iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** VIII **Month of publication:** August 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Advanced and Dynamic process IP Traceback to Detect DOS Attacks

Hasthiteja[1], Appini Narayanarao[2]
[1]*M. Tech, Shree Institute of Technical Education*
[2]*Associate Professor, Shree Institute of Technical Education*

Abstract— The unwavering quality and accessibility of system administrations are being undermined by the developing number of Denial-of-Service (DoS) assaults. This paper proposes a multivariate relationship examination way to deal with research and identify the Dos assault. The proposed framework applies the possibility of Multivariate Correlation Analysis (MCA)to network movement portrayal and utilizes the essential of peculiarity based location in assault acknowledgment. One noteworthy trouble to safeguard against Appropriated Disavowal of-administration assault is that assailants frequently utilize fake, or satirize IP addresses as the IP source address. To catch the spoofers, this paper proposes passive IP traceback (PIT) that sidesteps the organization troubles of IP traceback strategies. PIT explores Web Control Message Convention mistake messages (named path backscatter) activated by parodying movement, and tracks the spoofers taking into account open accessible data (e.g., topology). Thusly, PIT can discover the spoofers with no arrangement necessity.

I. INTRODUCTION

The distributed denial of service (DDoS) attack is a serious threat to the security of cyberspace. It typically exhausts bandwidth, processing capacity, or memory of a targeted machine or network. To launch a DoS attack, malicious users first build a network of computers that they will use to produce the volume of traffic needed to deny services to computer users. To create this attack network, attackers discover vulnerable sites or hosts on the network. Vulnerable hosts are usually those that are either running no antivirus software or out-of-date antivirus software, or those that have not been properly patched. Vulnerable hosts are then exploited by attackers who use their vulnerability to gain access to these hosts. The next step for the intruder is to install new programs (known as attack tools) on the compromised hosts of the attack network. The hosts that are running these attack tools are known as zombies, and they can carry out any attack under the control of the attacker. Many zombies together form what we call an army. DoS attack detection is essential to the protection of online services. Network-based detection mechanisms are widely used. Network– based detection systems[1] are classified into misuse-based detection systems and anomaly-based detection systems[2].Due to various drawbacks of misuse-based detection systems, anomaly based detection systems are widely used. Since spoofed packets are used for DoS attack, it is difficult to find out the route of attack. An effective method for tracebacking is also necessary.

II. LITERATURE SURVEY

A. Efficient Packet Marking for Large-Scale IP Traceback

Author proposed a new approach to IP traceback based on the probabilistic packet marking paradigm [7]. Our approach, which we call randomize-and-link, uses large checksum cords to ”link” message fragments in a way that is highly scalable, for the checksums serve both as associative addresses and data integrity verifiers. The main advantage of these checksum cords is that they spread the addresses of possible router messages across a spectrum that is too large for the attacker to easily create messages that collide with legitimate messages. Our methods therefore scale to attack trees containing hundreds of routers and do not require that a victim know the topology of the attack tree a priori. In addition, by utilizing authenticated dictionaries in a novel way, our methods do not require routers sign any setup messages individually.

B. Practical Network Support for IP Traceback

This paper [8] describes a technique for tracing anonymous packet flooding attacks in the Internet back towards their source. This work is motivated by the increased frequency and sophistication of denial-of-service attacks and by the difficulty in tracing packets with incorrect, or ”spoofed”, source addresses. In this paper we describe a general purpose traceback mechanism based on probabilistic packet marking in the network. Our approach allows a victim to identify the network path(s) traversed by attack traffic

without requiring interactive operational support from Internet Service Providers (ISPs) [3]. Moreover, this traceback can be performed ”post-mortem” after an attack has completed. We present an implementation of this technology that is incrementally deployable, (mostly) backwards compatible and can be efficiently implemented using conventional technology.

