iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4138

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Recent Development of DDoS Prevention Technique

Shilpa Kumari[1], Aditi Shukla[2], Raghvendra Singh[3], Ashish Chopra[4]
[4]*Assistant Professor,* [1, 2, 3] *Dept. of Computer Application, National Institute of Technology (Kurukshetra)*

Abstract: ***In the recent few years we have seen in a drastic growth internet usage. In this paper we have review different DDoS attack in literature. Distribute Denial of services (DDoS) attack have tendency to block the network accessibility by flooding the victims with a high volume of unwanted traffic. Attackers commonly access innumerable by influencing utilization of their vulnerabilities to setup to attack botnet. DDoS attack is the attempt to make the legitimate or genuine user from accessing the services provided by internet. Attacker takes the control of large number of computer. It can be done with help of exploiting their vulnerabilities. These affected computers called botnets. Denial of services attack can be accomplished by flooding the server, target machine or resource with not required unwanted request. These requests make server overloaded and crash the server or web resource. This traffic is generating by the attackers and prevent the request of genuine user to be fulfilled. DDoS attack often targets the famous sites services on the high profile. In this paper we try to put light on types of DDoS attack, mitigation and prevention technique of DDoS attack.***
Keywords: DDoS, UDP, Botnet, Zombies.

I. INTRODUCTION

DoS create huge problem for legitimate user by blocking the network resources. Attackers have two ways to launch these attacks. First is by sending some malformed packet to the victim with these malformed packets the victim get confuse. Second method is simply exhausted bandwidth and other server resources for example CPU, memory which is needed by the legitimate user.
Botnets uselessly send same packets to increase the traffic for victim. With these activities target system get affected and get slow down sometimes crash completely. With these attacks it becomes difficult to defend the victim from these spoofed packets. When large numbers of these packets are sending then it is impossible to know about the original attacker.
Some example of these attacks- Yahoo 2000 February, Sco 2004 February. This attack is done with help of previously been infected devices.

II. COMPONENT OF DDOS ATTACK

A. Person who initiates the attack. Attacker has to think many useful strategies for attack strategies like IP- spoofing, flood packets. Attack source is the machine [2].
B. Master or handlers are those who perform command and control on the number of slaves. These masters help to implement attack on the host computer in a coordinated manner.
C. Slaves or zombies: Zombies are those computers which are connected through the internet that has been controlled by the master. Most owners of zombies are not aware that their system is being used for attack. Victim are the nodes on which attack perform. To perform DDoS attack on any network we need an attack platform. Attack platform is the main component [1] of DDoS attack .

III. MOTIVE OF ATTACKERS

A. Here are some categories of Motive of Motive of Attacker Every Attack has Some Motive

1) *Financial Motive:* The most obvious motive is financial motive. This type of attack is great concern for the corporations for doing this kind of attack attacker should have technical knowledge and has to be experienced. These kind of attack is very hard to stop and most dangerous.
2) *Revenge:* Sometimes the frustrated individuals have the tendency to do this kind of attack. They usually carry out these attacks in revenge if perceived injustice.
3) *Ideological:* Ideological belief sometimes motive the attacker to do these activities:- Eslonia has encountered by ideological attack in 2017.

4) *Intellectual challenge:* Experiment and passion to learn how these attacks are launched is the motive attackers. They have done this kind of attack with the hacking. Now the tools are available to amateur in order to show their capability.
5) *Cyber warfare:* Politically motivated and terrorist organization uses this kind of attack. Sometimes the cyber warfare can be done in the range of critical section of another country. The targeted systems are commercial banks agencies, mobile service providers. The attackers of these attack is experienced have needed resources. It disrupts the resources or services and severally affects a country.

