Multivariate Correlation Analysis for Denial-of-Service Attack Detection.

Dipali A. Kamble , Amruta Amune

Abstract— **Net servers, info servers, cloud computing servers etc, are interconnected systems and they are currently below threads from network attackers. Mutually of commonest and aggressive suggests that Denial-of-Service (DoS) attacks cause serious effect on these computing systems. In this paper, present the DoS attack detection system that uses MCA (Multivariate Correlation Analysis) for exact characterization of network traffic by extracting the geometrical correlations between features of network traffic.**

Proposed MCA-based DoS attack detection system employs a principle of anomaly based detection in attack recognition. This makes the solution capable of finding unknown and known DoS attacks effectively by learning patterns of legitimate network traffic only.

Index Terms— **Denial of Service Attack, multivariate correlations, Network traffic characterisation, Triangle area**

I. INTRODUCTION

DENIAL-OF-SERVICE attacks are one type of menacing intrusive behavior aggressive and for online servers. DoS attacks severely decrease the availability of a victim, which can be a node, a router, a host, or an entire network. They inflict intensive calculation tasks to the victim by flooding it with huge amount of useless packets or exploiting its system vulnerability. The victim can be forced out of the service from a several days to even few minutes. It causes serious damages to a services running on the victim. Therefore, effective finding of DoS attacks is important to a protection of online services. Work on DoS attack detection the primary focuses on the development of network-based detection techniques.

Detection systems based on these techniques monitor transmitting traffic over protected networks. These mechanisms release the protected online servers from the monitoring attacks and ensure that the servers can dedicate themselves to provide quality services with minimum delay in response. Distributed opportunistic scheduling (DOS) is inherently more complicated than conventional opportunistic scheduling due to the absence of a central entity that knows the channel state of all stations [6]. Interconnected systems, such as cloud computing servers, database servers and web servers etc., are now under threads from network attackers. As one of most common attack is Denial of Service (DoS) these attacks cause serious impact on the computing system [8].

Denial of Service (DOS) attacks are unlimited threat to internet sites and among the hardest security problems in today's Internet. The problem of DoS attacks has become well known, but it has been difficult to find out the Denial of Service in the Internet. Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on an availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. Researchers have come up with more and more specific solutions to a DDoS problem [10].

With DOS, stations [9] use random access to dispute for the channel and upon winning a competition, they measure the conditions of channel. After measuring a channel conditions it gives up the transmission opportunity if channel quality is not good; otherwise, the station only transmits if the channel quality is good. For selfish users the distributed nature of DOS makes it vulnerable. A selfish user can gain a greater share of wireless resources at charges of well-behaved users by using more transmission opportunities and deviating from.

II. OVERVIEW OF DOS ATTACKS

A. Denial of Service Type

A Denial of Service attack is characterized by the attackers to prevent legitimate users of a service by an explicit attempt from using that service. Examples include, attempts to disrupt connections between two machines thereby preventing access to the service, attempts to flood a network, thereby preventing legitimate network traffic.

Attempts to prevent the particular individual from accessing a service, Attempts to disrupt service to the specific system or person. Maintaining Integrity of the Specifications [10]. The following figure shows the basic structure of Denial of Service Attack. The DoS structure consists of three components as Attacker, Internet and the target on which the attacker can attack for prevention of user from its service access.

Manuscript received June, 2015.

Dipali A.Kamble*, Department of Computer Networks, G.H. Raisoni College of Engineering & Management, Chas, Ahmednagar. Savitribai Phule Pune University, Maharashtra, India.*

Amruta Amune*, Department of Computer Networks, G.H. Raisoni College of Engineering & Management, Chas, Ahmednagar. Savitribai Phule Pune University, Maharashtra, India.*