C. FIT: Fast Internet Traceback

[9] E-crime is on the rise. The costs of the damages are often on the order of several billion of dollars. Traceback mechanisms are a critical part of the defense against IP spoofing and DoS attacks. Current traceback mechanisms are inadequate to address the traceback problem Problems with the current traceback mechanisms:

1) Victims have to gather thousands of packets to reconstruct a single attack path
2) They do not scale to large scale attacks
3) They do not support incremental deployment

General properties of FIT:

a) IncDep
b) RtrChg
c) FewPkt
d) Scale
e) Local

D. ICMP Traceback with Cumulative Path, An Effcient Solution for IP Traceback

DoS/DDoS attacks constitute one of the major classes of security threats in the Internet today. The attackers usually use IP spoofing to conceal their real location. The current Internet protocols and infrastructure do not provide intrinsic support to traceback the real attack sources. The objective of IP Traceback is to determine the real attack sources, as well as the full path taken by the attack packets. Different traceback methods have been proposed, such as IP logging, IP marking and IETF ICMP Traceback (ITrace). In this paper [10], we propose an enhancement to the ICMP Traceback approach [11], called ICMP Traceback with Cumulative Path (ITrace-CP). The enhancement consists in encoding the entire attack path information in the ICMP Traceback message. Analytical and simulation studies have been performed to evaluate the performance improvements. We demonstrated that our enhanced solution provides faster construction of the attack graph, with only marginal increase in computation, storage and bandwidth.

E. Trace IP Packets by Flexible Deterministic Packet Marking (FDPM)

Currently a large number of the notorious Distributed Denial of Service (DDoS) attack incidents make people aware of the importance of the IP traceback technique. IP traceback is the ability to trace the IP packets to their origins. It provides a security system with the capability of identifying the true sources of the attacking IP packets. IP traceback mechanisms have been researched for years, aiming at finding the sources of IP packets quickly and precisely. In this paper, an IP traceback scheme, Flexible Deterministic Packet Marking (FDPM) [12], is proposed. It provides more flexible features to trace the IP packets and can obtain better tracing capability over other IP traceback mechanisms, such as link testing, messaging, logging, Probabilistic Packet Marking (PPM) [13] [14], and Deterministic Packet Marking (DPM) [15]. The implementation and evaluation demonstrates that the FDPM needs moderately a small number of packets to complete the traceback process and requires little computation work; therefore this scheme is powerful to trace the IP packets. It can be applied in many security systems, such as DDoS defense systems [4], Intrusion Detection Systems (IDS), forensic systems, and so on.

Volume 4 Issue VIII, August 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

III. PROPOSED SYSTEM ARCHITECTURE

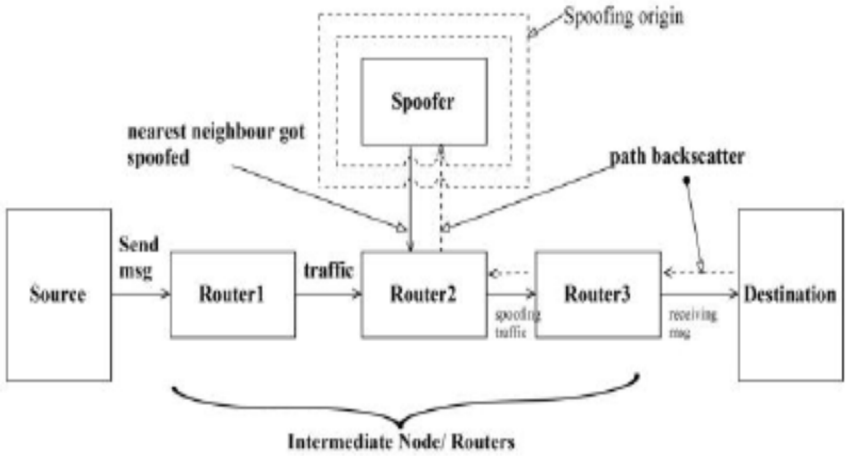


Fig 1. Proposed Architecture

The Distributed Denial of Service (DDoS) attacks are launched synchronously from multiple locations and they are extremely harder to detect and stop. Identifying the true origin of the attacker along with the necessary preventive measures helps in blocking further occurrences these types of attacks. The issue of tracing the source of the attack deals with the problem of IP traceback.

A. Goals and objectives

1) Designing the IP traceback techniques to disclose the real origin of IP traffic or track the path.

2) A practical and effective IP traceback solution based on path backscatter messages.

3) Passive IP traceback (PIT) that bypasses the deployment difficulties of IP traceback techniques.