IV. TYPES OF DDoS ATTACK

To implement DDoS attack and increase the impact of DDOS attacker need large number of devices

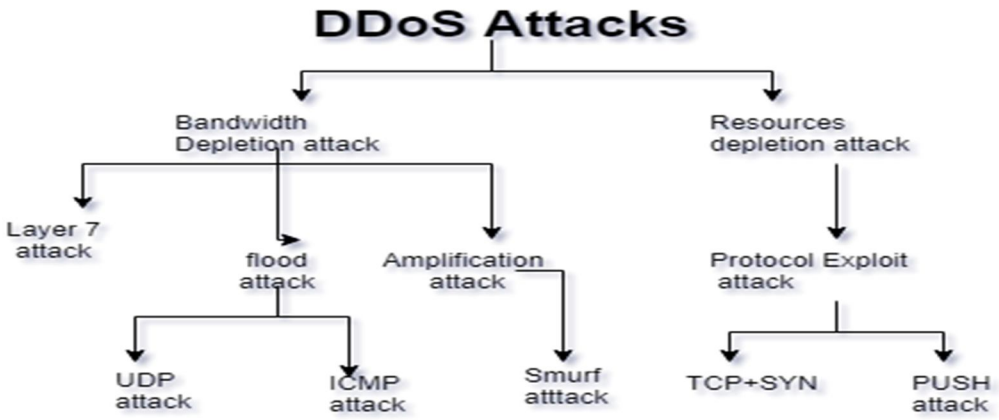


Figure 1. Types of DDoS attack

A. *Acknowlegment(ack) Flood Attack*

Who want to communicate over the internet they use protocol known as TCP\IP three way handshaking. We use push ACK packet for connection establishment between the server and user. The client will send the SYN to the server then after receiving it will send SYN+ACK back to the client and the client need to send ACK message to the server and connection established [3].Attacker will send SYN packets to the server using fake IP address. Server will get confuse and server will become unable to close the connection. Server will not be able to response to the legitimate client. It provides communication for a time period until session is closed. In ACK Flood Attack, the ACK packet are send to the server not related to the session but only to increase the traffic[3].It causes the crash or depletes the resources.

B. *Domain Name Services (dns) Amplification Attack*

It is sophisticated denial of service attack that advantages of DNS servers behavior in order to amplify the attack.
DNS server resolves internet domain names into IP addresses. If we want to visit a website the IP address of that website should be known by the computer. Computer known as the DNS resolver. It sends a DNS query to a DNS server asking the IP address of that particular website. In order to launch the DNS amplification attack the attacker does two malicious tasks:-First, it spoofs the IP address of DNS resolver and replaces it with victims IP address. This will cause all DNS replies will sent to victim's server. Second the attacker finds the internet domain that is registered with many DNS records. It sends the DNS query to entire list of all the DNS records for that domain. This results in the large replies from the DNS servers. Now the attacker ready for attack using very few computers. The attacker send high rate of short DNS queries to the multiple DNS servers asking for the entire list of records for that domain it chose earlier, the DNS server looks for the answer and provide it to the DNS resolver. The attacker achieves an amplification effect because for each shorts it sends DNS query, DNS replies with a larger response sometimes up to 100 times larger. The victim is bombed with a high rate of large DNS replies, where each reply is split over several packets. This requires the victim to reassemble the packet. Which is a resource consuming task, and to attend to all of the attack traffic. soon enough the victims servers become so busy in handling the attack traffic that they can't service any other request from legitimate users and the attackers achieves a denial of service. The difference in the size of sent and received enquiries, overburden the victim's faster line.

C. *Internet control Media Protocol(icmp) Flood Attack*

ICMP is used for the error message deliver to the sender. It used by the Attacker because no authentication is used. It helps unintentionally in attack. In this the attacker sends the huge amount of ICMP packet to the server, server tries to process every

incoming packet which results in the denial of services. It becomes successful when server properly responds to it. Result of this attack is disconnection from the internet.

D. Smurf Attack

Smurf attack is an old mechanism actually dates back to early 1998.It's a mechanism for carrying out dos on a target system. Smurf works is it takes advantage of particular protocol that is ICMP which is stands for Internet Control Message Protocol being able to determine the status of a given machine. One can initiate ICMP protocol via command that is actually known as "ping" [3]. This attack occurs by sending number of ICMP packets to the server and server's system will have spoofed ping messages. Attacker will send the Echo Request to the server and after receiving server will reply by giving Echo Response back. If the attacker will send so much ping requests to the server. It will not be able to handle those requests from legitimate traffic [3].In the SMURF attack the ICMP packet sends to the victim server by using fake IP addresses. As most devices in the network have default IP address replying by default, they are automatically trying to respond. As in DDOS large number of computer participated victim server is flooded in short time [3]. The higher the number of computers in the network the more is the impact of the attack.