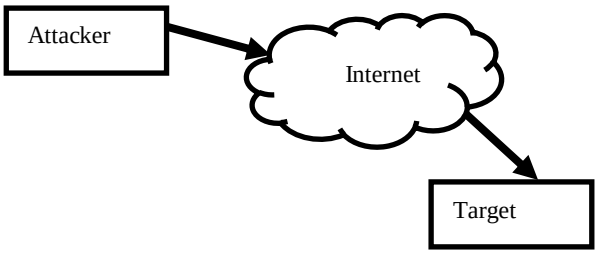


Figure 1.Overview of DOS Attack

DoS Attacks

DoS attacks see a Fig. 1, a single machine can sent a huge number of malicious packets, with the purpose of exhausting a target‘s networking resources and computational, or crashing the target. The aim of such attacks is to despoil appropriate access of users to the target‘s services**.** In a DoS attack, one internet connection and one computer is used to flood a server with packets, with the purpose of overloading the targeted server‘s bandwidth and resources [10].Following are the different DoS Attack classification:

- **Network Device Level**: DOS attacks in the Network Device Level include attacks that might be caused either by taking the advantage of bugs in software or by trying to exhaust the hardware resources of network devices [10].
- **Operating System Level**: In an OS Level DOS attacks take advantage of the ways operating systems implement protocols [10].
- **Application based attacks**: A great number of attacks try to settle a machine or a service out of the order either by taking advantage of specific bugs in network applications that are running on the target host or by using such applications to dram a resources of their victim [10].
- **Data Flooding**: An attacker may attempt to use a bandwidth available to a network, host or device at its greatest extent, by sending massive quantities of data and so causing it to the process extremely large amounts of data [10].
- **Attacks based on protocol features**: DOS may take advantage of certain standard protocol features, for example the several attacks exploit a fact that source addresses can be spoofed [10].

III. RELATED WORK

There are different Denial Of service Attack detection techniques proposed by the researchers over time to time which have some advantages over and vice-versa. There are many techniques used like K-map, combination of stateful and stateless signature with trace back technique, game-theoretic, Multivariate Correlation Analysis (MCA).

Suseela T. Sarasamma, Qiuming A. Zhu, and Julie Huff [2] put a new K-Map (Kohonen Net) multilevel hierarchical structure for an intrusion finding system is presented. Each step of the hierarchical map is organized as the simple winner takes all K-Map. One important advantage of this K-Map multilevel hierarchical is its calculation capability. Apart from other statistical inconsistency detection techniques such as K-means clustering or probabilistic analysis, nearest neighbour approach that engage distance measurement in a feature interval to recognize the outlines our request does not carry costly point to point calculations in organizing a data into clusters. One more advantage is network size reduced. It uses the grouping efficiency of the K-Map for detecting anomalies on selected dimensions of data set. Randomly selected data subsets that contain both the attacks and normal records from a KDD Cup data are used to train the hierarchical net.

The paper [2] illustrate the multilevel hierarchical Kohonen Net or Kohonen self-ordering map (K-Map) to implement an inconsistency based intrusion detection system (IDS sensor). We did our testing and training using the pre -processed KDD Cup data set. Main objective was to detect different types of attacks as possible. The experiment was done in two levels. Firstly we used a single level winner takes all K-Map to do a development of IDS.

John Haggerty, Qi Shi and Madjid Merabti [3], can combines both stateless and stateful signatures to provide early finding of the DoS attacks due to this enterprise network is protect. This paper is mostly focuses on how domain based way response to an attacks is used by mechanism to block traffic attack. This new solution is enables the blockage of the attack to be gradually propagated only through affected domains toward the attack sources.

Albert Banchs, Joerg Widmer, Andres Garcia Saavedra and Pablo Serrano [6], put game theory we address the problem of selfishness from a game-theoretic standpoint in DoS . They propose algorithm that satisfies the following properties: a) Wireless network is driven to the optimal point of operation when all the stations implement the algorithm and b) one or more selfish stations cannot obtain any gain by deviating from an algorithm.

Ruiliang Chen, Jung-Min Park and Randolph Marchany [4], put mitigation of attack plan actively strangle traffic attack produced attacks in Distributed Denial of Service (DDoS). In such paper presents Attack Diagnosis (AD), a new mitigation of attack scheme that adopts a divide and conquer technique. Packet marking and pushing concepts are combined in AD, and its architecture is in chain with the ideal DDoS attack countermeasure pattern for finding attack is performed near the packet filtering and sufferer node is executed close to the attack of sources.

