# Wireshark Window Authentication Based Packet Captureing Scheme to Pervent DDoS Related Security Issues in Cloud Network Nodes

Waqar Ali[1,2 *], Jun Sang[1,2], Hamad Naeem[1,2]
[1]*Key Laboratory of Dependable Service Computing in Cyber Physical Society, Ministry of Education, Chongqing 400044, China*
[2]*School of Software Engineering, Chongqing University, Chongqing, 401331, China*
abro_king@yahoo.com

Rashid Naeem[1,2], Ali Raza[3]
[3]*Department of computer science, International Islamic University, Kuala lumpur, 50728, Malaysia*

***Abstract*—DoS (Denial of Service) attack forces a cloud network node to handle few unauthorized access that employ unwanted computing cycle. As a result, the cloud node response is slow as usual and resource on cloud network becomes unavailable. Some Dos attacks are Ping of Death, Teardrop, Snork, Locking authentication, SYN flooding, Operating System Attacks etc. The most vulnerable incident happen when the adversary is committed DDoS (Distributed Denial of Service) attack with comprised cloud network. In this paper, the prevention techniques for DDoS (Distributed Denial of Service) attack in cloud nodes were discussed. a dynamic window scheme in cloud nodes to determine a message verification to resolve unnecessary packet processing was proposed**

***Keywords- DoS attack, DDoS attack, cloud network, Cloud Nodes, dynamic winodws***

## I. INTRODUCTION

Cloud computing has emerged as a new trend in the field of information technology. A huge number of researcher is working and contributing in the development of cloud computing. The simple example to have a Health Information System under cloud is proposed by A. Memon [1]. DoS is the most advanced and malicious types of attacks that intruder performs to break security. DoS attack is the way to broadcast unnecessary message and occupy the resource of network node so that it cannot performs its functionality properly. In cloud networks the security is big problem and DoS attacks can produce severe consequences [2]. Due to DoS attack, a network node or server processes some extra unwanted computing cycle and response slow. It keeps node resources unavailable. The adversary commits a DoS attack may vary. Most commonly it provides efforts to temporarily or permanently interruption or suspension services of a host connected to the Internet [3].For clarification, DoS attacks are sent from one system or by one hacker. But DDoS attacks are committed by compromised system with multiple hackers [4].
Many forms of DoS or DDoS attacks violate the security of a network such as Ping of Death, Operating System Attacks, Teardrop, Locking authentication, SYN flooding, Snork and many more. This type of incursion aims the system or sites have great interest on financial service and user traffic like online payment system, credit card payment gateways, DNS server, control server, administrative server and so on. At August, 2009, micro blogging site Twitter was victim of DDoS execution and was inaccessible for several hours [5].
Fig. 1describes a DoS attack on intermediate node by hacker using computer virus especially on distributed cloud nodes over a network.
Cloud server level security need to be ensured to protect any cloud node from external attacks such as DoS attack.

In this paper, we will discuss about a variety of DoS attack and its techniques. Then we will recommend the prevention techniques for DoS attack. Later, Distributed Dos attack technique and its remedy is discussed

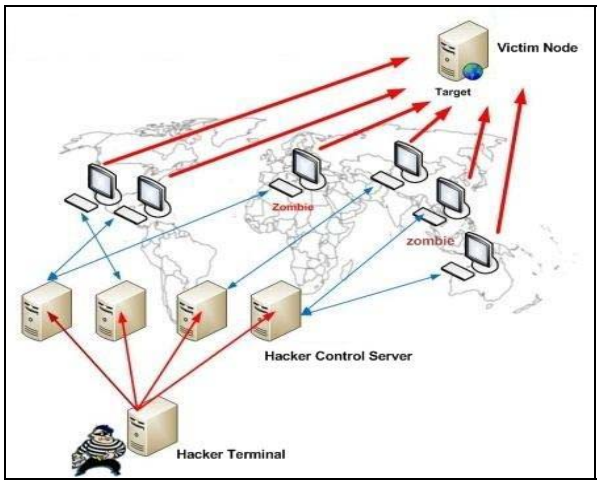


Figure 1: Denial of Service (DoS) Attack; Intermediate node zombie comprised by hacker and computer virus

## I. DISCRIPTION OF DOS A SECURITY THREAT IN CLOD

DoS attack is an attempt to lose valuable resources which may have sensitive critical enterprise system. Some types of DoS attacks even use up all of the process in cloud server. The

**978-1-4799-8353-7 /15/$31.00 ©2015 IEEE**

receiving end of a DoS attack may reduce useful performances, such as e-mail solutions, Internet connections or cloud storage access. Some forms of DoS attacks can occupy all the bandwidth or even can utilize full system resource, such as server memory. Some of the worst-case circumstances we analyze over previous times several decades are a Website, used by many individuals having to stop function because of excessive DoS attack.
The countermeasure studies of DDoS attacked its effects on cloud need to analyze the attacking techniques first.