E. User Datagram Protocol (udp) Attack

UDP is internet protocol. UDP contains the port number of the application. It is session less protocol so it doesn't need any of the authentication to establish and expire communication time. This attack can be done by flooding large number of UDP packets to random port to the victim server. Server must respond to the packets. In this the server check whether these any of its applications, when it gets detected it must send the information about the target destination inaccessible. It uses ICMP to send error messages and let the user know about the error. The server has to reply of the received UDP packet. If these packet are very large it exhausts internet connectivity and communication becomes impossible.

F. Teardrop Attack

In teardrop attack a fragmented packet sends to the server. This packet contain the jumbled and crosswords. Receiver is not able to reassemble that packet's data and then packet will overlap IP header contain fragment offset field which specify the starting address and offset contained in this packet relative to the data in the original packet. If the sum of size and offset of packet differs from the next fragment packet then packet will overlap. System will crash when this attack happens.

G. Resource Depletion Attack

In resource depletion attack the attacker motive is to use the resources or misuse network protocol communication by sending packets. All resources are busy by attackers.

H. Protocol Exploit Attack

1)TCP SYN: TCP SYN attack target preprocessor resources. Attacker gives instruction to zombies to make server busy by sending TCP SYN request. It takes advantage of 3 way handshake between client and server. It deluges the TCP SYN packet to server with the take or spoofed IP address so it results server sends ACK SYN to any of non-requesting device. When server found so many SYN request is processed by or but not found any ACK SYN server in this process exhaust the memory and processor resources.

I. Layer 7 Attack

Layer 7 is application layer which needs few packets and bandwidth to perform DDoS attack. If goal is to take down. This attack causes execute so many requests and load many file. Layer 7 not easy to detect because connection already established legitimate user request comes with the attack and if server deny all then it cause of denial of service.

HTTP GET METHOD: The strategy of this attack is to send incomplete header or part of HTTP header as complete header not reached so socket resources keeps alive. By this legitimate user not able to get resource. Advantage of this attack for attacker is server restore it [9]. Attacker uses slow Loris tool for this attack.

V. COUNTER MEASURE FOR TCP

This method checks whether the request is from genuine user of from fake IP only TCP handshake not able to defend attack. Here server found TCP request it send a message to change window size with SYN+ACK packets. As in TCP attack the victim send response to non-requesting device by asking for reduces window size server able to know packet in spoofed or not. TCP-probing develop host based architecture. TCP probe set some specification to make connection. If client have to verify specification otherwise no connection protocol analyzer that whether client verifies specification or not. Detector is use to take big decision to accept or drop. With this technique attacker not able to give reply of TCP probe.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

VI. COUNTER MEASOR ON NETWORK LAYER FOR SYN FLOOD ATTACK

Filtering is done to prevent attack on this layer. It uses some filtering operation which drops source IP address of an attacker. If applies routeblackholing and threshholding techniques.

A. Routeblackholing

It simply reconfigure the routing protocol with this attacker not able to do attack.

B. Threshholding

It sets the amount of traffic according to the bandwidth.

When attack is found in network layer it stops the communication. The filter table contains. FORWORD: It processes those packets which are routed through The following command runs when SYN attack happens. Command: - (#hping3—flood-s-p81 192.16.0.1) Flood: This is flag to send packet fast S: It SYN flag P-81: Sends the packet to 81 server come from a specific address within a given window of time. E.g.: Rule is to accept only 20 packets per second from and to IP address 146.20.Y.Y.Here accept as well as drop rule when packets more than 20 packets the no packet match accept rule.

VII. COUNTER MEASURE ON SMURF ATTACK

We can prevent the smurf attack by developing host separately and make them in a way to not pass any kind of acknowledgement to ping requests. The interception of smurf attack can be succeed when the firewalls and the routers will be emaciated. The vantage package has been developed for the prevention. When it gets the attack can happen it provides the warning to get updated to the organizer that attack can occur. The administrator from the provided equipment of that organization in which the attack can occur prevents the attack before it can damage the whole network down.

VIII. COUNTER MEASURE ON DOMAIN NAME SERVICES AMPLIFICATION ATTACK

The prevention of DNS amplification attack can be done with a proper knowledge of the key parts. There are some techniques provided for prevention:-DNS Security Extensions-The modification of the data cannot be done by using this method. The region operator provides the digital signature for that particular region so that no integration of data can be possible in between the transmission. The domain will be secure using this from the attack that can harm the system. DNS Traffic monitoring-It is the method to provide the information of new occurring attack while the domestic band trying to have the connection with the exterior band. it provides commanding of DNS data and it is beneficial method to detect the attack that is about to occur through monitoring the traffic. Configuration best practices-It is the method in which during the creation the functionality get placed individually. The caching will be deserted from the official acknowledgement.