Gautam Thatte, Urbashi Mitra, *Fellow,* and John Heidemann [7] , develops parametric technique to find network anomalies using contrast to other works requiring flow separation in only aggregate traffic statistics, even when the anomaly of total traffic is a small fraction . By adopting

simple statistical models for background traffic and anomalous in the domain of time. One can forecast standard parameters in the real time, thus to avoid the need for manual parameter tuning or long training phase. Additionally, it uses both traffic-rate yielding a bivariate standards and packet-size statistics that ignore most false positives.

Wanlei Zhou, Weijia Jia, Feilong Tang ,Song Guo, and Yong Xiang [5] , describe denial of service attack in distributed is a complex threat to the botnets and net are usually the engines behind them. By mimicking the patterns of traffic of flash crowds the sophisticated bot masters try to disable finders this poses a complicated challenge to those who justify against distributed denial of service attacks. According to deep study of organization of current botnets and size, we found that as compared to the flows of flash attack the current attack flows are usually more same to each other. Based on this [5] it propose the algorithm of discretion using the flow correlation coefficient as a similarity metric among doubtful flows. We formulated the problem and represent theoretical proofs for the applicability of the proposed technique of discrimination in theory. Our extensive experiments confirmed the demonstrated effectiveness and theoretical analysis of the proposed technique in practice.

IV. PROPOSED WORK

The overview of proposed DoS attack detection system architecture is given in this portion, where the system framework and detection mechanism are discussed. The whole detection process consists of three levels as shown in Fig.2. **Level 1.** Multivariate correlation analysis

Level 2. Normal profile generation.

Level 3. Attack Detection.

A. Proposed Architecture

The framework consists of three Levels

Level 1: In this level the basic features are generated from network traffic ingress to internal network where proposed servers resides in and are used to form the network traffic records for well-defined time period. Monitoring and analysing network to reduce the malicious activities only on relevant inbound traffic.

To provide a best protection for a targeted internal network. This also enables our detector to provide protection which is the best fit for the targeted internal network because legitimate traffic profiles used by the detectors are developed for a smaller number of network services.

Level 2: In this step the Multivariate Correlational Analysis is applied in which the Triangle Area Map Generation module is applied to extract the correlation between two separate features within individual traffic record. The distinct features are come from level 1 or "feature normalization module" in this step. All the extracted correlation are stored in a place called Triangle area Map(TAM), are then used to replace the original records or normalized feature record to represent the traffic record. It's differentiating between legitimate and illegitimate traffic records.

Level 3: The anomaly based finding mechanism is adopted in decision making. Decision making involves two phases as

- Training phase.
- Test phase

Normal profile generation module is work in "Training phase" to generate a profiles for various types of traffic records and the generated normal profiles are stored in a database. The "Tested Profile Generation" module is used in the "test phase" to build profiles for individual observed traffic records. Then at last the tested profiles are handed over to "Attack Detection" module it compares tested profile with stored normal profiles. This distinguishes the Dos attack from legitimate traffic.

This needs the expertise in the targeted detection algorithm and it is manual task. Particularly, two levels (i.e., the Training Phase and the Test Phase) are included in Decision Making. The Normal Profile Generation module is operated in a Training Phase [1] to generate profiles for various types of legal records of traffic, and the normal profiles generated are stored in the database. The tested profile generation module is used in a Test Phase to build profiles for the each observed traffic documentation. Next, the profiles of tested are passed over to an attack detection part, which calculates the tested profiles for individual with the self-stored profiles of normal. A threshold based classifier is employed in the attack detection portion module to differentiate DoS attacks from appropriate traffic [8].

B. Multivariate Correlation Analysis

DoS attack traffic treat differently from the appropriate traffic of network and the behaviour of network traffic is reflected by its geometric means. To well describe these statistical properties, here a novel multivariate correlation analysis (MCA) moves toward in this part. This multivariate correlation analysis approach use triangle area for remove the correlative data between features within a data object of observed (i.e. a traffic record).

C. Detection Mechanism

In this section, we present a threshold based on anomaly finder whose regular profiles are produced using purely legal records of network traffic and utilized for the future distinguish with new incoming investigated traffic report. The difference between an individual normal outline and a fresh arriving traffic record is examined by the planned detector. If the variation is large than a pre-determined threshold, then a record of traffic is coloured as an attack otherwise it is marked as the legal traffic record.

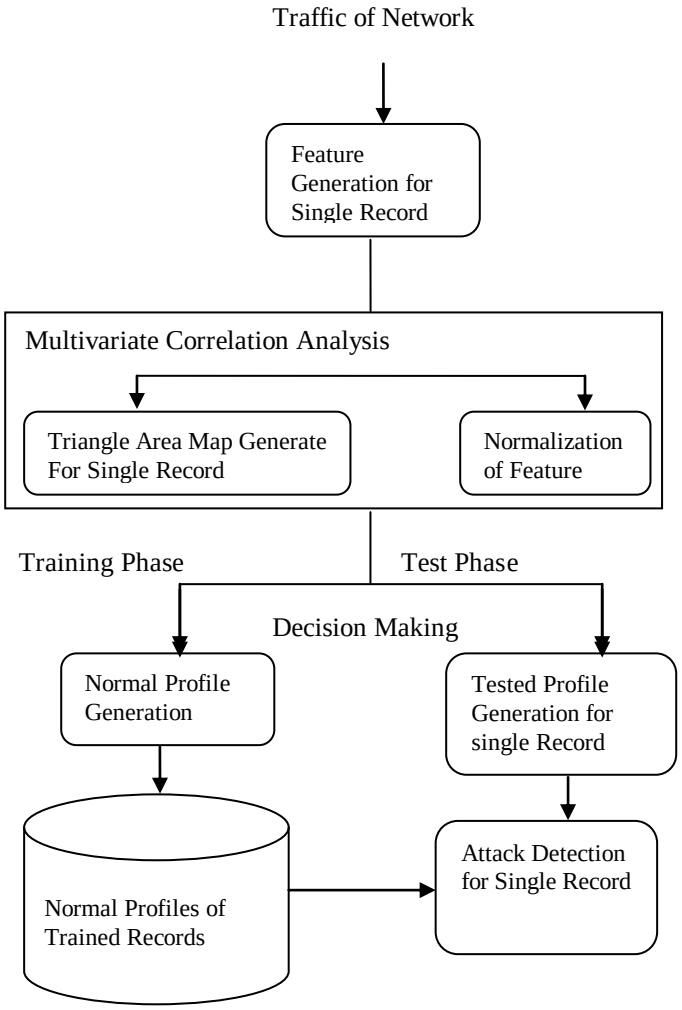


Figure 2. Framework of Denial of Service Attack Detection System

D. Algorithm for Normal Profile Generation

In this algorithm [1] the normal profile Pro is built through the density estimation of the MDs between individual legitimate training traffic records (TAM normal, i, lower) and the expectation (TAM normal, lower) of the g legitimate training traffic records.

Step 1: Input network traffic records.

Step 2: Extract original features of individual records.

Step 3: Apply the concept of triangle area to extract the geometrical correlation between the jth and kth features in the vector xi.

Step 4: Normal profile generation

i. Generate triangle area map of each record.
ii. Generate covariance matrix.
iii. Calculate MD between legitimate record's TAM and input records TAM
iv. Calculate mean
v. Calculate standard deviation.
vi. Return pro.

Step 5: Attack Detection.

i. Input: observed traffic, normal profile and alpha.
ii. Generate TAM for i/p traffic
iii. Calculate MD between normal profile and i/p traffic
iv. If MD < threshold
Detect Normal

Else
Detect attack.

In the training phase, we employ only the normal records. Normal profiles are built with respect to the various types of appropriate traffic using the algorithm describe below. Clearly, normal profiles and threshold points have the direct power on the performance of the threshold based detector. An underlying quality usual shape origins a mistaken characterization to correct traffic of network.

E. Naïve Bayes Algorithm for Attack Detection

This algorithm is used for classification purpose.

Step1: Task is to classify new packets as they arrive, i.e., decide to which class label they belong, based on the currently existing traffic record.

Step2: Formulated our prior probability, so ready to classify a new Packet.

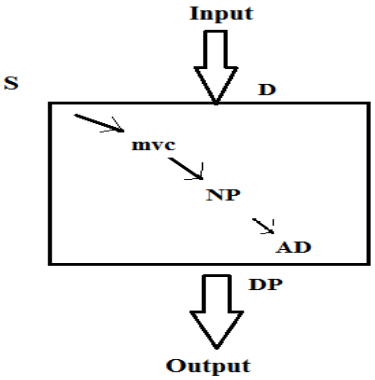
Step 3: Then we calculate the number of points in the packet belonging to each traffic record.

Step 4: Final classification is produced by combining both sources of information, i.e., the prior and to form a posterior probability.

F. Mathematical Modeling

Let S be the system which we use to find the DoS attack detection system. They equip proposed detection system with capabilities of accurate characterization for traffic behaviors and detection of known and unknown attacks respectively.

- **Input:** Given an arbitrary dataset $X = \{x1, x2, \cdots, xn\}$
- **Output:** DP (Detected Packets) : DP={n,m}
  Where n is normal packets and M is the malicious packets.
  Process: S= {D, mvc, NP, AD, DP}
  Where, S= System.
  D= Dataset
  mvc = Multivariate correlation analysis.
  NP = Normal profile generation.
  AD =Attack detection.
  DP= Detected packets.



V. Evaluation And Analysis

we can see in fig.3 , it shows the graph of accuracy achieved while DDoS attack detection in distributed networks. There are 2 methods use for detection. First is MCA based attack detection method and second is our proposed work method which shows that our proposed method achieves highest accuracy of 99 % and existing method achieves accuracy of 80%.

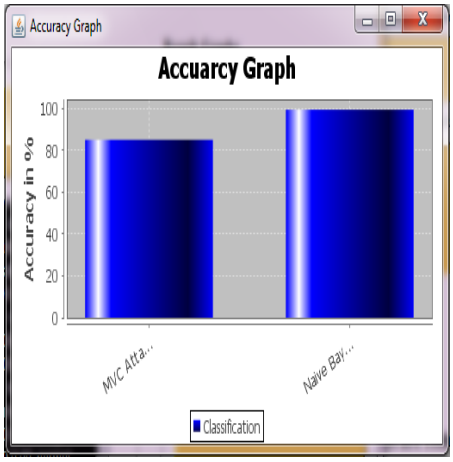


Figure 3. Accuracy Graph

As we can see in fig.4, it shows the graph of detection rate achieved while DDoS attack detection in distributed networks. The following graph shows that proposed method i.e. naïve bayes classifier has highest detection rate of 95% as compared to previous method i.e. MCA method who achieves 81% detection rate.

As we can see in fig.5 , it shows the graph of false alarm rate achieved while DDoS attack detection in distributed networks. The below given graph shows that proposed has lowest false alarm rate as compared to existing MCA based method.

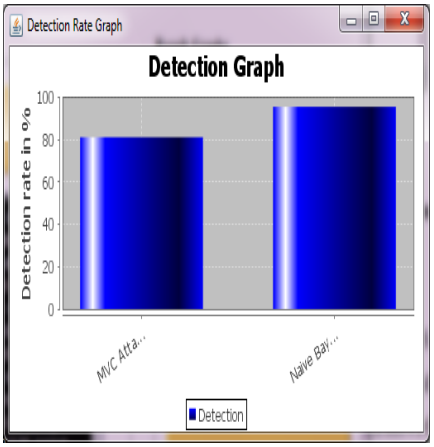


Figure 4. Attack Detection Rate Graph

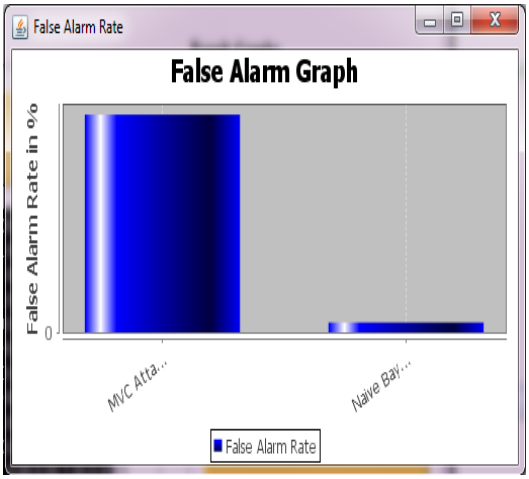


Figure 5. False Alarm rate graph

PERFORMANCE ANALYSIS

- **Detection Rate:** The detection rate is defined as the number of intrusion instances detected by the system (True Positive) divided by the total number of intrusion instances present in the test set.
- **False Alarm Rate:** Defined as the number of 'normal' patterns classified as attacks (False Positive) divided by the total number of 'normal' patterns.

ALERT TYPE:

- **True Positive:** : Attack - Alert
- **False Positive:** : No attack - Alert
- **False Negative:** : Attack - No Alert
- **True Negative:** : No attack - No Alert

Terms:

- **True Positive:** A legitimate attack which triggers IDS to produce an alarm.
- **False Positive:** An event signalling IDS to produce an alarm when no attack has taken place.
- **False Negative:** When no alarm is raised when an attack has taken place.
- **True Negative:** An event when no attack has taken place and no detection is made.

VI. CONCLUSION

This paper has presented a MCA-based DoS attack detection system which is powered by a triangle-area based MCA technique and an anomaly-based detection technique. The former technique extracts geometrical correlations hidden in individual pairs of two distinct features within the each network traffic record, and offers more accurate characterization for network traffic behaviors. The latter technique facilitates our system to be able to distinguish both known and unknown DoS attacks from proper network traffic. In this techniques are Time complexity is reduced, also Results are taken on real time dataset and false positive rate is reduced.

ACKNOWLEDGMENT

We would like to thank all the authors of different research papers referred during writing this paper. It was very knowledge gaining and helpful for the further research to be done in future.

REFERENCES

[1] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Senior Member, Priyadarsi Nanda, and Ren Ping Liu, "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, 2013

[2] S. T. Sarasamma, Q. A. Zhu, and J. Huff, "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," Systems, Man and Cybernetics, Part B: Cybernetics, IEEE Transactions on, vol. 35, pp. 302-312, 2005.

[3] J. Haggerty, Qi Shi, "Early Detection and Prevention of Denial-of-Service Attacks: A Novel Mechanism with Propagated Traced-Back Attack Blocking" IEEE Transaction on, Vol. 23, 2005.

[4] R. Chen, Jung-Min Park, R. Marchany, "A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks", IEEE Transactions, Vol. 18, 2007

[5] R Nagadevi, P Nageswara Rao, Rameswara Anand, "A New Way of Identifying DOS Attack Using Multivariate Correlation Analysis", International Journal of Computational Engineering Research (IJCER), Vol.04, 2014.

[6] A. G. Saavedra, P. Serrano, J. Widmer, "A Game-Theoretic Approach to Distributed Opportunistic Scheduling Banch", IEEE Transactions on, vol. 21, 2013.

[7] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," Networking, IEEE/ACM Transactions on, vol. 19, no. 2, pp. 512-525, 2011.

[8] S. Gomathi, "An Efficient Way of Detecting Denial-Of-Service Attack Using Multivariate Correlation Analysis", International Journal of Innovative Research in Computer and Communication Engineering (IJRCCE) Vol.2, 2014.

[9] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," Parallel and Distributed Systems", IEEE Transactions on, vol. 23, pp. 1073 -1080, 2012.

[10] Darshan Lal Meena Dr. R.S.Jadon , "A Survey on Different Solutions to DDoS Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, 2014.

[11] V. Jyothsna, V. V. Rama Prasad, " A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications, Vol.28, 2011.

Miss. Dipali Ankush Kamble Research Scholar, G. H. Raisoni Collage of Engineering and Management Ahmednagar, University of Pune, India. She received B.E. in Information Technology Padmashri Dr. Vital Rao VK Patil Collage of Engineering, Vilad Ghat, Ahmednagar.

Prof. Amruta Amune received the B.E. and ME degrees in Computer Science and Engineering. Currently she is working as Assistant Professor at Computer Engineering Department in G. H. Raisoni Collage of Engineering and Management, Ahmednagar, India.