### *A. TYPES OF DOS ATTACKS ON CLOUD*

There are a number of ways to conduct DoS attacks which result the vulnerable DDoS attacks over cloud network. Some major types of attacks are discussed below:

**Flood Attack***:* Flood attacks are well known form of a DoS attack. The procedure of a flood attack is basic where intruders send traffic beyond a server can manage. Even if a network admin restricts more data transfer usage, still this is not an adequate security against a flood attack. The will affect more badly on public cloud network as the services are rendered there are public.

**Ping of Death is Attack:** Ping of Death is an attack using the security hole and a known bug in TCP/IP protocol stack. A Ping of Death attack is simply delivering an IP datagram, the size of which surpasses the factors. When such a datagram is obtained, this accident downs the victim system [6] this kind of attack will affect private cloud systems over distributed networks using TCP/IP protocols.

**Teardrop Attack:** It is an attack taking advantage of a weak point in the restore of IP packet and potentially confuses the receiving system. The attacker form a sequence of IP fragments with extending offset fields. When this excessive size of packets are received the received nodes tries to reassemble the malformed fragments and failed. As a result the node is reboot or alert critical error. This will highly effect on personal cloud storage especially when information is accessing.

**SYN Attack:** SYN flooding is an attack taking advantage of the three-way handshaking of TCP. When a connection is recognized using TCP/IP protocol, this includes a handshaking procedure, which includes the return of SYN and ACK information. When a hacker is flooding the receiving packet with SYN messages, this will fill up the SYN buffer. In this case the receiving party cannot deliver an ACK messages and no TCP/IP connection with any cloud network servers are possible. Therefore, Losing TCP/IP connection may result in losing cloud access over a TCP/IP network.

Smurf Attack: The procedure of a Smurf attack is more sensitive and the complex task is to identify a broadcast server. When a hacker knows the transmitted servers in a network, he or she issues a ping command. The source IP address in this ping command is counterfeit and it searches as if the ping comes from inner network. When the broadcast server gets the ping request, then it relays the ping request to the entire network and all the machines in the network return a response. These responses are again rerouted by the transmitted server to the target machine. Secure broadcast cloud server is required to avoid smurf attacks.
Snork Attack: Snork is an attack towards Windows NT RPC service. It allows an attacker with little network resources to cause a distinct NT system to use up 100% CPU utilization for an endless time period. The security of incoming transmission from cloud nodes need to be secured to prevent victim from being attacked.

### *B. TECHNIQUES OF DDOS ATTACKS*

DDoS is an advanced level of DoS attack. Similar DoS, DDoS also tries to stuck the valuable services running on a server by broadcasting packets to the receiving server in a manner that the server cannot handle it. As cloud storage is expending among organizations and e-commerce and their interconnection results in distributed cloud environments. More distributed cloud storage many results in more DDoS attacks over cloud nodes.
Generally, DDoS follows of 3 segments: Master, slave and last one is the victim. The master is the main attacker who is the person behind machine. The slave is the network node which is controlled by Master. Victim (can be cloud node) is the target resourceful server. Master informs the slaves to launch attack on the victim's computer. Hence it's also known as co-ordinate attack.
Attacker logs into Master Node and send command to slaves' terminal to perform an attack on a specific target server (victim). Slaves then react by starting ICMP, TCP, UDP or Smurf attack on victim. The DDoS attack is committed generally in distributed environment and attacker uses multiple Master machines. Each master pc controls a large number of slave computer as zombie server to perform the attack. So the real scenario is big enough for blustering the attack from a large number of machines rather from specific node [7]. An example of DDoS environment is depicted in Fig. 2.

