International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

Detection of DoS Attacks in MANET using LIBSVM

Divya Gautam, Vrinda Tokekar

Abstract: ***In MANET(Mobile Ad Hoc Network) nodes are moving constantly so it is difficult to identify benign request and attacker's request. Denial of service attack (DoS) is one of the prominent threat in all types of networks. In MANET, DoS attacks are one of the factor for resource depletion of the victim node. The objective of this paper is to develop a framework to identify the DoS attacks in MANET. This paper emphasizes on the detection of DoS attacks in MANET based on various parameters like bit rate, PDR, delay etc. The simulation will compare and classify the benign and the malicious traffic by classification and testing using SVM. In this paper the behaviour of network traffic is analysed in normal scenerio and attack scenerio and then compairsion is done. The entire work is carried on the LIBSVM simulator and dataset for MANET is generated on NS2.***

Index Terms: DoS, MANET, LIBSVM, Adhoc networks.

I. INTRODUCTION

The Mobile Ad-hoc Network (MANET) is a collection of self configuring mobile machines (node) having novel established communication network. In MANET each node gets connect by using wireless radio interface with0 the help of wireless links. DoS attacks came in picture in June 1998. Many machines start attacking on the Internet. The attacker installs software for launching DoS attacks on the machines, which will act as zombies or agents. These agents launch attacks to the target website in a coordinated manner. DoS attacks are a major and frequent disturbance on the Internet [1].

MANET is used widely in various sectors like military, research and development etc. So security has become a priority to secure nodes in network.
There are various factors that are responsible for alteration of security in network:
1. Dynamic Topology
2. Lack of central server
3. Unreliable Wireless links
4. Nomadic Environment

There are basically two approaches to secure network in MANET(Figure 1).

Manuscript published on 30 June 2019.
* Correspondence Author (s)
Ms. Divya, assistant professor at Amity University has obtained Masters in Engineering degree from Institute of Engineering and Technology, Devi Ahilyabai Vishwavidhyalaya, Indore
Dr. Vrinda Tokekar, Professor Dept. of Information Technology, Institute of Engineering and Technology (UTD) and Head, Information Technology Centre (IT Centre), Devi Ahilya University, Indore, (M.P.) (NAAC 'A' Grade, has obtained Ph.D. (Computer Engineering), 2007, Devi Ahilya University, Indore

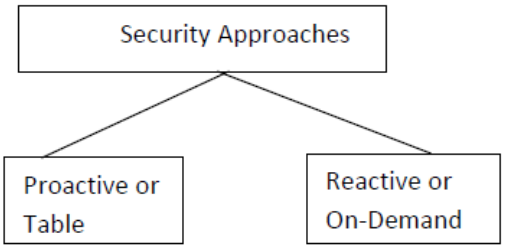

Figure 1: Various Security Approaches

1. Proactive Approach: In proactive method various cryptographic techniques are used to secure the network. In this sender encrypts the data by using some code and receiver decrypts the data by using same code method.
2. Reactive Approach: Reactive approach detects threats posterior and behaves accordingly.

Each approach has its own features and drawbacks and addresses different security problems in MANET. For E.g Proactive approach is used by secure routing protocols to secure messages that route between nodes and Reactive method is used to protect packet transfer operations.

A. Other Security Approaches

1. Wormhole Attack: In the wormhole attack attacker store packet at one location and route packets to its known location and retransmit packets there into the network. This retransmission creates confusion as nodes cannot distinguish between genuine packets and retransmitted packets. An extra information called LEASH is attached to packet. Packet's maximum route distance is restricted by LEASH. There are two main leashes:

Geographical Leash: It states that the receiver of the data packet is in some specific interval of the sender. Signature scheme is used in conjunction with the geographical leash to catch the intruders that reside at multiple locations.

Temporal Leash: In temporal leash there is an higher bound on each packet that limits the maximum travel path of the packet. Receiver sends some information to sender if packet travels more distance than the specified.

2. Black Hole Attack: Black hole attack also called packet drop attack. A router discards packets. For this security aware routing (SAR) protocol is used. A security unit is added into route request packet (RREQ) At the intermediate node if the faith level is described, the node will transfer the RREQ. RREP is generated by destination with the specific security metric.

3. Repudiation Attack: For this authenticating routing ad hoc network (ARAN) is used. ARAN ensures authentic services by using signature or pattern techniques. Each node verifies the pattern of previous neighbouring node and replaces it with its own pattern.

4. Digital Signature: Digital signature is based on cryptographic techniques i.e. Asymmetric Key Cryptographic (basically use RSA algorithm) via encryption and decryption operations. In this the attacker feed the node with large number of fake signatures to destroy the energy and resources of victim node. That's why it is less resilient against DOS attack.

5. Intrusion Detection Techniques: In this each node runs IDS agent. Adjacent nodes cooperate with each other. Nodes observe the behaviour of neighbouring nodes, detect intruders, make decisions and take actions.

6. Watchdog: Watchdog always improves the performance of the network by intensifying the disruptive nodes. Watchdog firstly sends packets in buffer storage and observes the nature of neighbouring nodes. Watchdog investigates the packet if the neighbouring nodes transfer the packet without any modification or not. Packets are discarded if the packet that are investigated match with the node's buffer. Packets that remain in storage exceeding time period without any match are dropped and discarded. The node that forwards the data is flagged as malicious. If the number of violations exceeds the specified threshold, violation node is marked as suspicious.

7. Secure Message Transmission: The protocol that has complete information about network determines the set of diverse path that connect the source and the destination. Then it disperses the message into N Pieces and allows the successful reception of N pieces at the receiver. Each piece is attached with cryptographic header that provides authenticity and is transferred with along one of the paths. On reception of packets receiver generates an acknowledgement response and inform that all packets are intact. If packets that are received is less than the specified the source retransmit the packet over intact path.

8. Message Authentication Elements: There are three elements that check the authenticity of message transmitted between nodes. HMAC (Hashed Message Authentication Code): In these two nodes uses a common private symmetric key that verifies the authenticity of message using one way hash function. The computation by HMAC is very systematic that small sensor devices can easily afford.

II. DOS Attack in MANET

In Rutvij H jhaveri et al.[2], explains DOS attack, Denial of service attack or DOS attack suspicious nodes generates false messages and slows down the operation of network or consume network resources. Malicious node exhausts the power or battery of affected node by consuming network services and resources. Thus resources or services are available to the unintended users.

In [3] Singh,A. states that As the name implies DOS tries to access the resources. DOS is attack on security of system and MANET that causes drop of resources or services to legitimate users. There is drop of network connection, resources and services through the unused exhaustion of bandwidth of network or overloading the resources of system.

III. EFFECT OF DOS ATTACK ON MANET

A survey of DOS attack on network that are used in to determine the effect of DOS attack in MANET was carried out by Rutvij H jhaveri et al. [2]. DOS attack is extreme severe attack on MANET. Network can easily be crashed because each hop on the network has limited power or battery. Network can easily be congested because malicious node generates false messages or network has limited bandwidth as compared to wired network. Singh,A.[3] says that DDOS(Distributed Denial of Service) attack main aim is not o break the system. It retards the use of network services or resources to the intended users who actually need them. Its harmful effects are:

1. Crash the system.
2. Prevents transmission between nodes.
3. Network or system is down or reduce speed that's why productivity is affected.
4. Hang the system so there is no reboot.

It is very difficult to protect against DoS because there is no specific vulnerability of the system to be targeted. Here the attacker is also the member of the network.

III. DOS COMBAT FRAMEWORK

Intrusion Detection System and Intrusion Prevention Systems are very known terms in security domain. In the same way there is a framework (Figure 2) which contains DDoS attack detection and DDoS attack prevention [4]. However, it is required to differentiate the legitimate traffic from attack traffic. The definitions of detection and preventions vary in various contexts of DDoS attacks [5] [6].

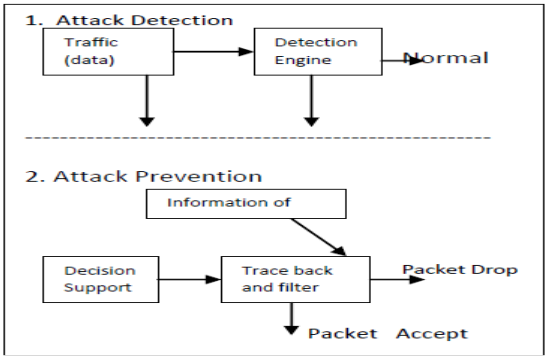

Figure 2 : Simple DoS Combating Framework

In this research work one of the machine learning algorithm is applied known as Support Vector Machine (SVM) developed by V.N.Vapnik[7] based on statistical learning theory.

LIBSVM is a library for Support Vector Machines (SVMs). This package is actively being developed continuously from the year 2000. The ultimate goal is to help researchers to apply support vector machines on their applications. In machine learning, LIBSVM is a very popular tool. In LIBSVM two step processes is done; first is to train the data set to get a model and then to test the data set to predict the model.

LIBSVM is a tool for checking the parameters grids. For each and every parameter setting, cross validation accuracy is obtained by LIBSVM. At the end the highest cross validation accuracy is obtained. RBF also called as Gaussian kernel is used with other kernels. LIBSVM gives the output by plotting contours of cross validation accuracy.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

IV. LITERATURE REVIEW

Rajani Muraleedharan et al. [8] elaborated the attack system and assessed the attack like worm hole, sybil and jamming attacks by applying swarm intelligence algorithm. They also discussed how the efficiencies of a system can be augmented by adding Bayesian Network (BN) algorithm.

Anupama Mishra et al. [9] provide another good approach to combat with Dos attacks and provide a security mechanism to handle the threat. In this paper they denied the complete protection against the DoS attack, therefore, they suggested one should try to improve quality of service using intrusion tolerance mechanisms.

Jawwad Shams et al. [10] presented a model to evaluate quality of service for a network under severe attacks. Their model is able to assess the disruptive network behaviour even though a network is under DoS attacks.

K. Pradeep Mohan [11] elaborated a detection system to analyse computer systems and network traffic in order to detect any unusual behavior of the original user behavior. Numbers of experiments were conducted on the hybrid PSO-SVM model with PMU2015 datasets to assess the effectiveness of their feature selection and its parameters in building effective IDS.

Khalid A. Fakieh et al. [12] have mentioned about various work done on DoS attack and in addition of this they have analysed the prevention and detection techniques of DDoS attacks in cloud.

Jin Ye et al. [13] have worked with software defined networks. They have used SVM for classification and testing. The accuracy rate they have achieved is about 95%.

V. PROPOSED DOS DETECTION ENGINE

This paper proposes a novel detection method based on Support Vector Machine (SVM) for DoS attack in mobile ad hoc networks. Steps for Proposed Methodology (Figure 3):

1. Prepare Data Sets for both the scenarios (attack and normal) MANET using simulator containing various attributes of the nodes such as PDR, bit rate, delay etc. the synthesis of the attack data set is done by changing the properties of packets of various nodes. These nodes will act as malicious nodes.
2. Apply both the dataset (attack and normal) on LIBSVM for classification and testing of dataset.
3. This paper specifies six parameters i.e. bit rate, delay etc (Table 1).
4. Results obtained in both the scenarios will be compared and finally classified data set will be obtained. Results are shown in Table 2 and 3. Following is the framework of proposed DDoS detection engine.

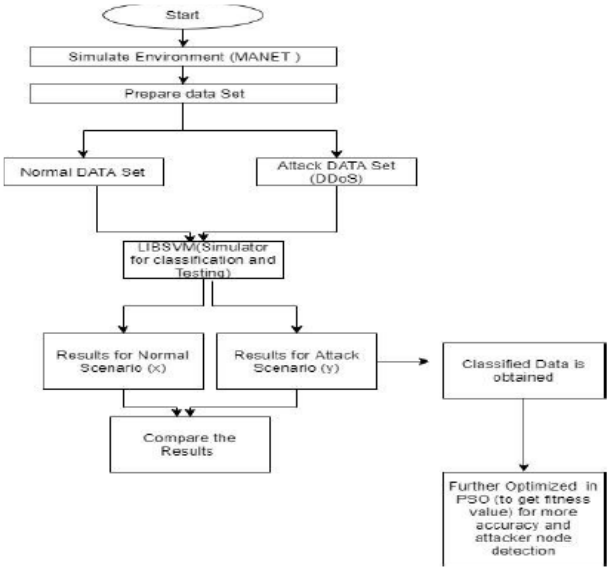

Fig 3. Proposed Framework for DDoS Detection Engine

VI. RESULTS AND SIMULATION

In this work NS-2 simulator is used to simulate the Mobile Ad-hoc network. A scenario is designed to create some mobile node and these nodes are able to communicate wirelessly. The communication range of each node is 250 meters. When simulation runs it generate a trace file, in which all the activities of network is recorded. Using this trace, Packet Delivery Ratio, Bit rate, Delay, Entropy, Change in Bit rate and change in Delay are calculated and save all those parameters in a text file [14]. AWK script is used to calculate the parameters. In this way for on run of a ns-2 simulation a record is saved in the file. Simulation runs (Algorithm 1) for 1000 times and for each time a record is entered in the text file (Figure 4). This file is used as a dataset for the SVM. In this work LIBSVM [15] tool is used to apply SVM on the dataset generated. LIBSVM is simple, easy-to-use, and efficient software for SVM classification and regression. It can solve C-SVM classification, nu-SVM classification, one-class-SVM, epsilon-SVM regression, and nu-SVM regression. It also provides an automatic model selection tool for C-SVM classification.

Algorithm 1. (Creation of Dataset for Training of LIBSVM)

Step 1: Start

Step 2: Create NS-2 Scenario

Step 3: for (i=1 to 1000) //For creation of dataset of 1000 records.

{

Step 4: Run NS-2 Simulation

Step 5: Perform an entry of PDR, Bit Rate, Entropy, Delay, Change in Delay, Change in Bit Rate to a file.

Step 6: Perform an entry of parameters of previous step for each individual node.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

//In step 5 and step 6 a dataset is created for whole scenario and for each individual node into separate files.

}

Step 7: End.

Format of the text file generated as a result of 1000 ns-2 simulation run shown in figure (Figure 4) and six columns in figure 4 represents parameters in described in Table 1.

```
1 74.26 2.86 330.66 1.87 72.26 2.50
2 74.40 3.16 347.00 1.87 73.40 3.41
3 74.34 2.91 342.83 1.87 74.00 2.19
4 74.15 2.91 325.58 1.87 74.10 2.19
5 73.88 2.91 332.61 1.87 74.00 2.01
6 73.99 2.84 356.83 1.87 74.00 2.24
```

Figure: 4: Data Set obtained on NS-2

Table 1 : Data set Parameters

Column 1	PDR
Column 2	Delay
Column 3	Bitrate
Column 4	Entropy
Column 5	Change in Bitrate
Column 6	Change in Delay

Libsvm do not accept dataset in this format so it should be changed in to the format of libsvm. For this purpose some files are written for manipulating the program to change above file into the format that is accepted by the libsvm.

```
1 +1 1:74.26 2:2.86 3:330.66 4:1.87 5:72.26 6:2.50
2 +1 1:74.40 2:3.16 3:347.00 4:1.87 5:73.40 6:3.41
3 -1 1:74.34 2:2.91 3:342.83 4:1.87 5:74.00 6:2.19
4 +1 1:74.15 2:2.91 3:325.58 4:1.87 5:74.10 6:2.19
5 -1 1:73.88 2:2.91 3:332.61 4:1.87 5:74.00 6:2.01
6 -1 1:73.99 2:2.84 3:356.83 4:1.87 5:74.00 6:2.24
```

Figure 5: Format of the text file accepted by libsvm:

In libsvm the file format which is accepted shown in figure 5. So dataset is converted in the format of LIBSVM.

A. Calculation of threshold

A threshold is also calculated using awk script. All the six parameters are taken shown above in calculation of threshold value of the network.

Libsvm: Apply libsvm on the dataset generated by running the ns-2 simulation for 1000 times. As a result, accuracy graph has been obtained (Figure 5).

B. Result and Analysis

To carry out this research, LIBSVM is used for classification purpose. NS-2 simulator is used to generate the dataset in normal scenario and attack scenario. To create mobile ad hoc environment, total 11 nodes are used to generate the dataset. Dataset is created using above listed parameters (Table 1) and converted this dataset in the format accepted by LIBSVM. The dataset is created in normal scenario and obtained the simulation results (Accuracy). Then 3 malicious nodes are introduced in the scenario (total nodes are still 11) and got a new traffic (dataset). While applying LIBSVM on both the dataset, the ratio between training and testing dataset is kept as 7:3. On comparing the two; attack and normal traffic, it has been found that accuracy(Table 2) in normal traffic achieved is very high (upto 97%) in comparison to the accuracy (Table 2) achieved in attack traffic (upto 73%).

Table 2: Parameter of Simulation

Parameters	Value
No of nodes	11
Grid size	100*100
Simulation Run time	200 sec
Dataset parameters[ ]	1. pdr 2. delay 3. bitrate 4. entropy 5. increase rate of bitrate 6. increase rate of delay
Train dataset : test dataset	7:3

A. Normal Scenario

While running the normal scenario (non attack traffic) different accuracies have been achieved by using LIBSVM (Table 3). Figure 6 shows the accuracy obtained during simulation where testing data is 450 and training data is 1500.

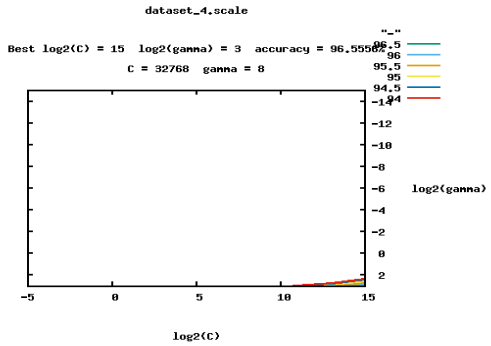

Figure 6. In Normal scenario accuracy obtained 96.5%.

Table 3: Normal scenario

S No.	Training Data	Testing Data	Features	Accuracy (%)
1	300	90	6	96.55
2	500	150	6	97.33
3	1000	300	6	88
4	1500	450	6	96.45
5	2000	600	6	88.5

B. Attack Scenario

While running the attack scenario (attack traffic) for different testing and training data set accuracy obtained is in between 68 to 81% (Table 4). The Figure 7 shows the accuracy obtained during simulation where testing data is 450 and training data is 1500.

Table 4: Attack scenario

Sr. No.	Training Data	Testing Data	Features	Accuracy(%)
1	300	90	6	70
2	500	150	6	68
3	1000	300	6	72
4	1500	450	6	81.81
5	2000	600	6	69

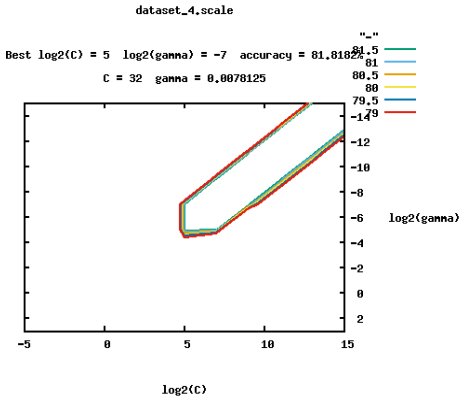

Figure 7. In Attack scenario maximum accuracy obtained is 81.81%.

VII. CONCLUSION

In this paper network traffic of MANET is generated on NS 2. Six tuple characteristic values are extracted which are related to DoS attack and then applied SVM. These six attributes of DoS attacks characteristics have taken for the purpose of analysing the network traffic as shown in table 1. The entire work is focussed on comparing the traffics generated on NS-2 in MANET experimental environment. It is clearly visible that the accuracy coming in normal traffic is very high in comparison to attack traffic. In case of attack scenario the accuracy ranges from 69% to 81% which is much lesser than the accuracy obtained in normal scenario. There is a need to improve the accuracy to identify the attack traffic and attacker node. Hence, from this study it can be concluded that SVM alone is not capable of detecting DoS attack properly. Besides, it is required to use an optimisation technique such as PSO along with SVM in order to improve the accuracy of DoS detection in attack scenario.

REFERENCES

1. Xiang Xu, Ding Wei, Yuelei Zhang, "Improved Detection Approach for Distributed Denial of Service Attack Based on SVM" IEEE 978-1-4577-0856 (2011).
2. Jhaveri, Dr Rutvij & Patel, Sankita & Jinwala, Devesh. (2012). DoS Attacks in Mobile Ad Hoc Networks: A Survey. Proceedings - 2012 2nd International Conference on Advanced Computing and Communication Technologies, ACCT 2012. 535-541. 10.1109/ACCT.2012.48.
3. Singh, A. "Demystifying Denial-Of-Service attacks", part one. A report on Symantec site.
4. Sriparna Saha, Ashok Singh Sairam, Asif Ekbal, " Genetic Algorithm Combined with Support Vector Machine for Building an Intrusion Detection System" International Conference on Advances in Computing, Communications and Informatics ICACCI : 566-572 (2012) .
5. Anupama Mishra, B. B. Gupta, R. C. Joshi, "A Comparative study of Distributed Denial of Service Attacks, Intrusion Tolerance and mitigation Techniques," in the proceedings of 2011 European Intelligence and Security Informatics Conference (EISIC 2011), September 12-14, 2011, DOI: 10.1109/EISIC.2011.15, Athens, Greece.
6. Jin Ye,1,2 Xiangyang Cheng, Jian Zhu, Luting Feng, and Ling Song "A DDoS Attack Detection Method Based on SVM in Software Defined Network", Hindawi,Security and Communication Networks, Volume 2018, Article ID 9804061, 8 pages.
7. Vapnik V., "Statistical Learning Theory", Wiley, New York, 1998.
8. Rajani Muraleedharan and Dr. Lisa Ann Osadciw "An intrusion detection framework for sensor networks using ant colony" , ACM Digital Library, Proceeding Asilomar'09 Proceedings of the 43rd Asilomar conference on Signals, systems and computers Pages 275-278.
9. Anupama Mishra, B. B. Gupta, R. C. Joshi, " A Comparative study of Distributed Denial of Service Attacks, Intrusion Tolerance and mitigation Techniques" EISIC '11 Proceedings of the 2011 European Intelligence and Security Informatics Conference Pages 286-289 IEEE Computer Society Washington, DC, USA ISBN: 978-0-7695-4406-9 (2011).
10. Jawwad Shamsi and Monica Brockmeyer "Evaluation of QoS-compliant overlays under Denial of Service Attacks" Proceedings of the 2010 Spring Simulation Multiconference, SpringSim 2010, Orlando, Florida, USA, April 11-15, 2010.
11. Dr.Aramuthan K.Pradeep Mohan Kumar "Hybrid Network Intrusion Detection for DoS Attacks", International Journal of Control Theory and Applications. Volume 9 Issue 26 Pages 15-22.
12. Khalid A. Fakieh, King Abdullaziz University "An Overview of DDOS Attacks Detection and Prevention in the Cloud", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868, Foundation of Computer Science FCS, New York, USA, Volume 11 – No. 7, December 2016.
13. Jin Ye, Xiangyang Cheng, Jian Zhu, Luting Feng, and Ling Song, "A DDoS Attack Detection Method Based on SVM in Software Defined Network," Security and Communication Networks, vol. 2018, Article ID 9804061, 8 pages, 2018. https://doi.org/10.1155/2018/9804061.
14. Loukas, George & Oke, Gulay & Gelenbe, Erol. (2008). Defending against Denial of Service in a Self-Aware Network: A practical approach. Conference : NATO Symposium on Information Assurance for Emerging and Future Military Systems, At Ljubljana, Sloveni (2008).
15. Chih-Chung Chang and Chih-Jen Lin, LIBSVM : a library for support vector machines. ACM Transactions on Intelligent Systems and Technology, 2:27:1--27:27, 2011. Software available at http://www.csie.ntu.edu.tw/~cjlin/libsvm

AUTHORS PROFILE

Ms. Divya Gautam is currently a research scholar at Institute of Engineering and Technology, Devi Ahilyabai Vishwavidhyalaya, Indore and working as assistant professor at Amity University has obtained Masters in Engineering degree from Institute of Engineering and Technology, Devi Ahilyabai Vishwavidhyalaya, Indore in Information Technology(Specialisation in Information Security) and Bachelor's of Engineering from Madhav Institute of Science and Technology(Autonomous Institute), Gwalior. She is having 12 years of experience. 5 years as Head of Department –Information Technology at Malwa Institute of Technology, Indore.

Dr. Vrinda Tokekar is currently a Professor and Head, Dept. of Information Technology, Institute of Engineering and Technology (UTD) and Head, Information Technology Centre (IT Centre), Devi Ahilya University, Indore, (M.P.) (NAAC 'A' Grade, has obtained Ph.D. (Computer Engineering), 2007, Devi Ahilya University, Indore (M.P.), M.E. (Computer Engineering), 1992, S.G.S.I.T.S.,

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

Indore (M.P.), B.E. (Hons.) (Electrical and Electronics Engineering), 1984, BITS, Pilani (Raj.). She has teaching experience of more than 29 years and specialized in the field of Computer Communication Networks, Wireless and Mobile Adhoc Network and Information Security. She has Guided many PhDs.