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

B. Methodologies of Problem Solving And Efficiency Issues

1) Find the shortest path from source (s) node to destination (d) node.

2) The messassge can be send from r to d through many intermediate nodes i.e. routers (r).

3) There may any spoofer origin available in between the path

Assume, that 'sp' is the spoofer node in the network. There are two assumptions for locating such spoofing origin while routing the packets in the network.

a) Loop-Free Assumption: This assumption states there is noloop in the paths. This assumption always holds unless misconfiguration or the routing has not converged.

b) Valley-Free Assumption: This assumption states there should be no valley in the some node level network

paths. Though the increased complexity of node relationship has reduced the universality of this assumption, it is still the most common model of intermediate network level routing.

i) If suppose any intermediate node has being spoofed by spoofer node then the destination node will send the path backscatter message to all intermediate node indicating that spoofing has occurred at somewhere in the network.

ii) Then each node in network will send the acknowledgment for that path backscatter message. The node which fails to give back acknowledgment that will be assumed as spoofer node.

C. PIT: Tracking Based On Path Backscatter

The below algorithm helps us to trace the source of attack.

1) Function GetSuspectSet_LoopFree(G,r,od)

2) *suspectset←Ø*
3) *c←null*
4) *p←shortest path from r to od*
5) *For vertex v in p do*
6) *If v==r then*
7) *Continue*
8) *End if*
9) *G^1←G.remove(v)*
10) *If r and od are disconnected in G^1then*
11) *c←v*
12) *break*
13) *end if*
14) *end for*
15) *SG←G.remove(c)*
16) *For Vertex v in SG do*
17) *If v and r are connected in SG then*
18) *suspectset←suspect+v*
19) *End if*
20) *End for*
21) *Return suspectSet*
22) *End function*

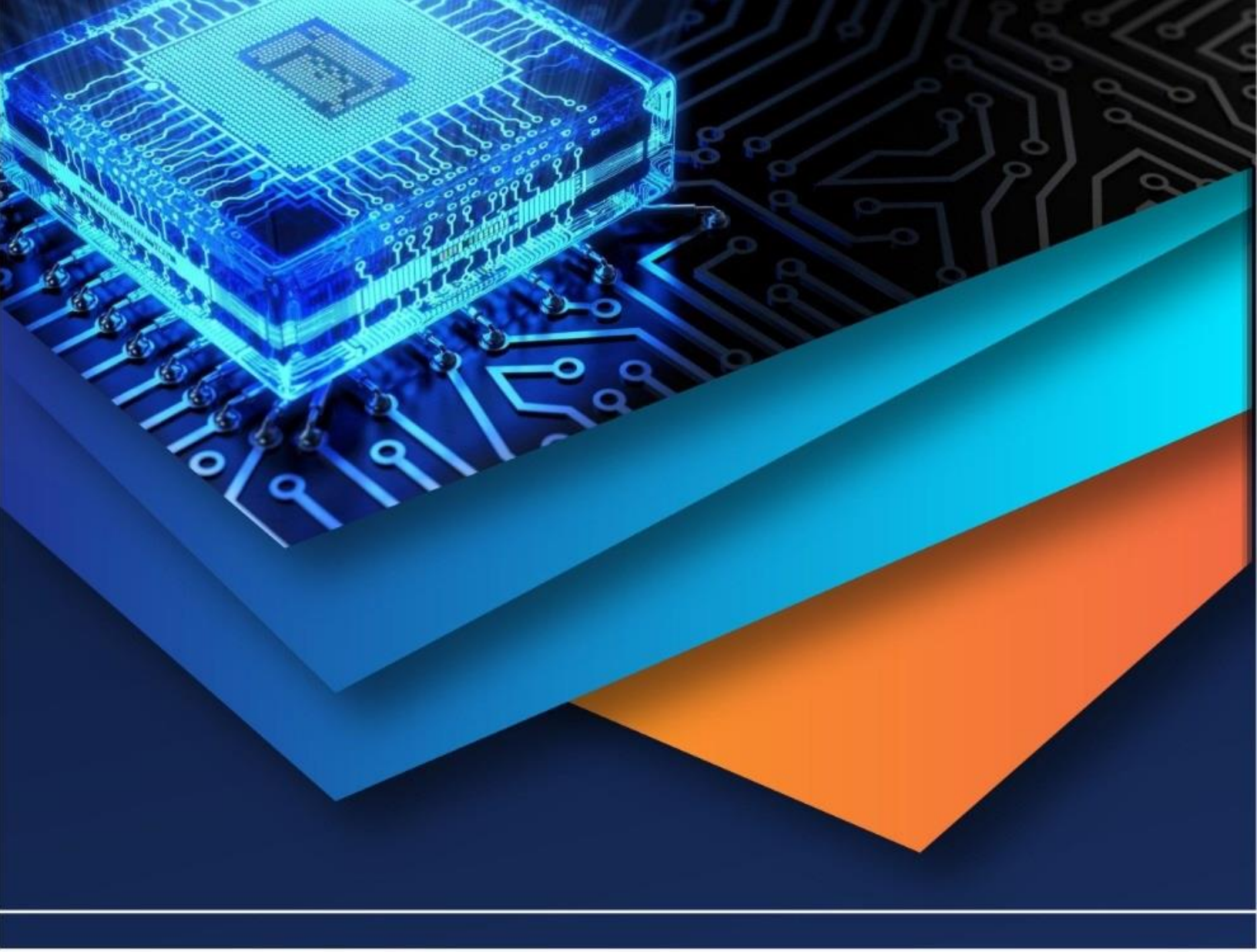
IV. CONCLUSION

This proposed one provides an effective method to detect DoS attack based on Multivariate Correlation analysis along with proper tracebacking with Passive IP tracebacking algorithm to find the source of attack. This system is able to distinguish both known and unknown DoS attacks from legitimate network traffic. The proposed IP traceback scheme based on information metrics can effectively trace all attacks until their own LANs (zombies).

REFERENCES

[1] S. M. Bellovin, "Security problems in the TCP/IP protocol suite," ACM SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 32–48, Apr. 1989.
[2] ICANN Security and Stability Advisory Committee, "Distributed denial of service (DDOS) attacks," SSAC, Tech. Rep. SSAC Advisory SAC008, Mar. 2006.
[3] C. Labovitz, "Bots, DDoS and ground truth," presented at the 50th NANOG, Oct. 2010.
[4] The UCSD Network Telescope. [Online]. Available: http://www.caida.org/projects/network_telescope/
[5] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun. (SIGCOMM), 2000, pp. 295–306.
[6] S. Bellovin. ICMP Traceback Messages. [Online]. Available: http://tools.ietf.org/html/draft-ietf-itrace-04, accessed Feb. 2003.
[7] A. C. Snoeren et al., "Hash-based IP traceback," SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 3–14, Aug. 2001.
[8] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," ACM Trans. Comput. Syst., vol. 24, no. 2, pp. 115–139, May 2006. [Online]. Available: http://doi.acm.org/10.1145/1132026.1132027
[9] M. T. Goodrich, "Efficient packet marking for large-scale IP traceback," in Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS), 2002, pp. 117–126.
[10] 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.
[11] 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.
[12] J. Liu, Z.-J. Lee, and Y.-C. Chung, "Dynamic probabilistic packet marking for efficient IP traceback," Comput. Netw., vol. 51, no. 3, pp. 866–882, 2007.
[13] K. Park and H. Lee, "On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack," in Proc. IEEE 20th Annu. Joint Conf. IEEE Comput. Commun. Soc. (INFOCOM), vol. 1. Apr. 2001, pp. 338–347.
[14] M. Adler, "Trade-offs in probabilistic packet marking for IP traceback," J. ACM, vol. 52, no. 2, pp. 217–244, Mar. 2005.
[15] A. Belenky and N. Ansari, "IP traceback with deterministic packet marking," IEEE Commun. Lett., vol. 7, no. 4, pp. 162–164, Apr. 2003.
[16] 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.
[17] R. P. Laufer et al., "Towards stateless single-packet IP traceback," in Proc. 32nd IEEE Conf. Local Comput. Netw. (LCN), Oct. 2007, pp. 548–555. [Online]. Available: http://dx.doi.org/10.1109/ LCN.2007.160
[18] M. D. D. Moreira, R. P. Laufer, N. C. Fernandes, and O. C. M. B. Duarte, "A stateless traceback technique for identifying the origin of attacks from a single packet," in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2011, pp. 1–6.