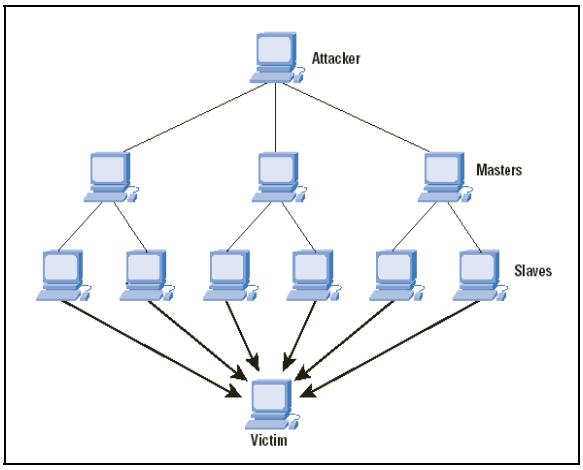

Figure. 2.A typical Distributed Denial of Service (DDoS) attack scenario

The most vulnerable DDoS attack is happen at Layer 7 in OSI model which are come in many form like HTTP Flood Attack, Random URLs, Random Searches. A complicated Layer 7 DDoS attack can focus on specific section of a website and able to make it a complex form to isolate from usual traffic of that site. Fewer Layer 7 DDoS attacks aim web page elements, like logo or a keyword, and continuously obtain resources expecting to fatigue the server.

DNS Query attack, Query length buffer overflow, DNS cache poisoning attacks, amplification attack, DDoS application exploit attack (relevant to sql injection) are all different types DDoS susceptible invaded form. Since attackers use many more new techniques in DDoS methodology, a new term used to explain its effective burden and ventures that are still unknown called "Zero Day" attack.

A French website was invaded on February 13, 2014 by a strong organized DDoS attack which hit the site at data range rate from 325 Gbps to 400 Gbps. It was observed as the worst DDoS attack ever. CloudFlare, a company of web performance evolution analyzed that a strong DDoS is committed on a French Website with a record of almost 400 Gigabit transfer per Second. The Company found that to produce the roughly 400 Gbps of attack rate, the attacker employed 4,529 NTP servers from 1,298 comprised networks. Then average rate for each server in this incident sent 87 Mbps of traffic to the victim french server. NTP DDoS attacks are the latest one and were first observed in last December by Symantec Corporation. NTP is mainly used to sync times for systems over the Internet or from local time server. In a short period of time, numerous NTP request and processing on a target machine have become popular DDoS attacks [8]

### *C. METHODOLOGY TO OVERCOME ISSUE OVER CLOUD NETWORK*

To protect cloud node and cloud network from becoming a sufferer of DoS attacks, many precautionary alternatives are applied by network administrators which include:

- Implement router filters. This will reduce the exposure to several DoS attacks. If attack is committed to the system, security patches need to install for preventing TCP SYN flooding.
- All the inner and outer traffic must go through content filter or firewall so that malware, viruses and data sniffing can be prevented. The system administrator must have authority to monitor all users' activity whenever needed.
- Disable any unwanted network services. This can restrict the ability of an intruder to take advantage of those solutions to perform a DoS attack.
- Restrict service and user by quota systems. Notice the system efficiency and set up baselines for common action. Use the baseline to evaluate uncommon levels of disk activity, CPU utilization, or network traffic.
- Routinely analyze physical security with regard to present needs.
- Use "Packet Tracer", "Nagios" or a similar tool to identify changes in settings information or other files.
- Ensure spare parts and redundant server so that any critical server affected by DoS attack can be replaced immediately without service interruption.
- Establish and sustain frequent back-up plans and guidelines, particularly for important settings information.
- Establish and sustain appropriate security password guidelines, especially access to extremely privileged accounts such as UNIX root or Microsoft Windows Administrator.

By capturing traffic with Wireshark (a packet monitoring tool), a DoS attack can be identified. DoS attacks are commonly recognized as SYN floods arriving from all part of the world. To figure out the source of a packet, it needs to enable the GeoIP localization in the Name Resolution configuration in the Wireshark preferences after running this application for monitoring purpose. Fig 3 shows Wireshark windows for capturing packets over cloud network.

## II. PURPOSED DYNAMIC WINDOW SCHEME

All the attempts mentioned at earlier section are applied for preventing DDoS attack and is applicable for network layer and configuration. Further, broadcast messages, unnecessary message sending, icmp flooding are the common form of this request .An easy way to handle this type of attacks is to check each message before forwarding it (known as authentication

first method). The faked messages will be discarded after passing first-hop neighbors of the harmful nodes, so nodes apart them will not be impacted. However, this is difficult to accomplish, because cloud nodes have no information

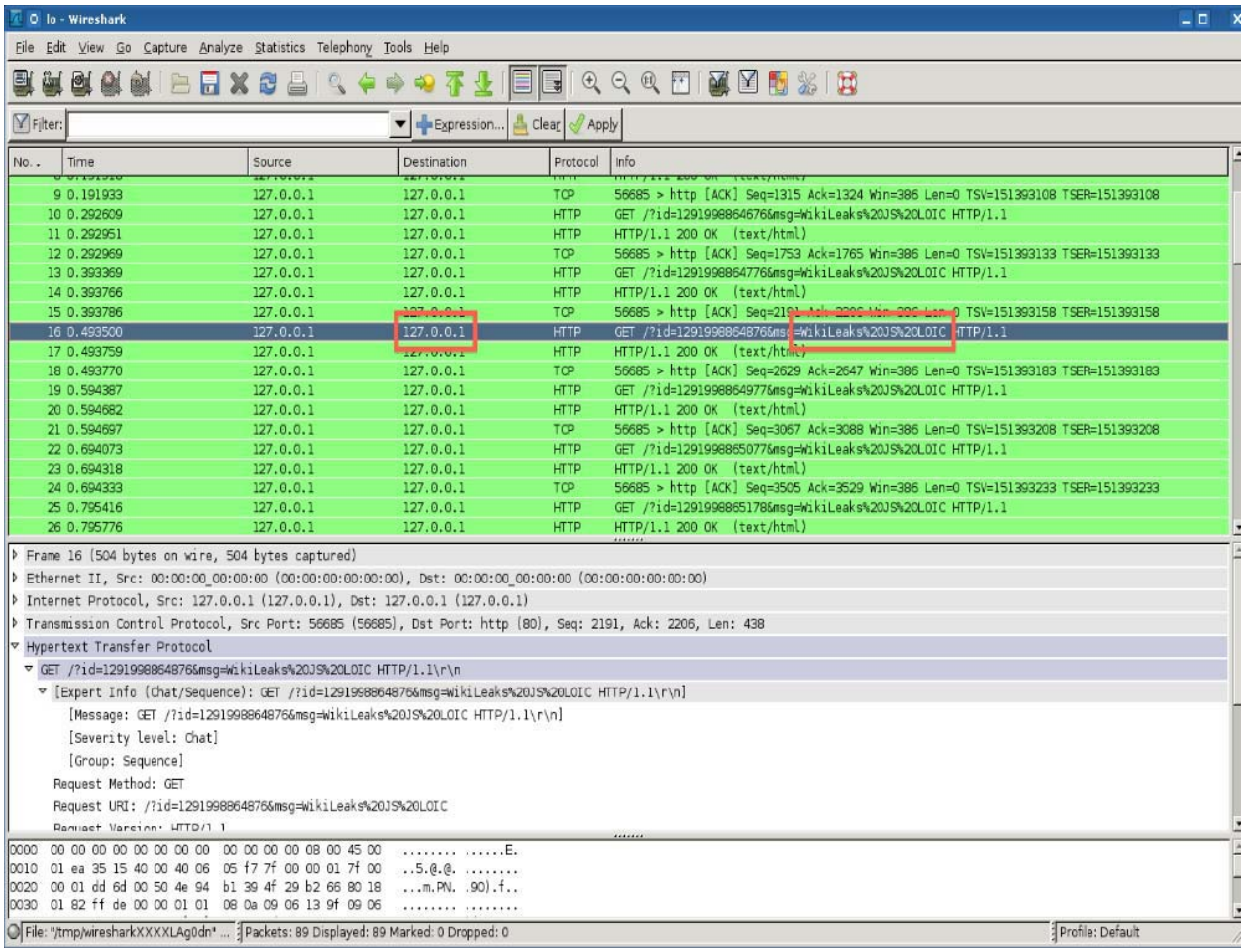


Figure 3. Wireshark window for packet capturing

regarding the attack and either they are victims in such attack or not. To overcome such issue, a dynamic window scheme is introduced where network nodes determine a message verification or message forwarding by them. The proposed dynamic window scheme is the combination of the authentication-first and the forwarding-first plan that can achieve by the broadcast delay for real messages and energy savings for unwanted messages [9].

In the dynamic window technique, each network nodes needs to manage a new parameter: authentication window size (ω). This parameter identifies the maximum number of hops that an incoming message can be transmitted without verification. Correspondingly, each broadcast message m keeps record of a new field: distance (da), which is used to record the number of hops the message has passed since its last authentication. When node s gets the message m, it compares the size (ω) with the number of passing hops form since its last authentication (da). If da $<\omega$, s is in the forwarding-first mode: it increases da, and forwards m without verification. da $\geqslant\omega$, s is in the authentication-first mode, which authenticates m first: if the authentication fails, s drops m; otherwise, s resets da to 0,and forwards m to its next hop neighbors.

