Simulation Modelling Practice and Theory 98 (2020) 101984

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat

Facing DDoS bandwidth flooding attacks☆

Angelo Furfaro*,[a], Pasquale Pace[a], Andrea Parise[a]

Dipartimento di Ingegneria Informatica, Modellistica, Elettronica e Sistemistica Università della Calabria, P. Bucci 41C – 87036 Rende (CS) Italy

ARTICLE INFO

Keywords:
Denial-of-service attacks
DDoS mitigation
Network security
Quality of Service
Network simulation

ABSTRACT

Distributed Denial of Service (DDoS) attacks are among the most effective cybersecurity threats. In the last few years their diffusion, dimension and complexity have increased to reach critical levels. The devising of robust and scalable defense mechanisms to counteract such attacks is an urgent demand from the cyberspace to ensure its secure operation. This paper proposes a filter-based defense mechanism, derived as an extension of the *StopIt* technique, which (*i*) is able to face bandwidth flooding attacks and (*ii*) works on more realistic scenarios. The effectiveness of the technique, in the context of networking architectures providing Quality of Service (QoS) enforcing policies (e.g. DiffServ), has been evaluated by means of a modular model implemented into the ns-3 simulator. In particular, the performance of the technique, in the context of a video streaming scenario, having high bandwidth demand and stringent QoS constraints, has been assessed.

1. Introduction

The ever growing diffusion of systems connected to the Internet and, in particular, of those embedded into small devices, which gave birth to the so called Internet of Things, makes the privacy, the security and the availability of the information and of the services, which they store/offer, very critical issues that must be adequately addressed [2–4]. Cybersecurity is an active and prominent research field that focuses on devising solutions and defense mechanisms against the various threats affecting IT systems (either connected or not).

In this context, Distributed Denial of Service (DDoS) is one of the common and effective cyber attack. It is the preferred attack by activists, through which they are capable of causing large-scale damage and acquiring media visibility simply.

Verisign observed, in its 2018 “DDoS Trends Report” [5], that 52% of DDoS attacks that were mitigated in Q2 2018 employed multiple attack types. There was a 35% increase in the number of attacks, with a 49% decrease in the average of attack peak sizes, when compared to Q1 2018; however, the average of attack peak sizes has increased by 111%, year over year.

Among the areas most affected by this kind of cyber attack we find IT services, cloud services, public/financial services and media/entertainment content. The most common DDoS attacks performs over UDP protocol exploiting vulnerabilities of the Domain Name System (DNS), Lightweight Directory Access Protocol (LDAP), Network Time Protocol (NTP) and Simple Network Management Protocol (SNMP) in order to achieve amplification attacks.

According to the Kaspersky Labs [6] the last quarter of 2018 witnessed the longest attack seen in recent years, lasting almost 14 days (329 hours).

☆ Preliminary results about the technique proposed in this paper were reported in the proceedings of the 7th International Conference on Internet and Distributed Computing Systems – IDCS 2014 [1]

* Corresponding author.
E-mail addresses: a.furfaro@dimes.unical.it (A. Furfaro), ppace@dimes.unical.it (P. Pace), andrea.parise92@gmail.com (A. Parise).

https://doi.org/10.1016/j.simpat.2019.101984
Received 24 June 2019; Received in revised form 4 September 2019; Accepted 5 September 2019
Available online 06 September 2019
1569-190X/

DDoS attacks often aim seek to cause extensive economic damage to the victims by denying their service. Economic damages can persist even after the attack is ended as a result of image damage, the service is actually seen by the customer as unreliable.

For this reason, a defense strategy to a DDoS attack not only should keep the services attainable but also try to offer an appropriate quality of service.

In this paper we evaluate the effectiveness of the *StopIt* [7] based mechanisms presented in [1] weakening some assumptions made in the previous work. In particular the original *StopIt* mechanism has been modified to achieve a more reasonable solution in which the malicious traffic detection is moved from the victim server to the access router, so that both direct and indirect attacks are treated in the same way. Moreover, we integrated the support to the DiffServ [8] policy within the StopIt-enabled routers to reduce the effect of DDoS bandwidth attack, because the traffic classes outside the queue affected by DoS have a minimum guaranteed bandwidth.

The goodness of the proposal has been tested through a simulation based approach, which is consolidated practice even in other research domains [4,9], by implementing different communication scenarios in which a distributed denial of service targeted a media service provider; in such case, the QoS perceived by the consumer is essential to avoid reputation damages of the company.

The conducted simulations studies and the obtained results, with different communication topologies and traffic sources (*i.e.,* HTTP, VoIp, Video), demonstrated how the high scalability of the improved *StopIt* mechanism can be a valid solution to face distributed DDoS attacks by reacting in a fast way and by guaranteeing a fair quality of service to traffic source with different and specific characteristics.

The remainder of the paper is organized as follows. We review the main related works in Section 2. The standard *StopIt* mechanism, the generic security aspects, the limitations and the ways to handle the indirect flooding according to previous conducted works, are presented in Sections 3 and 4. The novel scalable and effective solution to further mitigate the DDoS attacks is described in Section 5 while all the aspects on the implemented simulation model are presented in Section 6. Finally, we provided detailed simulation results investigating several communication scenarios with different traffic sources in Section 7 and meaningful conclusions and research directions in Section 8.

2. Related work

The wide analysis of different DDoS attacks have been the main focus of various surveys published in the last years [10–16].

A discussion on the potential weaknesses of existing defense mechanisms has been started since the works published in [10] and in [11] which highlighted the need for an integrated solution able to handle the various flavors of DDoS attacks. The work published in [15] reports a systematic analysis of this type of attacks including motivations and evolution, protection and mitigation techniques.

In [13], the coordinated nature of DDoS attacks is explained by recalling that an effective defense strategy should also be designed in a collaborative fashion, i.e. the involved routers have to work collaboratively by exchanging caveat messages with their neighbors. For this reason, hybrid defense mechanisms are more effective than centralized ones because their components are distributed over multiple locations such as source, destination or intermediate networks by implementing cooperative behaviors among the deployment points.

In later years, the authors of Zargar et al. [12] discussed about the growing need of comprehensive, collaborative and distributed defense approaches after they categorized the different forms of DDoS flooding attacks and classified existing countermeasures according to their ability to prevent, detect, and respond to such attacks.

Finally, Hoque et al. [14] presented a complete overview on different tools, taxonomies and systems for network attacks by highlighting how, among the other attacks, the DDoS one is very catastrophic to any information system since it uses a large number of compromised hosts and it is very difficult to detect the original source of such an attack. Moreover, they argued that a great number of very powerful attack tools are available on the Internet although they can be easily used to crash networks and Websites even if their use to launch an attack in a public network is a real crime.

Few famous hybrid DDoS defense strategies are based on the following mechanisms:

- *Throttling / filtering* and *Hybrid packet marking* [17,18] consisting into the installation, by the victims side, of a router throttle at upstream routers several hops away with the aim of limiting the forwarding packets data rate. Unfortunately, these defense strategies only limit the rate of malicious packets. A comprehensive survey on filtering-based defense mechanisms has been published in [16].
- *Capability-based* [19,20] consisting into a short-term authorization from the receivers by adding specific stamps on their packets. In this way, the recipients explicitly authorize the traffic it would like to receive. In this context, the recent work in [21] proposes the first DDoS mitigation system that offers readily deployable and proactive DDoS prevention requiring only limited deployment from the cloud, rather than widespread.
- *Active Internet Traffic Filtering (AITF)* [22] consisting into the default acceptance of all the traffic and the explicit refusal of that traffic identified as undesirable. According to this filtering scheme, the main limitation is the need of a bounded amount of filtering resources from participating ISPs.

Recently, DDoS attacks have targeted specific categories of devices/applications and consequently suitable defense schemes have been developed. The current landscape in the IoT field is surveyed in work published in [23], while those of cloud computing and Software Defined Networking are discussed in [24] and [25].

Although in the last years other network-based mechanism have been proposed with the aim of facing DDoS, we argue that our

proposal, which extends the capabilities of the *StopIt* [7] filtering strategy by exploiting the cooperation with capability based techniques, is more effective in handling *indirect* DDoS attacks thanks to the presence of different *StopIt* enabled routers located in the victims nearness on which, after the detection phase, specific filters can be installed to enlarge the restricted and protected area around the victim with the aim of providing a more scalable and effective defense mechanism.

3. The StopIt mechanism

The defense techniques proposed in this work is based on a hybrid filter mechanism called *StopIt* [7]. The advantages and the limitations of such reference technique are investigated in this section also pointing out the main operation. In particular, this technique implements an effective, quick and automatic strategy to face DDoS attacks, once they are detected, by exploiting specific network filters installed on the access router of the Autonomous Systems (AS) that has to be protected. Moreover, the use of the *StopIt* mechanism is very effective in those environments where suitable provision against IP address spoofing are already implemented, *e.g.* Passport [26].

Considering the Fig. 1 in which a typical network topology is depicted, the standard operation of *StopIt* can be summarized as follows. The reference communication scenario consists of two ASs connected through the Internet. A *StopIt* server is implemented in each AS and all the *StopIt* servers use BGP [27] to make aware of the presence of other *StopIt* servers in the neighborhood and IGP [28] to exchange data with their ASs. Moreover, a suitable DoS detection system [29,30] is also available within the AS under protection.

The following steps represent the *StopIt* operation:

1. The victim host H_d, either directly or indirectly, detects the DoS attack and sends a specific source blocking request back towards the access router R_d;
2. The access router R_d, to avoid the case in which an attacked server uses the *StopIt* mechanism to block legal users, has to verify that the source H_s is really sending data to the server before to install a local filter; then it can send a specific flow blocking request $< source - server >$ to the *StopIt* server SS_d within its own AS;
3. The received request needs to be authenticated by the *StopIt* server SS_d before to be forwarded toward the *StopIt* server belonging to the sourcing AS. This last forwarding procedure is supported by the BGP protocol;
4. The *StopIt* server SS_s within the sourcing AS, once received the request, notifies the blocking request to its access router R_s;
5. Finally, the access router within the sourcing AS can install the filter to block the anomalous flow $< source - server >$ for a certain period also sending a request to the attacking source. After receiving this request, a compliant host H_s installs a local filter to stop sending to H_d. If H_s does not stop the transmission, it will be punished by its own access router R_s.

A more detailed description of the *StopIt* mechanism operation can be found in [7].

3.1. Security aspects

Several security features are supported by the previously described *StopIt* mechanism that make it able to easy address the following security issues:

- *Spoofing* - Since the *StopIt* architecture is coupled with the Passport [26] system, it does not allow to use spoofed addresses also guaranteeing a robust inter and intra domain security support.
- *Filter exhaustion* - A way to bypass the defense mechanism should be the saturation of the available filters on a router; thus, this strategic attack can be limited implementing wiser filter installation strategies such as *Random Filter Replacement* and *Filter Aggregation*.
- *Compromised Server* - The access router within the victim's AS needs to verify that the source to be blocked is really active in sending data traffic in order to avoid the activation of the *StopIt* mechanism by a compromised server. To support this feature, the access router first checks the actual data sending toward the server in a recent time interval; then, it sends a traffic interruption request to the server by using a specific request message named *End-To-End StopIt* request.

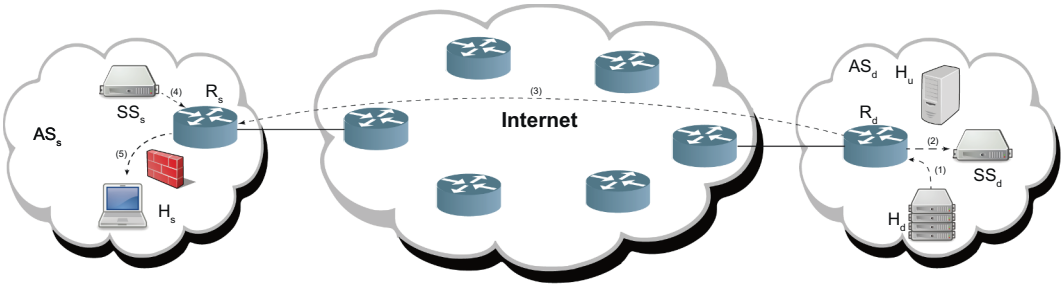


Fig. 1. StopIt operation.

3.2. Limitations

Although, the *StopIt* mechanism has been widely tested in several communication scenarios showing its effectiveness respect to different types of massive DDoS flooding attacks, it fails when the DDoS attack is performed in an indirect way by congesting a link shared with the victim. Fig. 1 shows a typical example in which, if the DDoS attack is launched against a host H_u belonging to AS_d, the server H_d within the same AS, experiences a high performance decrease because it shares the same link with the victim.

4. Handling indirect flooding

StopIt is able to achieve better performances with respect to filter-based mechanisms like AITF, as discussed in the study reported in [7], by ensuring resilience to a wide range of DDoS attacks. However, the main weakness of *StopIt* is that it fails to handle indirect DDoS attacks, i.e. those scenarios where the attack is directed to exhaust the bandwidth available to the victim by flooding other hosts reachable by a common link.

Standard capability-based mechanisms (*e.g. TVA* [31], *TVA+* [7]) are more effective in these cases, however they have some drawbacks mainly due to *(i)* the dependency on the accuracy and reliability of the attack detection strategy implemented by the receiver, *(ii)* the high processing and memory costs due to the notable amount of per flow state information to be maintained at each router.

During an indirect attack *TVA+* and *StopIt* reacts differently: as the data traffic increases *StopIt* experiences a growth of the data transfer time while *TVA+* is not able to complete the data transfer if the bandwidth is not big enough.

A good solution would consist in a strategy able to get the advantages of both these defense mechanisms by merging together the two techniques. However, the creation of such a new hybrid mechanism from scratch is not trivial and thus we devised to make the *StopIt* system able to exploit priority-based strategies, already available within the AS routers, with the aim of offering privileges to traffic having as destination the server that is experiencing a degradation of its performance.

Starting from this idea, our approach consists in an *uncommon* usage of the *DiffServ* [8] model for IP traffic differentiation as a simple, but effective, technique to make the *StopIt* more robust against the indirect flooding attacks [1]. In this way, the *StopIt* mechanism will face an indirect DDoS attack by using a technology already supported by the access routes and designed to provide a specific QoS level within the network.

In case of an indirect DDoS attack where the flooding traffic is sent to a normal host H_u sharing a link with a DNS Server H_d, the dynamic activation of the *DiffServ* support by the server H_d, experiencing a performance degradation, is implemented according to the following assumptions within the communication network:

- each AS is served by at least one *StopIt* server running inside its boundaries;
- each AS ia associated to a given *DiffServ* domain;
- in each *DiffServ* domain, the packets coming from a *StopIt* server are handled throughout the highest priority Assured Forwarding (AF) queue;
- the *DiffServ* system is able to install new Service Level Agreements (SLAs) at run time;
- the server H_d, experiencing a performance degradation, is able to detect anomalous traffic conditions by using a suitable detection algorithm.

Specific fields, i.e. the Hop counter, the SLA identifier, the Rspec and Tspec representing traffic and request specifications respectively, have been added to the standard packet format exchanged among the involved network entities in order to achieve the integration between *StopIt* and *DiffServ*.

In order to activate the jointly operation of *StopIt-DiffServ* defense mechanism, a node H_d detecting a decrease in its performance, executes the following steps:

1. H_d sends a temporary *DiffServ* activation request to the access router R_d within its AS;
2. R_d forwards the request to the *StopIt* server after filling the packet with the information about all the interfaces connected to the AS;
3. the *StopIt* server installs the specific SLA for a certain time T_b, then it decreases by one the hop limit field and forwards the request to all the neighbour ASs
4. the other *StopIt* servers, once received the request packet, repeat the actions from point 2 until the hop limit field reaches zero.

After this procedure is completed, the ASs in which the SLA has been installed, will give priority to the traffic directed to H_d making it immune to the DDoS attack.

It is worth to note that, the proposed technique for packet diffusion is similar to the selective flooding strategy used by the OSPF [32] routing protocol and can be implemented in a similar way.

5. A more scalable technique

The mechanism extension, shown in the previous section, is able to handle indirect attacks partly. It is effective only to protect those servers that are able to activate the *StopIt* defense strategy. Anyhow, this approach can only mitigate the effects of an indirect

attack without actually stopping it, because zombies do not get identified and hence their traffic cannot be blocked.

Another limitation of *StopIt* is due to the too strong assumption that there is a *StopIt* server in each AS. By relaxing this constraint, when some zombies are located in ASs that do not have a *StopIt*-enabled access router,the technique becomes ineffective because filters get installed only on the victim access router.

Here, we propose a different *StopIt* approach which overcomes the above issues and it is able to operate under more realistic assumptions. In particular, it requires a *StopIt* server in the victim's AS and a set of *StopIt*-enabled routers located in the nearness of this AS. This is a more reasonable assumption since in a real scenario only services providers will be interested to install a defense mechanism. Each *StopIt* enalbed-router requires a system able to handle traffic policies such as DiffServ.

Unlike the basic approach, the malicious traffic detection is moved from the victim server to the access router, so that both direct and indirect attacks are treated in the same way. The router alerts the *StopIt* server when a traffic flow exceeds the bandwidth limit assigned to its *DiffServ* queue. Then a detection algorithm analyses and starts monitoring tail log's looking for malicious sources. As in the previous mechanism, for each identified bot, a block request is sent to the sources' ASs in order to stop malicious traffic as close as possible. In addition, at the same time, filters are installed in the *StopIt* enabled routers located in the victim nearness to cope with the situations where zombies' ASs are not equipped with *StopIt* server and hence cannot fulfill blocking requests.

DiffServ policy reduces the effect of DDoS bandwidth attack, because the classes outside the queue affected by DoS have a minimum guaranteed bandwidth. Nevertheless a huge amount of bandwidth is unavailable so only DiffServ cannot be a valid solution to DoS.

The proposed solution is resumed in the following steps:

1. The access router R_d detects an anomaly inside a diffserv queue q_i and sends an alert to the *StoptIt* server S_d;
2. S_d asks R_d for the ith queue's logs;
3. R_d transfers the logs to S_d;
4. S_d detects the malicious addresses through a suitable detection algorithm [29,30];
5. S_d installs the proper filters on R_d;
6. S_d requests filter installation on malicious Access Router R_s, which can exist or not;
7. R_d propagates the installation of filters to all the reachable *StopIt*-enabled routers in the nearness;

In the experimental result described in next session we have evaluated the effectiveness of the proposed defense mechanism, taking into account the quality of the service, varying the range dimension around the victim.

6. Simulation model

6.1. Simulation configuration and topologies

In order to validate the proposed technique we developed a new model through the well known ns-3 discrete-event network simulator [33]. In particular, we decided to use ns-3 because this simulation environment allows to build a solid simulation core that is well documented, easy to use and debug, and that caters to the needs of the entire simulation workflow, from configuration to trace collection and analysis. Moreover, ns-3 supports the development of models for both IP and non-IP based networks and thus it enables a large number of popular research analyzes including TCP and mobile ad hoc routing protocol performance evaluation. Finally, it implements a real-time scheduler that facilitates a number of *simulation-in-the-loop* use cases for interacting with real systems.

To implement the behavior of the *StopIt* mechanism, two specific components have been developed (Fig. 2): the *StopItServer* and the *StopItRouter*. Both componentes are developed as ns-3 applications and rely to some components to the lowest level such as DiffServ queue and routing module. In particular the *StopItRouter* enabled class requires to be installed on a DiffServ enabled router and it monitors the current queue size of each service class. Standard DiffServ model [34] has been modified to make it able to trigs an alert if some queue size overcomes a fixed threshold for a defined time interval. This alert is achieved by the *StopItRouter* enabled class that notifies the alert to the *StopItServer* and waits for the permission to transfers queue logs. Detection phase is out of the scope of this paper so it is simply simulated through a waiting phase and it is able to detect all malicious sources. Traffic source introduced in the model are HTTP [35],VoIp [36] and VIDEO [37]. Such applications clients are modified in order to switch between two states, Sleep and Run, to simulate a more realistic traffic source.

The network topology which has been considered is depicted in Fig. 3a while the used simulation parameters are shown in Fig. 3b. There are eight ASs connected together by a backbone (representing Internet) where packets are routed according to OSPF strategy [32] and equal cost paths are randomly selected. Each AS hosts three types of traffic sources, i.e. HTTP, VoIP and video, whose characteristics are summarized in Table 1 and described in next sub-section. Each source node, except those in AS_{src}, directs its traffic to another host randomly chosen outside its AS. Traffic sources located in AS_{src} communicate only with hosts of AS_{dst}.

ASs other than AS_{src} and AS_{dst} are infected and belong to the botnet. Each of them contains 10 zombie that start performing a bandwidth flooding DDoS at time 9s over VoIp service.

The network topologies chosen for the simulation allow to evaluate the proposed defense mechanism because, as in a real environment, it is possible for the traffic to reach the destination through different paths. In this way, it is possible to clearly evaluate the reduction of the DDoS attack effectiveness once the defense mechanism is able to get close to the source.

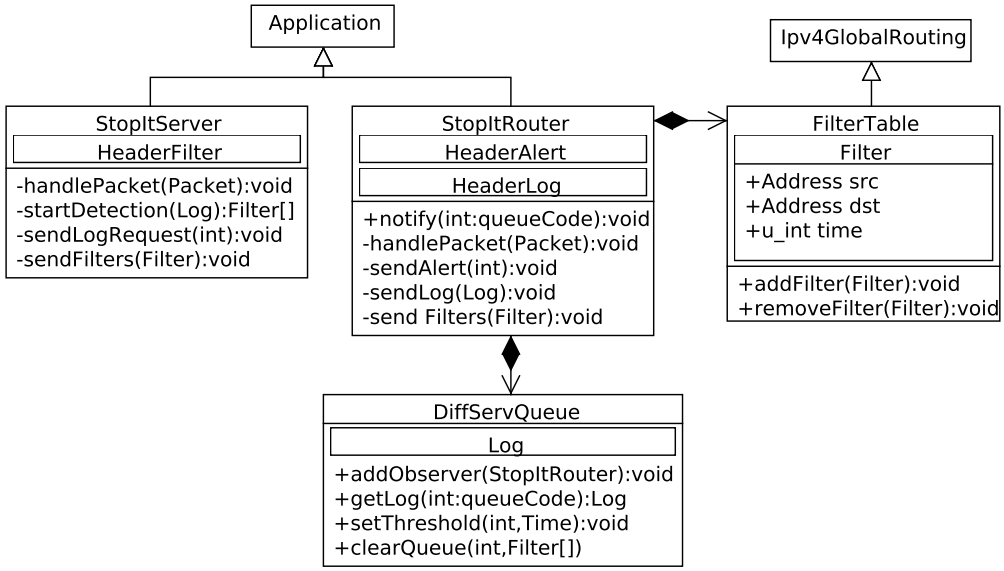
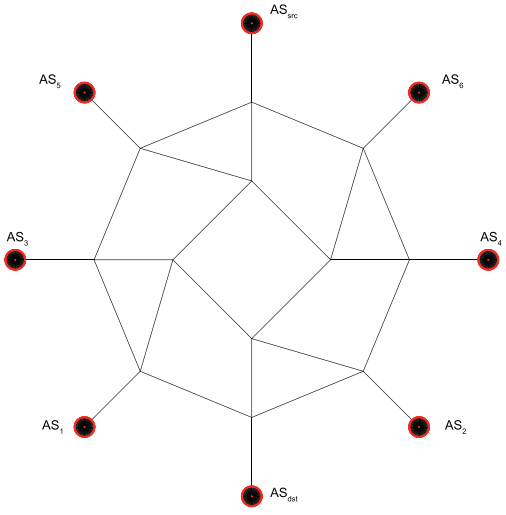


Fig. 2. Simulation model class diagram.



(a)

Parameter	Value
Intra-AS link	5 Mbps
Inter-AS link	20 Mbps
Flooded link	5 Mbps
Simulation time	70s
Traffic Sources start time	2s
DDOS attack start time	9s

(b)

Fig. 3. (a) Network topology - (b) Simulation parameters.

Table 1
Traffic sources characteristics.

Type	Codec or Model	Sources per AS
HTTP	HTTP/1.0	40 Client and 20 Server
VoIp	ilbc_mode_30 @ 13.33kbps	12 Client and 12 Server
	G726 @ 16kbps	12 Client and 12 Server
Video	MPEG4 - CIF resolution	1 Client and 1 Server
DDOS	packet size = 1400 byte packet rate = 100 packet/s	10 bot except for src and dst

6.2. Traffic sources characterization

Concerning the multimedia traffic, we chose to use four different video sequences of commonly used video test contents in the 4:2:0 YUV format freely downloadable at [38]. These video sequences have the same CIF resolution (352*288) and different

Fig. 4. Multimedia video contents and average data rates.

properties in terms of data rate and change of scene. In particular, we coded the uncompressed YUV files using an MPEG-4 codec in order to create compressed raw videos with different data rate as shown in Fig. 4.

6.3. Video quality assessment

Over the last years, emphasis has been put on developing methods and techniques for evaluating the perceived quality of digital video content. These methods are mainly categorized into two classes: *subjective* and *objective*. The subjective test methods involve an audience of people, who watch a video sequence and score its quality as perceived by them, under specific and controlled watching conditions and the arithmetic mean of all the collected opinion scores represents the MOS (Mean Opinion Score) index that has been standardized by ITU-T [39].

Since the preparation and execution of subjective methods is costly and time consuming, researchers have turned to simple error measures such as MSE (Mean-Squared Error) or PSNR (Peak Signal Noise Ratio), suggesting that they would be equally valid since they can also be easily integrated within enhanced simulation framework. In particular, EvalVid [40] represents a complete framework and tool-set for quality evaluation of videos transmitted over a real or simulated communication network. It is able to measure QoS parameters of the underlying network, like loss, delays and jitter; moreover, it supports a subjective video quality evaluation of the received video based on the frame-by-frame PSNR calculation [2,41]. It has a modular and network independent structure allowing all the interactions with the network via different trace files.

EvalVid can be combined with the well known NS3 simulator as suggested by Bustos-Jimenez et al. [42] in order to obtain a robust and reliable framework for evaluating the perceived quality of service of every multimedia video content. The resulting tool-set from this integration allows network researchers and practitioners to analyze their proposed new network designs in the presence of real video traffic in a straightforward way. On the other hand, mechanisms for enhancing the delivery quality of video streams can be evaluated in more complex simulated network scenarios, including characteristics like relatively large topologies, broadband access, limited bandwidth, wireless, node mobility, and whatever functionality is available at the network simulator. For sake of simplicity we skipped many details about the EvalVid quality of service evaluation process and the integration with standard network simulators but a complete study on these issues can be found in [43].

Since, the EvalVid tool integrates the module for computing the PSNR value of a transmitted video, we can take advantage from this feature to evaluate the goodness of our proposal; moreover, according to the work conducted in [43] it is possible to match few ranges of PSNR values with the corresponding MOS (Mean Opinion Score) index, standardized by ITU-T [39], in order to use both subjective and objective quality indexes as pointed out in Table 2.

7. Results

Simulation results have been achieved performing four different simulation scenarios. In each scenario the defense level has been

Table 2
PSNR and video quality.

PSNR Value	MOS Value (Quality)
$> 37dB$	5 (Excellent)
$31 \div 37dB$	4 (Good)
$25 \div 31dB$	3 (Fair)
$20 \div 25dB$	2 (Poor)
$< 20dB$	1 (Bad)

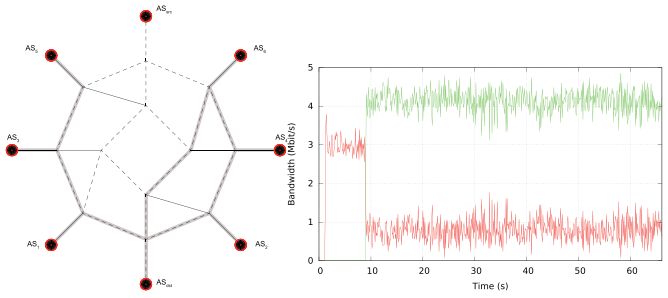


Fig. 5. Level 0 - No defense mechanism is supported. (a) Network Topology - (b) Bandwidth reduction at the victim side after the DDoS attack.

increased by one hop, starting from zero to three hops. Figs. 5–8 show on the left side the network topology of the different scenarios. In each of them, the links flooded by malicious network traffic, are highlighted with a solid line. Instead the dashed lines denote paths from source to destination ASs. Square points indicate the *StopIt* enabled routers.

The first simulation shows the scenario in which no defense mechanism is provided and DDoS attack can easily reach the victim's AS. Fig. 5(b) focus the attention on the victim's access router clearly showing how the malicious traffic (green line) floods 75% of available bandwidth. No actions can be made in this case by the victim to cope the attack.

The second scenario enables the defense mechanism only on the access router of the victim's AS. This configuration represents the situation in which standard *StopIt* is installed, but malicious AS's do not have a *StopIt router* or have hacked it. After 5 seconds from the beginning of the attack, the standard *StopIt* system installs filters on the victim's router while fails to install them on access router of the malicious ASs. Fig. 6(b) shows the benefits of the *StopIt* inside the restricted area in terms of bandwidth used from the victim respect to the previous case; however, even after the filters installation, traffic behavior presents several variations and it appears troubled. This can be explained by looking at the Fig. 6(c) that shows as much of the network traffic, outside the restricted and protected area, is made up by bad traffic.

The third and fourth simulation results show the beneficial effects due to the further expansion of the defense mechanism as close as possible to the sources of the attack. As can be seen in Figs. 7 and 8, more links are clean up from bad traffic and some access routers of malicious ASs are effectively filtered. However Figs. 7(b) and 8(b) show similar behaviors without any significant difference close to the victim's AS.

On the contrary, to evaluate the advantages to switch from second to third level is necessary to look at quality of service during the distributed denial of service attack. Fig. 9 shows the trend of perceived video quality (psnr) during simulation tests. As can be seen the DDoS is able to significantly degrade transfer quality marking a loss of 95% of frames corresponding to a very bad psnr index. Using the first level scheme, it is possible to face the attack by halving the loss rate but this is not enough to guarantee a good video quality. With the implementation of the second level scheme, the average value of the perceived video quality (psnr) rises from 17dB to 27dB thus switching from bad to fair video quality. Last simulated protection level reaches excellent results as reported in Table 3. Frames loss rate is almost negligible (0.07%) and the transmission achieves an excellent video quality.

Regarding the quality offered to other traffic sources such as VoIp and HTTP, the Fig. 10(a) shows the effects due to the DDoS attack without any protection. In particular, without any diffServ policy enabled, the HTTP traffic source experienced almost no transmission capacity while the VoIp source can only reach the minimal guaranteed quality of service. On the contrary, thanks to the activation of the proposed scheme only on the access router of the victim's AS, the VoIp traffic source can recover the original transmission rate while the HTTP source can increase the bandwidth available as shown in Fig. 10(b).

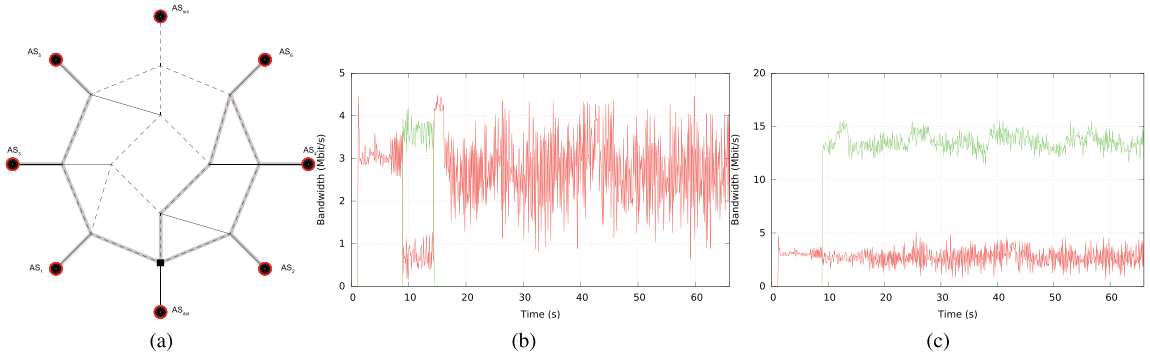


Fig. 6. Level 1 - Defense mechanism installed only on the access router of the victim's AS. (a) Network Topology - (b)Bandwidth at the victim side - (c) Impact of the bad traffic out or the protected area.

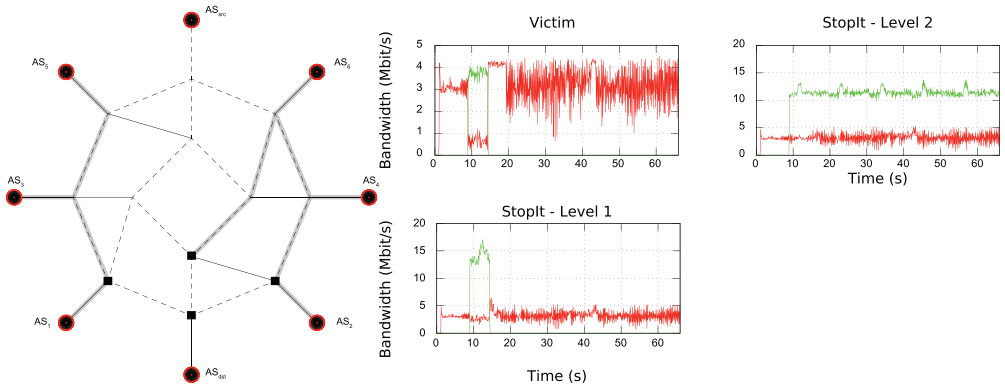


Fig. 7. Level 2 - Defense mechanism installed on the second level access routers. (a) Network Topology - (b)Bandwidth use at the victim side, StopIt router level 1 and StopIt router level 2.

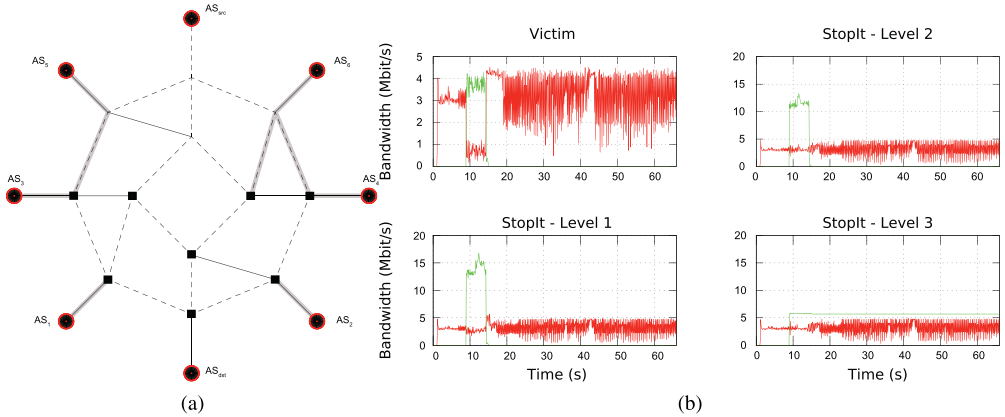


Fig. 8. Level 3 - Defense mechanism installed on the third level access routers. (a) Network Topology - (b) Bandwidth use at the victim side, StopIt router level 1, StopIt router level 2 and StopIt router level 3.

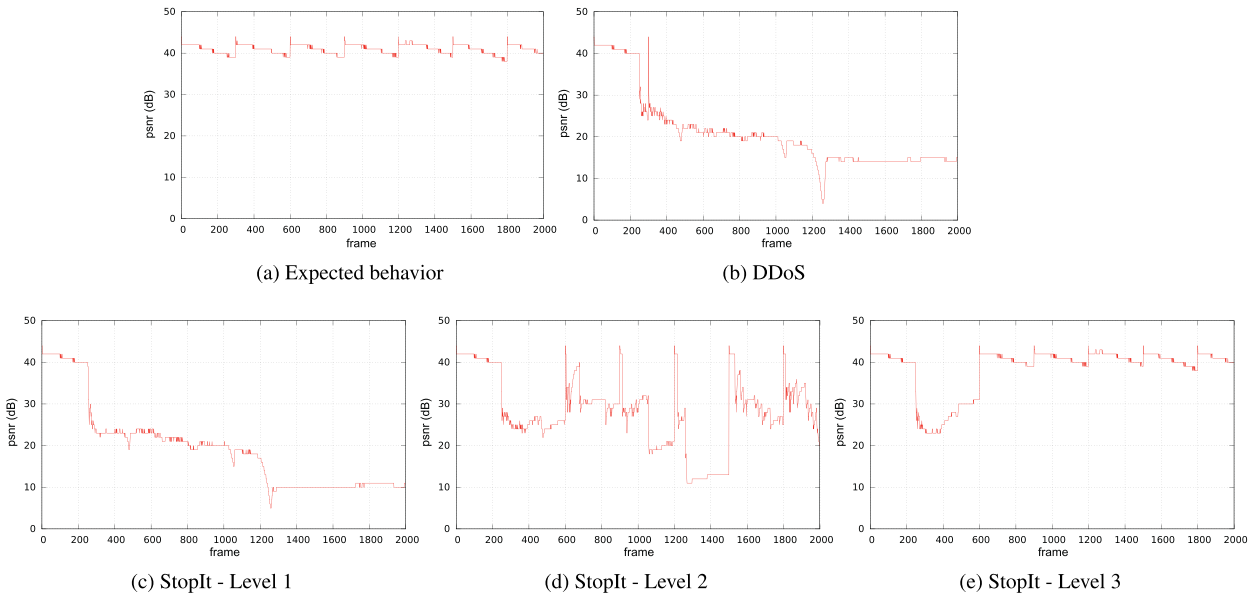
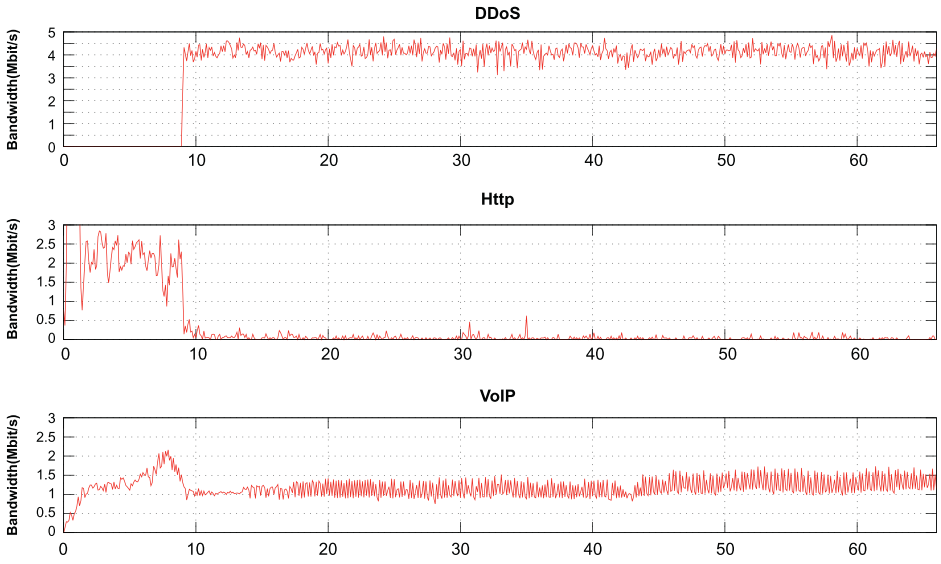


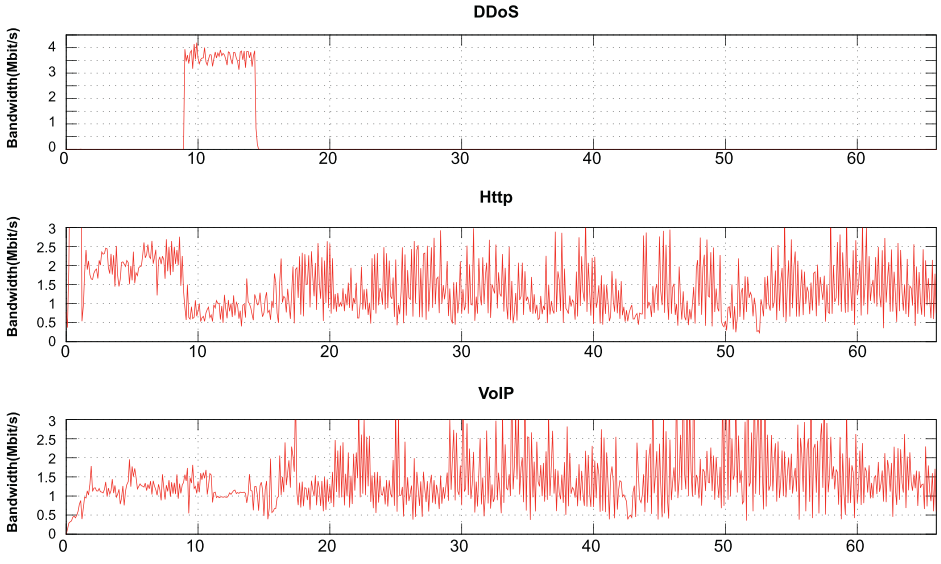
Fig. 9. PSNR evolution under the evaluated scenarios: (a) Expected behavior; (b) DDoS attack without any defense mechanism; (c) DDoS attack using StopIt at Level 1; (d) DDoS attack using StopIt at Level 2; (e) DDoS attack using StopIt at Level 3.

Table 3
Video traffic flow statistics between 600 and 2000 frames.

	Packet Loss	Max e2e delay	Avg e2e delay	DevStd e2e delay	Avg psnr [dB]	DevStd psnr [dB]
No attack	0%	0.2307	0.1021	0.0487	41.49	1.06
DDoS attack	95.15%	9.5162	7.6058	0.2402	16.96	3.17
StopIt Lv1	59.46%	4.7358	0.2015	0.6955	17.02	5.06
StopIt Lv2	6.49%	0.2229	0.1268	0.0454	27.23	8.32
StopIt Lv3	0.07%	0.2136	0.1034	0.0484	41.47	1.23



(a) No defense mechanism is supported



(b) Defense mechanism installed only on the access router of the victim's AS: StopIt - Level 1

Fig. 10. DDoS effects on HTTP and VoIp traffic sources with and without the proposed defense mechanism.

8. Conclusion

In this paper, we proposed a filter-based defense mechanism, derived as an extension of the well-known *StopIt* technique to face bandwidth flooding attacks in more realistic communication scenarios in which different traffic sources (*i.e.* HTTP, VoIp and Video),

presenting different QoS levels, require to be satisfied.

The proposed solution is scalable and effective as witnessed by the reported simulation results, achieved using the ns-3 simulator, which considered different scenarios. In particular, it has been validated with respect to its reactiveness, in terms of time to face the DDoS attack, and to its effectiveness in safeguarding the bandwidth needed for data transmission and the agreed quality of service for the different traffic sources. The specific case of video applications, which have more stringent QoS constraints, has been also considered.

Future research will be focused on a wider testing of the defense mechanism in a large scale topology in which the reaction time could play a vital role in reducing inefficiencies caused by security attacks.

In conclusion, we would like to remark that, to the best of our knowledge, the *StopIt* mechanism has not been really deployed on the Internet; thus the presented work can be considered as a methodology that still require a massive adoption by the main Autonomous Systems (ASes) operators. Furthermore, the DiffServ architecture is nowadays a well standardized architecture and it is widely available in off-the-shelf routers (*i.e.* Cisco ASR 1000) to support and configure different levels of Quality of Service (QoS). For this reason, the DiffServ configuration can be used to support the designed communication scenario making the proposal easy to be implemented although a small change still need to be implemented in the DiffServ model to make it able to trig an alert if some queue size overcomes a fixed threshold for a defined time interval.

Acknowledgments

This work has been partially supported by INdAM GNCS Project 2019 “Innovative methods for the solution of medical and biological big data”.

References

[1] A. Furfaro, P. Pace, A. Parise, L. Molina, Modelling and simulation of a defense strategy to face indirect DDoS flooding attacks, in: G. Fortino, G.D. Fatta, W. Li, S. Ochoa, A. Cuzzocrea, M. Pathan (Eds.), Internet and Distributed Computing Systems, Lecture Notes in Computer Science, 8729 Springer International Publishing, 2014, pp. 263–274, , https://doi.org/10.1007/978-3-319-11692-1_23.

[2] A. Furfaro, L. Argento, A. Parise, A. Piccolo, Using virtual environments for the assessment of cybersecurity issues in IoT scenarios, Simul. Modell. Pract. Theory 73 (2017) 43–54, https://doi.org/10.1016/j.simpat.2016.09.007. Special Issue on Smart Cities and Internet of Things

[3] M. Frustaci, P. Pace, G. Aloi, G. Fortino, Evaluating critical security issues of the iot world: present and future challenges, IEEE Internet Things J. 5 (4) (2018) 2483–2495, https://doi.org/10.1109/JIOT.2017.2767291.

[4] A. Furfaro, A. Piccolo, A. Parise, L. Argento, D. Saccà, A cloud-based platform for the emulation of complex cybersecurity scenarios, Future Gener. Comput. Syst. 89 (2018) 791–803, https://doi.org/10.1016/j.future.2018.07.025.

[5] Verisign, DDos trends report, tech. rep, (2018). https://www.a10networks.com/wp-content/uploads/a10-tps-eb-verisign-distributed-denial-of-service-trends-report-vol-5-issue-2.pdf

[6] O. Kupreev, E. Badovskaya, A. Gutnikov, DDoS Attacks in Q4 2018, Tech. rep, Kaspersky, 2019. https://securelist.com/ddos-attacks-in-q4-2018/89565/

[7] X. Liu, X. Yang, Y. Lu, To filter or to authorize: Network-layer DoS defense against multimillion-node botnets, Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication, SIGCOMM ’08, ACM, New York, NY, USA, 2008, pp. 195–206, https://doi.org/10.1145/1402958.1402981.

[8] IETF, rfc 2475: An architecture for differentiated services, tech. rep, (1998). http://www.ietf.org/rfc/rfc2475.txt

[9] P. Legato, R.M. Mazza, A decision support system for integrated container handling in a transshipment hub, Decis. Support Syst. 108 (2018) 45–56, https://doi.org/10.1016/j.dss.2018.02.004.

[10] T. Peng, C. Leckie, K. Ramamohanarao, Survey of network-based defense mechanisms countering the DoS and DDos problems, ACM Comput. Surv 39 (1) (2007), https://doi.org/10.1145/1216370.1216373.

[11] V.L. Thing, M. Sloman, N. Dulay, A survey of bots used for distributed denial of service attacks, in: H. Venter, M. Eloff, L. Labuschagne, J. Eloff, R. Solms (Eds.), New Approaches for Security, Privacy and Trust in Complex Environments, IFIP International Federation for Information Processing, 232 Springer, US, 2007, pp. 229–240, , https://doi.org/10.1007/978-0-387-72367-9_20.

[12] S.T. Zargar, J. Joshi, D. Tipper, A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks, IEEE Commun. Surv. Tutorials 15 (4) (2013) 2046–2069, https://doi.org/10.1109/surv.2013.031413.00127.

[13] P.A.R. Kumar, S. Selvakumar, Distributed denial-of-service (DDoS) threat in collaborative environment - A survey on DDoS attack tools and traceback mechanisms, 2009 IEEE International Advance Computing Conference, Institute of Electrical & Electronics Engineers (IEEE), (2009), pp. 1275–1280, https://doi.org/10.1109/iadcc.2009.4809199.

[14] N. Hoque, M.H. Bhuyan, R. Baishya, D. Bhattacharyya, J. Kalita, Network attacks: taxonomy, tools and systems, J. Netw. Comput. Appl. 40 (2014) 307–324, https://doi.org/10.1016/j.jnca.2013.08.001.

[15] T. Mahjabin, Y. Xiao, G. Sun, W. Jiang, A survey of distributed denial-of-service attack, prevention, and mitigation techniques, Int. J. Distrib. Sens.Netw. 13 (12) (2017), https://doi.org/10.1177/1550147717741463. 155014771774146

[16] K. Kalkan, G. Gur, F. Alagoz, Filtering-based defense mechanisms against DDos attacks: a survey, IEEE Syst. J. 11 (4) (2017) 2761–2773, https://doi.org/10.1109/jsyst.2016.2602848.

[17] R. Mahajan, S.M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, S. Shenker, Controlling high bandwidth aggregates in the network, SIGCOMM Comput. Commun. Rev 32 (3) (2002) 62–73, https://doi.org/10.1145/571697.571724.

[18] R. Chen, J.-M. Park, R. Marchany, Track: a novel approach for defending against distributed denial-of-service attacks, tech. rep, Technical Report TR-ECE-06-02, Dept. of Electrical and Computer Engineering, 2006.

[19] T. Anderson, T. Roscoe, D. Wetherall, Preventing internet denial-of-service with capabilities, ACM SIGCOMM Comput. Commun. Rev. 34 (1) (2004) 39–44, https://doi.org/10.1145/972374.972382.

[20] V. Kambhampati, C. Papadopoulos, D. Massey, A taxonomy of capabilities based DDoS defense architectures, 2011 9th IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), IEEE, 2011, https://doi.org/10.1109/aiccsa.2011.6126615.

[21] Z. Liu, H. Jin, Y. Hu, M. Bailey, Practical proactive ddos-attack mitigation via endpoint-driven in-network traffic control, IEEE/ACM Trans. Netw. 26 (4) (2018) 1948–1961.

[22] K. Argyraki, D.R. Cheriton, Scalable network-layer defense against internet bandwidth-flooding attacks, IEEE/ACM Trans. Netw. 17 (4) (2009) 1284–1297, https://doi.org/10.1109/TNET.2008.2007431.

[23] M.M. Salim, S. Rathore, J.H. Park, Distributed denial of service attacks and its defenses in IoT: a survey, J. Supercomput. (2019), https://doi.org/10.1007/s11227-019-02945-z.

[24] B. Wang, Y. Zheng, W. Lou, Y.T. Hou, DDoS attack protection in the era of cloud computing and software-defined networking, Comput. Netw. 81 (2015) 308–319, https://doi.org/10.1016/j.comnet.2015.02.026.

[25] J. Cui, M. Wang, Y. Luo, H. Zhong, DDoS detection and defense mechanism based on cognitive-inspired computing in SDN, Future Gener. Comput. Syst. 97 (2019) 275–283, https://doi.org/10.1016/j.future.2019.02.037.
[26] X. Liu, A. Li, X. Yang, D. Wetherall, Passport: secure and adoptable source authentication, Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation, NSDI'08, USENIX Association, Berkeley, CA, USA, 2008, pp. 365–378.
[27] D. Medhi, K. Ramasamy, Network Routing: Algorithms, Protocols and Architectures, Morgan Kaufmann, 2007.
[28] S. Sendra, P.A. Fernández, M.A. Quilez, J. Lloret, Study and performance of interior gateway IP routing protocols, Netw. Protoc. Algorithms 2 (4) (2011) 88–117, https://doi.org/10.5296/npa.v2i4.547.
[29] L. Feinstein, D. Schnackenberg, R. Balupari, D. Kindred, Statistical approaches to DDoS attack detection and response, Proceedings DARPA Information Survivability Conference and Exposition, IEEE Comput. Soc, 2003, https://doi.org/10.1109/discex.2003.1194894.
[30] P. Kamboj, M.C. Trivedi, V.K. Yadav, V.K. Singh, Detection techniques of DDoS attacks: a survey, 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON), IEEE, 2017, https://doi.org/10.1109/upcon.2017.8251130.
[31] X. Yang, D. Wetherall, T. Anderson, A DoS-limiting network architecture, Vol. 35, Association for Computing Machinery, (ACM), New York, NY, USA, 2005, pp. 241–252, https://doi.org/10.1145/1090191.1080120.
[32] IETF, rfc 2328: Ospf - open shortest path first, tech. rep, (1998). https://www.ietf.org/rfc/rfc2328.txt
[33] nsnam, ns-3 network simulator, http://www.nsnam.org.
[34] S. Ramroop, A diffserv model for the ns-3 simulator, 2011, http://www.eng.uwi.tt/depts/elec/staff/rvadams/sramroop/index.htm.
[35] S.d. Mata, Http model for ns-3, 2013a, http://www.saulodamata.com.br/codes/http-traffic-generator.
[36] S.d. Mata, Voip model for ns-3, 2013b, http://www.saulodamata.com.br/codes/voip-traffic-generator.
[37] GERCOM, evalvid model for ns-3, https://github.com/gercom/evalvid-ns3.
[38] Video Traces Research Group, YUV 4:2:0 Video Sequences, Arizona State University, 2014. http://trace.eas.asu.edu/yuv/
[39] I.T. Recommendation, Subjective video quality assessment methods for multimedia applications, Tech. Rep. TUT P.910, International Telecommunication Union, 1999.
[40] D. Saladino, A. Paganelli, M. Casoni, A tool for multimedia quality assessment in ns3: Qoe monitor, Simul. Modell. Pract. Theory 32 (2013) 30–41.
[41] P. Pace, G. Aloi, Wevcast: wireless eavesdropping video casting architecture to overcome standard multicast transmission in wi-fi networks, Telecommun. Syst. 52 (4) (2013) 2287–2297.
[42] J. Bustos-Jimenez, R. Alonso, C. Faundez, H. Meric, Boxing experience: measuring QoS and QoE of multimedia streaming using NS3, LXC and VLC, 39th Annual IEEE Conference on Local Computer Networks Workshops, Institute of Electrical & Electronics Engineers, (IEEE), 2014, pp. 658–662, https://doi.org/10.1109/lcnw.2014.6927717.
[43] J. Klaue, B. Rathke, A. Wolisz, Evalvid–a framework for video transmission and quality evaluation, Computer Performance Evaluation. Modelling Techniques and Tools, Springer, 2003, pp. 255–272, https://doi.org/10.1007/978-3-540-45232-4_16.