more vulnerable to security threats and questions the reliability of data [5]. The state of art in IoV networks depicts that research is focused on IoV architectures and reliable delivery of data but less focused on evaluation of the reliability of data sent by the nodes [6]. This motivated us to work on evaluating the of data transmitted by nodes. Evaluation of data quality and reliability is quite necessary for a node to make reliable decision. The data quality can be measured by estimating the trust on the sender node. By measuring the trust level, a trusted, malicious, faulty and selfish node can be easily differentiated [7]. But modelling trust is a challenging task in IoV network. In this paper a trust model is proposed for segregating trusted and malicious nodes.

The rest of the paper as below. Section 2 presents related work. Section 3 defines the proposed system model followed by result and discussion in Section 4. Lastly, Section 5 concludes this paper and highlights the future work.

## 2 Related Work

Various trust models have been proposed by different researchers for VANET, e.g. [8–14]. But trust management in IoV network is still in infant stage.

Few trust models have been proposed so far for the IoV network [15–18]. Prevailing trust models for VANETs suffers with various limitations which hampers their implementation practically [7]. For example, some trust models use history of past interactions for trust calculation which is not feasible to implement in vehicular network. Some of the existing trust models make use of the email ids of senders or unique identities of each node for trust computation which violates user privacy. Some trust models are not resilient against attacks in network. Furthermore, most of the trust models are rater-based which do not work efficiently when a node encounters an unknown node. Some are rater-based which also has limitations that are unaddressed i.e. cold start problem and scalability problem. To fill these gaps, we propose a probability-based trust model that efficiently handles the above-mentioned limitations

## 3 System Model

The proposed PDBTM for IoV works as distributed data protocol where nodes act as client and online trusted centers act as server. PDBTM is an probabilistic distribution based trust model to compute the direct trust in a node Figure 1. By doing so, we evaluate the communication nodes that are immediately next in both trustworthiness and sincerity. As soon as it sends out a data or control packet, the node will put its receiver into promiscuous mode. As soon as the transmitting node hears that its immediate neighbor is forwarding the packet, the transmitting node does an integrity check on the packet and Infers, by either confirmation or modification. If the integrity check fails, or the forwarding node behaves in a non-compliant manner your corresponding trust vector is decreased. In either of these cases we say that trust goes down. We express the trust of node A for node B as TAB, with the following formula:

$$T_{AB} = P(S_1|P_{Ns1}) \times P(S_2|P_{NS2}) \ldots P(S_m|P_{NSm}) \tag{1}$$

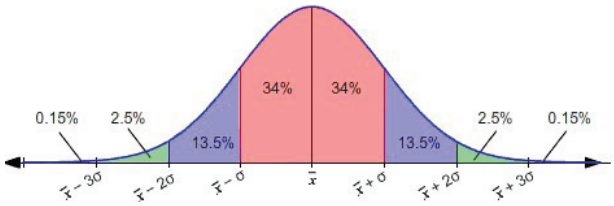


**Figure 1** Probability distribution for estimating the trust of the nodes.

where $P(S_1|P_N)$ represents the estimated trust of node B by A if using statistic $S_1$ given the Trust distribution of $S_1$ as $P_{s1}$ and Conditional probability being $P(S_1|P_{Ns1})$. The $P(S_1|P_{Ns1})$ estimates the probability of having normal statistic S1 if the trust distribution for statistic $S_1$ is given as $P_{S1}$.

The normal distribution given input variable X, mean $\mu$ and standard deviation $\sigma^2$

$$\textit{Normal Distribution}\ (x, |\mu, \sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\ \mu)^2}{2\sigma^2}} \tag{2}$$

the PDF(Probability density function) of a given statistic $S_m$ can be modeled as

$$PDF(S_m, |\rho, \tau^2) = \frac{1}{\sqrt{2\pi\tau^2}} e^{-\frac{(S_m-\rho)^2}{2\tau^2}} \tag{3}$$

where the $\rho$ is the mean of statistic $S_m$ and $\tau^2$ is the standard deviation, the $\rho$ and $\tau^2$ are collected by executing the network in normal mode without presence of malicious nodes. We have utilized three direct PDF and two derived PDF as parameters for evaluation including Packet delivery ratio (PDR), Packet Loss Ratio (PLR), Average Speed ($\omega$) of the nodes in network and two standard PDR given mean speed and PDR given distance. These PDR and PLR metrics will allow for real-world calibration of the statistical distributions.

The classification is done for any metric $S_m$ given the mean $\rho$ is standard deviation $\tau^2$ as,

$$\text{if } \begin{Bmatrix} S_m > \rho + 2\tau^2 \\ S_m < \rho - 2\tau^2 \end{Bmatrix} \quad \text{Abnormal Behaviour} \tag{4}$$

and

$$\text{if } \begin{Bmatrix} S_m \leq \rho + 2\tau^2 \\ S_m \geq \rho - 2\tau^2 \end{Bmatrix} \quad \text{Normal Behaviour} \tag{5}$$

Thus, the statistical behaviour $S_m$ is bounded by $[\mu - 2\sigma^2 \geq \omega \leq \mu + 2\sigma^2]$ for normal node, if the behavior of the node crosses the bound the node is marked as abnormal node.

The proposed trust model works on the following assumptions.

- Initial trust values all nodes in the Internet of Vehicles (IoV) network is assumed as 0.5. This uniform assumption is considered because at the start of interaction, nodes doesn't have no prior knowledge or history of interactions between nodes.

- The model assumes that the behaviours of nodes, such as Packet Delivery Ratio (PDR), Packet Loss Ratio (PLR), and speed, follow a normal distribution.
- The trust classification algorithm assumes a binary outcome, where nodes are either normal (trusted) or abnormal (non-trusted).
- The algorithm assumes that nodes have short-lived interactions and vehicles may not have the opportunity to form long-term communication histories.
- The model implicitly assumes that environment conditions such as signal interference and weather conditions do not impact the vehicular communication significantly.

## 4 Result and Discussion

To accomplish the simulations, Simulation of Urban MObility (SUMO) as a traffic simulator and MATLAB as event simulator are used. We consider an IoV environment in which some of the nodes are randomly set as abnormal nodes. We assume that every node has the trust value of 0.5 initially. The conducted simulations show easily how the normal (trusted) nodes are separated from abnormal (non-trusted) nodes based on trust value and Packet delivery ratio. The proposed PDTM model is compared to existing ratee based scheme [22] and rater-based scheme [23] in terms of transaction number growth.

### 4.1 Average Trust

The value of average trust gradually increases with every successful interaction and decreases with every misbehavior of non-trusted node. Figure 2 shows the average trust of the normal node gradually increases with time maximum value of trust is 1. This increases their margin of safety for being good node even when there is any bad interaction accidently.

Figure 3 shows the average trust of the abnormal node gradually decreases and become zero with time. Threshold policy does not have much effect on the average trust.

### 4.2 Packet Delivery Ratio

It defines how many numbers of packets transmitted have be received successfully by the target node. The conducted simulations show how the average PDR varies with time for both normal as well as abnormal nodes. The graphs in Figures 4 and 5 shows that average PDR for the normal nodes

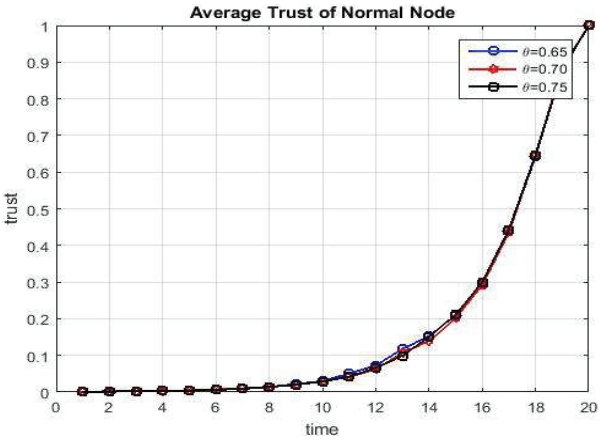


**Figure 2** Average trust of normal nodes.

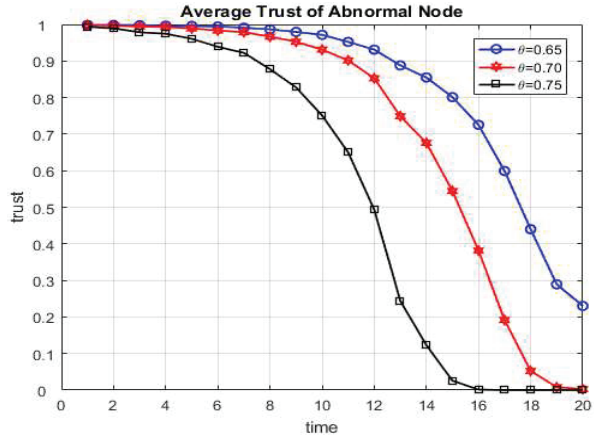


**Figure 3** Average trust of abnormal nodes.

is 0.065 whereas the PDR for abnormal node is 0.015. It means the PDR of normal nodes is more in comparison with abnormal nodes. Both graphs presented that the progression of PDR is higher for less strict threshold policies.