## III. Effects of Purposed Dynamic Window Scheme in Infoemation Security System

Any purposeful attempt to cut off web application or network from its desired clients qualifies as a DoS attack. Such attacks have been efficiently implemented against major internet businesses such as Visa and MasterCard transaction, social network sharing and WordPress. DoS attacks successfully affect the services as offline, cost estimation business and unfavorable advertising. This also force IT staff to spend useful sources protecting against the assailants. Webhosting systems and networks are vulnerable to interruptions. Security gaps need to be identified, new technological innovation applied, and resources and best methods developed for reducing risk and preventing the effects of service interruptions. Users of cloud environment complete the user

authentication process as mandatory for the service provider whenever they use new cloud service. Generally a client signup with offering personal information and a service provider provides a user ID and authentication method for user verification after the sign is done. After then the client uses the ID and the verification technique to function user validation when the user accesses to use the offered cloud computing service. Unfortunately, there is a probability that safety of verification technique can be penetrated by an attack during the process of verification, and then it could cause several informative losses. Moreover, to avoid network failure or to resolve website availability problem, the system must maintain redundant link connectivity. The web server must have enough bandwidth allocation to serve webpage to external user [10]

## IV. Future Improvements

Security issues are rising in the cloud computing environment. Cloud system authentication and access control are principle concern for secure data transaction. A user in the Cloud Computing environment has to complete the user validation process required by the service provider while attempts to new login. In this process, weak validation key assists to the network attacker and there will be a risk to expose personal information stored in the database.

There are no solid security technologies in Cloud Computing. Since we consider Cloud Computing as the extension of the existing IT technologies so it is possible to apply access control and user authentication process from IT perspective. Access control is one of the securing techniques that control a process in the operating system not to approach the area of another process. Improving security through advanced redundancy and error checking features will keep user material safe and secure in the cloud server [11]

## V. Conclusions

A variety of attacks often result in a loss of availability of the important cloud node. In particular, the directed diffusion is vulnerable to DoS type attacks, due to the robust nature of flooding.

Computer threats come in many different forms like File Viruses, Trojan viruses, Worms spread in many ways. These can be used to steal any information and initialize any massive attack in a cloud node. DDoS attacks cause Resource Depletion, Radio Interference, Hello Flood (a malicious node can send or record or replay the interest message at a high transmission rate)[12].

## VI. Acknowledgments

This work was supported by Specialized Research Fund for the Doctoral Program of Higher Education of China (SRFDP) (No. 20130191110027).

## VII. Refrences

[1] Memon, A. A., Naeem, M. R., Tahir, M., Aamir, M., & Wagan, A. A. (2014). A New Cloud Computing Solution for Government Hospitals to Better Access Patients' Medical Information. *American Journal of Systems and Software*,*2*(3), 56-59.

[2] Dhanalakshmi S, & Divya, D. (2015). Identification and Avoidance of DDoS Attack for Secured Data Communication in Cloud, *CSE*.

[3] Gillman, D., Lin, Y., Maggs, B., & Sitaraman, R. K. (2015). Protecting Websites from Attack with Secure Delivery Networks. *Computer*, 48(4), 26-34.

[4]Juliadotter, N. V., & Choo, K. K. R. (2015). Cloud Attack and Risk Assessment Taxonomy. IEEE Cloud Computing, (1), 14-20.

[5]ICMP Ping, *ICMP Ping Report*,IOWA State University, USA. 2007.

[6] T. Dübendorfer, Past and Future Internet Disasters: DDoS attacks survey and analysis, *Seminar Security Protocols and Applications* April 2003, pp. 10-12.

[7] S. J. Vaughan-Nichols, Worst DDoS attack of all-time hits French, *Arbor Networks' ninth Annual Worldwide Infrastructure Security Report (WISR)*, Web:http://www.zdnet.com/worst-ddos-attack-of-all-time-hits-french-site-7000026330/ (February 13, 2014)

[8] Wang, R., Du, W., & Ning, P. (2007, September). Containing denial-of-service attacks in broadcast authentication in sensor networks. In *Proceedings of the*

[9]Chester, A. P. (2011). Towards effective dynamic resource allocation for enterprise applications (Doctoral dissertation, University of Warwick).

[10]Chi, S. H., & Cho, T. H. (2006). Fuzzy logic anomaly detection scheme for directed diffusion based sensor networks. *In Fuzzy Systems and Knowledge Discovery* (pp. 725-734). Springer Berlin Heidelberg.

[11]Hallberg, McGraw-Hill, Securing your network, *Networking: A Beginners Guide (4th Edition)*, pp. 135-150.

[12] McCarthy, Twitter crippled by denial-of-service attack, *CNET News' Stephen Shankland contributed to this report*. Web:http://www.cnet.com/news/twitter-crippled-by-denial-of-service-attack/ (August 6, 2009).