IX. PREVENTION TECHNIQUES FORDDOS ATTACK

A. Disable Not Used Services

If server has less open ports and application it will lead to less prone to the attack. So the services need to disable for the sake of prevent from attackers [6].The port that are not in use should be disable for that convenience that the numbers of attacks will be lesser than before and it will be beneficial to prevent those attacks that could occur before[6].

B .Firewalls

Effective means of protection a local system from network based security threats While affording access to the world via WAN's [6].The firewall is itself immune to the penetration. If the attack will occur on web service firewall will be not able to protect it because they can't find the difference for better traffic from the DDoS attack traffic. Firewall is used to prevent the server by some rules for allow or deny the IP address[6]. Simple flood attack can be prevented by firewall but some attacks like port do web services can't be prevented by firewall.

C. Honeypot

Honeypot is a part of intrusion detection technologies.

Honeypot make the attackers to be lure, it generally diverts the attacker and collects the information about the attackers for making the mission successful. They make them able to make the attackers consistently stay long enough to honeypot, and then we can observe that what they will do with the intended system and network [7].Honeypot contains fabricated information. It is not real

system not even used by real user. it consumes large amount of attackers and it has high detection accuracy [7].it is primarily used for specific research. it is a security resource who's values lies in being attacked. Based on the deployment, honeypot may classified as-

1) *Production Honeypot:* It is easy to use. It contains limited information. It is placed inside the production network. Production honeypots are low interaction honeypots which are easier to diffuse. It gives less information about the attackers.
2) *Research Honeypot:*It is used to research the risks and to learn how to get protect against those risks. Research honeypot is complex to diffuse and it contains extensive information. Usually used by military or government organization.[7]In summary, it is a machine placed on the network for the intension of performing as an enticing target but triggers alarms when it is being attacked[7].they help to get information by storing the records of attackers and want to find what exact software they used.

D. Ingress Filtering Technique

Ingress filtering is developed by Ferguson [4]. Ingress filtering is like packet filtering. ISP uses this method when they find suspicious traffic in the network. Packet header contain information of packet therefore packet header is checked by the edge device like router, firewall. All incoming packets have to meet the requirement like Network Ingress Egress Filtering [5].With this filtering user is prevent from the attack and also it ensures that its network not participating in any attack.

E. Egress Filtering

It is outbound filtering. In this technique only those IP addresses go outside the networks which meet the requirement set by the edge device. Ingress and egress filtering done by the edge devices and edge devices has the great knowledge of interface of the network. So we check the source address of incoming packet and then check whether flow out in the same path or interface through which it comes or not.

F. IP Hopping

IP hopping is the method in which server ip address is changing dynamically. It changes the ip address or location of the server .The changes are used pseudo random law and all the genuine users know that law. The new Ip address is changes with the pre specified available set of Ip addresses. By doing this Ip address of the victim's system is invalidated.it is protocol level defense method. Bots are now not able to generate the high load on the server. It works like the radio system as radio changes the frequency to other frequency at the time of transmission.

X. CONCLUSIONS AND PROPOSED WORK

This paper provide us a information about the DDoS attacks and its characteristics also the types of the DDoS attack, The various counter measures to mitigate DDoS attack, tolerance and also the prevention techniques. DDoS assaults are the measures risk to the web group and we can expect a considerable measure of safety efforts. The future work is design the prevention technique.