[19] A. Mankin, D. Massey, C.-L. Wu, S. F. Wu, and L. Zhang, "On design and evaluation of 'intention-driven' ICMP traceback," in Proc. 10th Int. Conf. Comput. Commun. Netw., Oct. 2001, pp. 159–165.
[20] H. C. J. Lee, V. L. L. Thing, Y. Xu, and M. Ma, "ICMP traceback with cumulative path, an efficient solution for IP traceback," in Information and Communications Security. Berlin, Germany: Springer-Verlag, 2003, pp. 124–135.
[21] H. Burch and B. Cheswick, "Tracing anonymous packets to their approximate source," in Proc. LISA, 2000, pp. 319–327.
[22] R. Stone, "CenterTrack: An IP overlay network for tracking DoS floods," in Proc. 9th USENIX Secur. Symp., vol. 9. 2000, pp. 199–212.
[23] A. Castelucio, A. Ziviani, and R. M. Salles, "An AS-level overlay network for IP traceback," IEEE Netw., vol. 23, no. 1, pp. 36–41, Jan. 2009. [Online]. Available: http://dx.doi.org/10.1109/MNET.2009.4804322
[24] A. Castelucio, A. T. A. Gomes, A. Ziviani, and R. M. Salles, "Intradomain IP traceback using OSPF," Comput. Commun., vol. 35, no. 5, pp. 554–564, 2012. [Online]. Available: http://www.sciencedirect.com/ science/article/pii/S0140366410003804
[25] J. Li, M. Sung, J. Xu, and L. Li, "Large-scale IP traceback in high-speed internet: Practical techniques and theoretical foundation," in Proc. IEEE Symp. Secur. Privacy, May 2004, pp. 115–129.
[26] B. Al-Duwairi and M. Govindarasu, "Novel hybrid schemes employing packet marking and logging for IP traceback," IEEE Trans. Parallel Distrib. Syst., vol. 17, no. 5, pp. 403–418, May 2006.
[27] M.-H. Yang and M.-C. Yang, "Riht: A novel hybrid IP traceback scheme," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 789–797, Apr. 2012.
[28] C. Gong and K. Sarac, "A more practical approach for single-packet IP traceback using packet logging and marking," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 10, pp. 1310–1324, Oct. 2008.
[29] R. Beverly, A. Berger, Y. Hyun, and K. Claffy, "Understanding the efficacy of deployed internet source address validation filtering," in Proc. 9th ACM SIGCOMM Conf. Internet Meas. Conf. (IMC), 2009, pp. 356–369.
[30] G. Yao, J. Bi, and Z. Zhou, "Passive IP traceback: Capturing the origin of anonymous traffic through network telescopes," in Proc. ACM SIGCOMM Conf. (SIGCOMM), 2010, pp. 413–414. [Online]. Available: http://doi.acm.org/10.1145/1851182.1851237
[31] J. Postel. Internet Control Message Protocol, RFC792. [Online]. Available: https://tools.ietf.org/html/rfc792, accessed Sep. 1981.
[32] W. Richard Stevens, TCP/IP Illustrated: The Protocols, vol. 1. Boston, MA, USA: Addison-Wesley, 1993.
[33] H. Wang, C. Jin, and K. G. Shin, "Defense against spoofed IP traffic using hop-count filtering," IEEE/ACM Trans. Netw., vol. 15, no. 1, pp. 40–53, Feb. 2007.
[34] 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.
[35] L. Gao, "On inferring autonomous system relationships in the internet," IEEE/ACM Trans. Netw., vol. 9, no. 6, pp. 733–745, Dec. 2001.
[36] X. Dimitropoulos et al., "AS relationships: Inference and validation," ACM SIGCOMM Comput. Commun. Rev., vol. 37, no. 1, pp. 29–40, Jan. 2007.
[37] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On power-law relationships of the internet topology," ACM SIGCOMM Comput. Commun. Rev., vol. 29, no. 4, pp. 251–262, 1999.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY