International Journal of Organizational and Collective Intelligence
Volume 12 • Issue 4

A New Information-Based Heuristic for Distributed DDoS Detection and Mitigation: Distributed and Collaborative DDoS Detection

Abdenacer Nafir, University 20 August 1955, Skikda, Algeria*
https://orcid.org/0000-0003-0494-7579

Smaine Mazouzi, University 20 August 1955, Skikda, Algeria
https://orcid.org/0000-0003-3587-7657

Salim Chikhi, Abdelhamid Mehri Constantine 2 University, El Khroub, Algeria
https://orcid.org/0000-0002-8369-8533

ABSTRACT

In this paper a novel collective method for DDoS detection is introduced. The method is distributed and implemented as a multi-agent system, and where local decision is based on an information-based heuristic, namely the entropy. According the calculated entropy a router exchange data with its neighbors aiming at collectively decide if a DDoS is ongoing or not. Most of the works of the literature that are based on the entropy they have used source addresses. The authors' method is based on the entropy of the distances traveled by the packets, so spoofing IP packets will be hard to perform by hackers. Each router combines its decision with those of its neighbors. Such a collective detection allows to apply defense against the attack despite the victim is out of service or cannot perform DDoS mitigation because the traffic is congested in its neighborhood. Conducted experiments using the platform OMNet++ show the potential of the new method for efficient collaborative and distributed detection and mitigation of DDoS attacks.

KEYWORDS

Collaborative DDoS, DDoS Detection, DDoS Mitigation, Distance-Based Entropy, Entropy, Intrusion Detection, Network Security, OMNet++

INTRODUCTION

With the high connectivity to the internet, connected devices undergo hundreds of attacks every day (Thonnard et al. 2012; Mahjabin et al. 2017). This intensive and harmful activity can be explained by the emergence of a new profile of hackers. Indeed, in the last years, attacks are performed for lucrative reasons (Al-rimy et al., 2018; Thonnard et al., 2012), which results in a large community of hackers that design and use ingenious attacks and eventually hire or sell them on internet.

DOI: 10.4018/IJOCI.312221 *Corresponding Author

Code vulnerabilities continue to be detected every day (Kamble & Bhutad, 2018), which let unsecure both computers and networks. Code vulnerabilities make defense mechanisms ineffective that allow to hackers to easily perform attacks against unsecured computers. The latter, after they are intruded, can be used as bots to perform Distributed Denial of Service (DDoS). The DDoS-for-hire server (Webstresser.org) (Kaspersky Lab, 2018), which is one of the widest DDoS servers, was shut down by the Europol in 2018. When it was inspected, it recorded more than 3600 users which have committed more than 6 million DDoS attacks. So, researchers and professionals in security are called to propose new solutions for the new schemes of attacks, which are now mostly distributed. Typically, the Distributed Denial of Service (DDoS) attack is performed with a large set of compromised computers against a targeted victim. On an isolated computer or network router, such an attack is hard to detect because it seems like an ordinary, or in worst case, an intensive traffic. To efficiently detect such an attack several routers and hosts, forming the network nodes, must collaborate.

To do that, connected routers in a network should exchange security records, mainly those concerning DDoS attacks. Such a way allows to the ensemble of routers to collectively detect if a DDoS attack is conducted or not. Nevertheless, two problems must be addressed and resolved: First, how interconnected nodes efficiently communicate security information without making heavier the network traffic. Second, how the anomalies in the network traffic are detected. It is performed by discriminating normal situations and abnormal ones that are observed during a DDoS attack. Such an issue is hard to deal with because the measures used by the hackers in order to make that attack furtive, which is classically performed by spoofing techniques.

This paper introduces a new collaborative technique for DDoS detection and mitigation that can be used in wide area networks (WAN), or in dynamic networks such as wireless sensor networks (WSN). The proposed technique aims at detecting a DDoS at both network level and host level. It consists of an early detection that starts at the routers in the core of the network. Indeed, a host-based mitigation is usually ineffective because the latter finds itself down if it was reached by the attack. According to the proposed technique, a local detector of traffic anomalies, which works like a classical Behavior-based IDS (Intrusion Detection System) is installed at every router. The latter continuously compute the entropy of the distances travelled by the packets that cross it. Such entropy allows establishing an informational heuristic that allows to notice a DDoS if the computed entropy is low. Based on such entropy the router can decide that a DDoS attack is observed at its location. Each router exchanges its local decision that was computed according to the observed anomalies of the traffic with the routers with which it is directly connected. So, if a router detects an anomaly in the transited traffic, it shares its decision with its neighboring routers. So, the overall decision at a given router will result from its own decision and those of the routers within its neighboring routers.

For anomaly detection, it has been proposed a new heuristic for the analysis of the traffic that is based on entropy of distances. It is assumed that a bias of the traffic should be present and can be detected during a DDoS attack. Indeed, with a normal traffic the packets that cross a given router likely income from everywhere in the networks, so the corresponding source addresses should be uniformly distributed. Such a fact lets the entropy of source addresses high. Instead of entropy of source addresses, that was used by all the works which were reviewed (Ma & Chen, 2014), the entropy of distances was adopted. With such choice, a hacker cannot prevent traveled distances because it is hard to compute and correctly spoof the TTL (Time To Live) attribute, contrary to sources addresses that can be easily spoofed. Indeed, in order to correctly modify the TTL attribute, one shoulds know all the nodes of the network and how they are connected. Otherwise an inappropriate value of TTL could make the packet lost in the network. However, the IP source addresses can be simply randomly selected within the legitimate range of addresses that are allowed on a given network. Furthermore, the addresses can be randomly spoofed by setting them in the range of addresses that can be used in the considered network.

Furthermore, how entropy varies during a DDoS attack depends on the assumption on how the bots in the network conduct the attack. In some work, authors have assumed that during an ongoing

DDoS new addresses that correspond to bots forming the botnet are observed (Shojaeiet al., 2011 ; Ouerfelli et al., 2018). In this case the traffic anomaly is detected when the entropy increases and goes over a given threshold. This is explained by the fact that bots generate new addresses increasing the address diversity within the network, which increases in its turn the entropy. Unlike such work, other authors assume that there are not new addresses during a DDoS but there is an increased traffic coming from some specific sources that are the bots in the network (Bhuyan et al., 2016). In such cases, flows from these sources are intensive and leads to decrease the entropy. It seems that the latter scheme is more realistic than the first and it was adopted for traffic anomaly detection in the conducted work. In overall, in this work it was introduced a new entropy-based metric that allows to reliably detect traffic anomalies. Then it has been used in a new distributed and collaborative scheme that allows to the routers in the networks to collaborate in order to early detect DDoS and mitigate them.

The remainder of the paper is structured as follows: Section 2 introduces some related work having dealt with DDoS detection, where they were summarized the main drawbacks of the reviewed works. Section 3 is devoted to the proposed method introduced in this paper, where principle if first presented and how it is performed DDoS collaborative detection based of entropies of traveled distances of packets. It is also shown how mitigation by throttling is performed by some self-selected routers. In Section 4 the experimentation and discussion are provided. Finally, a conclusion summarizes the conducted work, and provides some related perspectives.

RELATED WORK

In the security threat literature, several researches have dealt with Distributed Denial of Service (DDoS), where some of them have recently proposed collaborative detection (Mahjabinet al., 2017, Behal et al. 2017). Operational systems are called Collaborative Intrusion Detection Systems (CIDS). They do not deal in particular with DDoS, however, they allow us to introduce the general approaches for collaborative attack detection. Recently, proposed DDoS defenses tend to be collaborative (Mahjabinet al., 2017, Behal et al. 2017, Zargar et al. 2013) and form a part of Collaborative Intrusion Detection Systems (CIDS) where DDoS prevention, detection, and mitigation are considered in such systems.

A well referenced taxonomy of such systems was proposed in (Zhou et al., 2010). According to this taxonomy, CIDS can be centralized, hierarchical, or fully distributed. In the two first categories, there is some kind of central control and decision. The latter present the major drawback of such systems that do not allow them to be used with large-scale networks. Obviously, it is not possible to perform a central control over a large scale network by dedicating a node or a set of nodes to which all the security information over the network is forwarded to be processed (Cha et al., 2011; Sirivianos et al., 2011 & Modi et al. 2013). In the third category, where the conducted work can be placed, a CIDS is fully distributed. So, there is no central entity dedicated to control the system. Certainly, it is hard to handle control and decision in such systems, but they are more suitable for large-scale networks in particular for DDoS detection, given that the attack itself is distributed.

Fully distributed systems, for which no node has any privileges, are organized according a security viewpoint, like in P2P networks. Every node of the network performs local intrusion detection where it is located. Then it exchanges security data with nodes with which it cooperates. So, every node looks to validate its local decision by analyzing occurred events on other nodes (Selvakumar, 2012). Fully distributed systems are scalable, and can be deployed on large-scale networks, such internet. However, they suffer from a common and major drawback which consists in the locality of interaction which it results in a partiality of the information, used to make decision on a given node, and at a given time. According to the local scheme of communication, no information can be considered as global within the network. It is always considered as local and concerns only a local subset of nodes within the network.

Several taxonomies for prevention, detection, and mitigation of DDoS attacks were proposed in the literature (Mahjabin et al., 2017 ; Modi et al., 2013 ; Bhuyan et al., 2014 ; Zargar et al., 2013),

where the location of the deployment of the detection/mitigation location was the most used criterion. Indeed, the performance of a DDoS detection and mitigation is strongly dependent on where it**t)** will be located within the network (Mahjabin et al., 2017 ; Modi et al., 2013). According such a criterion DDoS defense methods can be spite in four categories: source-based, destination-based, network-based, and distributed-based methods. Except for the last category, the first ones are considered centralized given that no collaboration is needed within the nodes of the network.

In this short review only the category of distributed DDoS detection and mitigation is focused on, where collaboration within nodes and hosts is highlighted. According the distributed and collaborative approach, the cheek for a DDoS is performed initially at each node of the network, including hosts, and destinations, and on all the routers on the edge and in the core of the network. In some work, the victims were considered known. So, routers close to the victim are responsible to detect the attack, and send a command to the routers close to the sources in order to proceed to mitigation by packet filtering (Behal et al., 2018). In such schemes, it is required that hosts and edge routers must communicate over the network to exchange mitigation commands. Such extra communication amount aggravates the network flooding, in particular close to the victim.

Obviously, a DDoS attack can be better detected close to the victim. However, and in opposite, the defense mechanism is well suited close the sources of the attack. Independently of the adopted architecture, decision making methods in DDoS detection could be split in different categories, where several taxonomies were recently proposed in the literature for instance that of Devi and Prriyadarshini (2020). Mainly, DDoS detection methods are split in three categories: Signature-based, behavior-based, and hybrid methods. In behavior-based category, anomaly detection is the well adopted class of methods, where we can distinguish Artificial Intelligence (AI) methods and information theory methods, for which it belongs the proposed method in this paper. Recently, Deep neural networks are widely used as AI techniques for DDoS detection (Shieh et al., 2021). They have scored better that the classical machine-learning based methods. Recently, Security dedicated to Cloud becomes an emerging new trend. As a sample of work having dealt with malware identification at edge devices in Cloud computing, that published by Amandeep SinghSohal et al. (2018) where authors combined several technologies in order to deal with this problem, namely Markovian models, Intrusion Detection Systems, and Virtual Honeypot Devices. Indeed, in such systems, security defense should include several aspects. So, the developed systems are organized in layers such as that proposed by Victor Chang et al. (2016).

It results from the literature that, despite recent work having dealt with, distributed mechanisms for DDoS defense, especially the decision integration remains a challenge and an open issue. Indeed, the reviewed systems do not allow enough interaction between nodes and hosts in the network, and where the communication is restricted to data exchange but not to decision. In addition to the architectural aspect proposed in this paper, it can be assumed that the conducted work can be considered as a new distributed Framework for DDoS detection and mitigation. The Framework is fully distributed in the sense that the global decision is not represented at any entity in the network. Any resulted system according the proposed Framework consists in a collaborative solution for DDoS detection that can be deployed WANs and MSNs.

COLLECTIVE DISTANCE-ENTROPY-BASED DDOS DETECTION

As it was introduced before, the proposed framework DDoS detection is a collaborative distributed architecture involving the whole entities of the network. In a network a router is in a neighboring of routers with which it is physically connected. A Local DDoS detector is installed at every router, where it analyzes the traffic and concludes is an anomaly exists within or not. According to the analysis by controlling the entropy of the distances traveled by the packets that cross it, the local detector makes its own initial decision. Then, when a router notices a traffic anomaly it tries to confirm it by requesting from its neighbors their own decisions. It should be noticed that all the routers are considered by

controlling the traffic that transits by them, and an one can take a decision that a DDoS is detected at its location. The resulting scheme exchanging local decisions reinforce the certainty if a DDoS is ongoing or not. Such scheme of communication allows sharing local decisions within the neighbors, and so, they will be forwarded beyond the local neighborhood.

Therefore, in the situation where a router is not certain about the traffic, because the latter seems to be normal, the router requests the local decisions of its neighbors and shares its own one, aiming at establishing a collective decision in the neighborhood. The own initial decision at a given router is established by controlling the traffic that crosses the router. In order to detect traffic anomalies, an information-based heuristic was proposed and which consists of the entropy of the packets that cross a router. However, instead of computing entropy based on source addresses as many works have done, traveled distances were considered. The latter can be deduced from the TTL (Time To Live) attribute of the IP packet in IP-v4 (or Hop Limit in IP-v6 which explicitly indicates the number of hops allowed to a packet to perform before it is destroyed). The TTL of a packet is set at the source, and it is decremented at each router the packet crosses. Such distance-based entropy is adopted because it is hard to spoof the TTL field, compared with source addresses, which can be simply spoofed. The unique considered traffic anomaly in this work is the traffic bias, expressed by the fact that the distances are not sufficiently random at a given router. So, it can be assumed that a part of such traffic provides from bots that conduct the DDoS.

Collaborative Router-end DDoS Detection

For a safe traffic, without an ongoing DDoS, it can be assumed that at a given router source addresses income randomly from source hosts. So, it results that the distances traveled by the packets and come cross the router are also randomly distributed. In order to formally express this fact, it is supposed that for a time interval ΔT, the number of packets having crossed a router r is N. Let $d_{p,r}$ the distance traveled by a packet p from the source having generated it to the router r. At the router r it results a set of distances $\{ d_{p,r}, p = 1..N\}$ which can be partitioned into M clusters, $\{C_i, i = 1..M\}$. Each cluster contains the same distances: $C_i = \{ d_{p,r} / \forall p', p'' \, d_{p',r}=d_{p'',r}\}$.

The distance $d_{p,r}$ traveled by a packet that arrives on the router r is calculated from the TTL (Time To Live) attribute, recorded in the header of the IP packet.

Thus, and according to the Shannon theory of information, the entropy of the distances, $E_r^{\{\Delta T\}}$ at the router r for a time interval ΔT can be computed. Let $\Omega(C_i)$ the size of C_i, so, the entropy $E_r^{\{\Delta T\}}$ can be expressed as follows:

$$E_r^{\Delta T} = -\sum_i \frac{\Omega\left(C_i\right)}{\sum_j \Omega\left(C_j\right)} \log \frac{\Omega\left(C_i\right)}{\sum_j \Omega\left(C_j\right)}$$

According to the entropy concept, the value of the entropy is high with normal traffic. Such fact indicates that the sources from where packs generated are random. The entropy is maximal in the case where the whole clusters of equal distances have the same sizes. In such a case, $\Omega(C_i)$ is constant and $\sum_j \Omega\left(C_j\right) = M\Omega\left(C_i\right)$. The maximum entropy () in this case will be equal to log M.

Overall, at each time interval ΔT a router r calculates the distance entropy $E_r^{\{\Delta T\}}$. If the latter is over a threshold Tr_r^E, which indicates the randomness nature of distances, it will be assumed that the traffic is not biased. Otherwise, it will be assumed that the traffic is biased and an anomaly is considered detected, which indicate a potential ongoing DDoS attack. The threshold Tr_r^E is specific to each router r given that routers do not record the same density of network traffic.

In the example of Figure 1, six packets ($N = 6$) cross the router r_3, from hosts h_1 to h_6. The resulting set of distances is nominally {3,2,4,3,4,3}, which expresses the numbers of hops from the source hosts to the router r_3. By partitioning the set of distances, it results three clusters: $C_1 = \{3,3,3\}$, $C_2 = \{2\}$, and $C_3 = \{4,4\}$. So, the resulting entropy at this router is:

$$E_r^{\Delta T} = -\frac{3}{6}\log\frac{3}{6} - \frac{1}{6}\log\frac{1}{6} - \frac{2}{6}\log\frac{2}{6}$$

The principle of the local detection performed at the neighborhood of a given router having detected an anomaly, consists in confirming the detected anomaly as certainty reinforcement when some of the neighboring routers have also noted the anomaly. Indeed, when a DDoS is ongoing, and with assuming that the botnet that carry out the attack is sufficiently dense (necessary condition in order succeed the DDoS attack), the resulting traffic anomaly within the network should be noticed at several routers. Obviously, the anomaly is more detected at the routers forming the path between the bots and the victim (Figure 2).

In Figure 2, the three routers detect the traffic anomaly according to the distance entropies. It can be noticed that in this case, the three routers belong to the path between the bots and the victim.

Figure 1. Distance clustering and entropy calculation: the distance entropy $E_r^{\{\Delta T\}}$ is calculated at the router r_3 according the distances to the different hosts

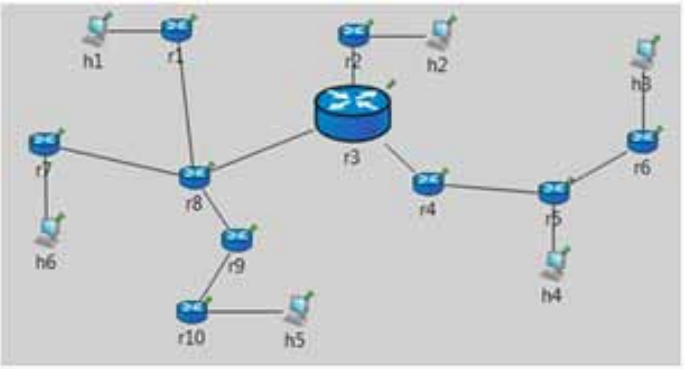
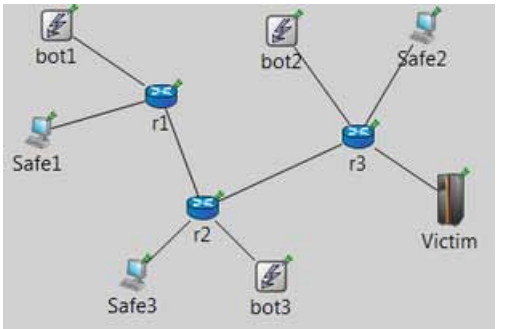


Figure 2. Each router has detected the anomaly and has confirmed it given that its neighbors have detected also anomalies



The router r_2 in Figure 2 has detected the traffic anomaly and has sent a request to all its neighbors, asking them if they have detected an anomaly too. When all the responses are received, or when a timeout is expired, a giver router confirms the anomaly if at least 50% of the neighboring routers have noticed too the anomaly. So, the router in question considers that a DDoS attack is in progress in the network. However, the router does not start DDoS mitigation if only its entropy is significantly low (see Section DDoS Mitigation). In this work, it has been experimented the entropy of distances, obtained from TTL attribute, which consists of the unique parameter that a router uses to detect the traffic anomaly (local decision). The overall decision at a given router is taken according to the decision of the majority of the neighboring routers.

DDOS MITIGATION BY IP THROTTLING

The introduced strategy consists of throttling the edge routers connected to the sources hosting the bots that conduct the DDoS attack. The problem is how to select these edge routers, without a central control, among the set of routers that have detected and confirmed the traffic anomaly.

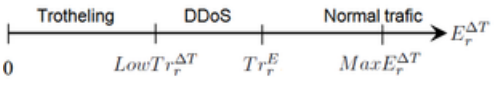
Assuming that the bots which conduct the DDoS attack, are among the set of hosts that legally use the network. It results that the entropy anomaly is more noticed and could be detected at some routers close to the bots that conduct the attack, because the masse of packets traveling these routers come likely from the same close to the sources, which are the bots. An idea to mitigate the DDoS attack is to throttle the routers that have confirmed the DDoS and are close to the bots. Indeed, it is not a good idea to proceed by throttling at the routers close to the victim, because during a DDoS attack the traffic is more congested around the victim.

Here, the distance entropy to select the routers that will be concerned by traffic throttling is also used. These are the routers having first confirmed the DDoS, and having an entropy lower than a lower threshold $LowTr_r^E$, which is in turn lower than the threshold of detection Tr_r^E. Figure 3 shows the different states of a router according to he calculated entropy at the end of each time interval.

So, the traffic is decreased near the bots, away from the victim, which results in the reduction of the network congestion, and the victim itself is decongested.

Unlike techniques using throttling by sending pushback messages, the proposed one does not require sending such messages and the throttling is self-decided by each router, which adds nothing to the network traffic, that is congested during a DDoS attack. Pushback techniques by the victim of the attack (Kamarsamy & Asokan, 2011). Such a method cannot be applied in large-scale networks: On the one hand because of the congestion of the network near the victim, and on the other hand because of the high number of routers and hosts in the network. Furthermore, it is not easy to confidently determine where are situated the bots that conduct the DDoS. So, instead of selecting bots that are connected to an edge router, using entropy allows to select the routers that are more likely close to theses bots. Throttling just at these routers allows to mitigate the ongoing attack, without degrading the effective bandwidth of the network. For this, a threshold $LowTr_r^E << Tr_r^E$ specific to the router *r*, is used to determine if *r* is concerned by throttling or not. If the calculated entropy $E_r^{\{\Delta T\}}$ is less than $LowTr_r^E$ then the router proceeds to traffic throttling at its level. Furthermore, a router *r* concerned by throttling selects the packets that have high frequencies of distance in order to discard them. Indeed, given their high frequencies, these packets are more likely coming from a bot sources.

Figure 3. Router state according the calculated entropy at the end of the time interval ΔT



EXPERIMENTATION

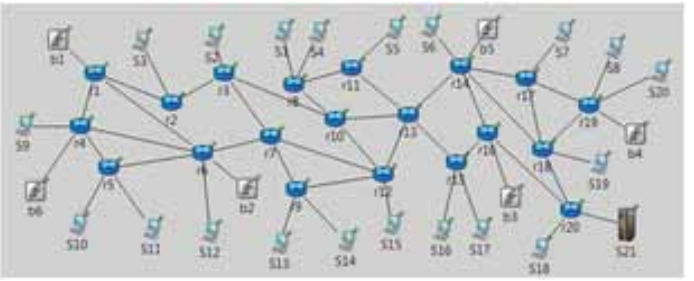
Due to many technical and legal reasons it is hard to experiment the proposed method on a real wide networks, with several routers and connected computers that must be accessed. For this reason, simulations by using well known and used network simulators were conducted. Moreover, and as far as we know, all the DDoS dedicated datasets such as CAIDA (Claffy, 2001), and DARPA (Lippmann et al., 2000) that are cited in several related work, have been used exclusively for victim-end methods for DDoS detection, and the data that contain do not allow to experiment collaborative and distributed DDoS defense methods such as the method introduced in this paper. Indeed, the data of these datasets were recorded at victims of DDoS attacks. Since several years, some authors have noticed that the community of DDoS defense needs a specific of DDoS attacks (Francois et al., 2012). In such dataset data are collected at the whole routers and hosts of the network.

So, the OMNet++ platform and its INet library (Varga 2018) were used to simulate network elements and traffic. Simulated networks are with irregular topologies, where routers and hosts are connected according to a mesh like in a WAN of a WSN. In the first experimentation, a network of 20 routers is simulated where they are connected 27 hosts (Figure 4). It has been assumed that 21 hosts are safe ($S_1...S_{21}$), and the remaining 6 hosts form the botnet ($b_1...b_6$). A simulation with low number of routers and hosts allows analyzing the traffic and providing its details, and how the decisions are established at different routers according to the entropy and the communication within the set of routers. For all the conducted simulations, each router is connected to a set of neighbors where the number ranges randomly from 1 to 5.

The duration of each simulation is 2 minutes, where hosts are randomly selected then exchange packets. Each time, the source and the destination are randomly selected. It consists of the normal activity without an ongoing DDoS and which result in high entropies of distances. Periodically, routers exchange their decisions regarding the traffic. A given router requests from its neighbors their respective decisions. During the 2 minutes of simulation, a number ranging from 50000 to 100000 iterations are performed. At each iteration a randomly selected host sends a packet to a randomly selected destination. However, when a DDoS is simulated and if the sender host is a bot it sends also a set of packets towards the victim (S_{21}). The number of the malicious packets sent to the victim ranges from 1 to 3. The victim can be set manually by the user or randomly selected by the simulator. In the first simulation bellow, the victim was set as the host S_{21} connected to the router r_{20} (Figure 4). According to several simulations, the threshold Tr_r^E is set to 0.80% of $MaxE_r^{\{\Delta T\}}$. $LowTr_r^E$ is set to 0.50% of $MaxE_r^{\{\Delta T\}}$.

First, we show that the collaboration within routers enhance the detection of DDoS by comparing final results with those obtained with only entropy-based decision, as the most of works have done in the literature (Bhuyan et al., 2016; Francois et al, 2012 & Yu and Zhou, 2008 & Zargar et al., 2013

Figure 4. A network of 20 routers and 27 hosts: $S_1,S_2...S_{21}$ are safe hosts and $b_1,b_2...b_6$ are the bots



; Mahjabin et al., 2017). So, in order to show how collaboration enhances results, the entropy-based decisions are compared with those updated by the decisions of the neighboring routers.

Table 1 shows the distances recorded at the set of the 20 routers of the network. According to theses distances, routers calculate their respective entropies, make initial decision if there is an ongoing DDoS or not. Furthermore, and according to the decisions taken in the neighborhood of a given router, the latter confirms the DDoS and then proceeds to mitigation if its corresponding entropy is lower than the threshold $LowTr_r^E$.

Table 2 shows the obtained simulation results for the network in Figure 4. The aim is to show that the collaboration within routers by exchanging their initial decisions has allowed enhancing DDoS detection, especially at the routers that are far from the victim, and where some of them start DDoS by router throttling. In Table 2, the columns 2 and 6 are the numbers of respectively the neighboring routers and the neighbors having detected the anomaly. The latter information has allowed to show

Table 1. Clusters of distances traveled by packets at each router in the network, at the end of the time interval Δ*T*: case of traffic anomaly due to an ongoing DDoS

Router	Distances							$E_r^{\{\Delta T\}}$	$MaxE_r^{\{\Delta T\}}$
	1	2	3	4	5	6	7		
1	4431							0	0
2	777	4299						0,428	0,693
3	751	777	4265					0,76	1,099
4	4498	79						0,087	0,693
5	794	57	46					0,435	1,099
6	4445	5288						0,689	0,693
7	740	4632	5293	141				0,953	1,386
8	717							0	0
9	732	77	128	166	45			1,119	1,609
10	727	1222	544	4077				1,059	1,386
11	711	59						0,27	0,693
12	685	1492	4450	4931	55			1,187	1,609
13	765	2026	2247	4728	8782			1,331	1,609
14	4508	644	1494	1687	4482	8426		1,518	1,792
15	750	121	268	265	136	179		1,563	1,792
16	4504	4783	207	476	548	3986	7745	1,546	1,946
17	745	324	217	513	575	251	352	1,861	1,946
18	737	649	108	255	280	128	174	1,712	1,946
19	632	164	105	246	275	128	162	1,753	1,946
20	4856	4492	105	242	293	3847	7573	1,476	1,946

Table 2. Different cases of anomaly detection, and local neighborhood decision for the 20 routers of the simulated network: With ongoing DDoS

Router (1)	Number of Neighbors (2)	$MaxE_r^{\{\Delta T\}}$ (3)	$E_r^{\{\Delta T\}}$ (4)	Initial Decision (5)	Neighbors with DDoS (6)	Final Decision (7)	Throtting (8)
1	3	0	0	+	2	+	Performed
2	2	0,693	0,428	+	2	+	
3	3	1,099	0,76	+	3	+	
4	3	0,693	0,087	+	2	+	Performed
5	2	1,099	0,435	+	1	+	Performed
6	4	0,693	0,689	-	4	+	
7	4	1,386	0,953	+	3	+	
8	2	0	0	+	2	+	Performed
9	2	1,609	1,119	+	2	+	
10	4	1,386	1,059	+	4	+	
11	2	0,693	0,27	+	1	+	Performed
12	4	1,609	1,187	+	3	+	
13	5	1,609	1,331	-	3	+	
14	4	1,792	1,518	-	1	-	
15	2	1,792	1,563	-	1	+	
16	3	1,946	1,546	+	1	+	
17	3	1,946	1,861	-		-	
18	4	1,946	1,712	-	1	-	
19	2	1,946	1,753	-		-	
20	2	1,946	1,476	-	1	+	

in column 7 the set of routers having confirmed the anomaly. In the simulation with a DDoS attack, the whole routers having detected the anomaly have to confirm it. Indeed, every router of them has more than 50% of neighbors that have also noticed the anomaly. The last column of Table 2 shows the routers have performed throttling as a mitigation measurement against the ongoing DDOS.

According to the obtained results, it can be established that the routers which are situated far from the victim are those having detected the DDoS. Such a result can be explained by the fact that the routers near the victim concentrate packets towards the victim from different locations in the network during the attack. This results in high variety of the distances values of the incoming packets, leading to low entropies. However, the routers near the bots likely forward packets with low distances. Furthermore, at these routers distances are biased by packets from the bots that are sent to the victim, and are routed according to invariant paths.

It can be noticed from the obtained results, introduced in Table 2 that the routers that are far from the victim are those which are concerned by throttling. At these routers the traffic is less congested than at the routers that are close to the victim. Table 3 shows simulation results in the case of a safe traffic, without an ongoing DDoS.

Table 4 introduces the detection results, where it can be noticed that only six routers have initially decided that there is an ongoing DDoS attack. However, two routers have modified the decision after

Table 3. Clusters of distances traveled by different packets at each router in the network, at the end of the time interval Δ*T*: Safe traffic, no DDoS

Router	Distances							$E_r^{\{\Delta T\}}$	$MaxE_r^{\{\Delta T\}}$
	1	2	3	4	5	6	7		
1	3798							0	0
2	3687	3134						0,69	0,693
3	3682	3687	2919					1,093	1,099
4	3776	432						0,331	0,693
5	3782	280	228					0,445	1,099
6	3717	7510						0,635	0,693
7	3807	4649	7522	660				1,181	1,386
8	3796							0	0
9	3838	380	640	823	221			1,095	1,609
10	3725	6192	2557	2020				1,293	1,386
11	3809	354						0,291	0,693
12	3741	7662	3701	5776	219			1,382	1,609
13	3751	10878	11634	5010	6684			1,522	1,609
14	3716	3239	8216	8740	3808	5095		1,713	1,792
15	3772	512	1353	1461	598	813		1,536	1,792
16	3829	5216	1028	2749	2957	1279	1634	1,811	1,946
17	3742	1492	1101	2735	2945	1296	1710	1,856	1,946
18	3709	3272	584	1359	1389	616	852	1,714	1,946
19	3073	715	566	1356	1530	642	855	1,763	1,946
20	5715	3857	531	1414	1482	637	852	1,605	1,946

exchanging local decisions with their respective neighboring routers. Only the router, r_6, has changed decision from safe traffic to DDoS attack after decision exchange, and two routers have proceeded to router throttling.

Aiming to quantify the overall performance of the proposed method and comparing it with a well referenced one (Francois et al. 2012), the simulation was run 20 times. In the first 10 rounds, a DDoS against a randomly selected victim was simulated. In this simulation, 20 to 30% of the hosts are randomly considered as bots. It was be calculated the 3 most metrics, that are used in similar work (Francois et al. 2012). They are namely: Detection rate (DR), False Positives (FP), and False Negatives (FN). Because the global decision in the whole network is not recorded anywhere for the introduced method and in order to compare the obtained results to those of other methods, it is considered that a DDoS is detected in the whole network if at least 50% of the routers have detected it and confirmed the detection. Table 5 shows the results of the whole simulations.

Table 4. Different cases of anomaly detection, and local neighborhood decision for the 20 routers of the simulated network: Safe traffic, no DDoS

Router (1)	Number of Neighbors (2)	$MaxE_r^{\{\Delta T\}}$ (3)	$E_r^{\{\Delta T\}}$ (4)	Initial Decision (5)	Neighbors with DDoS (6)	Final Decision (7)	Throttling (8)
1	3	0	0	+	1	-	
2	2	0,693	0,69	-	1	-	
3	3	1,099	1,093			-	
4	3	0,693	0,331	+	2	+	Performed
5	2	1,099	0,445	+	1	+	Performed
6	4	0,693	0,635	-	3	+	
7	4	1,386	1,181	-	1	-	
8	2	0	0	+	1	+	
9	2	1,609	1,095	+		-	
10	4	1,386	1,293	-	1	-	
11	2	0,693	0,291	+	1	+	
12	4	1,609	1,382	-	1	-	
13	5	1,609	1,522	-	1	-	
14	4	1,792	1,713	-		-	
15	2	1,792	1,536	-		-	
16	3	1,946	1,811	-		-	
17	3	1,946	1,856	-		-	
18	4	1,946	1,714	-		-	
19	2	1,946	1,763	-		-	
20	2	1,946	1,605	-		-	

According the used metrics, the obtained results were as follow: DR = 95%, FP = 05%, FN=0%. In the cases where there is no DDoS, only few routers have proceeded to mitigation (one or two among 20 routers). For the cases where a DDoS was conducted, approximately only half of the routers having detected the DDoS have proceeded to traffic mitigation. According to a previous work having proposed a collaborative entropy based detection (Francois et al., 2012), it can be noticed that the average performance of the proposed method is better than the average performance of the considered work. Indeed, the obtained detection rate (DR) is higher than the average one of the involved method in comparison, which scores a detection rate between 78.7% and 90.5%, and a false positive rate between 6.8 and 10.3%.

According to the obtained results it can be stated state that the proposed method can efficiently detect DDoS attacks in the overall of the network, despite that no information or knowledge is

Figure 5. Entropies at all the routers of the network: Entropies in cases of an ongoing DDoS are significantly low, compared to the ones corresponding to the safe traffic. If the entropy at a given router is drastically low, the router is self-selected for traffic throttling.

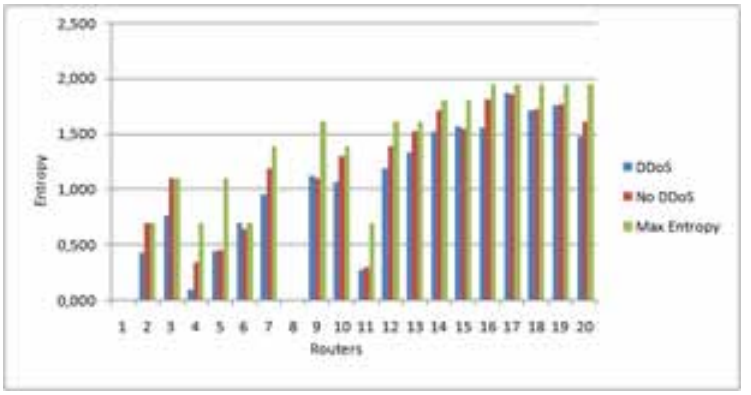


Table 5. Overall results for 20 simulations, where the 10 first ones a DDoS was simulated, and for remainder the traffic was simulated as safe (no DDoS)

No.	Is DDoS simulated ?	Nbr. of Routers with initial decision	Nbr. of Routers with final decision	Overall Decision	Nbr of Throttling routers
1	No	7	5	No	1
2	No	8	6	No	2
3	No	10	11	Yes	4
4	No	6	4	No	2
5	No	6	4	No	1
6	No	6	5	No	2
7	No	5	4	No	1
8	No	7	5	No	2
9	No	6	4	No	2
10	No	5	4	No	1
11	Yes	14	16	Yes	7
12	Yes	15	16	Yes	7
13	Yes	13	14	Yes	6
14	Yes	14	15	Yes	6
15	Yes	15	17	Yes	7
16	Yes	15	16	Yes	7
17	Yes	15	15	Yes	6
18	Yes	16	16	Yes	7
19	Yes	16	17	Yes	7
20	Yes	15	16	Yes	6

explicitly represented anywhere in the network. Indeed, it is just the exchange of decisions between neighboring routers that allows to confirm or to infirm if a DDoS is in progress in the network or not. Some of them proceed to traffic throttling according to their traffic bias, expressed by the entropy of the distances traveled by the incoming packets. During experimentation, it has been noticed that the routers near the bots that generate the malicious traffic, are those which likely detect the attack and proceed to its mitigation. High bias of the traffic was recorded at these routers where the anomaly is easily noticed. Contrary to several work having used entropy with source addresses, distance-based entropy was adopted. Such a choice does not allow the packet spoofing because TTL values are hard to prevent, contrary to source addresses.

It has been also introduced through this paper a novel method to select the routers that proceed to DDoS mitigation. It consists of selecting the routers with drastically low entropies. It has been shown that these routers are those close to the bots that conduct the attack. Moreover, such routers are self-selected based on their own entropies, and no communication among them is needed. Considering the overall detection results (Table 5), it can be established that the proposed method is sensitive to DDoS detection where several routers were alerted despite it was the case of safe traffic (number ranging from 4 to 6, shown on rows 1..10 of Table 5). However, such alerts do not involve mitigation in all the alerted routers. Only some of them are selected for mitigation (1 or 2 routers). For the cases where a DDoS was simulated, the number of routers having detected the DDoS and those that were selected for mitigation is widely higher (respectively ranging from 14 to 17 for detection and from 6 to 7 for mitigation). According to its architectural and decisional aspects that can easily implemented, the proposed method for DDoS detection and mitigation, introduced in this paper, should allow security developers to integrate collaboration within their developed tools for DDoS detection, and in general for several security issues, such most of the cyber threats including botnets and malwares.

CONCLUSION

A new distributed and collaborative method for DDoS detection in WAN and WSN was introduced in this paper. Traffic anomaly detection is based on distance entropy that is computed periodically at each router in order to establish an initial local decision. Then local decisions are shared between neighboring routers in order to reinforce their certainty if a DDoS in in progress in the network or not. The proposed method can be qualified as fully distributed and scalable, because it does not require any central control. A decision if DDoS attack is ongoing is established in 2 levels: At the router level an initial local decision based of distance entropy is calculated. At the neighborhood level each router that has detected a traffic anomaly checks if there a majority decision within its neighborhood to confirm its local decision. The obtained results from simulation have shown that the proposed method enhance detection accuracy and reduce false positives. So, on the practical aspect, the proposed method is suitable for developing new DDoS collective detection systems that can be deployed on WAN and WSN and for which it is hard for hackers to spoof IP packets and hide attacks. On the theoretical aspect, the proposed method can be considered as a general framework for collective decision in distributed and collaborative systems. However, it remains a major limitation of such distributed approach that consists of accessing all the hosts and the routers of a network in order to install the local detectors. As perspectives of this work, several measures in addition to distance-based entropy can be associated. Also, more evolved statistical models are suitable to use, such as markovian models for decision, where an agent at a given router decides according to only its previous states. It is expected that such a decision model enhances the decision time and accuracy at the routers.

REFERENCES

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures. *Computers & Security*, *74*, 144–166. doi:10.1016/j.cose.2018.01.001

Behal, S., Kumar, K., & Sachdeva, M. (2017). Characterizing ddos attacks and flashevents: Review, research gaps and future directions. *Computer Science Review*, *25*, 101–114. doi:10.1016/j.cosrev.2017.07.003

Behal, S., Kumar, K., & Sachdeva, M. (2018). D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events. *Journal of Network and Computer Applications*, *111*, 49–63. doi:10.1016/j.jnca.2018.03.024

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys and Tutorials*, *16*(1), 303–336. doi:10.1109/SURV.2013.052213.00046

Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2016). E-ldat: A lightweight systemfor ddos flooding attack detection and ip traceback using extended entropy metric. *Security and Communication Networks*, *9*(16), 3251–3270. doi:10.1002/sec.1530

Cha, S. K., Moraru, I., Jang, J., Truelove, J., Brumley, D., & Andersen, D. G. (2011). Splitscreen:Enabling efficient, distributed malware detection. *Journal of Communications and Net-works*, *13*(2), 187–200. doi:10.1109/JCN.2011.6157418

Chang, V., Kuo, Y., & Ramachandran, M. (2017). Cloud computing adoption framework: A security framework for business clouds. *Journal of Future Generation Computer Systems*, *57*, 24–41. doi:10.1016/j.future.2015.09.031

Claffy, K. (2001), CAIDA: Visualizing the Internet. Internet Computing, p. 88.

Devi, S. R., & Prriyadarshini, M. A. (2020). A review on detection of DDoS attacks using supervised learning techniques. *International Journal of Advanced Science and Technology*, *29*(04), 54–81.

Francois, J., Aib, I., & Boutaba, R. (2012). Firecol: A collaborative protection network for the detection of flooding DDoS attacks. *IEEE/ACM Transactions on Networking*, *20*(6), 1828–1841. doi:10.1109/TNET.2012.2194508

Indirani, G., & Selvakumar, K. (2012). Swarm based detection and defense technique for malicious attacks in mobile ad hoc networks. *International Journal of Computers and Applications*, *50*(19), 1–6. doi:10.5120/7915-9258

Jia, W., Doss, R., Yu, S., & Zhou, W. (2010). Traceback of DDoS attacks using entropy variations. *IEEE Transactions on Parallel and Distributed Systems*, *22*, 412–425.

Kamble, A., & Bhutad, S. (2018), Survey on internet of things (IoT) security issues and solutions. In *2nd International Conference on Inventive Systems and Control (ICISC*), pp. 307–312.

Kumarasamy, S., & Asokan, R. (2011). Dietributed denial of service (DDOS) attacks detection mechanism, International Journal of Computer Science. *Engineering and Information Technology*, *1*(10), 39–49.

Lippmann, R., Haines, J. W., Fried, D. J., Korba, J., & Das, K. (2000). The 1999 DARPA off-line intrusion detection evaluation. *Computer Networks*, *34*(4), 579–595. doi:10.1016/S1389-1286(00)00139-0

Ma, X., & Chen, Y. (2014). DDoS detection method based on chaos analysis of network traffic entropy. *IEEE Communications Letters*, *18*(1), 114–117. doi:10.1109/LCOMM.2013.112613.132275

Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial of service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, *13*(12), 1550147717741463. doi:10.1177/1550147717741463

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). Review: A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, *36*(1), 42–57. doi:10.1016/j.jnca.2012.05.003

Ouerfelli F. Z., Barbaria, K., Bou-Harb, E., Fachkha, C., & Zouari, B. (2018), On the collaborative inference of DDoS: An information-theoretic distributed approach, In14th International Wireless *Communications & Mobile Computing Conference*, (pp. 518–523). Limassol, Cyprus.

SecureList, Kaspersky Lab, (2018) DDoS attacks in Q2 2018. https://securelist.com/ddos-report-in-q2-2018/86537/.

Shieh, C. S., Lin, W. W., Nguyen, T. T., Chen, C. H., Horng, M., & Miu, D. (2021). Detection of unknown DDoS attacks with deep learning and gaussian mixture model. *Applied Sciences (Basel, Switzerland)*, *11*(11), 5213. doi:10.3390/app11115213

Shojaei, M., Movahhedinia, N., & Ladani, B. T. (2011), An entropy based approach for DDoS attack detection in IEEE 802.16 based networks. In *Advances in Information and Computer Security - 6th International Workshop*, (pp. 129-143). Tokyo, Japan.

Sirivianos, M., Kim, K., & Yang, X. X. (2011), Socialfilter: Introducing social trust to collaborative spam mitigation, In *Proceedings IEEE INFOCOM*, (pp. 2300–2308).

Sohal, A. S., Sandhu, R., Sood, S. K., & Chang, V. (2018). A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Journal of Computer Security*, *74*, 340–354. doi:10.1016/j.cose.2017.08.016

Thonnard, O., Bilge, L., O'Gorman, G., Kiernan, S., & Lee, M. (2012), Industrial espionage and targeted attacks: Understanding the characteristics of an escalating threat. In RAID, (pp. 64–85).

Varga, A. (2018), Inet framework for the omnet++ discrete event simulator. https://inet.omnetpp.org

Zargar, S. T., Joshi, J., & Tipper, D. (2010). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys and Tutorials*, *15*(4), 2046–2069. doi:10.1109/SURV.2013.031413.00127

Zhou, C. V., Leckie, C., & Karunasekera, S. (2010). A survey of coordinated attacks and collaborative intrusion detection. *Computers & Security*, *29*(1), 124–140. doi:10.1016/j.cose.2009.06.008

Abdenacer Nafir is an associate professor at 20 Août 1955-Skikda University (Algeria). He is a member of the team Artificial Intelligence of the Laboratory of Informatics and Communication of the University of Skikda (LICUS). His main research interests concern distributed artificial intelligence, multi-agent systems, and distributed intrusion detection systems.

Smaine Mazouzi received his M.S and Ph.D. degrees in computer science from university of Constantine, respectively in 1996, and 2008. He is a professor at 20 aout 1955 university of Skikda and the head of the team Artificial intelligence of the LICUS laboratory (Laboratoire d'Informatique et de Communication de l'Université de Skikda), at the same university. His fields of interest are pattern recognition, machine vision, distributed systems, and computer security. His current research concerns using distributed and complex systems modeled as multi-agent systems in image understanding and intrusion detection. He is member of several national and international research projects in computer vision and computer security.

Salim Chikhi obtained his degree in computer engineering in 1983 at the prestigious computer engineering school of Algiers, Algeria (former CERI currently called ESI). He received his M.S. degree in computer systems from Glasgow University UK, in collaboration with Constantine University, Algeria, in 1993, and the Ph.D. degree in computer science from Constantine University, Algeria in 2005. He has led several international cooperation projects including the laboratory LE2I (now ImVia) of the University of Burgundy, France in the field of embedded systems, wireless networks, sensor networks and the Internet of things architectures, with the school of mines of Saint Etienne, France in the field of logistics, with the engineering school of Valencia, Spain in the field of automatic language processing, and with the MIRACL laboratory, Sfax and Monastir Universities, Tunisia in the field of data sciences. He is the author of twelve book chapters, more than 120 articles. Currently, he is a full professor at the University Constantine2, Algeria. Prof. Chikhi is the head of MISC laboratory (Modeling and Implementation of Complex Systems) and the leader of the SCAL team (Soft Computing and Artificial Life). His research areas include soft computing and artificial life techniques and their applications to real life problems, namely networks and logistics routing, IoT architectures, biometry, optimization, and natural language processing.