An Improved Trustable Routing and Security in Wireless Sensor Network

Manjeeta Damahe
M.Tech. Scholar
Technocrats Institute of Technology- Advance
Bhopal (M.P.)

Pankaj Soni
Professor
Technocrats Institute of Technology- Advance
Bhopal (M.P.)

Manish Gurjar
Professor
Technocrats Institute of Technology- Advance
Bhopal (M.P.)

ABSTRACT

Wireless sensor networks establish a specific type of wireless data communication networks. WSNs have acknowledged remarkable deliberation in current years due to probable applications in armed sensing, fitness care, wildlife tracking, traffic investigation, building constructions monitoring, atmosphere monitoring etc. The central of trust route deceits in gaining trust. Conversely, the present-day trust-based route approaches have some challenging concerns. Finding the trust of a sensor node is most difficult, and just how it can be completed is still uncertain. Routing rules of wireless sensor network naturally adjust themselves with the current environments which may vary with high mobility to low mobility in extremes along with high bandwidth. Detection of malicious node and information safety in a wireless sensor network is an essential work in any sensor network. To achieve availability, integrity and reliability routing rules should be robust against malevolent attacks. We proposed a secure trust value which helps authenticate the sensor node and similarly preserve and safe the sensor network from malicious nodes. We also proposed a novel approach to detect the black hole attack and also keep safe the network from malicious nodes. The network lifetime will improve and energy consumption reduced. Experimental outcomes demonstrate that our scheme is good for wireless sensor network security.

Keywords

Wireless Sensor Network, Network Security, Trust Value, Routing, Confidence value.

1. INTRODUCTION

Ad hoc Wireless network does not have some collective server but is a novel distributed, almost autonomous of any pre-established arrangement system. A MANET [1] is a gathering of moving wireless nodes that can enthusiastically be set up anytime and anywhere without using any preexisting network arrangement. The nodes in the network are themselves responsible for routing the packets from the source to the destination. It is a widely used routing protocol for mobile ad hoc networks (MANETs). These nodes are also responsible to make the transfer of packets secure. Ad hoc On-Demand Distance Vector (AODV). AODV [2] is, as the name suggests, a distance vector routing protocol. It is also used for other wireless ad-hoc networks. AODV is an approachable routing set of rules i.e.it founds a source to a endpoint only on request. In dissimilarity, the widely used routing protocols of the WWW are proactive, i.e. they find routing track autonomously of the usage of the paths.

A wireless sensor network (WSN)[3] encompasses of several lesser sized sensor nodes that have low working out power. It also have communication ability and sensing functionalities. Wireless sensor networks establish a specific type of wireless data communication networks. Every sensor node can sense physical characteristics. WSNs have been the favorite choice for the succeeding generation monitoring and control systems. It can sense temperature, light, vibration, humidity, and electromagnetic strength and so on, and communicate the sensed info[3] to the other node complete a series of numerous in-between nodes that assistance to forward the data.

Sensor node is the central module of WSN. Sensor nodes can be castoff to sense moistness and high temperature. It is similarly used to intellect light and temp. Since particular sensor conveyances only incomplete information; a network of these sensors is used to accomplish large surroundings. The communication component in sensor nodes is used to transfer information. . The design challenges of WSN are limited energy capacity, sensor locations[4], random and massive node disposition, inadequate hardware devices, network system features and data aggregation, unreliable environment, scalability, and assorted recognizing application necessities. In WSNs severe happening data composed by the sensor nodes compulsion to be consistently distributed to the sink for efficacious observing of an environment.

Therefore, error free and reliable data transfer between source and destination is the challenges in WSN. Consistent transfer of data is the surety that the packet carrying event's information reaches at the endpoint. In WSNs, consistency can be categorized into diverse levels end-to-End or Hop-by-Hop dependability Level, and Event or Packet dependability Level. The communication of WSN is not only effected by antenna angle but also weather conditions, obstacles. It is also depends on interference. Nodes in WSNs are disposed to letdown due to hardware letdown, energy reduction, communication link faults, mischievous attack, and so on. The various applications of wireless sensor network are smart grids and energy control systems, industrial applications, transportations and logistics, smart building for example indoor climate control, health care for example medical health diagnostics and health monitoring, precision agriculture, animal tracking, urban terrain tracking and civil structure monitoring, entertainment, security and surveillance. Consistency of WSN is affected by mistakes that may happen due to numerous reasons such as software malfunctions, malfunctioning hardware, dislocation, or environmental hazards. Nodes in sensor networks have very limited energy. The main WSN objectives are less power consumption, better channel utilization, less node cost, small node size, scalability, security, fault tolerance, adaptability, Qos support and self configurability. Routing rules of wireless sensor network naturally adjust themselves with the current environments which may vary with high mobility to low mobility in extremes along with high bandwidth. In ad-hoc network batteries [5] can be replaced as and when needed. The wireless sensor system rules are location based rules [6], mobility based protocols, data centric protocols, QoS based protocols, hierarchical protocols, multipath based protocols, and heterogeneity based protocol. Location based protocols are GAF, TBF, SMECH [7], GeRaF, MECN, GEAR, Span, BVGF.

The network lifetime [8] will improve and energy consumption [9] reduced. We proposed a secure trust value which helps authenticate the sensor node and similarly preserve and safe the sensor network from malicious nodes. We also proposed a novel approach to detect the black hole attack and also keep safe the network from malicious nodes.

2. PROPOSED WORK

Step 1: Initialization of required parameters

Threshold value initialization

Number of nodes, required area setup

Transmission node and destination node initialization

Step 2: Calculation of initial trust value for authentication

Trust value is calculated from timestamp provided by network

Step 3: Request send by source using generated trust value

Step 4: Calculation of Confidence key.

Node number, trust value generated during network initialization and threshold values are used to calculate confidence key.

Confidence key = Product of Threshold value, node value and trust key

This confidence key value is used to validate the node.

Step 5: Path calculation using nearest neighbor, its trust key used to authenticated node.

Step 6: Check whether number of nodes is equal to initial number of nodes.

If yes then Network is valid

Otherwise System is invalid

Stop the simulation

Step 7: Find request reply from node having valid confidence and trust key

If confidence value and trust value is equal to request node trust and confidence value then

Node is authenticated

Node can transfer data

Step 7: Check nodes to find black hole attack in the network

If node dropping packets at regular interval and performance is degraded below threshold value then black hole attack is identified in the node.

The threshold value is used to check the performance of the network.

Node is marked as malicious node and system reject any request from that node.

Step 8: The source can select other authenticate node from available neighbors

If other nodes are authenticated nodes then select nodes for path creation

Otherwise backup nodes are used to select different authenticated nodes from list.

Step 9: Secure path creation from source to destination.

Step 10: End

The first step initializes all the required parameters, number of nodes, and threshold value for the network. The threshold key is agreed as 0.75. The required dimensional are setup is also provided to the system. The system also initializes transmission node and destination node for algorithm. The next step is the calculation of initial trust value for authentication. The trust value is calculated from timestamp provided by network. This trust value along with confidence key is used for node authentication.

In the next step the request send by source using generated trust value. The trust value is system timestamp in seconds. The subsequent stage is to compute the confidence key. Node number, trust value generated during network initialization and threshold values are used to calculate confidence key. Confidence key is equal to product of threshold value, node value and trust key. This confidence key value is used to validate the node.

The next step is the path calculation using nearest neighbor, its trust key used to authenticated node. The next step is to check whether number of nodes is equal to initial number of nodes. If yes then Network is valid otherwise system is invalid. The system can stop the simulation. The next step is to find request reply from node having valid confidence and trust key. If confidence value and trust value is equal to request node trust and confidence value then marked node is authenticated, node can transfer data using confidence and trust key.

The next step is to check nodes to find black hole attack in the network. If node dropping packets at regular interval and performance is degraded below threshold value then black hole attack is identified in the node. The threshold value is used to check the performance of the network. Node is marked as malicious node and system reject any request from that node. The next step is he source can select other authenticate node from available neighbors. If other nodes are authenticated nodes then select nodes for path creation. Otherwise backup nodes are used to select different authenticated nodes from list. The last step is secure path creation from source to destination. After path creation source can transmit data using secure path.

3. IMPLEMENTATION AND RESULT ANALYSIS

Network Simulator 2 simulator tool is used for implementation of our suggested algorithm. NS2 uses TCL programming language for front end and C/C++ language for back end. We performed our experiment in PIV 3.0 GHz machine with 1GB RAM.

For implementation 50 nodes are used with and without mobility. The nodes are arbitrarily positioned in dissimilar parts of positioning part with a static density.

For this implementation, network parameters, such as Dimension, Number of nodes, traffic, transmission rate,

Routing protocol, transmission range, sensitivity, transmission power etc., are used. The simulation is 500 X 500 m in range. Transmission range is specified as 300m. Movement model is used as random waypoint. Simulation duration is set as 90s. Traffic type is set as constant bit rate. Radio range is set as 250m. Data pay load is set as 512 bytes.

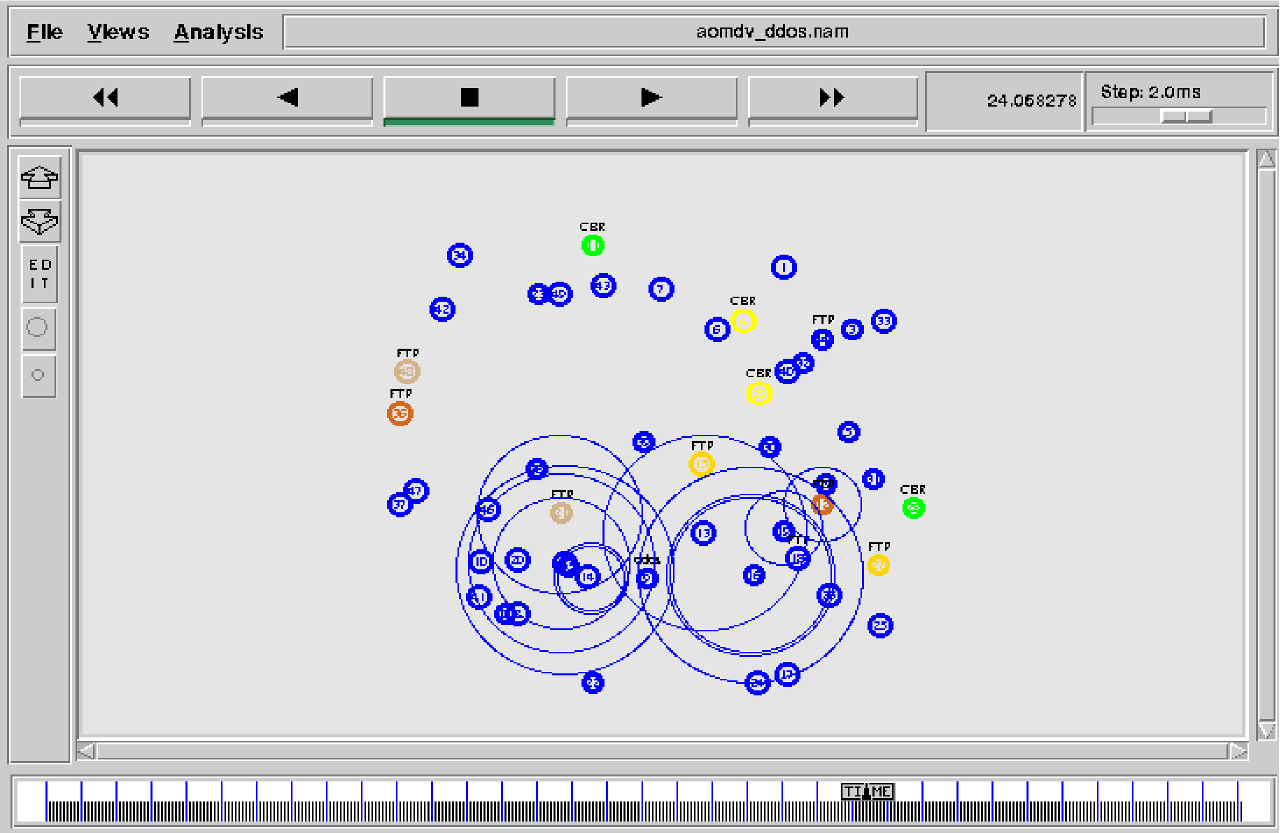

Figure1: Simulation with Path Discovery in Network

Figure above represented the path discovery in a network. The nodes are sending request to the neighbors and the nearest secure node is selected as secure node with trust and confidential key.

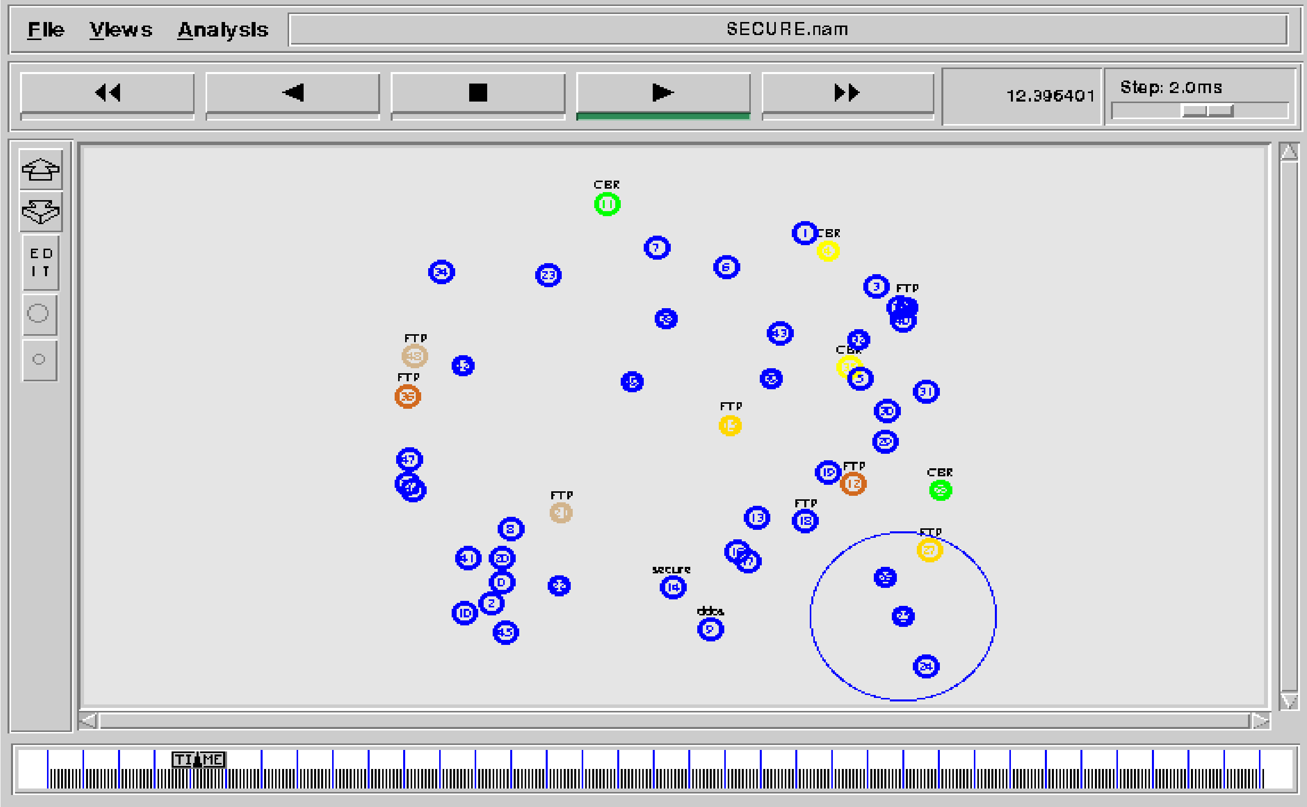

Figure2: Simulation with Secure Data Transmission in a Network

The final screen represented the secured data transmission in a network with the help of confidential and trust key.

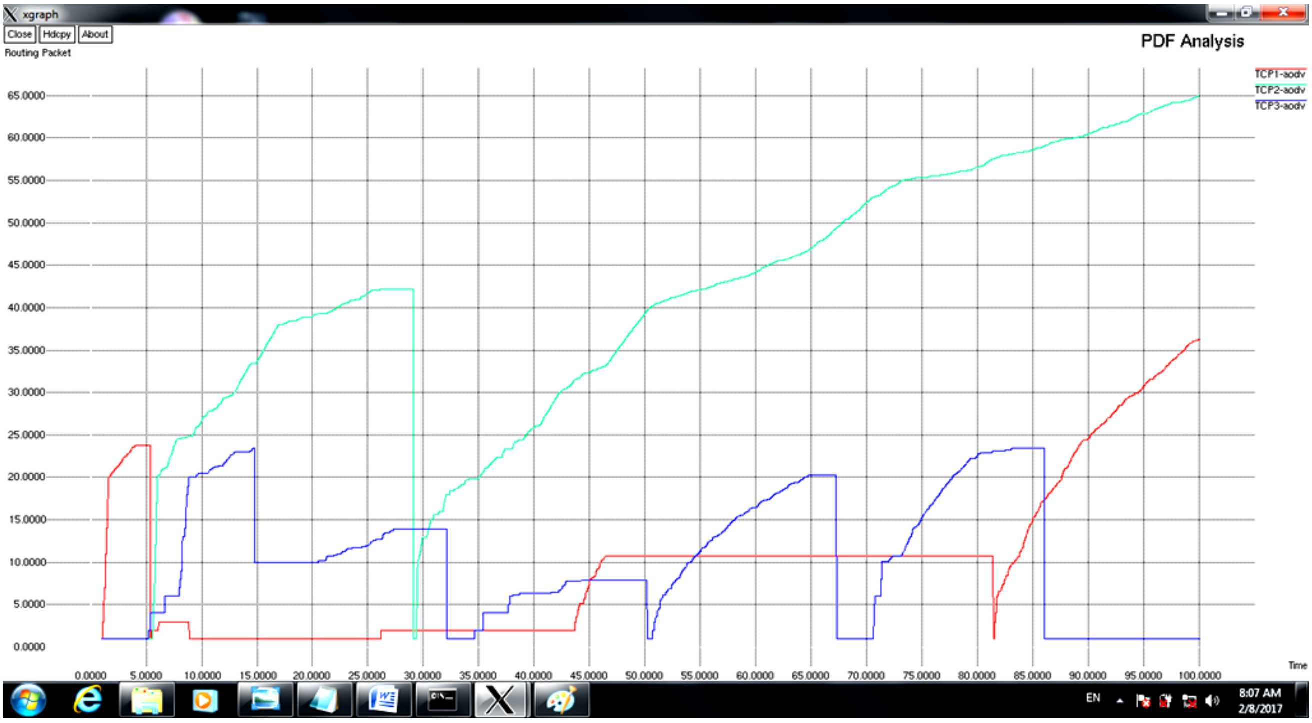

Figure 3: PDR Analysis

The Packet Delivery Ratio(PDR) performance of black hole attack and security scheme is describe in this graph. By black hole attack technique the attacker drop of packet is humiliates the percentage ratio of data receiving. Before the attacker drop of packets is maximum and after using black hole attacker the drop of packets ratio is minimum.

4. CONCLUSION

We proposed an innovative methodology keep safe the network from malicious nodes and detect the black hole occurrence in the wireless sensor system.

We used secure trust and confidential keys which help authenticate the sensor node and similarly preserve and safe the sensor network from black hole malevolent nodes. This algorithm used different secure neighbor node to discover altered secure pathway if there is black hole attack in the scheme. The data distribution rate is also tested to discover performance of the system. The proposed system improved network lifetime and energy ingestion reduced to improve the quality of services. The experiment performed using NS2 network simulator and can be executed in physical wireless sensor networks for security and quality of services.

In future we are planning to improve energy proficiency of the wireless sensor network so that quality of services increases.

We are also planning to practically implement our system in remote security system to improve privacy of the network.

5. REFERENCES

[1] Yuxin Liu, Mianxiong Dong, Kaoru Ota, and Anfeng Liu, ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks, IEEE Transactions on Information Forensics And Security, Vol. 11, No. 9, pp-2013-2018, September 2016,

[2] M. Dong, K. Ota, A. Liu, and M. Guo, "Joint optimization of lifetime and transport delay under reliability constraint wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 1, pp. 225–236, Jan. 2016.

[3] X. Liu, M. Dong, K. Ota, P. Hung, and A. Liu, "Service pricing decision in cyber-physical systems: Insights from game theory," *IEEE Trans.ServicesComput.*, vol. 9, no. 2, pp. 186–198, Mar./Apr. 2016.

[4] A. Liu, M. Dong, K. Ota, and J. Long, "PHACK: An efficient scheme for selective forwarding attack detection in WSNs," *Sensors*, vol. 15, no. 12, pp. 30942–30963, 2015.

[5] P. Zhou, S. Jiang, A. Irissappane, J. Zhang, J. Zhou, and J. C. M. Teo, "Toward energy-efficient trust system through watchdog optimization for WSNs," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 613–625, Mar. 2015.

[6] Vittorio P. Illiano and Emil C. Lupu, Detecting Malicious Data Injections in Event Detection Wireless Sensor Networks, IEEE Transactions 0n Network And Service Management, Vol. 12, No. 3, September 2015, pp-496-512

[7] Qiang Ma, Kebin Liu, Zhichao Cao, Tong Zhu, Yunhao Liu, Link Scanner: Faulty Link Detection for Wireless Sensor Networks, IEEE Transactions on Wireless Communications, Vol. 14, pp 4428-4438, Aug 2015

[8] W. Dong, Y. Liu, Y. He, T. Zhu, and C. Chen, "Measurement and analysis on the packet delivery performance in a large-scale sensor network," IEEE/ACM Trans. Netw., vol. 22, no. 6, pp. 1952–1963, Dec. 2014.

[9] Q. Ma, K. Liu, T. Zhu, W. Gong, and Y. Liu, “BOND: Exploring hidden bottleneck nodes in large-scale wireless sensor networks,” in Proc. IEEE ICDCS, Madrid, Spain, 2014, pp. 399–408.

[10] X. Li, Q. Ma, Z. Cao, K. Liu, and Y. Liu, “Enhancing visibility of network performance in large-scale sensor networks,” in Proc. IEEE ICDCS, Madrid, Spain, 2014, pp. 409–418.

[11] Z. Li, Y. Liu, M. Li, J. Wang, and Z. Cao, “Exploiting ubiquitous data collection for mobile users in wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 2, pp. 312–326, Feb. 2013.

[12] Q. Ma, K. Liu, X. Miao, and Y. Liu, “Sherlock is around: Detecting network failures with local evidence fusion,” in Proc. IEEE INFOCOM, Orlando, FL, USA, 2012, pp. 1430–1440.

[13] Y. Liu et al. Does wireless sensor network scale? A measurement study on greenorbs,” in Proc. IEEE INFOCOM, Shanghai, China, 2011, pp. 873–881.

[14] H. Zhang, “Experimental analysis of link estimation methods in low power wireless networks,” Tsinghua Sci. Technol., vol. 16, no. 5, pp. 539–552, Oct. 2011.

[15] E. Magistretti, O. Gurewitz, and E. Knightly, “Inferring and mitigating a link’s hindering transmissions in managed 802.11 wireless networks,” in Proc. ACM MobiCom, Chicago, IL, USA, 2010, pp. 305–316.

[16] Y. Liu, K. Liu, and M. Li, “Passive diagnosis for wireless sensor networks,” IEEE/ACM Trans. Netw., vol. 18, no. 4, pp.1132–1144, Aug.2010.

6. AUTHOR PROFILE

Ms. Manjeeta Damahe has received her Engineering degree in Electronics & Telecommunication in June 2014 from Shri Shankaracharya Engineering College (CSVTU), BHILAI(C.G.) India and currently pursuing Master of Technology degree in Digital Communication from Technocrats Institute of Technology- Advance under Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV), Bhopal, (M.P.) India.

Prof. Pankaj Soni has received his Engineering degree in June 2008 and Master of Technology degree in Dec 2012 from Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV), Bhopal, (M.P.) India. He is currently working as Professor in department of Electronics & Communication in Technocrats Institute of Technology- Advance, Bhopal, (M.P.) India. He has five years teaching experience. He has published ten international research papers. His research interest is in Digital Communication, Wireless Communication and VLSI Design.

Prof. Manish Gurjar has received his Engineering degree in June 2003 and Master of Technology degree in June 2011 from Rajiv Gandhi Proudyogiki Vishwavidyalaya (RGPV), Bhopal, (M.P.) India. He is currently working as Professor in department of Electronics & Communication in Technocrats Institute of Technology- Advance, Bhopal, (M.P.) India. He has five years teaching experience. He has published six international research papers. His research interest is in Digital Communication, Wireless Communication and VLSI Design.