Swarm and Evolutionary Computation 38 (2018) 94–108

Contents lists available at ScienceDirect

Swarm and Evolutionary Computation

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

Adaptive artificial immune networks for mitigating DoS flooding attacks

Jorge Maestre Vidal*, Ana Lucila Sandoval Orozco, Luis Javier García Villalba

Group of Analysis, Security and Systems (GASS), Department of Software Engineering and Artificial Intelligence (DISIA), School of Computer Science, Office 431, Universidad Complutense de Madrid (UCM), Calle Profesor José García Santesmases s/n, Ciudad Universitaria, 28040 Madrid, Spain

ARTICLE INFO

Keywords:
Anomalies
Artificial immune system
Denial of Service
Forecasting
Intrusion detection system
Network

ABSTRACT

Denial of service attacks pose a threat in constant growth. This is mainly due to their tendency to gain in sophistication, ease of implementation, obfuscation and the recent improvements in occultation of fingerprints. On the other hand, progress towards self-organizing networks, and the different techniques involved in their development, such as software-defined networking, network-function virtualization, artificial intelligence or cloud computing, facilitates the design of new defensive strategies, more complete, consistent and able to adapt the defensive deployment to the current status of the network. In order to contribute to their development, in this paper, the use of artificial immune systems to mitigate denial of service attacks is proposed. The approach is based on building networks of distributed sensors suited to the requirements of the monitored environment. These components are capable of identifying threats and reacting according to the behavior of the biological defense mechanisms in human beings. It is accomplished by emulating the different immune reactions, the establishment of quarantine areas and the construction of immune memory. For their assessment, experiments with public domain datasets (KDD'99, CAIDA'07 and CAIDA'08) and simulations on various network configurations based on traffic samples gathered by the University Complutense of Madrid and flooding attacks generated by the tool DDoSIM were performed.

1. Introduction

By definition, Denial of Service (DoS) has the objective of disabling computer systems or networks. The DoS attacks with origin in multiple sources are referred as Distributed Denial of Service (DDoS) attacks. In recent years, the number of incidents related with these threats reported by the various organizations for cyber defense shows an alarming growth. According to the European Network and Information Security Agency (ENISA), between 2013 and 2014 an increase of 70% was observed [48]. In addition, they pose a threat that has begun to be used in order to achieve other objectives. These include disguising activities in relationship with malware spreading, concealment of fraudulent money transfers [61] or compromising anonymous networks, such as Tor or Freenet [35]. This growth is attributed to various reasons: the first of them is that DDoS attacks are usually triggered by previously infected systems, which in most of the cases are part of botnets. The botnets have been adapted to be resilient against the classical detection schemes, thus allowing the construction and maintenance of larger collections of zombies and increasing their difficulty to be identified. [60]. Another important reason is that attackers are able to take advantage of amplifying elements, in this way enhancing their potential to be harmful. To do this, they exploit vulnerabilities in protocol implementations on the intermediate network devices, particularly at DNS, NTP and SNMP. On the other hand, as the European Police Office (Europol) warns [25], the DDoS is becoming increasingly linked with the organized crime. Rent botnets for execution of these attacks is a very profitable business on the black market, often supplied as Crimeware-as-a-Service (CaaS). Finally, offenders with lack of formation have a wide variety of tools for easily configuration and deployment of flooding attacks. The black market also offers technical support, a situation that expands the range of user profiles which are able to attack with success.

The most common DDoS methods are based on flooding. Because of this, they are the principal object of study in this research. The flooding attacks modus operandi involves the injection of large volumes of traffic in order to saturate the victim systems [70]. The popularity of this group of DoS attacks is mostly due to cheap price and simple implementation, in comparison with the good results they provide. Thus, there are lots of proposals aimed at their detection and mitigation. However few of them meet all the requirements to be effective in real use cases, emphasizing the needs of high true positive rates, unrepresentative false positive rates, low consumption of computational resources and real time performance. In addition it is noteworthy that proposals of the literature seldom consider advantages

* Corresponding author.
E-mail addresses: jmaestre@ucm.es (J.M. Vidal), asandoval@fdi.ucm.es (A.L.S. Orozco), javiergv@fdi.ucm.es (L.J.G. Villalba).

http://dx.doi.org/10.1016/j.swevo.2017.07.002
Received 23 November 2016; Received in revised form 5 May 2017; Accepted 3 July 2017
Available online 04 July 2017

of the new trends on networking. It is expected that the emerging networks, taking the example of 5G, increasingly move towards self-management. The use of novel technologies such as Software-defined networking (SDN), Network-Function Virtualization (NFV), Artificial Intelligence or Cloud computing, facilitates the design of Self-Organizing Networks (SON). This should encourage the appearance of more interesting proposals that are capable of reacting with a much more comprehensive view of the problem being treated.

To serve this cause, a strategy for detection and mitigation of DDoS flooding attacks is proposed. Therein the deployment of a sensor network that integrates an Artificial Immune System (AIS) inspired by the biological defense mechanisms of human beings is introduced. Unlike similar proposals, conventional bio-inspired methods for pattern recognition were not applied. Instead a combination of strategies for DDoS detection based on the study of variations of the entropy on the network traffic by thresholding, with the adaptation of the biological immune reactions is proposed. This makes it possible to apply real time countermeasures, building an immune memory and establishment of quarantine areas, all in accordance with the current state of the protected network.

In view of this, it is important to highlight the two major contributions of this paper: firstly, a new method for detecting DDoS that is able to forecast anomalies on the entropy of the traffic analyzed, and thereby recognition of flooding attacks is introduced. This is performed by representation of the entropy in time series and the definition of prediction intervals. It has been evaluated considering public domain datasets (KDD'99 [37], CAIDA'07 [15] with CAIDA'08 [16]) samples, and traffic monitored in the University Complutense of Madrid (UCM) and flooding attacks generated by the tool DDoSIM [22]. The first two allow its comparison with previous detection approaches, and the latter offers a more realistic view of its behavior. The preliminary experiments showed promising results, which motivates the development of a cooperative deployment strategy. This is the second main contribution, where a method for management of immune agents that implements the previously described detection system is proposed. Within this, the decisions are made as to when and how they will act and in what level of restriction, all this depending on the status of the network and orchestrated by an artificial immune approach. To evaluate the effectiveness of the deployment of the AIS, a simulator capable of generating traffic distributions and different networks with various locations of the sensors acting as immune agents has been implemented. In the generation of new networks, several parameters had been taken into account: number of nodes, legitimate traffic volume, branching component, and cyclic component; demonstrating in all of them the improvements offered by the cooperation and the emulation of the defensive capabilities of the biological immune systems.

The paper is divided into seven sections, and the first of them is the present introduction. The background necessary for a better understanding of the approach is described in Section 2. The proposed AIS is introduced in Section 3. The novel DDoS detection method implemented in the various agents of the AIS is detailed in Section 4. Experiments, datasets and methodology are described in Section 5. Results are discussed in Section 6. Finally, conclusions and future work are presented in Section 7.

2. Background

The following describes all aspects necessary for understanding the proposal. Among them it is important to highlight those involving the characteristics of the DDoS flooding attacks and their countermeasures, a general review of the human being immune system and the different approaches with this in mind, in order to provide defenses against cybercrime.

2.1. Flooding threats: Attacks and countermeasures

According to [67], there are two types of traffic injection able to compromise a system or network by flooding. The first one is based on the constant and continuous generation of large volumes of information, and is well known as high rate flooding. This is a method which is usually very visible that easily overflows the computing capacity of the victim. On the other hand, the victim may be compromised by less noisy attacks, which are able to exploit vulnerabilities in the various communication protocols. They are known as low rate flooding attacks, using as a typical example, the attacks with On/Off patterns addressed against the TCP [62,42]. In both cases, the malicious traffic may be sent to the victim in a direct or reflected way [12,6]. There are different ways of exploiting the capacity of the flooding attacks, as is the case of the link-flooding and target link-flooding attacks [66,28]. They are based on depleting the bandwidth of the victim by aiming to certain network links or target regions. Since they concentrate the flood at specific points of the network and are able to reuse legitimate traffic to congest the victim, they are often much more difficult to detect than the conventional threats. Most efforts of the community to deal with denial of service assume these behaviors, and from them different methods for detection, mitigation and identification of sources are proposed. Their most important features and evaluation schemes are described below.