### 4.3 Transaction Number Growth

Transaction number is defined as no. of transactions/ communications that takes place amongst any two of the nodes. In this simulation, we have

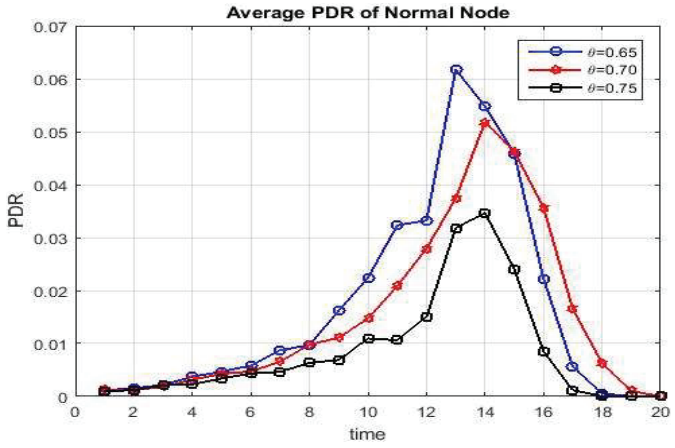


**Figure 4** Average PDR of normal node.

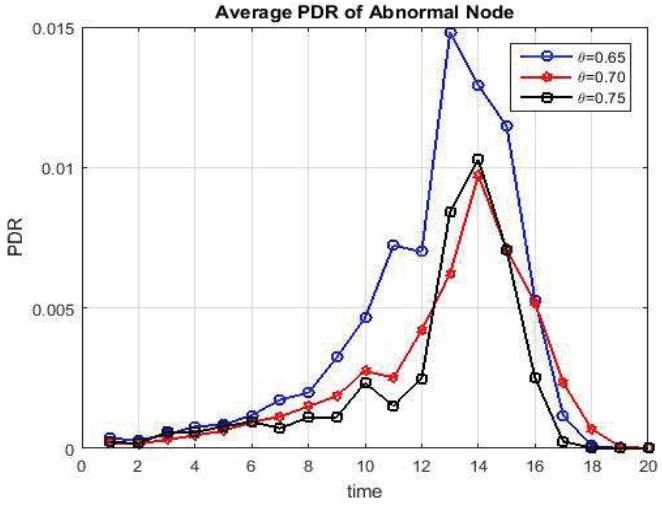


**Figure 5** Average PDR of abnormal node.

recorded the number of transactions taking place between vehicular node for 10 hours, and the transaction growth is calculated every hour for all the three methods. The simulation outcomes are shown in Figure 6.

During first simulation hour, growth of transaction no. is less in PDTM as compared to ratee methods and rater method is slowest. The reason behind the same is that in the early stage of network, few nodes are interrelated and share the information which is to be accumulated to evaluate trust. The

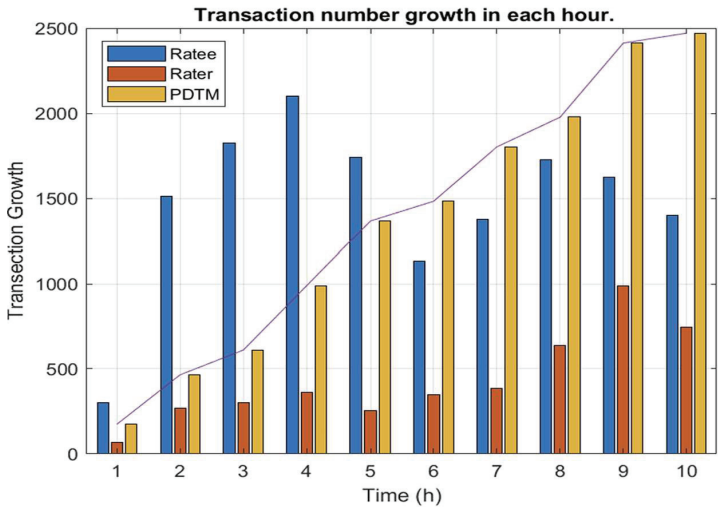


**Figure 6** Transaction number growth in each hour.

transaction number growth for rater-based models is quite less as compared to both ratee- based and PDTM throughout the simulation. But the comparison of the transaction number of ratee based models and PDTM shows that the transaction growth is initially low in proposed PDTM in comparison with Ratee model. This is because in PDTM we have allocated preliminary trust to all given nodes so malicious nodes may also participate in network and does not allow the transaction to take place. But as the time progresses, the proposed model works well as compared to ratee based model as the transaction number growth in PDTM is increasing in a continuous manner with progression of time and peaks at more than 2300 transactions in 9th hour. In long run PDTM has more transaction growth in each hour whereas continuous manner with progression of time and peaks at more than 2300 transactions in 9th hour. In long run PDTM has more transaction growth in each hour whereas transaction number growth in ratee-based model fluctuates up and down. During first four hours the transaction growth of ratee based is very high having peak at more than 2000 transactions. But after t= 4 hours it starts fluctuating with peak at 1800 transactions.

## 5 Conclusion

This work presented a trust model that is neither ratee based nor rater based as Trust values are stored online at trusted center making use of Internet of

things. The simulation shows that this model easily segregates abnormal/non trusted nodes and normal node based on trust values. Malicious nodes can be easily separated from ideal ones using this model as their average trust value will undergo graceful degradation with each misbehavior. The model is scalable in the sense that every node stores the trust value of limited sets of nodes only that are required for it. The model does not make use of cryptography for the authentication of entities in network discovery phase that reduces the computation and time complexity of the model. The simulation -based comparison of proposed model with rater and ratee based model concludes that the proposed PDTM outperforms the rater based as well as ratee based model in terms of transaction number growth.

Despite its strengths, the PDBTM has certain limitations, including its reliance on a fixed threshold for trust classification and the potential inability to adequately address outlier behaviors or anomalies. Future work will focus towards the adaptability of proposed model to real-world conditions by using dynamic trust thresholds and integrating advanced anomaly detection techniques. Additionally, further empirical validation through real-world deployment is necessary to assess the model's performance in diverse vehicular environments.

Overall, the PDBTM offers a scalable and lightweight solution for trust management in IoV systems, providing a foundation for future advancements in secure vehicle communication. By addressing its limitations and evolving the model, we aim to contribute significantly to the development of robust and secure IoV networks.

## References

[1] M. Amadeo, C. Campolo, and A. Molinaro, "Priority-based content delivery in the internet of vehicles through named data networking," *J. Sens. Actuator Networks*, vol. 5, no. 4, 2016.

[2] Y. Toor, P. Muhlethaler, A. Laouiti, and A. La Fortelle, "Vehicle Ad Hoc networks: applications and related technical issues," *IEEE Commun. Surv. Tutorials*, vol. 10, no. 3, pp. 74–88, 2008.

[3] F. Bao and I. R. Chen, "Trust management for the Internet of Things and its application to service composition," *2012 IEEE Int. Symp. a World Wireless, Mob. Multimed. Networks, WoWMoM 2012 – Digit. Proc.*, 2012.

[4] L. Angeles and L. Angeles, "Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds," *IEEE 10.1109/WF-IoT.2014.6803166*, pp. 241–246, 2014.

[5] K. Zaidi and M. Rajarajan, "Vehicular internet: Security & privacy challenges and opportunities," *Futur. Internet*, vol. 7, no. 3, pp. 257–275, 2015.

[6] J. Zhang, "A survey on trust management for VANETs," *Proc. – IEEE Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp. 105–112, 2011.

[7] Z. Huang, S. Ruj, M. Cavenaghi, and A. Nayak, "Limitations of trust management schemes in VANET and countermeasures," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, 2011, pp. 1228–1232.

[8] F. Gómez Mármol and G. Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 934–941, 2012.

[9] X. Hong, D. Huang, M. Gerla, and Z. Cao, "{SAT:} Building New Trust Architecture for Vehicular Networks," in *The Third International Workshop on Mobility in the Evolving Internet Architecture*, 2008, pp. 31–36.

[10] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A Data Intensive Reputation Management Scheme for Vehicular Ad Hoc Networks," *Mob. Ubiquitous Syst. Netw. Serv. 2006 Third Annu. Int. Conf.*, no. i, pp. 1–8, 2006.

[11] U. F. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards Expanded Trust Management for Agents in Vehicular Ad-hoc Networks," vol. 2, no. 1, 2016.

[12] F. Dötzer, L. Fischer, and P. Magiera, "VARS: A vehicle ad-hoc network reputation system," *Proc. – 6th IEEE Int. Symp. a World Wirel. Mob. Multimed. Networks, WoWMoM 2005*, no. 1, pp. 454–456, 2005.

[13] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," *IEEE 27th Conf. Comput. Commun.*, pp. 1238–1246, 2008.

