Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 5, May-2016

Disclose The Location Of Spoofer Through Path Back Scatter

Swapnil Mahadik, Amarjeetkumar Sharma, Vijayendra Kumbhar, Shahabuddin Khan, Vishal Waghmode,
Prof. Dhananjay Bhosale (MTech Computer)
Department Of Computer Engineering, Keystone School Of Engineering,Pune,

Abstract — It's miles long regarded attackers can also use designed source IP vicinity to cowl their actual areas. To seize the spoofers, special IP traceback structures were proposed. Alternatively, but, because of the problems of association, there has been no longer a normally received IP traceback arrangement, in any event at the net level. Accordingly, the fog on the regions of spoofers has by no means been scattered till now. We proposes passive IP traceback (PIT) that sidesteps the sending challenges of IP traceback strategies. PIT examines internet manipulate Message Protocol blunder messages (named manner backscatter) activated with the aid of mocking motion, and tracks the spoofers in mild of open available facts (e.g., topology).Alongside these lines, PIT can locate the spoofers with out a game plan want. Here constitute to the reasons, accumulation, and the real outcomes on manner backscatter, presentations the structures and adequacy of PIT, and shows the got regions of spoofers via making use of PIT in transit backscatter records set. Those results can assist in addition with uncovering IP spoofing, which has been tested for lengthy however never without a doubt recognized. Notwithstanding the truth that PIT can not work in all the spoofing assaults, it is probably the maximum precious device to follow spoofers earlier than an internet-degree traceback framework has been sent in genuine.

Keywords: PIT(Passive IP Trackback), Computer network management, computer network security, denial of service (DoS), IP traceback.

I. INTRODUCTION

Numerous scandalous attacks rely on IP spoofing, including perspective flooding, smurf, DNS hyperbole etc. A Domain Name System (DNS) amplification assault which severely degraded the service of the Top Level Domain (TLD) name machine is reported in. Although there has been a favorite conventional wisdom that attacks are launched from botnets and spoofing has ceased to be critical, the report of arbor on nanog 50th conference shows spoofing continues to be significant in observed DoS problems. Indeed, based on the captured backscatter messages from UCSD Network Telescopes, spoofing activities are still frequently observed. To capture the origins of IP spoofing traffic is very important. As long as the actual and real locations of spoofers are not disclosed, they cannot be deterred, stopped and avoided from launching further episodes. Even just approaching the spoofers, for example, deciding the systems they reside in, opponents can be located and traced in a smaller area, and filters can be put and organized closer to the opponent before attacking traffic get aggregated. The last but not minimal, identifying the origins of spoofing traffic can help build a reputation system, which would be useful to push the related ISPs to verify IP source address.

II. RELATED WORK

1)The Survey for IP Traceback (October 2014)

Author: Hong Cheng Tian , Jin An Lin

Description: IP traceback can be used to confirm locations of attackers, stop on-going attacks, and take legal actions against attackers, and then impede attackers. This paper describes the background where IP traceback problem generates, and presents what the functions of IP traceback are. Furthermore, this paper classifies existing IP traceback methods and analyzes advantages and disadvantages of each method. In addition, future researches on IP traceback are proposed. This paper is of valuable reference for network researchers and engineers to be engaged in the further study on IP traceback.

2) PRACTICAL DETECTING SPOOFED PACKETS (2003)

Author: S.J. Templeton , K. E. Levitt

Description: Packets sent using the IP protocol include the IP address of the sending host. The recipient directs replies to the sender using this source address. However, the correctness of this address is not verified by the protocol. The IP protocol specifies no method for validating the authenticity of the packet's source. This implies that an attacker can forge the source address to be any desired. This is almost exclusively done for malicious or at least inappropriate purposes. Given that attackers can exploit this weakness for many attacks, it would be beneficial to know if network traffic has spoofed source addresses. This knowledge can be particularly useful as an adjunct to reduce false positive from intrusion detection systems. This paper discusses attacks using spoofed packets and a wide variety of methods for detecting spoofed packets. These include both active and passive host-based methods as well as the more commonly discussed routing-based methods. Additionally, we present the results of experiments to verify the effectiveness of passive methods.

3) A Robust packet- filtering method for high band width Aggregates(2004)

Authors: Bao-Tung, H. Schulzrinne

Description: we propose a robust approach that integrates the concepts of ip traceback and packet filtering. on one hand, our approach employs an ip traceback technique to identify the paths and the sources of the attack at the victim's system; on the other, in accordance with the result from the ip traceback, the victim is eligible to request routers close to the attack origins for packet filtering. the reason that our approach is robust is that during the ip traceback process, the victim receives essential information indicating the origins of flooding packets. most importantly, the information will have been signed by the packet-filtering router itself. the request authentication is indispensable because otherwise an attacker can simply manipulate the packet filtering mechanism to intentionally drop specific ip packets and launch a successful dos attack.

4)IP Trackback for flooding attacks on Internet Threat Monitors (ITM) using Honypots(2012)

Author: k. munivara prasad, a. rama mohan reddy, v. jyothsna

Description: The Internet Threat Monitoring (ITM) is an efficient monitoring system used globally to measure, detect, characterize and track threats such as denial of service (DoS) and distributed Denial of Service (DDoS) attacks and worms. . To block the monitoring system in the internet the attackers are targeted the ITM system. In this paper we address the flooding attack of DDoS against ITM monitors to exhaust the network resources, such as bandwidth, computing power, or operating system data structures by sending the malicious traffic. We propose an information-theoretic frame work that models the flooding attacks using Botnet on ITM. One possible way to counter DDoS attacks is to trace the attack sources and punish the perpetrators. we propose a novel traceback method for DDoS using Honeypots. IP tracing through honeypot is a single packet tracing method and is more efficient than commonly used packet marking techniques.

5) IP Trackback through modified probabilistic packet marketing algorithm using chinese reminder theorem

Author: Y. Bhavni, V.Janaki, R. Sridevi

Description: Probabilistic Packet Marking algorithm suggests a methodology to identify all the participated routers of the attack path by probabilistically marking the packets. In this approach, these marked packets contain partial information regarding the routers of the attack path. At receiver, to get the complete information of every router, it requires more number of marked packets and hence more combinations and more false positives. To overcome this drawback we have presented a novel idea in finding the exact IP address of the routers in the attack path by applying Chinese Remainder Theorem. The result of our implementation reveals that our idea requires less number of marked packets and takes no time in constructing the attack path. The same idea is true even in the case of multiple attackers.

II. EXISTING SYSTEM:

Existing IP traceback approaches can be classified into five main categories: packet showing, ICMP traceback, logging on the router, link screening, overlay, and hybrid looking up.

1)Packet marking methods require routers modify the header of the packet to contain the information of the router and forwarding decision.

2)Different from box marking methods, ICMP traceback generates addition ICMP communications to a collector or the destination.

3)Attacking route can be reconstructed from log on the router when router the record on the packets submitted.

4)Link testing is an approach which determines the upstream of attacking traffic hop-by-hop while the assault is within progress.

5)Center Monitor proposes offloading the think traffic from edge routers to special tracking routers with an overlay network.

III. Disadvantages of Existing System:

1) Based on the captured backscatter messages from UCSD Network Telescopes, spoofing activities are still frequently observed. To build an IP traceback system on the Internet faces at least two critical challenges. The first one is the cost to adopt a traceback mechanism in the routing system. Existing traceback mechanisms are either not widely
2) Supported by current commodity routers, or will introduce considerable overhead to the routers (Internet Control Message Protocol (ICMP) generation, packet logging, especially in high-performance networks. The second one is the difficulty to make Internet service providers (ISPs) collaborate.
3) Since the spoofers could spread over every corner of the world, a single ISP to deploy its own traceback system is almost meaningless.
4) However, ISPs, which are commercial entities with competitive relationships, are generally lack of explicit economic incentive to help clients of the others to trace attacker in their managed ASes.
5) Since the deployment of traceback mechanisms is not of clear gains but apparently high overhead, to the best knowledge of authors, there has been no deployed Internet-scale IP traceback system till now.
6) Despite that there are a lot of IP traceback mechanisms proposed and a large number of spoofing activities observed, the real locations of spoofers still remain a mystery.

III. ENHANCED PROPOSED SYSTEM

Proposed System:

This paper proposes PIT which is very different from any existing traceback mechanism. The main difference is the generation of path ack scatter message is not of a certain probability. Thus, we separate the evaluation into 3 parts: the first is the statistical results on path backscatter messages; the second is the evaluation on the traceback mechanisms presented in section IV-B without considering uncertainness of path backscatter generation, since effectiveness of the mechanisms is actually determined by the structure features of the networks; the last is the result of performing the traceback mechanisms on the path backscatter message dataset. We propose a novel solution, named Passive IP Traceback (PIT), to bypass the challenges in deployment. Routers may fail to forward an IP spoofing packet due to various reasons, e.g., TTL exceeding. In such cases, the routers may generate an ICMP error message (named path backscatter) and send the message to the spoofed source address. Because the routers can be close to the spoofers, the path backscatter messages may potentially disclose the locations of the spoofers. PIT exploits these path backscatter messages to find the location of the spoofers. With the locations of the spoofers known, the victim can seek help from the corresponding ISP to filter out the attacking packets, or take other counterattacks. PIT is especially useful for the victims in reflection based spoofing attacks, e.g., DNS amplification attacks. The victims can find the locations of the spoofers directly from the attacking traffic.

Advantageous of Proposed Program:

1. IP traceback is a method to traceback to the source of the packets.
2. Packet marking schemes are the most successful implementation towards preventing DoS attacks by tracing to the source of attacks.
3. This is the first article known which deeply investigates path backscatter messages. These messages are valuable to help understand spoofing activities. Though Moore has exploited backscatter messages, which are generated by the targets of spoofing messages, to study Denial of Services (DoS), path backscatter messages, which are sent by intermediate devices rather than the targets, have not been used in traceback.
4. A practical and effective IP traceback solution based on path backscatter messages, i.e., PIT, is proposed. PIT bypasses the deployment difficulties of existing IP traceback mechanisms and actually is already in force. Though given the limitation that path backscatter messages are not generated with stable possibility, PIT cannot work in all the attacks, but it does work in a number of spoofing activities. At least it may be the most useful traceback mechanism before an AS-level traceback system has been deployed in real.
5. Through applying PIT on the path backscatter dataset, a number of locations of spoofers are captured and presented. Though this is not a complete list, it is the first known list disclosing the locations of spoofers.

Contributions of this paper:

1. This is the first article known which deeply investigates path backscatter messages. These messages are valuable to help understand spoofing activities. Backscatter messages, which are generated by the targets of spoofing messages, to study Denial of Services (DoS), path backscatter messages, which are sent by intermediate devices rather than the targets, have not been used in traceback.
2. A practical and effective IP traceback solution based on path backscatter messages, i.e., PIT, is proposed. PIT bypasses the deployment difficulties of existing IP traceback mechanisms and actually is already in force. Though given the limitation that path backscatter messages are not generated with stable possibility, PIT cannot work in all the attacks, but it does work in a number of spoofing activities. At least it may be the most useful traceback mechanism before an AS-level traceback system has been deployed in real.
3. Through applying PIT on the path backscatter dataset, a number of locations of spoofers are captured and presented. Though this is not a complete list, it is the first known list disclosing the locations of spoofers.

IV. MATHEMATICAL MODEL

Let S is the Whole System Consists:

S= {V, E, P, G}.

Where,

1. V is the set of all the network nodes.
2. E is the set of all the links between the nodes in the network.
3. P is path function which defines the path between the two nodes.
4. Let G is a graph.

Suppose, G (V, E) from each path backscatter, the node u, which generates the packet and the original destination v, Where u and v are two nodes in the network. i.e. u ∈ V and v ∈ V of the spoofing packet can be got.

We denote the location of the spoofer, i.e., the nearest router or the origin by s,
Where, s ∈ V.

Procedure:

1. For each path backscatter message, at first we check whether it belongs to the classes i.e. dataset or source list. If yes, the reflector should be near the attacker.
2. We simply use the source AS of the message as the location of the spoofer. If the message does not belong to the types, it is mapped into an AS tuple.
3. We determine whether the AS tuple can accurately locate the source AS of the attacker based on our proposed mechanisms. Then if the AS tuple can accurately locate the source AS of the message, the source AS of the spoofer is just this AS.
4. Then we also use the source AS as the location of the spoofer.

We assume some Probability for Accurate Locating on Loop-Free for spoofer based on the Loop-free assumption, to accurately locate the attacker from a path backscatter message (v, s),
There are three conditions:
1) LF-C1: the degree of the attacker s is 1;
2) LF-C2: v is not s;
3) LF-C3: u is s.

Based on the Assumption I, the probability of LF − C1 is equal to the ratio of the network nodes whose degree is 1.
To estimate our assumptions of probability, we introduce the power law of degree distribution from,

$$f_d \propto d^{\mathcal{O}}$$

Where fd is the frequency of degree d, and O is the out degree exponent.
Transform it to

$$f_d = \lambda d^{\mathcal{O}} + b_d$$

Where λ and bd are two constants. Then,

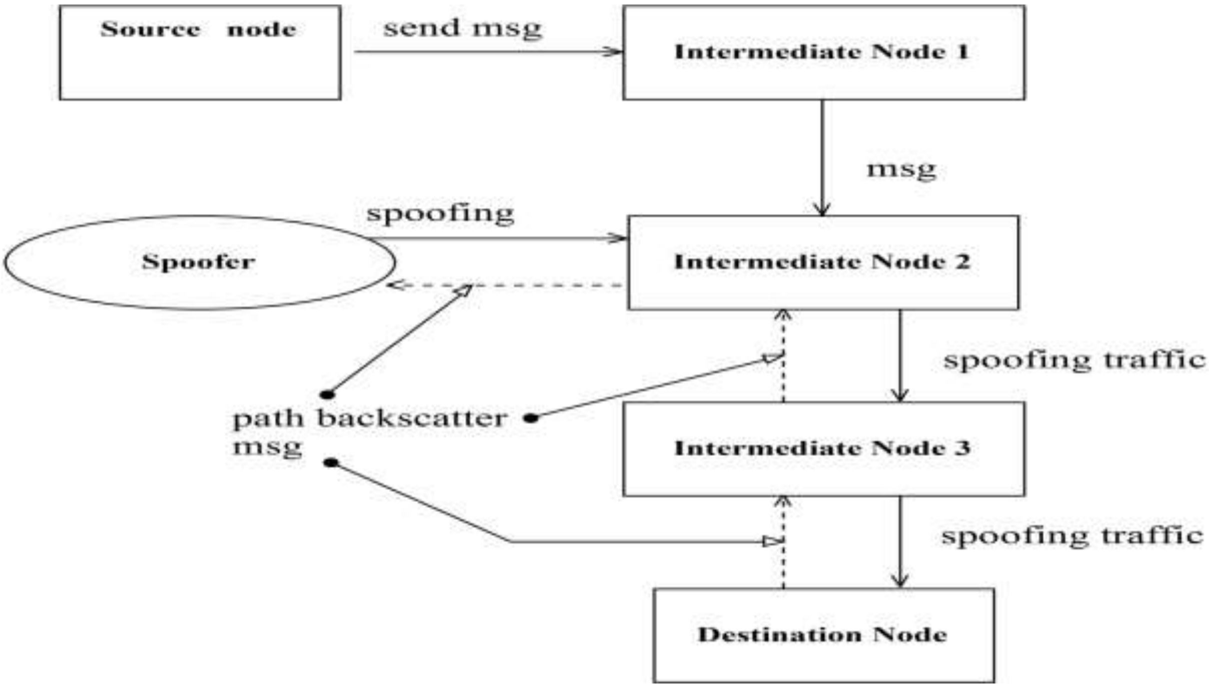
$$f_1 = \lambda + b_d.$$

Based on the Assumption II, the probability of LF − C2 is simply (N − 1)/N.
Based on the Assumption III, the probability of LF −C3 is equal to 1/(1+len(path(u, v)).
Because s and u are random chosen, the expectation of len (path (u,v)) is the effective diameter of the network δ_{ef} i.e. δ_{ef} =1+len(path((u,v)).
Based on our three assumptions, these conditions are mutually independent. Thus, the expectation of the probability of accurate locating the attacker is

$$E(P_{LF-accurate}) = \frac{N-1}{N} * \frac{\lambda + b_d}{1 + \delta_{ef}}$$

This form gives some insight on the probability of accurate locating of spoofer. If the power-law becomes stronger, λ will get larger and δef will get smaller. Then the probability of accurate locating will be larger.

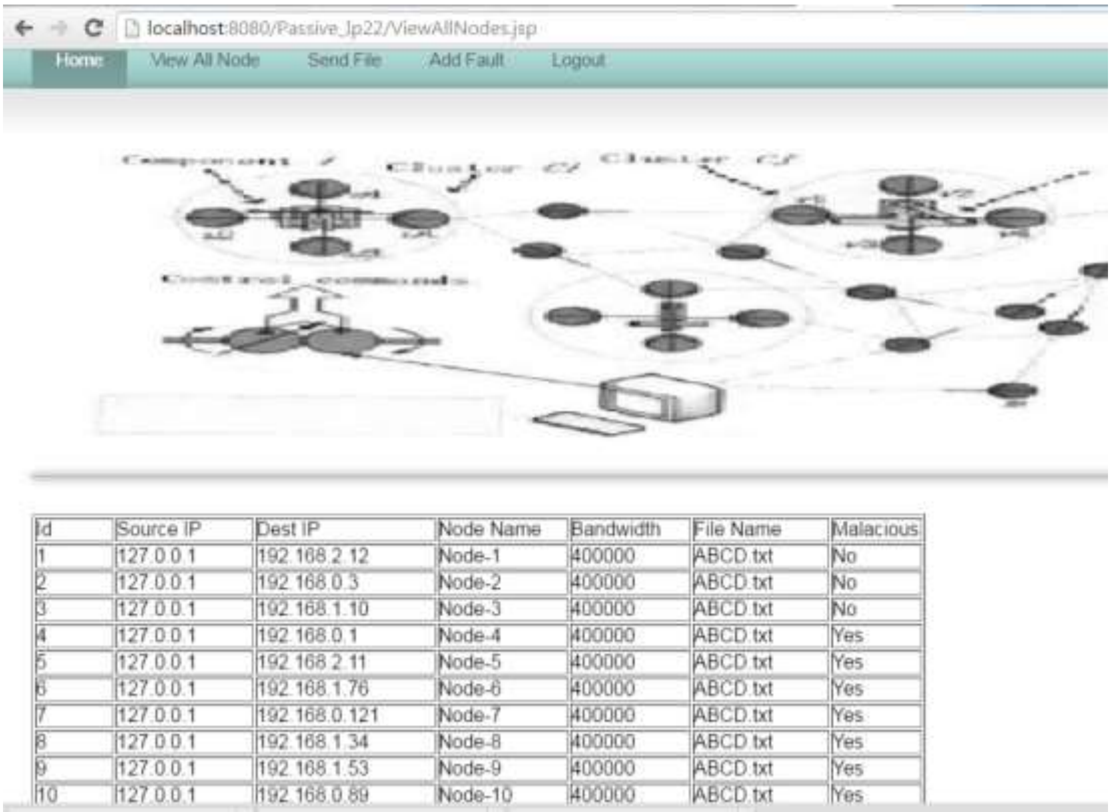
IV. BLOCK DIAGRAM OF SYSTEM ARCHITECTURE



V. RESULT ANALISYS

Here in result analysis part we are mainly fpcoused on the traceback technique. In trace back technique we define hacker and multiple node, multiple nodes sending the file to each other.That files are hacked by hacker through thetracebacking we are generating icmp message That ICMP message used in tracebacking technique and that gives status of hacked nodes with nearest neighbour node.

In the below snap we are showing that malicious node in **status** colum as **nok** i.e. not ok.



Id	Source IP	Dest IP	Node Name	Bandwidth	File Name	Malacious
1	127.0.0.1	192.168.2.12	Node-1	400000	ABCD.txt	No
2	127.0.0.1	192.168.0.3	Node-2	400000	ABCD.txt	No
3	127.0.0.1	192.168.1.10	Node-3	400000	ABCD.txt	No
4	127.0.0.1	192.168.0.1	Node-4	400000	ABCD.txt	Yes
5	127.0.0.1	192.168.2.11	Node-5	400000	ABCD.txt	Yes
6	127.0.0.1	192.168.1.76	Node-6	400000	ABCD.txt	Yes
7	127.0.0.1	192.168.0.121	Node-7	400000	ABCD.txt	Yes
8	127.0.0.1	192.168.1.34	Node-8	400000	ABCD.txt	Yes
9	127.0.0.1	192.168.1.53	Node-9	400000	ABCD.txt	Yes
10	127.0.0.1	192.168.0.89	Node-10	400000	ABCD.txt	Yes

VI. CONCLUSION AND FUTURE WORK

In this project we have presented a new technique, “backscatter analysis,” for estimating denial-of-service attack activity in the Internet. Using this technique, we have observed widespread DoS attacks in the Internet, distributed among many different domains and ISPs. The size and length of the attacks we observe are heavy tailed, with a small number of long attacks constituting a significant fraction of the overall attack volume. Moreover, we see a surprising number of attacks directed at a few foreign countries, at home machines, and towards particular Internet services.

We try to dissipate the mist on the locations of spoofers based on investigating the path backscatter messages. In this, we proposed Passive IP Traceback (PIT) which tracks spoofers based on path backscatter messages and public available information. We illustrate causes, collection, and statistical results on path backscatter. We specified how to apply PIT when the topology and routing are both known, or the routing is unknown, or neither of them are known. We presented two effective algorithms to apply PIT in large scale networks and proofed their correctness. We proved that, the effectiveness of PIT based on deduction and simulation. We showed the captured locations of spoofers through applying PIT on the path backscatter dataset.

REFERENCES

1) S.J. Templeton , K. E. Levitt, "practical detecting spoofed packets," DARPA Information Survivability Conference and Exposition, 2003. Proceedings (Volume:1) April 2003.

2) Bao-Tung, H.Schulzrinne "A robust packet –filtering method for high bandwidth aggregates" Electrical and Computer Engineering, 2004. Canadian Conference on (Volume:2), May. 2004.

3) k. munivara prasad, a. rama mohan reddy, v. jyothsna "IP Trackback for flooding attacks on Internet Threat Monitors(ITM)using Honypots" presented at the International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012

4) Y. Bhavni, V.Janaki, R. Sridevi "IP Trackback through modified probabilistic packet marketing algorithm using chinese reminder theorem," in Ain Shams Engineering Journal Volume 6, Issue 2, June 2015

5) S. Bellovin. *ICMP Traceback Messages*. [Online]. Available: http://tools.ietf.org/html/draft-ietf-itrace-04, accessed Feb. 2003.

6) M. T. Goodrich, "Efficient packet marking for large-scale IP traceback," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, 2002, pp. 117–126.

7) D. X. Song and A. Perrig, "Advanced and authenticated marking schemes for IP traceback," in *Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM)*, vol. 2. Apr. 2001, pp. 878–886.

8) A. Yaar, A. Perrig, and D. Song, "FIT: Fast internet traceback," in *Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM)*, vol. 2. Mar. 2005, pp. 1395–1406.

9) M. Adler, "Trade-offs in probabilistic packet marking for IP traceback," *J. ACM*, vol. 52, no. 2, pp. 217–244, Mar. 2005.

10) A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," *IEEE Commun. Lett.*, vol. 7, no. 4, pp. 162–164, Apr. 2003.

11) Y. Xiang, W. Zhou, and M. Guo, "Flexible deterministic packet marking: An IP traceback system to find the real source of attacks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 4, pp. 567–580, Apr. 2009.

12) S. Knight, H. X. Nguyen, N. Falkner, R. Bowden, and M. Roughan, "The internet topology zoo," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 9, pp. 1765–1775, Oct. 2011.

13) L. Gao, "On inferring autonomous system relationships in the internet," *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 733–745, Dec. 2001.

14) X. Dimitropoulos *et al.*, "AS relationships: Inference and validation," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 1, pp. 29–40, Jan. 2007.

AUTHORS

Vijayendra Kumbhar, pursuing B.E at Keystone School Of Engineering, Pune

Swapnil Mahadik, pursuing B.E at Keystone School Of Engineering, Pune

Shahabuddin Khan, pursuing B.E at Keystone School Of Engineering, Pune

Amarjeetkumar Sharma, pursuing B.E at Keystone School Of Engineering, Pune.

Vishal Waghmode, pursuing B.E at Keystone School Of Engineering, Pune.

Prof. Dhananjay Bhosale, Professor at Keystone School Of Engineering,Pune