Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.023858
Article

Tech Science Press

Enforcing a Source-end Cooperative Multilevel Defense Mechanism to Counter Flooding Attack

Saraswathi Shunmuganathan*

Department of Computer Science and Engineering, Sri Sivasubramaniya Nadar College of Engineering, Kalavakkam, Chennai, Tamil Nadu, 603110, India
*Corresponding Author: Saraswathi Shunmuganathan. Email: saraswathis@ssn.edu.in

Received: 24 September 2021; Accepted: 01 December 2021

Abstract: The exponential advancement in telecommunication embeds the Internet in every aspect of communication. Interconnections of networks all over the world impose monumental risks on the Internet. A Flooding Attack (FA) is one of the major intimidating risks on the Internet where legitimate users are prevented from accessing network services. Irrespective of the protective measures incorporated in the communication infrastructure, FA still persists due to the lack of global cooperation. Most of the existing mitigation is set up either at the traffic starting point or at the traffic ending point. Providing mitigation at one or the other end may not be a complete solution. To insist on better protection against flooding attacks, this work proposes a cooperative multilevel defense mechanism. The proposed cooperative multilevel defense mechanism consists of two-level of mitigation. In the first level, it is proposed to design a Threshold-based rate-limiting with a Spoofing Resistant Tag (TSRT), as a source end countermeasure for High-Rate Flooding Attacks (HRFA) and spoofing attacks. In the second level, the accent is to discriminate normal traffic after Distributed Denial of Service (DDoS) traffic and drop the DDoS traffic at the destination end. Flow Congruence-based Selective Pushback (FCSP), as a destination-initiated countermeasure for the Low Rate Flooding Attack (LRFA). The source and the destination cooperate to identify and block the attack. A key advantage of this cooperative mechanism is that it can distinguish and channel down the attack traffic nearer to the starting point of the attack. The presentation of the agreeable cooperative multilevel safeguard mechanism is approved through broad recreation in NS-2. The investigation and the exploratory outcomes show that the proposed plan can effectively identify and shield from the attack.

Keywords: Flooding; spoofing; cooperative solution; multilevel security; filtering; pushback

1 Introduction

Ever improving technology together with ever-expanding connectivity made the Internet available to everyone at high speed and low cost. The growth of telecommunication embeds the Internet in every aspect of communication. Internet communication is based on Internet Protocol (IP) that relies on best-effort service to forward packets from one end to another end. Irrespective of the legitimacy, packets are forwarded to the end host with minimal processing. This frictionless nature of the Internet made it vulnerable to various attacks like Phishing, Malware, Password, Man in the middle, Denial of Service (DoS).

A DoS attack is a packet flooding attack that is capable of degrading the performance of the communication infrastructure. The Internet has made it easy to launch a FA without the need for any special hardware or tool. Throughout the DoS attack, the illegitimate user floods plenty of attack traffic towards the destination. Traffic directed in this way to the destination makes the service provided by the destination to be unavailable to the legitimate user and also degrades the quality of services by consuming the resources provided by the destination.

McAfee Labs publishes quarterly threat reports about analytical examination and patterns in dangers measurements. Their insights on different dangers recognized by Threat Research Labs are in Fig. 1.

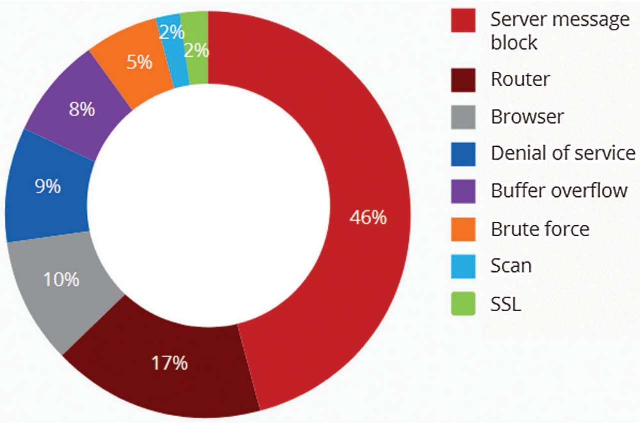


Figure 1: Network attack types from McAfee threat report

The Denial of Service Flooding Attack (DoS FA) can be classified into High Rate Flooding Attack (HRFA) and Low Rate Flooding Attack (LRFA) [1]. In HRFA, assailants send an enormous volume of attack packets to deny the service provided by the destination. In LRFA, a huge number of dispersed aggressors (bots) co-work in sending a little amount of attack traffic to the objective to escape from the discovery of the attack. In both types of FA, the assailants try to degrade the quality of services to legitimate users. Building a better system's fundamental need is to battle the attack. Also, it should build dependability and increase the reliability of the destination server. The attack moderation system can be conveyed anywhere at the source, destination, halfway, or in a dispersed way. Handling the attack at the destination end is simple yet it is subject to bandwidth consumption [2]. The attack rate will be high at the source end itself for HRFA while the attack rate will be high only at the destination end for LRFA. The HRFA merges at the soonest point even at the source end edge router. On the other hand, LRFA unites towards the destination end. To provide a superior nature of service to the legitimate user both HRFA and LRFA need to be handled efficiently. Hence it is preferred to deploy cooperative multiple defense mechanisms.

Most of the existing techniques use single-level mitigation that is effective against HRFA or LRFA but not for both. An effective mechanism to protect the Internet from each attack is possible exclusively through a cooperative multilevel defense mechanism [3]. This fact motivated us towards multilevel mitigation. This effort is a move towards an enhanced countermeasure for FA by deploying the mitigation at the early point of convergence like source end for HRF attack [4] and destination end for LRF attack. Threshold-based rate-limiting and Spoofing Resistant Tag technique (TSRT) is deployed at the source end edge routers to mitigate HRFA. The LRFA that converges at the destination end can be encountered at the destination end by Flow Congruence-based Selective Pushback (FCSP) technique. Further, the attack source can be located by deploying a flow similarity-based pushback technique at the specific routers.

The paper is formulated with Section 2, which discusses the related work followed by Section 3 that elaborates the network model and assumptions. Section 4 portrays the architecture and cooperative multilevel defense mechanism proposed. In continuation, Section 5 concentrates on the viability and effectiveness of the mitigation technique. Finally, Section 6 is all on conclusion.

2 Related Work

Extensive research has been made so far to mitigate the flooding attack. The literature survey reveals that the researchers focus on the source or destination end solutions capable of detecting and/or preventing the attack. This section discusses the existing defense against flooding attacks that is closely related to the planned work.

The StackPi [5] is a per packet-based marking technique capable of filtering the attack packets and detecting the spoofed source IP addresses. Individual packets are embedded with a total path recognizable value. The packet forwarded on a specific path will hold a similar value embedded within it. During an attack, this unique piece of embedded information increases the feasibility to identify and drop packets traveling through the same path. Peng et al., [6] proposed a probabilistic packet marking scheme for pushback of attack source. The packet marking is based on probability and code transformation. Yu et al., [7] proposed a traceback technique based on entropy variation of the flow rather than explicit packet marking. Zhang et al. [8] focus on router-based mitigation. They incorporated intelligence into the router. These routers are capable of incorporating cryptographic security that facilitates following back to the source of the attack launcher. Even though each technique overcomes the limitations of one or the other technique, it has its own limitations. In common, spoofing of packet marking by the attackers, the requirement for a large storage to reconstruct the path, high consumption of resources at the early stage of traceback, and the involvement of all internet routers are the major limitations of the traceback techniques.

Wang et al. [9] proposed a mechanism known as the Internet Protocol easy-pass mechanism. It is a simple access control filter, incorporated at the edge router to mitigate flooding attacks. Both this work provides protection at the source end of the attack. Also, they are capable of mitigating spoofing attacks but not LRFA and HRFA with legitimate source IP. Keromytis et al. [10] focused on separating the genuine traffic from attack traffic. They designed a dynamic topology-based Secure Overlay Service (SOS) network to transmit the genuine traffic.

Zhijun et al. [11] tried to classify LRFA using time domain and frequency domain analysis. Xie et al. [12] identified the low rate TCP attack using the mean distance algorithm at the ingress switches. Liu et al. [13] proposed a low rate DoS attack mitigation is a classification algorithm that is based on the K-nearest neighbor (KNN) algorithm that uses the features in the acknowledge (ACK) packet. The Hop count value incorporated in the packet provides some information on the legitimacy of the packet [14]. Expected hop count can be predicted and if there is an enormous difference between the received packet hop count and expected hop count then the packet is assumed to be an attack packet and dropped. Information theory and advanced entropy are used [15–17] to discriminate legitimate access from the illegitimate. In general attack packets are handled only at the destination end leading to more packet loss, illegitimate packets that consume scarcely available network resources are the problems with the above-mentioned destination-based solutions. Deka et al. [18] identified the spoofed attack using the relationship between the spoofed IP and the number of ports opened.

The literature review reveals that each technique is strong in its own focus but not on all attacks such as spoofing, HRFA, LRFA, replay attack. This study reveals that the source end mitigation is capable of defending against spoofing and HRFA but not able to protect efficiently against the distributed LRFA. On the other hand, the destination end solution is highly efficient in detecting HRFA and LRFA but with the tradeoffs like resource consumption, processing overhead, and so on. To overcome these shortcomings, this work proposes a cooperative multilevel mitigation mechanism.

3 Network Model and Assumptions

The sample network topology considered in this work is shown in Fig. 2, which includes distributed LAN sites LAN1, LAN8, routers R1,…, R11, and the destination. The nodes in the LAN sites may be legitimate or malicious, denoted as N or A respectively in Fig. 2. LAN sites and destination servers are connected to the external network through an edge router. In this topology edge router, R11 connects the destination server to the external network.

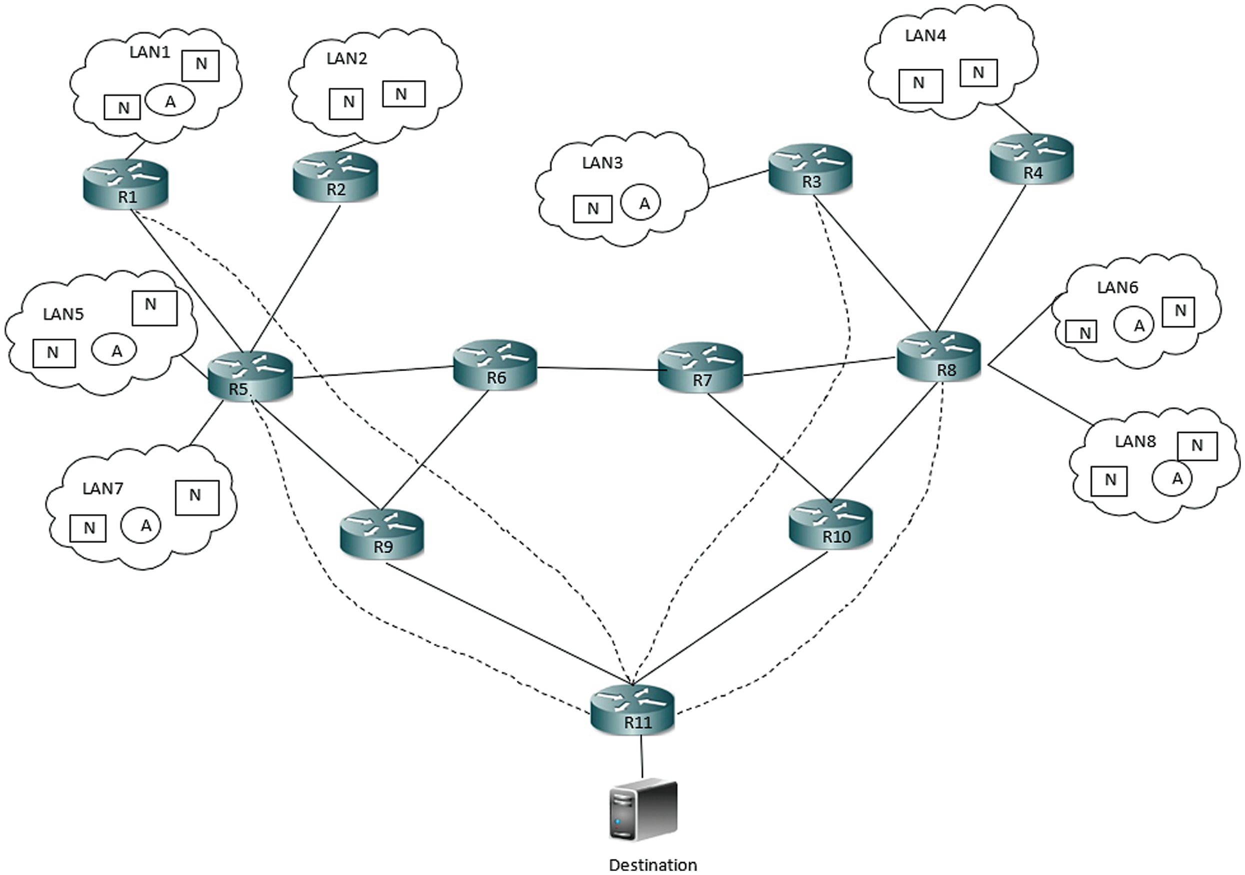


Figure 2: Sample network

This proposed work relies on the following assumption. Each LAN site is connected to an edge router through which all legitimate or attack traffic drives into the network. The attack traffic may arise from the compromised host residing in any of the LAN sites connected to the network. The flooding traffic includes spoofing attacks, HRFA, and LRFA traffic that is capable of bringing down the destination. The attacker may be an authorized or compromised insider or an outsider of a particular LAN site. The HRFA and spoofing attack can be launched by any malicious insider or outsider. The HRFA or LRFA can be launched by compromised bots. The LRFA targets the destination with the help of a botnet and the assumption made for this work is that only one botnet is active at any particular instance of time. The attack traffic generated cannot inundate the ISP network but it is capable of locking down the destination. The necessary cryptographic keys are shared through a secure channel and used by the hash algorithm and pseudo random number generator. The network topology is static, stable and has control over all the edge routers.

Security analysis of the network Model: The network model, Fig. 2, is considered as an IP-based network that is capable of providing security similar to that of a traditional IP network. The attack can arise from any of the LAN sites. It may be a spoofing attack, HRFA, LRFA. Spoofing attack and HRFA may utilize or even it is capable of exhausting the available bandwidth. Overall, it degrades the services provided by the network. LRFA in turn is capable of degrading the service provided by the destination server.

The traffic propelled through HRFA and LRFA converges at the destination side edge router. During this situation, the destination gets flooded and the service provided by the destination gets degraded. It is very important to protect such edge routers to avoid degradation of service. Applying the mitigation only at the destination side edge router will affect the maximum utilization of the network resources. Applying the mitigation mechanism closest to the source helps in proper utilization of the network resources but does not detect the low rate attack. In spite, the mitigation can be done at different levels. Mitigation at the source protects the network from spoofing and high-rate attack. In Fig. 2, the routers R5, R8 are connected to more than one LAN. Applying ingress filtering will protect from spoofing attack from unknown IP address but not from known IP address, for example, LAN 5 can spoof the address from LAN 7. The rest of the distributed attacks are detected at the destination end edge router. This work provides an acceptable and efficient cooperative multilevel defense mechanism to protect the network and destination from spoofing attacks, HRFA, and LRFA.

4 Defense Proposal

The architecture diagram of the proposed cooperative multilevel defense mechanism is shown in Fig. 3. It defends against the spoofing attack, HRFA and LRFA directed towards the network and destination. At the source end, this mechanism incorporates the first level of protection known as Threshold-based Rate limiting and Spoofing Resistant Tag (TSRT). The contemplated TSRT protects the network from spoofing attack and HRFA. At the destination end, this mechanism incorporates a second level of protection known as the Self-Similarity-based Selective Pushback technique (SSP). The contemplated SSP protects the destination from LRFA. The source end protection TSRT and the destination end protection SSP together build the cooperative multilevel defense mechanism that would provide uninterrupted service.

4.1 Level-1 Mitigation: TSRT Protection

The first level of mitigation, TSRT at the source end that is capable of protecting the network from spoofing attacks and HRFA is elaborated in this section. The network edge router, in Fig. 2, may connect more than one LAN site to the Internet, like LAN5 and LAN7 connected to R5 and LAN6 and LAN8 connected to R8. The routers that are deployed at the edge of the network must monitor both incoming and outgoing traffic that is from or to the LAN site. The routers then decide on forwarding or filtering the traffic as per the policies or filtering rules configured on it. The ingress filtering policy configured in the edge router allows the IP traffic only with registered subnet addresses and prevents traffic with un-routable addresses. A compromised host residing within a LAN site may forward a huge volume of attack traffic with its original IP address causing HRFA. Likewise, any LAN sites connected to a particular edge router can forward attack traffic with the IP address of one other causing a spoofing attack.

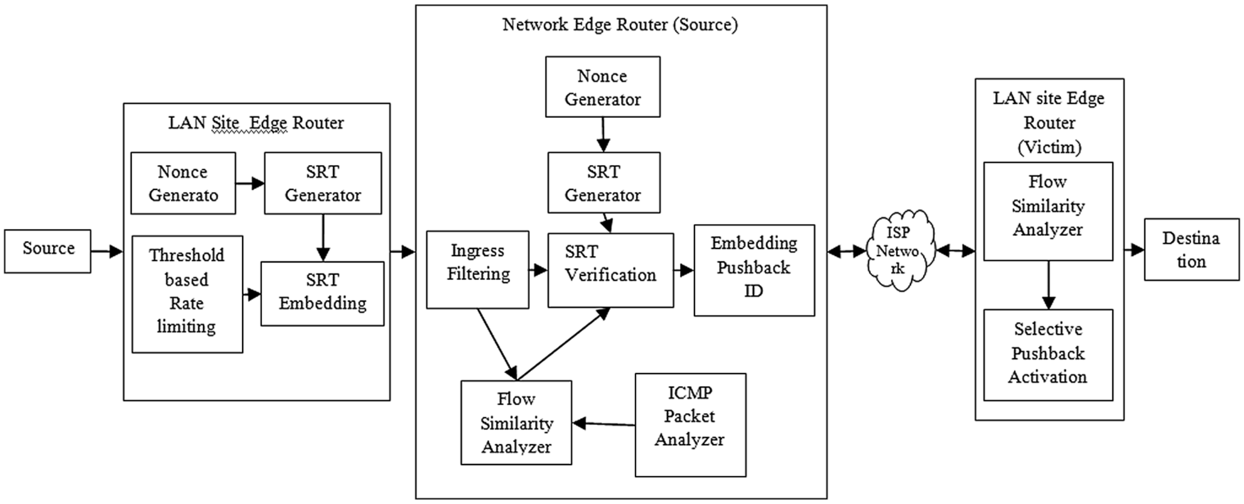
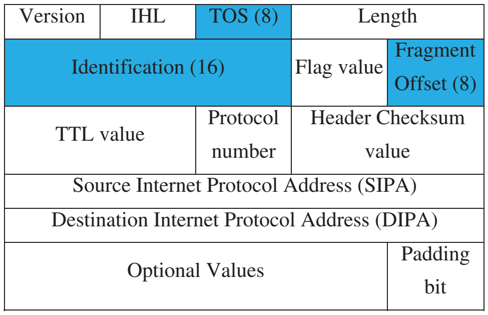


Figure 3: Cooperative multilevel defense mechanism architecture

The router transmits the traffic generated by any host on the LAN sites to the network. The packets entering the network are controlled and secured by the TSRT mechanism deployed in the router. TSRT mechanism incorporates the Threshold (T) based rate limiting and Spoofing Resistant Token (SRT) based filtering. HRFA is controlled by fixing a Threshold (T) for the amount of traffic each host in the LAN can forward for a particular time. The threshold is fixed offline based on the number of packets arising from each host during the normal behavior. The packets that get through the rate-limiting module are directed to the Spoofing Resistant Token (SRT) embedding module.

The SRT protection mechanism incorporates two processes; SRT tagging is done at the egress router of the LAN and SRT verification at the ingress router of the network. The pseudo-random number (PRN) generator with the same seed value runs at both routers at the LAN and network sides. It generates a 64-bit nonce to induce randomness into the SRT. In addition, both routers agree on a Hash algorithm ‘H’ used for generating the SRT. The packet that passes through the threshold limit enters the SRT tagging module. SRT tagging module concatenates the present Time Stamp (TS) with the source IP address (SIPA) and XOR it with the random number (PRN). The value that is generated is then hashed to generate the unique SRT as in Eq. (1). The SRT generated is then divided into 8, 16, and 8 bits and placed in the ToS ID and offset fields in the IP header respectively highlighted in Fig. 4. In real-time fragmentation of packets is very less to influence the packet delivery of the overloaded IP traffic [19].

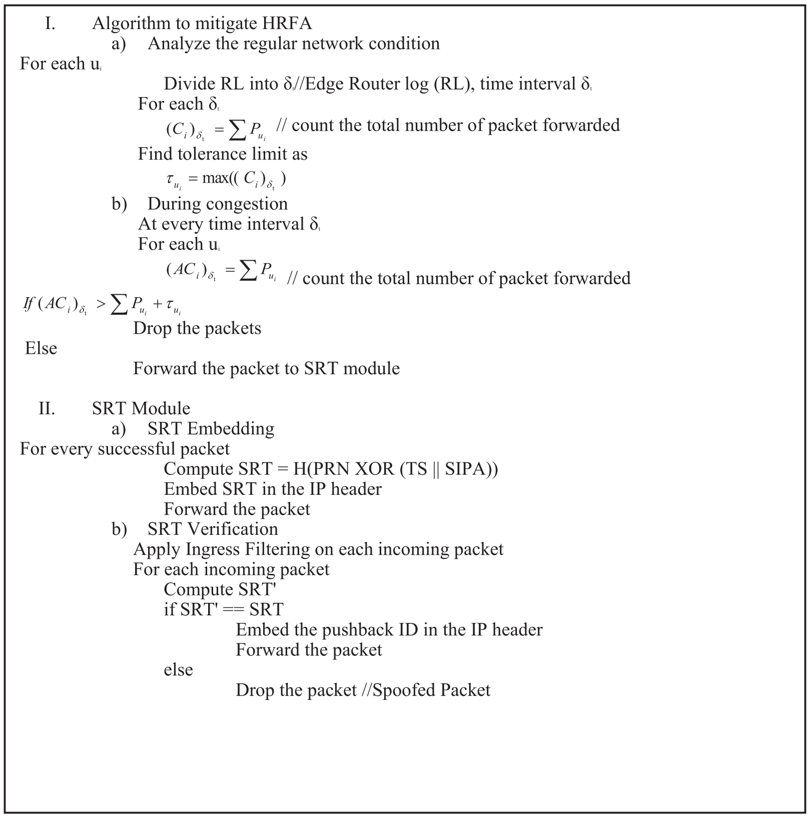
$$SRT = H(PRNXOR(TS||SIPA)) \tag{1}$$



Version	IHL	TOS (8)	Length
Identification (16)		Flag value	Fragment Offset (8)
TTL value		Protocol number	Header Checksum value
Source Internet Protocol Address (SIPA)			
Destination Internet Protocol Address (DIPA)			
Optional Values			Padding bit

Figure 4: Overloaded internet protocol header format

SRT embedded packet is transmitted to the network side router. The router applies the general filtering rules to the incoming traffic and forwards the traffic to the SRT verification module. SRT generator uses the source IP address in the incoming packet to generate the SRT'. Generated SRT' is compared with the received SRT; if they are the same then the packet is forwarded assuming to be a non-attack packet. It is not possible to generate SRT and SRT is completely random which makes it an effective solution to mitigate spoofing attacks. TSRT mechanism is described in Fig. 5. TSRT is effective in providing complete protection to the network. It protects the network from Spoofing and HRFA at the early stage before even the attack traffic enters the network.



```
    I.      Algorithm to mitigate HRFA
                a)   Analyze the regular network condition
For each u_i
                        Divide RL into δ_t//Edge Router log (RL), time interval δ_t
                    For each δ_t
                        $(C_i)_{\delta_t} = \sum P_{u_i}$ // count the total number of packet forwarded
                    Find tolerance limit as
                        $\tau_{u_i} = \max((C_i)_{\delta_t})$
                b)   During congestion
                    At every time interval δ_t
                    For each u_i
                        $(AC_i)_{\delta_t} = \sum P_{u_i}$ // count the total number of packet forwarded
$If\ (AC_i)_{\delta_t} > \sum P_{u_i} + \tau_{u_i}$
                    Drop the packets
Else
                    Forward the packet to SRT module

    II.     SRT Module
                a)   SRT Embedding
For every successful packet
                        Compute SRT = H(PRN XOR (TS || SIPA))
                        Embed SRT in the IP header
                        Forward the packet
                b)   SRT Verification
                    Apply Ingress Filtering on each incoming packet
                    For each incoming packet
                        Compute SRT'
                        if SRT' == SRT
                                Embed the pushback ID in the IP header
                                Forward the packet
                        else
                                Drop the packet //Spoofed Packet
```

Figure 5: TSRT algorithm

Once the verification is successful, the SRT is no more required and the fields occupied by it can be better utilized for push back mechanism to reduce additional overhead. The embedding pushback ID module in the network edge router replaces the SRT with its own IP address for source tracing.

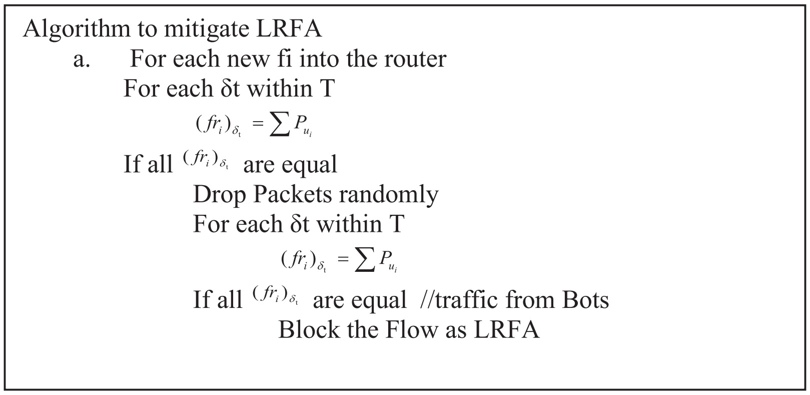
4.2 Level-2 Mitigation: Flow Congruence-Based Selective Pushback (FCSP)

The level-1 mitigation protects against spoofing attacks and HRFA but LRFA boycott the level-1 mitigation-TSRT.

LRFA exhibits the property of genuine traffic more towards the source and reveals its ingenuity towards the destination [20]. The LRFA are more effective in corrupting the benefit accessible to the genuine stream. This nature of the LRFA overlaps the TSRT mechanism and brings forth the needfulness of a distinctive component to moderate LRFA. This subsection describes the second level of mitigation SSP against LRFA.

LRFA advances from a botnet, a prebuilt program installed in many compromised systems that act like a bot. These bots initiate LRFA into the network. The traffic that is induced by diverse bots is more congruent with being evolved from the same program. All bots initiate the session at the same time [21,22] which induces flow congruence in the traffic that arrives at the destination. LRFA reflects the flow congruence in the arrival rate, timestamp, packet arrival interval, packet size, etc. The flow congruence is high in LRFA when compared to genuine flow.

This mitigation deployed at the destination side router monitors the new flow that arrives. The traffic flow rate fr_i is computed for each new flow f_i that enters the router. This is done for each time slot δ_i for some particular time limit T. If the traffic flow rate fr_i is the same for each time slot δ_i then consider dropping a few packets purposefully. This mitigation uses the nature of the TCP protocol, that when the flow f_i does not receive the acknowledgement for the packet it had sent then it has to resend the packet assuming that there is congestion in the network. It then reduces the traffic flow rate fr_i for that particular flow. In contrast, the bots will not reduce their traffic. This facilitates the mitigation by reducing the traffic flow rate fr_i for genuine packets and not for the LRFA. The flow f_i that is identified as LRFA is dropped to protect the destination and enabling uninterrupted service for genuine flow. The algorithm is given in Fig. 6.

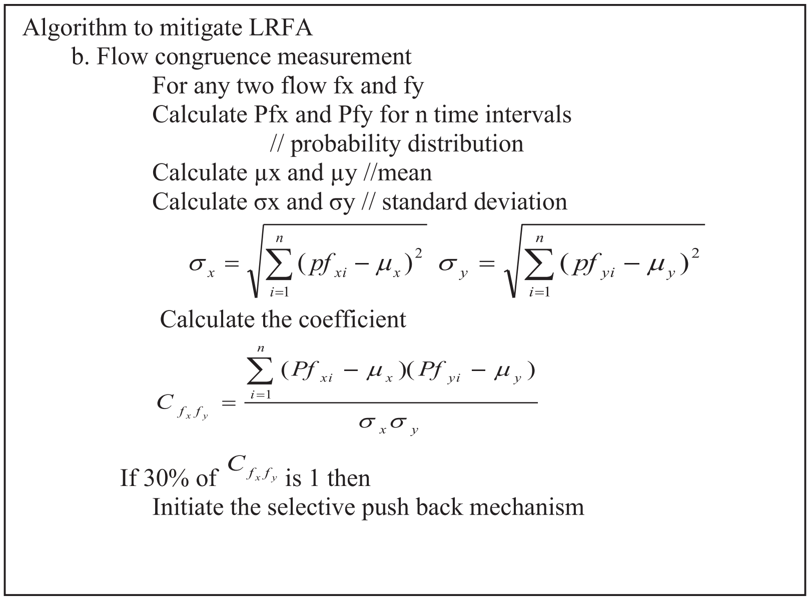


```
Algorithm to mitigate LRFA
    a.   For each new fi into the router
         For each δt within T
                 $(fr_i)_{\delta_i} = \sum P_{u_i}$
         If all $(fr_i)_{\delta_i}$ are equal
                 Drop Packets randomly
                 For each δt within T
                         $(fr_i)_{\delta_i} = \sum P_{u_i}$
                 If all $(fr_i)_{\delta_i}$ are equal  //traffic from Bots
                         Block the Flow as LRFA
```

Figure 6: LRFA identification

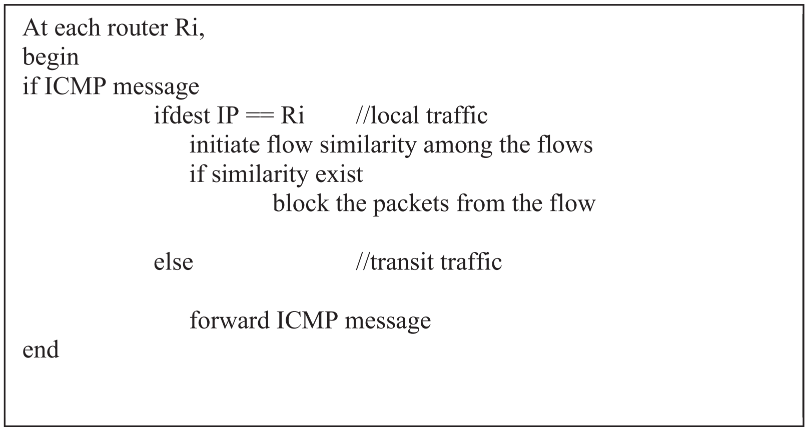
The flow congruence mechanism is incorporated in every network edge router and activated on demand. The flow congruence measurement is based on the standard Pearson Coefficient. It is used to measure the degree of likeness among two flows. If the Pearson coefficient value among the two flows is 1 then the flows are more congruent to each other. The comparison is made among all the flows. From the analysis, the congruence is fixed to 30%. If the congruence is less than 30%, there is a more chance for false positives. On the other hand, if more than 30% is fixed then the attack traffic may pass undetected. From the result of the person coefficient if 30% are correlated then it is confirmed that there is an LRFA. The algorithm is given in Fig. 7.

On suspicion of LRFA, the selective pushback mechanism will be activated by the destination edge router. In-order to activate, the destination edge router uses the overloaded IP header created by the embedding push back module at the source edge router. The overloaded IP header holds the source edge router's IP address. The destination edge router extracts the source edge router's IP address from the overloaded IP header and sends an ICMP message to the extracted IP address. The ICMP message indicates the possibility of LRFA and requests further screening of the outgoing packets by activating the flow congruence mechanism. On receipt of the ICMP message, the source edge router activates the flow congruence mechanism on the local traffic and blocks the IP address having the same distance. This will help in locating the source edge router and blocking the LRFA at the source edge router itself. The pushback algorithm is given in Fig. 8.



```
Algorithm to mitigate LRFA
    b. Flow congruence measurement
            For any two flow fx and fy
            Calculate Pfx and Pfy for n time intervals
                        // probability distribution
            Calculate µx and µy //mean
            Calculate σx and σy // standard deviation
                $\sigma_x = \sqrt{\sum_{i=1}^{n} (pf_{xi} - \mu_x)^2}$   $\sigma_y = \sqrt{\sum_{i=1}^{n} (pf_{yi} - \mu_y)^2}$
            Calculate the coefficient
            $C_{f_x f_y} = \frac{\sum_{i=1}^{n} (Pf_{xi} - \mu_x)(Pf_{yi} - \mu_y)}{\sigma_x \sigma_y}$
        If 30% of $C_{f_x f_y}$ is 1 then
            Initiate the selective push back mechanism
```

Figure 7: Flow congruence mechanism



```
At each router Ri,
begin
if ICMP message
            ifdest IP == Ri        //local traffic
                initiate flow similarity among the flows
                if similarity exist
                        block the packets from the flow

            else                    //transit traffic

                forward ICMP message
end
```

Figure 8: Selective pushback algorithm

5 Performance Analysis

The simulation topology used in this analysis is shown in Fig. 9. The cooperative mitigation mechanism proposed–TSRT and FCSP are incorporated in the edge routers. Each source-side edge router performs a simple threshold-based rate limiting on the incoming packet as a preprocessing step. Incoming packets beyond the threshold are dropped. In addition, each source-side edge router is designed to perform SRT embedding and the network side edge routers perform SRT verification. The destination side end router R11 performs flow congruence analysis on the incoming packets and initiates the pushback mechanism. The malicious packet drops as the effect of the flooding control mechanism, shown in Fig. 9. The router

R5 shows the spoofed packet drop of the first level mechanism-TSRT and R1 shows the packet drop of the second level mitigation-pushback.

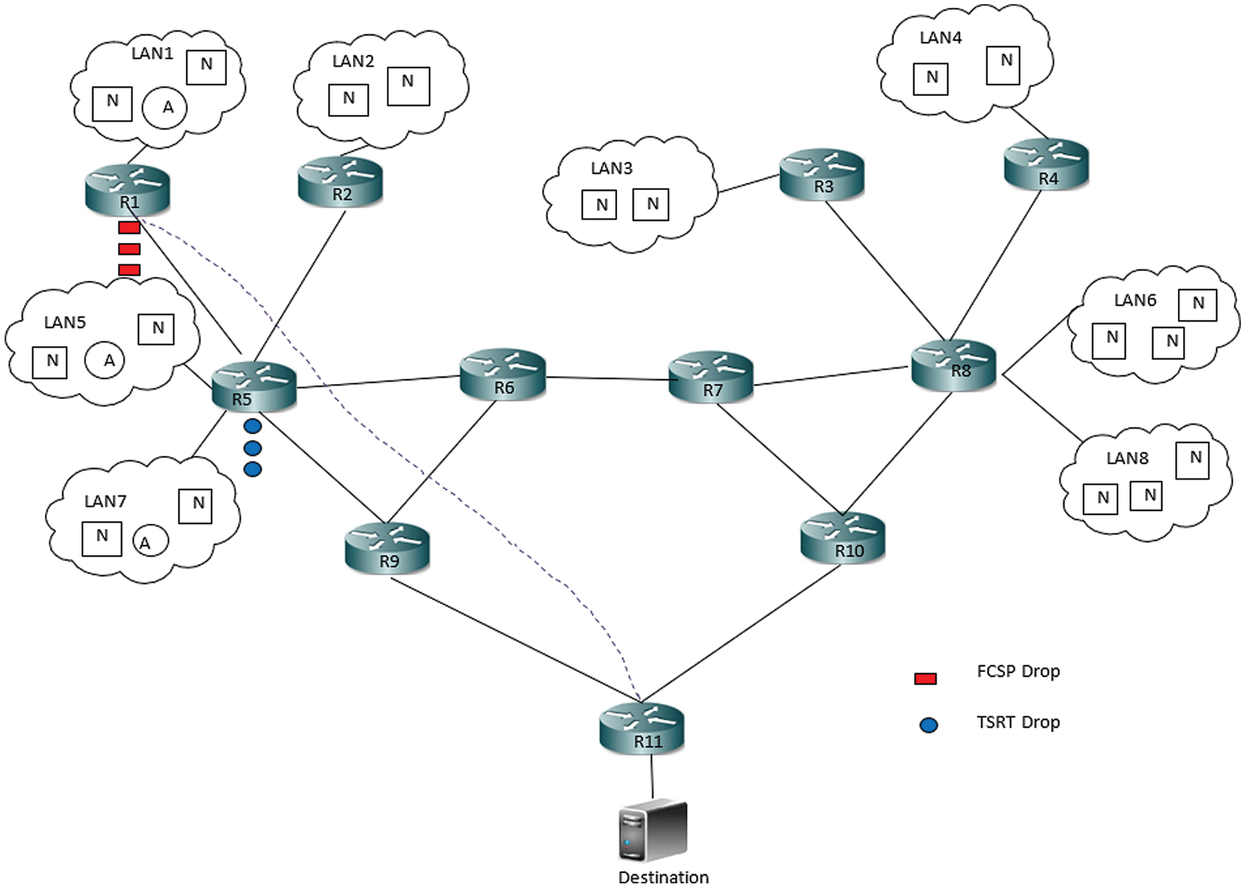
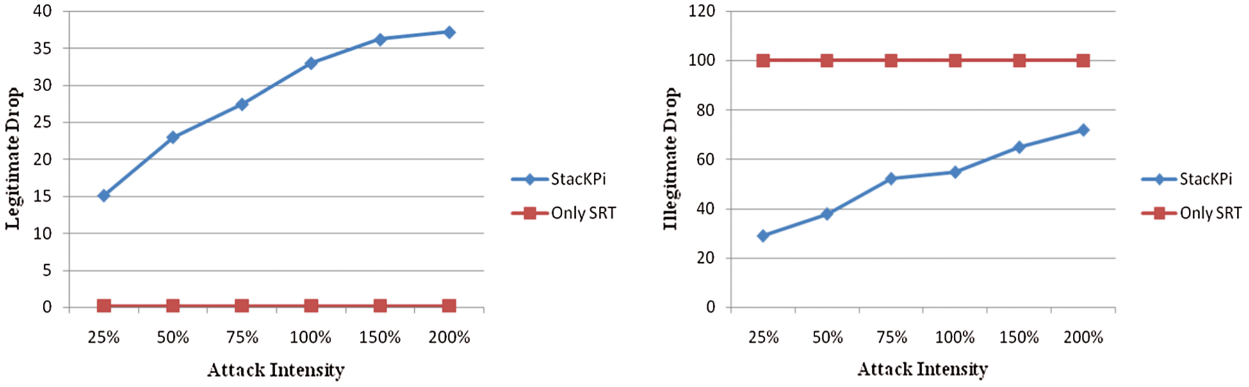


Figure 9: Simulation topology with illegitimate drop

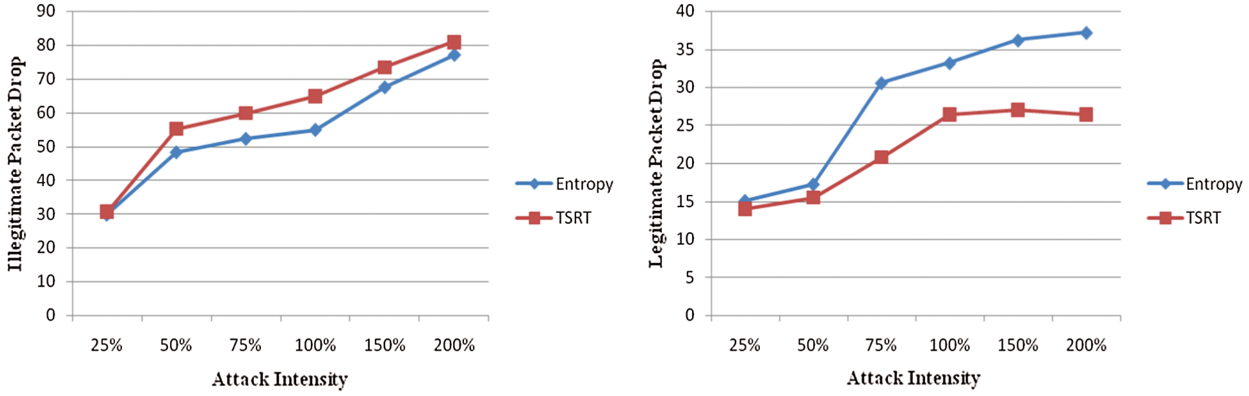
First, the level-1 mitigation mechanism is simulated. The SRT filtering mechanism is accessed against the normal spoofing attack. The comparison is made between the SRT filtering mechanism and the existing spoofing protection mechanism–Stack Pi [5]. The comparative result in Fig. 10 shows that the SRT can achieve complete protection against spoofing attack. Then HRFA is induced along with the spoofing attack and is compared with entropy [8] based filtering. The result shown in Fig. 11 proves that the TSRT performs better in mitigating HRFA and spoofing attack. The entropy-based filtering can only act on the HRFA. Since it cannot identify the spoofed packet, it allows the spoofed packet within the limit to pass through. The TSRT technique drops spoofed packets completely and restricts the high rate packets resulting in considerable improvements in performance over other techniques. TSRT is compared with other mitigations like entropy, Threshold-based rate-limiting, Stack Pi, SRT. In Fig. 12, the graph shows that the TSRT performance is better when compared to other techniques.

Next, the performance of the level-2 mitigation–FCSP is analyzed. The test traffic is induced from the LAN. The test traffic generated from each LAN may be genuine or a combination of genuine and attack traffic as represented in the sample network. The analysis is made by incorporating TSRT, FCSP, and both together forming the cooperative multilevel solution. The result shown in Fig. 13 proves that the cooperative multilevel mechanism outperforms single-level mitigation.



(a) (b)

Figure 10: Spoofing (a) illegitimate drop (b) legitimate drop



(a) (b)

Figure 11: Flooding and spoofing (a) illegitimate drop (b) legitimate drop

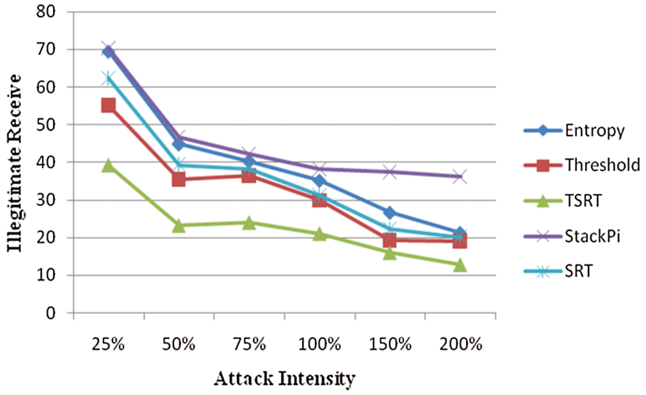


Figure 12: Comparison with other techniques

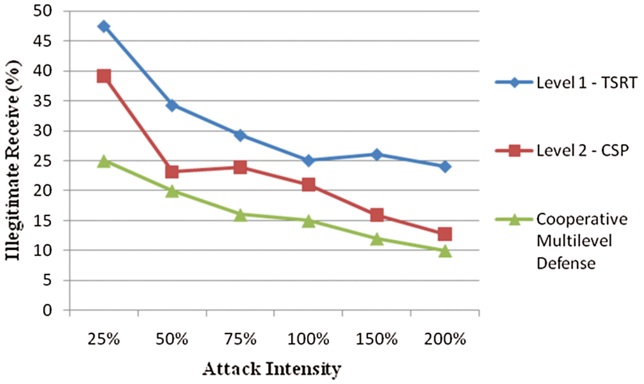


Figure 13: Comparison of cooperative multilevel mechanism with TSRT and FCSP

6 Conclusion

Extensive research has been carried out to alleviate flooding attacks. They are an effective relieving solution for either HRFA or Spoofing attack or LRFA but not for all. The solution that best suits one type of attack remains void for the other type. Adding to it, providing protection at the source or destination will not be a complete solution to protect the network from all types of attacks. A Cooperative multilevel defense mechanism is proposed to fill the inadequacies. The first contribution towards the cooperative multilevel defense mechanism is a Threshold-based Spoofing Resistance Tag (TSRT) mechanism to identify and react against spoofing attack and HRFA. As the second level of mitigation, a Flow Congruence-based Selective Pushback (FCSP) mechanism is implemented. The effectiveness of the proposed cooperative multilevel scheme against a well-distributed denial of service attack has been demonstrated. Simulation result shows that the proposed scheme detects and reacts effectively towards the flooding attack at the earliest point closer to the source of the attack. The work can be extended to a multilayer multilevel mechanism. The mitigation mechanism can be even implemented using Machine Learning Algorithms.

Acknowledgement: I show my gratitude to anonymous referees for their useful ideas.

Funding Statement: The author received no specific funding for this study.

Conflicts of Interest: The author declares that they have no conflicts of interest to report regarding the present study.

References

[1] X. M. Liu, G. Cheng, L. I. Qi and M. Zhang, “A comparative study on flood DoS and low-rate DoS attacks,” *The Journal of China Universities of Posts and Telecommunications*, vol. 19, no. 5, pp. 116–121, 2012.

[2] R. Xie, M. Xu, J. Cao and Q. Li, “SoftGuard: Defend against the low-rate TCP attack in SDN,” in *ICC 2019-IEEE Int. Conf. on Communications (ICC)*, Shanghai, China, pp. 1–6, 2019.

[3] T. Peng, C. Leckie and K. Ramamohanarao, “Survey of network-based defense mechanisms countering the DoS and DDoS problems,” *ACM Computing Surveys (CSUR)*, vol. 39, no. 51, pp. 1–42, 2007.

[4] G. T. Nguyen, V. Q. Nguyen, S. N. Nguyen and K. Kim, “Traffic seasonality aware threshold adjustment for effective source-side DOS attack detection,” *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 13, no. 5, pp. 2651–2673, 2019.

[5] A. Yaar, A. Perrig and D. Song, “StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense,” *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 10, pp. 1853–1863, 2006.

[6] S. H. Peng, K. D. Chang, J. L. Chen, I. L. Lin and H. C. Chao, “A probabilistic packet marking scheme with LT code for IP traceback,” *International Journal of Future Computer and Communication*, vol. 1, no. 1, pp. 51–56, 2012.

[7] S. Yu, W. Zhou, R. Doss and W. Jia, “Traceback of DDoS attacks using entropy variations,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 3, pp. 412–425, 2010.

[8] S. Zhang and P. Dasgupta, “Denying denial-of-service attacks: A router based solution,” in *Int. Conf. on Internet Computing*, Las Vegas, NV, United States, pp. 301–307, 2003.

[9] H. Wang, A. Bose, M. El-Gendy and K. G. Shin, “IP easy-pass: A light-weight network-edge resource access control,” *IEEE/ACM Transactions on Networking (TON)*, vol. 13, no. 6, pp. 1247–1260, 2005.

[10] A. D. Keromytis, V. Misra and D. Rubenstein, “SOS: An architecture for mitigating DDoS attacks,” *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 1, pp. 176–188, 2004.

[11] W. Zhijun, L. Wenjing, L. Liang and Y. Meng, “Low-rate DoS attacks, detection, defense, and challenges: A survey,” *IEEE Access*, vol. 8, no. 2, pp. 43920–43943, 2020.

[12] R. Xie, M. Xu, J. Cao and Q. Li, “SoftGuard: Defend against the low-rate TCP attack in SDN,” in *ICC 2019-2019 IEEE Int. Conf. on Communications (ICC)*, Shanghai, China, pp. 1–6, 2019.

[13] L. Liu, H. Wang, Z. Wu and M. Yue, “The detection method of low-rate DoS attack based on multi-feature fusion,” *Digital Communications and Networks*, vol. 6, no. 4, pp. 504–513, 2020.

[14] H. Wang, C. Jin and K. G. Shin, “Defense against spoofed IP traffic using hop-count filtering,” *IEEE/ACM Transactions on Networking*, vol. 15, no. 1, pp. 40–53, 2007.

[15] S. Yu, W. Zhou and R. Doss, “Information theory based detection against network behavior mimicking DDoS attacks,” *IEEE Communications Letters*, vol. 12, no. 4, pp. 318–321, 2008.

[16] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang *et al.,* “Discriminating DDoS attacks from flash crowds using flow correlation coefficient,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1073–1080, 2011.

[17] J. Zhang, Z. Qin, L. Ou, P. Jiang, J. Liu *et al.,* “An advanced entropy-based DDOS detection scheme,” in *Int. Conf. on Information, Networking and Automation (ICINA)*, Kunming, China, pp. 67–71, 2010.

[18] R. K. Deka, D. K. Bhattacharyya and J. K. Kalita, “Granger causality in TCP flooding attack,” *International Journal of Network Security*, vol. 21, no. 1, pp. 30–39, 2019.

[19] S. Savage, D. Wetherall, A. Karlin and T. Anderson, “Network support for IP traceback,” *IEEE/ACM Transactions on Networking*, vol. 9, no. 3, pp. 226–237, 2001.

[20] Y. Li, Q. Wang, F. Yang and S. Su, “TracebackDRDoS attacks,” *Journal of Information & Computational Science*, vol. 8, no. 1, pp. 94–111, 2011.

[21] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski *et al.,* “Your botnet is my botnet: Analysis of a botnet takeover,” in *Proc. of the 16th ACM Conf. on Computer and Communications Security*, Chicago, Illinois, USA, pp. 635–647, 2009.

[22] V. L. Thing, M. Sloman and N. Dulay, “A survey of bots used for distributed denial of service attacks,” in *IFIP Int. Information Security Conf.*, Boston, MA, pp. 229–240, 2007.