International Journal of Soft Computing 9 (4): 219-225, 2014
ISSN: 1816-9503

UDP Worm Detection in IPv6 Networks Using Entropy Variations

[1]D. Balamurugan, [2]P. Shanmugaraja, [3]S. Chandrasekar and [4]D. Jayaprakash
[1]Department of CSE, [2]Department of IT,
Sona College of Technology, Salem, Tamilnadu, India
[3]Gnanamani College of Technology, Pachal (PO), Namakkal (DT), Tamilnadu, India
[4]Department of CSE, Dhirajlal Gandhi College of Technology, Salem, Tamilnadu, India

Abstract: Distributed Denial of Service (DDoS) attacks are one of the most common threats to the internet. However, the unreliable communication is made through Routing System that formulates to trace the source of these attacks makes very tough. In IPv6, finding worms in UDP is not an easier task. Researchers propose a UDP worm detection technique in IPv6 which basically uses the entropy variations between regular flow and DDoS attacks. This is primarily different from commonly used packet evaluation techniques. In comparison to the existing DDoS entropy techniques, the proposed approach obtain a number of advantages it specially handles the UDP communication traffic, efficiently scalable, strong and not in favour of packet attack and free from attack traffic prototype. The investigational and model results are obtained to express the value and competence of the proposed method.

Key words: IPv6, UDP worms, DDoS, entropy, threshold, false positive

INTRODUCTION

The User Datagram Protocol (UDP) is the central part of the internet protocol group. UDP is suitable for purposes where error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. UDP worms do not require a connection to be established before infection can begin. The implementation of the worm is normally self-carried and included in the first packet sent to the target. Since, there is waiting time required as for UDP worms, UDP worms normally spread very rapidly and their speed is only limited by network bandwidth. UDP worms often have to compete with each other for network resources. In IPv6 UDP worm detection is more complicated because it does not support reliability or acknowledgements.

The User Datagram Protocol (UDP) transport is defined for the Internet Protocol Version 6 (IPv6) for IPv6 hosts and routers. The UDP transport protocol has a least set of features. This limited set has enabled a wide range of applications to use UDP but these applications do need to offer lots of essential transport functions on top of UDP. The UDP usage guidelines provides overall guidance for application designers. The lack of a possibility to detect UDP worm in IPv6 has been observed in the routers. The design of IPv6 elevates different issues when considering the safety of checking the entropy variations for UDP worms in IPv6 networks (Caicedo *et al*., 2009).

The victim first identifies which of its upstream routers are in the attack tree based on the flow entropy variations it has accumulated and then submits requests to the related upstream packet flows in the router. The entropy in routers identify where the attack flows came from based on their local entropy variations that they have monitored. Once the packet flows have identified the attack flows they will forward the requests to discard the packet flows in the routers, respectively (Yu and Zhou, 2008).

The proposed system going to be implemented using the entropy variation techniques. Entropy variation is used to find out the source of the attack with the help of entropy variation in dynamic by calculating the packet size which shows the variation between normal and DDoS attack traffic (Yu and Zhou, 2008). For DDoS attack detection, it is needed to compare the distribution of packet flows, under normal conditions and under attack conditions. A typical scenario is to send out UDP packets to random hosts while keeping very little state information for each target or none at all if the attack can be executed by sending a single UDP packet. In IPv6, UDP worms are high and there will be failure to detect the worms. The proposed system uses the entropy variations for

Corresponding Author: D. Balamurugan, Department of CSE, Sona College of Technology, Salem, Tamilnadu, India

detecting UDP worms. Entropy maintains the threshold level for incoming packets if the data flow reaches the noticeable level of variation from the threshold level, the entropy detects the worm and also keeps away from the malicious users' request. The analysis, experiments and simulations demonstrate that the proposed DDoS entropy mechanism is effective and efficient compared with the existing methods. In particular, it possesses the following advantages:

- The implementation of the proposed method gets no modifications on current routing software
- The proposed strategy is basically different from the existing entropy variations techniques. Because of this essential change, the proposed strategy overcomes the inherited drawbacks of packet marking methods such as limited scalability and vulnerability to packet pollutions
- The proposed method will be effective for future packet flooding DDoS attacks because it is independent of traffic prototype

BACKGROUND

UDP in IPv6: In IPv6, the packet header and the process of packet forwarding have been simplified. The packet processing by routers is generally more efficient thereby extending the end to end principle of Internet design. The IPv6 header is not protected by a checksum; integrity protection is assumed to be assured by both link-layer and higher-layer (TCP, UDP, etc.) error detection. IPv6 requires UDP to have its own checksum. Therefore, IPv6 routers do not need to recompute a checksum when header fields (such as the Time To Live (TTL) or hop count) change (Caicedo *et al*., 2009). This improvement may have been made less necessary by the development of routers that perform checksum computation at link speed using dedicated hardware but it is still relevant for software-based routers.

The current fast-propagate worms use UDP packets rather than TCP connections to target this vulnerability. As a result, these worms are network bandwidth limited rather than connection latency limited. So, while researchers are trying to increase the bandwidth of the current internet, researchers are just making a better environment.

Background of DDoS attacks: DDoS attacks are targeted at attacking the victim's resources such as operating system data structures, computing power and network bandwidth. To initiate a DDoS attack to the vulnerable host machine, the attacker first launching a network of computers that will be used to make the huge volume of traffic needed to refute services to authorized users of the victim. To build an attack network and the attacker find out vulnerable hosts on the network.

DDoS attack detection evaluate the packet number distribution of packet flows which are beyond the control of attackers once the attack is commenced and establish the relationship of attack flows is much higher than the relationship among legitimate flows (Yu *et al*., 2011).

Entropy variations: This UDP is based on the notion of packet dynamics rather than packet content as a way to deal with the increasing complexity of attacks. Researchers utilize a concept of entropy to measure time-variant packet dynamics. The entropy of network traffic should vary immediately on the router. It monitors the packet flows in router and when the packet count exceeds the prescribed limit, the vulnerability is detected.

LITERATURE REVIEW

Caicedo *et al*. (2009) has stated their research on IPv6 adoption exist within the networking community, including the vision that IPv6 is a failure and offer no important advantage over IPv4. 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. Yang and Ma (2009) has stated their research on the IPv6 security architecture. 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 study 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.

Yu and Zhou (2008) has stated their research on Denial of Service (DoS) attacks are considered within the state of a Shared Channel Model in which attack rates may be large but are bounded and client request rates vary within fixed bounds. It is exposed that clients can adapt effectively to an attack by raising their request rate based on timeout windows to approximate attack rates. The server will be able to process client requests with high probability while pruning out most of the attack by selective random sampling. The protocol Adaptive

Selective Verification (ASV) is shown to use bandwidth efficiently and does not require any server state or assumptions about network congestion. The main results of the study are a formulation of most favourable performance and a proof that Adaptive Selective Verification is most favourable. Khanna *et al.* (2012) has stated their work on adaptive selective verification attacks are a growing concern as they continue to cause an important threat to the reliability of the Internet. Such attacks can happen at all levels in the protocol stack and threaten both routers and hosts.

Yu *et al.* (2011) has stated their research 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 an 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. Lee *et al.* (2012) has stated their research on traceback of DDoS attacks using entropy variations. A Novel Traceback Method for DDoS attacks that is based on entropy variations between ordinary and DDoS attack traffic is proposed. Anitha (2012) has stated their research on zombie. It is a computer, connected to the internet that has been controlled by an attacker. Zombie computers are frequently used to launch distributed denial of service attacks. Research on DDoS detection improvement and filtering has been conducted pervasively. However, the efforts on IP traceback are limited.

Anusha (2011) has stated their research on trace back the source of the DDoS attacks in the internet is enormously hard. It is one of the unexpected challenge to trackback the DDoS attacks that attackers generate enormous amount of requests to victims through compromised computers (zombies), in order to rejecting regular services or degrading the quality of services. Yang *et al.* (2007) has stated their research on a link signature based DDoS attacker tracing algorithm under IPv6 security architecture, IPSec, plays a positive responsibility in the security of IPv6 networks. To some special attacks, particularly DDoS attacks; IPSec come into sight comparatively weak because IPSec can only support against DDoS attacks that spoof their source addresses. Li *et al.* (2013) discussed the various statistical techniques used in DDoS Attack Detection algorithms and their effectiveness in DDoS attack detection. Zhang *et al.* (2012) discussed the flow level detection of low rate DDoS attacks using entropy based technique. Sun *et al.* (2011) discussed the Packet Marking algorithm used in the detection of DDoS attacks in IPv6 networks. Rodriguez *et al.* (2008) analysed the entropy variation technique in detecting worm attacks in local area networks. Wang *et al.* (2012) proposed a new multi stage approach to detect low rate DDoS attacks which uses entropy variation technique as the base. Waddington and Chang (2002) discussed the various security issues to be solved when using IPv6 transition mechanisms.

PROPOSED RESEARCH

This model is developed in order to create a dynamic IPv6 network. In IPv6 network, nodes are interconnected with the admin which is monitoring all the other nodes in the UDP based IPv6 Internetwork. All nodes are sharing their information with each others. The client sends huge volume of data to the destination machine through UDP based IPv6 network.

DDoS attack network: 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 (Fig. 1).

Flow entropy variation: To classify the packets that is passing through a router into flows. A flow is defined by a pair of identities; the IPv6 address of the upstream

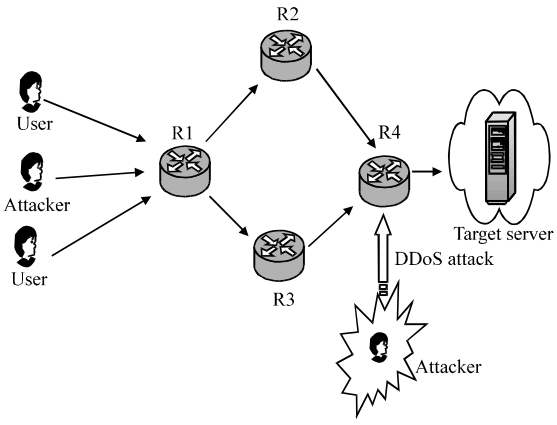

Fig. 1: DDoS attack

router where the packet came from and the destination IPv6 address of the packet. Entropy is an information theoretic concept which is used to compute the randomness of the packet flow. Entropy variation is occupied to compute the changes of randomness of flows at a router for a given time interval. Based on the above mentioned metric, a generic DDoS Detection algorithm is proposed. The algorithm makes use of the following assumptions and initialization parameters:

- I: the number of UDP packet flows
- R: total number of flows
- U = {u_i, i ∈ I}+{L}: IPv6, UDP flow on a local router where u_i is identity of the IPv6 network and L is the number of local UDP flows in the network u_i

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):

$$NE = \frac{H}{\log n_0}$$

Step 4: Compare NE with threshold value of the normal flow to identify deviation.
Step 5: If the deviation is very large identify the suspected flows which cause this deviation.
Step 5: Calculate the entropy rate:

$$H(X) = \lim_{n\to\infty} \frac{1}{n} H(x_1, x_2, ..., x_n)$$

of the suspected flows in that router and the routers on upstream.
Step 6: Compare $H_i(x)$ ∀ i∈ entropy rates on routers to find the deviation from normal flow.
Step 7: Compare $H_i(x)$ with the threshold value of the normal flow of all upstream router.
Step 8: If the deviation varies with all the upstream routers then
It is a DDoS attack.
Else
It is a legitimate traffic.
Step 9: Discard the attack flow.

Collect sample UDP flows for a time window T on the edge routers: The system has to collect the UDP data packet flows from the IPv6 network. The packet sniffer operation allows capturing UDP packets travelled through network adapter and also sniffing complete conversation between the network elements. This system can capture the source and destination machine complete information like IP address, port number, date and time of travelling and duration of packet traveling between the systems. Run the packet sniffer system for N hour of time in IPv6 network. This capture the complete packet transfer details of both legitimate user data flow and attacker data flow. All the captured flows are removing the attacker host by using entropy based system in the packet capture and analysis system.

Calculate flow entropy: The entropy variation technique begins with the calculation of entropy for each flow in the UDP/IPv6 network. This identifies the each source and destination packet flows and calculates the entropy for the distinct flow with the following equation:

$$H(x) = \sum_{-i=1}^{n} P(x_i)\log P(x_i)$$

Where:
x_i = A distinct flow
$P(x_i)$ = The probability of the flow
n = The total number of distinct flows

Calculate router entropy: Researchers calculate the router entropy by combining the total number of distinct flow which the source and destination is same. To count the total number of packets flow in the network.