REFERENCES

[1] ivya Kuriakose, V.Praveena," A Survey on DDoS Attacks and Defense Approaches"international Journal of innovative Research,2013

[2] Sumit Singh Panwar," An Effective Prevention Mechanism for TCP/SYN Attack", International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-6, September 2015

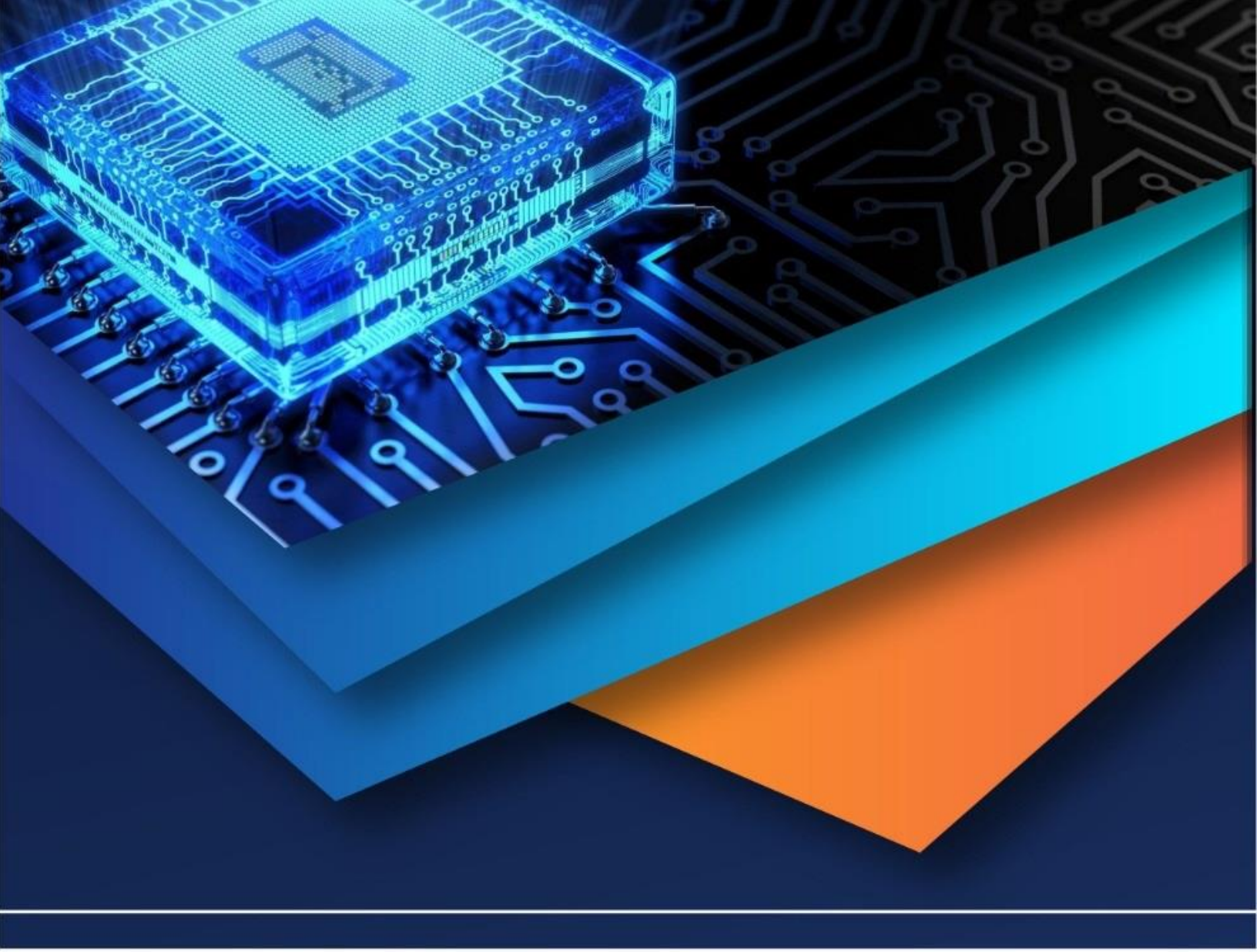
[3] Mohd Azahari Mohd Yusof, Fakariah Hani Md Ali, and Md Yusof Darus" Detection and Defense Algorithms of Different Types of DDoS Attacks" International Journal of Engineering and Technology, Vol. 9, No. 5, October 2017.

[4] P. Ferguson, and D. Senie, "Network ingress filtering: Defeating denial of ser-vice attacks which employ IP source address spoofing," RFC 2267, the Internet Engineering Task Force (IETF), 1998

[5] B.B Gupta ,R.Joshi," Distributed Denial of Service Prevention Techniques", International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010

[6] B. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE " Distributed Denial of Service Prevention Techniques" International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010 1793-8163

[7] Deepika Mahajan, Monika Sachdeva" DDoS Attack Prevention and Mitigation Techniques - A Revie" International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY