International Journal of Information and Computation Technology (IJICT)
ISSN 0974-2239 Volume 3, Number 10 (2013)

Analysis of Entropy Based DDoS Attack Detection to Detect UDP Based DDoS Attacks in IPv6 Networks

D. Balamurugan[1], S. Chandrasekar[2], D. Jaya Prakash[3], M.Usha[4]

[1]Associate Professor/CSE, Sona College of Technology, Salem.

[2]Principal, Gnanamani College of Technology, Namakkal Dist, Tamilnadu, India.

[3]Dept. Computer Science and Engineering, Sona College of Technology, Salem, Tamilnadu,

[4]Professor and Dean (Research)/CSE, Sona College of Technology, Salem, Tamilnadu

ABSTRACT

Distributed Denial of Service (DDoS) attacks is an important thread in internet. In IPv6 internet worms are difficult to identify, because of the total amount of traffic which does not allow the instant investigation of fine points. In Internet Protocol Version 6 (IPv6) networks one of the common traffic flows occurs is UDP data flows. It is an unreliable data flow. This characteristic can be used by the attackers to cause the DDoS attacks. The existing DDoS detection techniques mostly concentrate on attacks generated by TCP flows. Entropy based DDoS attack detection method is normally used to detect DDoS attacks generated by TCP flows. Here we use the same mechanism to detect UDP based DDoS attacks and analyze its performance.

Keywords: IPv6, UDP, DDoS, Entropy, threshold, false positive

1. INTRODUCTION

Internet is a common place for connecting huge number of systems and peoples in the way of transfers and shares the data from one place to another in efficiently and effectively. This open structure allows the both attacks as well as legitimate flows. The attacker aims to disturbing the flow of data from the network to generate the enormous data flow between the systems, in order to refuse ordinary services or corrupting the quality of services.

DDoS attack is achieved by the group of several nodes. The attacker consumes the high bandwidth and it will not allow transferring important data from the internet. Recent investigation shows that internet users in the world demonstrated that DDOS attack are rising significantly and individual attacks are more powerful and complicated. A DDoS attack is not easy to recognize the attackers, because an attacker attacks another system and sends huge number of data flows to the targeted machine.

UDP is connection less data flow, there is no automatic retransmission in time of data loss/failure and no proper packet restructuring at the receiving endpoint. So the user cannot expect that every transmitted packet cause the receiving host to respond among a packet. Accordingly, we cannot calculate the number of unreturned packets to acquire the number of unsuccessful connections. UDP based data transfer is generally a single-packet abuse. It means of attacking host sends a packet to the pointed host, if it is successful than they send huge number of packets in the same host. The main problem is UDP does not verify the source IP address, destination IP address, source port, destination port values which gets problem to identify the targeted machine; this will create the traffic on other data flows in IPv6 network. User Datagram Protocol (UDP) is a transport-layer protocol that presents least transport service. The protocol is not affording reliability or datagram organizing for this reason is less time-consuming to the end-points. It provides applications through access to the datagram service of the IP layer. An application that sprint above UDP has to contract with end-to-end communication problem.

DDoS attacks from the surge of legitimate traffic. In order to achieve these goals, we take use of information theory parameter, entropy, which is a measure for the randomness of a process, to raise the alarm for the potential attacks. We define the packages which share the same destination address as a flow, and entropy will be employed to measure the randomness of flows on a given router. Once an alarm is raised for a flow, we will employ, entropy rate, which is the rate of growth of entropy, on the path of the flow to the destination. If the flow is a DDoS attack, the entropy rates on different routers are the same or very close [2].

The proposed system going to analysis of entropy based DDoS attack detection to detect the UDP worms. This system identifies the UDP data flows in the IPv6 network. After that entropy system checks the source and

destination IP address and port address in the router. The entropy system first calculates the flow entropy for each UDP flow in the IPv6 network. The enhancement of this work will include normalized entropy (NE) calculation, which is based on flow entropy result. Now identify the false positive for the packet flow which is based on the number of attack flows as well as legitimate flows within the time. To set the threshold limits value then detect the normal flow and attack flows in the network. This entropy based UDP worm detection mechanism is avoiding the UDP data flow attacks in the IPv6 network. So this will make the network data flow is more efficient and effective transmission.

2. BACKGROUND AND RELATED WORK

2.1 UDP in IPv6

IPv6 is a fourth generation protocol are now getting development, the next hurdle in realizing the promises of IPv6 is the need for deployment on a wider scale. IPv6 takes the advantage of simplifying the process of packet forwarding and efficient usage of packet header. A router provides an efficient mechanism in packet processing that significantly adapts the principle of end-to-end internet design. IPv6 simplifies the process of checksum in UDP by gradually reducing the need to recompute the checksum when header fields change. The development of routers to perform checksum computation makes it less necessary for IPv6 by computing the checksum at link speed using dedicated hardware.

2.2 DDoS Attack

The Denial of Service (DoS) attack is the most basic implementation of the Distributed Denial of Service (DDoS) attack. The attack is spread to the availability given of the large number compromised systems to know the target victims. The target victim passes the huge number of packets to the targeted host and attack the network packet flows in the IPv6 network

2.3 Entropy Based Detection

UDP is based on the notion of packet dynamics, rather than packet content, as a way to deal with the increasing complexity of attacks. We utilize a concept of entropy to measure time-variant packet dynamics. The entropy of network traffic should vary immediately on the router.

Entropy variation is a technique for identifying the vulnerable request from the attacker. It monitors the packet flows in router, and when the packet count exceeds the prescribed limit, the vulnerability is detected. The entropy maintains the threshold level for providing uninterrupted communication in the internet.

2.4 Related Work

Carlos E. Caicedo et al [1]., has stated their work on IPv6 adoption exist within the networking community, including the vision that IPv6 is a failure and offer no important advantage over IPv4. Even as IPv6's latest features will probably generate newer protocol attacks, the older known IPv4-related attacks will morph into new forms. IPv6 was designed with security in mind; security concerns could delay its success if sufficient efforts and resources are not dedicated to fully understanding IPv6-related security issues and vulnerabilities in IPv6-based network infrastructures. Several attacks can only be executed by a node in the network sector. It shows some of these attacks, securities provided by the DoS attack on Duplicate Address detection (DAD) protocol, Man-in-the-middle attack, and fake router implantation attack. Given IPv6's growing importance, the development of techniques and tools to protect emerging IPv6-based networks is a current and pressing need. Ting Ma al [13]., has stated their work on the ipv6 security architecture, IPSec, plays a optimistic role in the security of IPv6 networks. To some special attacks, particularly DDoS attacks, IPSec shows comparatively weak, because IPSec can only protect against DDoS attacks that spoof their source addresses. In cases where attackers initiate DDoS attacks with their actual identity, IPSec is vulnerable. This paper recommends a link signature based DDoS attacker tracing algorithm. It can instantaneously rebuild the whole attack path after suffering a DDoS attack whether or not the source addresses are spoofed. In a DDoS attack, the attacker controls many dummy machines to simultaneously flood the victim with network traffic, rejecting them continuity of service. There are two fundamental means to employ DDoS attacks. One is to produce large volumes of traffic to victim and the other is to send abnormal packets. In both cases victims wear out their resources processing these malicious packets to the scope that normal service cannot be maintained. These two methods can work under IPv6. We will mainly deliberated on the more frequently used traffic volume type attack

Shui Yu et al [5]., has stated their work on Entropy-Based Collaborative Detection of DDoS Attacks on Community Networks community network frequently work with the similar Internet Service Provider domain or the virtual network of dissimilar entities that are collaborating with each other. In such a associated network environment, routers can work closely to raise early warning of DDoS attacks to void shattering damages. The attackers use the same mathematical functions to control the speed of attack package pushing to the victim. Based on this examination, the different attack flows of a DDoS attack share the same regularities, which is

different from the real surging accessing in a short time period. Information theory parameter, entropy rate are applied to discriminate the DDoS attack from the surge legitimate accessing. Attackers can use different types of techniques (referred to as scanning techniques) in order to discover vulnerable machines. Such as random scanning, the machine that is infected by the malicious code investigates IP addresses randomly from the IP address space and verifies their vulnerability. Robin Doss et al [6]., has stated their work on traceback of DDoS Attacks Using Entropy Variations, the Distributed Denial-of-Service (DDoS) attacks are a significant threat to the Internet. However, the memory less feature of the Internet routing mechanisms makes it tremendously hard to trace back to the source of these attacks. A novel traceback method for DDoS attacks that is based on entropy variations between ordinary and DDoS attack traffic is proposed.

3. PROPOSED WORK

3.1. DDoS Attacker

The attacker first establishes a network of computers that will be used to generate the huge volume of traffic needed to deny services to legitimate users of the victim. To create this attack network, attackers discover vulnerable hosts on the network. DDoS attack, the master computer orders the zombies to run the attack tools to send huge volume of packets to the victim [8].

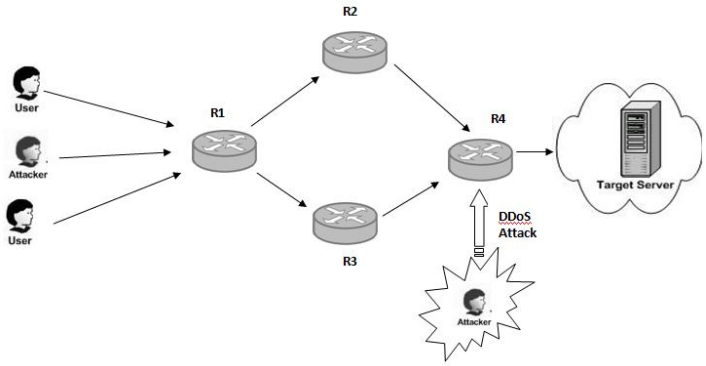

Figure 1. DDoS Attack

3.1. System Architecture

UDP in IPv6 network router is called local router. It receives the bulk of UDP data packets from the host machine in IPv6 network. The local router recognizes the upstream of the UDP packet flow and the destination address of a group of packets that are passing through the local route.

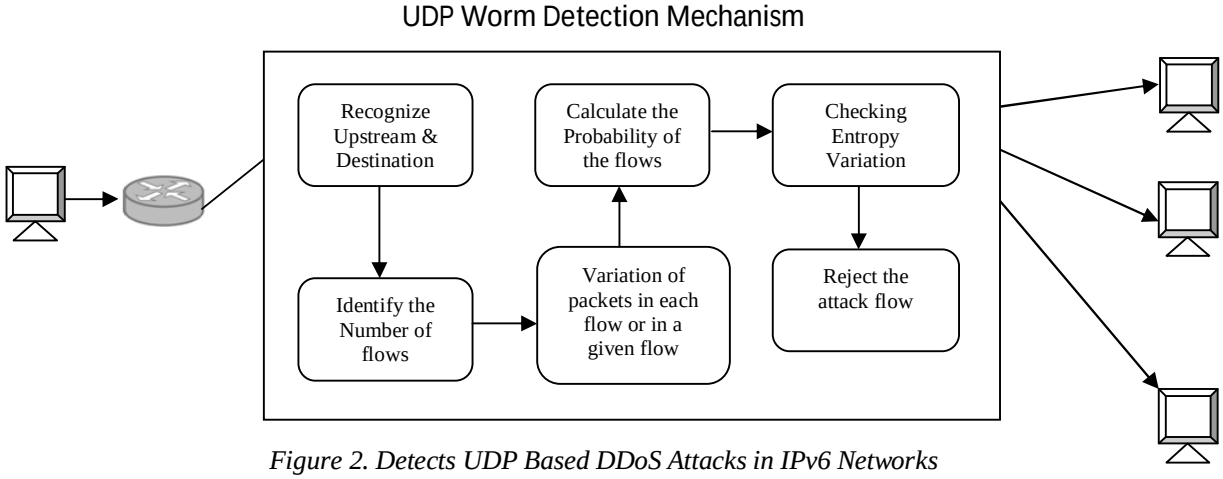

Figure 2. Detects UDP Based DDoS Attacks in IPv6 Networks

Subsequently identify the number of packets flow in the local router, than we, compare the upstream packets and the total number of packet flowing in a given flow. To calculate the probability of the flows and Entropy variations of the UDP packet in a IPv6 network. Finally, calculate the entropy variations of the given flow (if the flow maintains levels of packet flow). The steady of packet flow is maintained by using threshold limits, maximum threshold level is depends upon the number of users communication passed from source to destination machine, if the flow entropy leads the limits of threshold level, that system architecture specially designed for avoiding zombies attacks form the vulnerable host/attacker system. Since, we are proposing the new system for

detecting and correcting the UDP worms in the IPv6 network. It increases the effectiveness and efficiency of the internet.

3.2 DDoS detection algorithm

Step 1: Collect sample UDP flows for a time window T on the edge routers.
Step 2: Calculate router entropy H(x) = - $\sum_{i=1}^{n} P(xi) \log P(xi)$
Step 3: Calculate Normalized router Entropy (NE) = (H / log n0)
Step 4: If NE < threshold (δ1), identify the suspected attack flow.
Step 5: Calculate the entropy rate H (X) = $\lim_{n\to\infty} \frac{1}{n} H$
(x1, x2… xn) of the suspected flow in that router and the routers on downstream.
Step 6: Compare Hi (x) $\forall i \in$ entropy rates on routers.
Step 7: If Hi (x) ≤ threshold (δ_2), it is a DDoS attack.
Else legitimate traffics.
Step 8: Discard the attack flow.

4.CONCLUSION

In this paper I proposed an effective and efficient IPv6, UDP based DDoS attacks based on entropy variations. Here the traceback strategy is avoided, because it suffers a number of drawbacks and times. This paper employs by storing the information of flow entropy variations at routers. Once the DDoS attack has been identified it performs to delete the attacker request. The entropy variation first identifies its upstream router where the attack flows comes from and then submits the threshold level checking of the destination packets.

5. REFERENCES

[1] Caicedo, C.E.; Joshi, J.B.D.; Tuladhar, S.R (2009), "IPv6 Security Challenges", Published by IEEE, PP.36 – 42
[2] Shui Yu, Wanlei Zhou (2008), "Entropy-Based Collaborative Detection of DDOS Attacks on Community Networks", Sixth Annual IEEE International Conference on Pervasive Computing and Communications, PP. 566 – 571
[3] Khanna S, Venkatesh S.S, Fatemieh O, Khan F, Gunter C.A (2008), "Adaptive Selective Verification ", 27th Conference on Computer Communications, Published by IEEE, , PP.529 - 53
[4] Shui Yu, Wanlei Zhou, Doss, R, Weijia Jia (2011), "Traceback of DDoS Attacks Using Entropy Variations", IEEE Transactions on Parallel and Distributed Systems, PP. 412 – 425
[5] Khanna S, Venkatesh S.S, Fatemieh O, Khan F, Gunter C.A (2012), "Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks", Networking, IEEE/ACM Transactions, PP. 715 - 728
[6] Waddington, D.G; Fangzhe Chang (2002), "Realizing the Transition to IPv6", Communications Magazine on Digital Object Identifier, PP. 138 – 147
[7] Ting Ma (2009), "A link signature based DDoS attacker tracing algorithm under IPv6", International Journal of Security and Its Applications, PP.27-36
[8] Anusha. J (2011), "Entropy Based Detection of DDOS Attacks", International Journal of Soft Computing and Engineering (IJSCE), PP.564-567
[9] W. Timothy Strayer (2004), "SPIE-IPv6: Single IPv6 Packet Traceback", Local Computer Networks, 2004. 29th Annual IEEE International Conference on Digital Object Identifier, 2004, PP. 118 – 125
[10] Anitha G (2012),"Reliable Determination of Zombies Based on Entropy Variation", Journal of Computer Applications ISSN on Network security, PP.257-260
[11] You-ye Sun; Cui Zhang; Shao-qing Meng; Kai-ning Lu (2011),"Modified Deterministic Packet Marking for DDoS Attack Traceback in IPv6 Network", Computer and Information Technology (CIT), IEEE 11th International Conference on Digital Object Identifier, PP.245–248
[12] Xinyu Yang; Ting Ma; Yi Shi (2007), "Typical DoS/DDoS Threats under IPv6", Computing in the Global Information Technology, International Multi-Conference on Digital Object Identifier, PPs. 55
[13] Ting Ma; "A link signature based DDoS attacker tracing algorithm under IPv6", International Journal of Security and Its Applications, PPs. 27
[14] Sanjeev Khanna and Santosh S. Venkatesh (2008), "Adaptive Selective Verification", INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, PPs. 529 - 537