The entropy H(x) of a random variable x with possible values of {1, 2, ..., n} and distribution of probabilities P = {p_1, p_2, ... , p_n} with n elements where $0 \le pi \le 1$ and $\sum_{i=1}^{n} P_i = 1$ can be calculated as:

$$H(x) = \sum_{-i=1}^{n} P(x_i)\log P(x_i)$$

Here, total number of packets is the number of packets travelled for a time T. Likely researchers can estimate probability for each source (destination) port as.

Calculate Normalized router Entropy (NE) NE = (H/log n_0): Normalized entropy calculates the over all probability distribution in the captured flow for the time window T:

$$\text{Normalized entropy} = \frac{H}{\log n_0}$$

Identify the suspected flow: In the case of identifying the suspected flow by using threshold limit checking by using entropy rate and threshold detection range.

Entropy variations: Finally, researchers have to calculate the entropy of flow for each flow:

$$H(F) = -\sum_{i,j} P_{ij}(u_i, d_j)\log P_{ij}(u_i, d_j)$$

H(F) as entropy variation which measures the variations of randomness of flows. It measures the variations of randomness of flows on a particular local router.

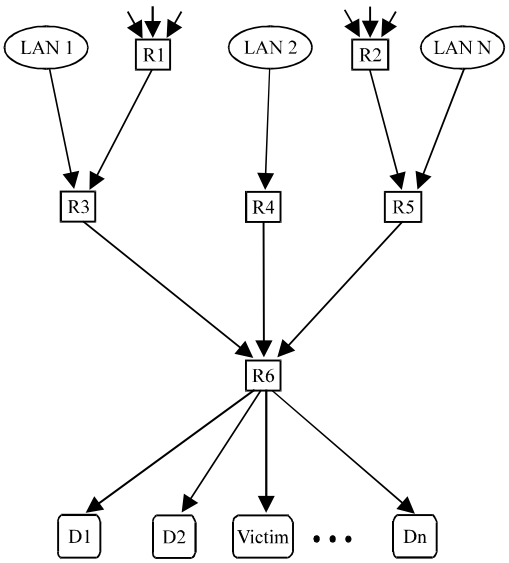

Fig. 2: UDP traffic flows at an attack path

UDP traffic flows are defined the data flow between the legitimate users request and also handles attacker flow. The attacker find the malicious users in the IPv6 network and capture the overall control of the system called victim. As shown in Fig. 2, the LAN1 passes the request from router R3, R6 and reaches the destination machine. LAN2 transfers the packets through R4, R6 then router R2 packets travelled in the R5, R6. The entropy variation is calculated for checking DDoS attacks at the router R6.

SIMULATION AND RESULTS

Experimental setup: Test bed model consists of 6 source nodes, 2 destination nodes, 4 attacker nodes and 4 legitimate nodes out of 16 nodes. The network bandwidth of legitimate data transfer and traffic is set stable and the model of attack traffic is accomplished by randomly generating large set of Variable Bit Rate (VBR) UDP flows in IPv6 network.

The legitimate user and the source nodes to send packets for the time duration of 30 mins to collect the required details of the data flow to calculate the entropy at normal condition. The attacker starts sending attack flows from 30 min 20 sec onwards along with normal traffic. The total system experiment lasts at 150 sec. Researchers sniffed no. of packets received in every 10 sec interval and then researchers calculated the entropy variation deviation for the attack flow from the normal flow using the traced data. Results of the experiments are cited in Table 1 and 2.

The packet sniffing is the initial step of the UDP network worm detection. The packet sniffing is to identify

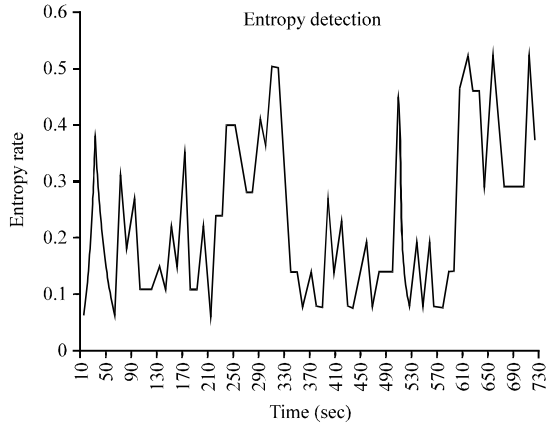

Fig. 3: Normalized UDP flow entropy

Table 1: Sample packet entropy rates under normal flow

Entropy rate	Time (sec)
0.04	10
0.08	20
0.45	30
0.52	40
0.68	50
0.60	60
0.46	70
0.64	80
0.45	90

Table 2: Sample packet entropy rates under attack flow

Entropy rate	Time (sec)
0.32	10
0.48	20
0.53	30
0.58	40
0.46	50
0.49	60
0.32	70
0.48	80
0.53	90

the UDP flow within the IPv6 network. Here, researchers identify the UDP packet flow and maintain the details of each packet flow in the network.

Figure 3 depicts the normal flow of packets without any system degradation. The X-axis represents the time involved in throughout the data flow and the Y-axis represents packet count. It is observed that the packets achieved a stable flow throughout packet count 135 in IPv6-UDP networks.

In Fig. 4, attack packets are encountered which results in overall system degradation due to large number of anonymous packet count.

Figure 5 concentrates on the attack flow. The system is prepared with the attacking data using entropy variation technique which detects attacker flow when the maximum flow of data is found, the pattern is observed which prevents the attack data and improves overall system performance.

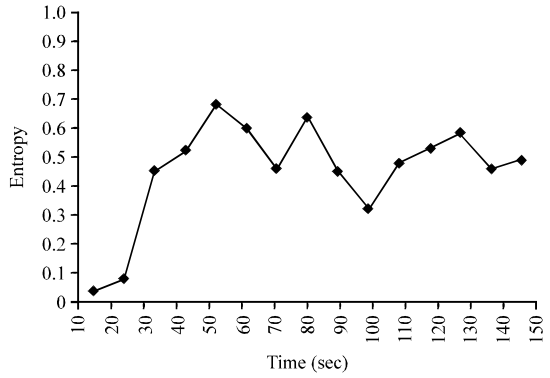

Fig. 4: Entropy variation in attack flow

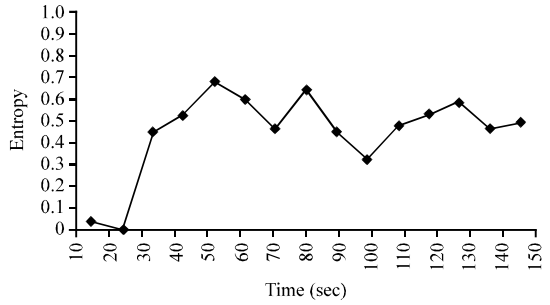

Fig. 5: Before threshold limit checking

The estimated threshhold limit is 0.57. Check the threshold limit to each flow in the network and then identify the normal flows and attacker flow. Attack detection rate and false-positive rate are the two metrics that are set as performance evaluation metrics of the proposed algorithm:

$$\text{Detection Rate (Rd)} = \frac{d}{n}$$

Where:

d = Number of attack packets identified as attack packets

n = Total amount of attack packets generated

The entropy rate increases in parallel with the increase in the false positive detection rate. In some cases the false positive detection rate shows an abrupt increase in value for a slight deviation in entropy rate. When the maximum false positive detection rate achieves a stable condition, it is stated as detection threshold value. This is depicted in Fig. 6.

False positive rate: It is measured by:

$$\text{Rfp} = \frac{p}{m}$$

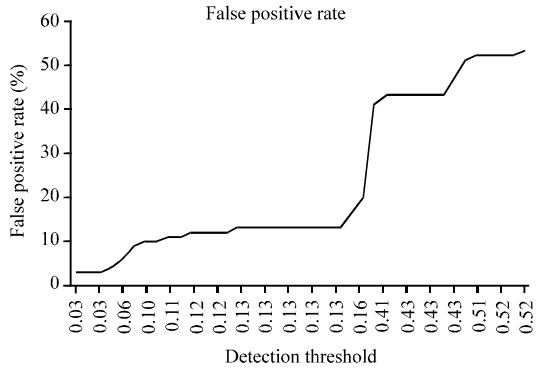

Fig. 6: DDoS attack detection rate

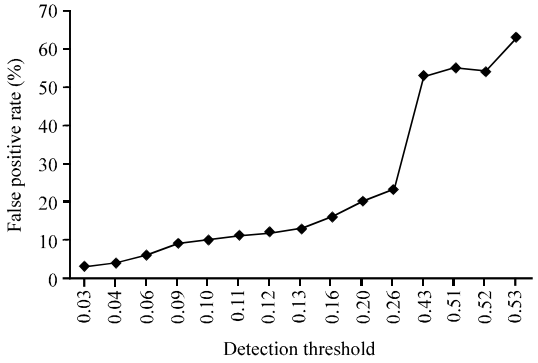

Fig. 7: False positive rate

Where:

P = Number of legitimate packets detected as attack packets

m = Total number of authorized packets

When calculating false positive rate, researchers originate that up to situation detection threshold 0.43 the false positive rate is 0 but putting threshold 0.41-0.53 increases false positive rate. This is depicted in Fig. 7.

CONCLUSION

In this study, an effective and efficient mechanism is proposed to detect UDP based DDoS attacks in IPv6 networks based on entropy variations. Here, the traceback strategy is avoided because it suffers a number of drawbacks and times. This study 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. The experimental results show

acceptable results when compared to other techniques. In the future this algorithm can be tested in a large IPv6 network with real time traffic situation for its efficiency.

REFERENCES

Anitha, G., 2012. Reliable Determination of zombies based on entropy variation. J. Comput. Applic., 5: 257-260.

Anusha, J., 2011. Entropy based detection of DDoS attacks. Int. J. Soft Comput. Eng., 1: 564-567.

Caicedo, C.E., J.B.D. Joshi and S.R. Tuladhar, 2009. IPv6 security challenges. Computer, 42: 36-42.

Khanna, S., S.S. Venkatesh, O. Fatemieh, F. Khan and C.A. Gunter, 2012. Adaptive selective verification: An efficient adaptive countermeasure to thwart DoS attacks. IEEE/ACM Trans. Networking, 20: 715-728.

Lee, S.M., D.S. Kim, J.H. Lee and J.S. Park, 2012. Detection of DDoS attacks using optimized traffic matrix. Comput. Math. Appl., 6: 501-510.

Li, B., G. Bebis, J. Springer and M.H. Gunes, 2013. A survey of network flow applications. Elsivier J. Network Comput. Applic., 36: 567-581.

Rodriguez, D.M. D. Torrez-Romain, C. Vargas-Rosales and P. Vearde-Alvarado, 2008. Entropy based analysis of worm attacks in a local network. Adv. Comput. Sci. Eng., 34: 225-235.

Sun, Y.Y., C. Zhang, K.N. Lu, S.Q. Meng and K.N. Lu, 2011. Modified deterministic packet marking for DDoS attack traceback in IPv6 network. Proceedings of the 11th International Conference on Computer and Information Technology, August 31-September 2, 2011, Pafos, pp: 245-248.

Waddington, D.G. and F. Chang, 2002. Realizing the transition to IPv6. IEEE Commun. Magazine, 40: 138-147.

Wang, F., H. Wang, X. Wang and J. Su, 2012. A new multistage approach to detect subtle DDoS attacks. Elsivier J. Math. Comput. Mod., 55: 198-213.

Yang X. and T. Ma, 2009. A link signature based DDoS attacker tracing algorithm under IPv6. Int. J. Secur. Applic., 1: 27-36.

Yang, X., T. Ma and Y. Shi, 2007. Typical DoS/DDoS threats under IPv6. Proceedings of the International Multi-Conference on Computing in the Global Information Technology, March 4-9, 2007, Gosier, Guadaloupe, pp: 55.

Yu, S. and W. Zhou, 2008. Entropy-based collaborative detection of DdoS attacks on community networks. Proceedings of the 6th Annual International Conference on Pervasive Computing and Communications, March 17, 2008, Piscataway, New Jersy, pp: 566-571.

Yu, S., W. Zhou, R. Doss and W. Jia, 2011. Traceback of DDoS attacks using entropy variations. Trans. Parallel Distrib. Syst., 22: 412-425.

Zhang, C., J. Yin, W. Chen, X. Luo and Z. Cai, 2012. Flow level detection and filtering of low-rate DdoS. Elsivier J. Comput. Networks, 56: 3417-3431.