[14] C. Chen and R. Cohen, "A Trust Modeling Framework for Message Propagation and Evaluation in VANETs," 2010.

[15] S. Yang, Z. Liu, J. Li, S. Wang, and F. Yang, "Anomaly detection for internet of vehicles: A trust management scheme with affinity propagation," *Mob. Inf. Syst.*, vol. 2016, 2016.

[16] A. Bhargava, S. Verma, B. K. Chaurasia, and G. S. Tomar, "Computational trust model for Internet of Vehicles," *2017 Conf. Inf. Commun. Technol. CICT 2017*, vol. 2018-April, pp. 1–5, 2018.
[17] F. Gai, J. Zhang, P. Z. B, and X. Jiang, "Wireless Algorithms, Systems, and Applications," vol. 10251, no. 1, pp. 344–355, 2017.
[18] Tarun Kumar, Suyel Namasudra, and Prabhat Kumar, "Providing data security using DNA computing in the cloud computing environment", International Journal of Web and Grid Services, vol. 19, no. 4, 2023. DOI: 10.1504/IJWGS.2023.10060351.
[19] Review of Nature and Computation Methods of Trust Models in Vehicular Networks", Indu Bhardwaj, Sibaram Khara Published in Journal of Advanced research in dynamical and control systems, ISSN: 1943-023X, Volume 11, 07-Special Issue, 2019.
[20] Tarun Kumar, Prabhat Kumar, Suyel Namasudra, "A DNA-based Authentication System for Securing Cloud Data Storage and Transactions," In 11th International Conference on Computing for Sustainable Global Development (INDIACom), IEEE New Delhi, India, pp. 1692–1698, 2024.
[21] Indu, Sibaram Khara. "Internet of vehicles (IoV): evolution, architecture, security issues and trust aspects." International Journal of Recent Technology and Engineering (IJRTE) 7, no. 6 (2019).
[22] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Trust on the Ratee: A Trust Management System for Social Internet of Vehicles," vol. 2017, 2017.
[23] M. Nitti, R. Girau, L. Atzori, and S. Member, "Trustworthiness Management in the Social Internet of Things," IEEE Trans. Knowl. Data Eng., vol. 26, no. 5, pp. 1–14, 2014.

## Biographies

**Indu Bhardwaj** has 10 years of expertise in teaching, and research and development. She received her Ph.D. degree in Electronics and Communication

Engineering from Galgotias University, Greater Noida, in wireless communication especially in securing vehicular communication with trust model. She has completed her postdoc from Federal Institute of Science, Education and Technology, IFCE Brazil. She has more than 40 publications in various indexed journals/conferences published by IEEE, Springer, Elsevier, among others. She has published 7 patents. With specialization in wireless Communication her field of Interest includes vehicular Ad-hoc Networks (VANET), Internet of Things (IoT), Internet of vehicles (IoV), Artificial Intelligence (AI), security techniques, Smart Cities, Healthcare, Transportation and Wireless Technologies. She has contributed in the research field as a Faculty Resource Person, Session Chair, Reviewer, Technical Committee member and Conference Secretary in various conferences and journals. She is also serving as member of Editorial Board for Global Journal.

**Ajay Bhardwaj** has 3+ years of expertise in the IT sector, specializing in research and development. He is currently pursuing his M.Tech. from Delhi Technological University (DTU). His research interests span across software development, cloud computing, artificial intelligence (AI), security techniques, and system optimization. He has contributed to the field through various research initiatives, technical innovations, and academic collaborations. Ajay has actively participated in various conferences and journals. His work includes publications in reputed indexed journals and conferences such as IEEE and Springer. He has also filed a patent, reflecting his contributions to technological advancements. With a strong background in software engineering, Ajay's areas of interest include cloud computing, AI-driven solutions, security frameworks, smart city technologies, healthcare IT, and intelligent transportation systems.

**Sibaram Khara** is an Electronics & Communication Engineer. He received Ph.D. in engineering from Jadavpur University, Kolkata, in next-generation wireless heterogeneous network–essentially in the area of interworking network and protocol convergence techniques for cellular and WiFi integrated networks. He did PG in Digital Systems from National Institute of Technology, Allahabad. His industry and teaching experience expands in wide areas of communication and networking engineering. He successfully completed the project for the defense services, to enhance the automation of Terminal Equipment of Message Switching network for efficient information management. Currently he is serving as Vice Chancellor in Sharda University. His major research interests cover the areas of cluster based wireless sensor networks, spectrum mobility in cognitive radio system, call admission control in heterogeneous network and carrier aggregation in LTE-A technology.