The detection of the attacks is often necessary to conduct either of the other defensive reactions. This is based on the analysis of traffic that flows through the protected environment, looking for signatures of previously known attacks or anomalous behaviors. For that purpose various techniques have been proposed, such as probabilistic models based on Markov [58], Genetic Algorithms (GA) [41], Chaos theory [20], CUSUM statistical analysis with wavelet transforms [17], forensic methods based on visualization [14], SVM (Support Vector Machines) [3,5], k-means [31], decision trees [52,53], artificial neural networks [43,59], fuzzy logic [40] or the study of variations on the traffic entropy [51,12]. In approaches like [72], the problem of the similarity of the nature of the DDoS attacks in comparison with non-malicious events is studied. This is the case of the well-known situations such as flash crowds, which often occur when a large amount of legitimate users converge on a certain service in a short time interval.

The total or partial reduction of the damage inflicted by the attacks is defined as mitigation. To do this, it is common to use honeypots [33], puzzles that recognize non-human users [73], bandwidth enlargement [38], reputation-based schemes [45], filtering or the adoption of security protocols such as IPsec [25]. As can be observed, the set of mitigation actions may also contain prevention strategies. These are characterized by not having direct dependence on the attack detection [46].

To find the compromised systems from which the malicious traffic is originated is referred to as the identification of their sources. Ideally, its objective is to track the cybercriminal. However, given the administrative difficulties that this process involves (different Internet Service Providers (ISPs), proxies, data privacy legislations, etc.), and the recent advances on footprint occultation, this goal is often very hard to carry out successfully. Consequently, many of the proposals in the literature just focus on getting as close as possible to the attacker, in order to sanitize the largest amount of regions within the protected network. On the identification of sources, the packet traceback is the most frequent approach. In [4] this issue is discussed, a lot of current approaches are collected, and a new scheme for uniform tracking is proposed. The Passive IP Traceback (PIT) that bypasses the deployment difficulties of the conventional IP traceback techniques by investigation of ICMP error messages is proposed in [69]. Finally, in [36,69] the influence of the characteristics of the network topology on the effectiveness of the strategies for packet marking is studied.

The evaluation of defense systems against DoS/DDoS is a controversial issue today. Over the years, various collections of traffic samples and methodologies for assessment of these tools were pro-

posed. They are mainly based on public domain datasets containing both legitimate traffic and DoS/DDoS threats. The malicious content usually corresponds with real traffic captures (KDD'99, DARPA'99, FIFA World Cup'98, etc.) or traffic generated by tools that imitate the behavior of the real attacks (D-ITG, Harpoon, Curl-loader, DDOSIM, etc.). In [11] each of them is discussed in depth, and the lacks on the current verification methods are summarized. Thus they conclude that the traffic captures which were traditionally applied are outdated and widely disparate of the current traffic. For this reason, it is recommended to consider only CAIDA 07 [15] among them, labeled as the best of the bad solutions. On the other hand, the use of simulation tools entails the loss of realism. Also it is difficult to compare new proposals with those on the bibliography [40]. This is because every paper defines their own scenarios of experimentation according to their requirements.

2.2. Human beings immune system

All living beings have developed multiple immune mechanisms, emphasizing among them defenses of vertebrate species due to their sophistication. Many types of proteins, cells, organs and tissues form part of these systems, and they are related through an elaborate and dynamic network. As part of this more complex immune response, the human immune system, over time, adapts to recognize specific antigens, which is called adaptive immunity. The defense mechanisms compose the innate immunity, and usually are the first line of protection.

Each component of the innate immunity is able to recognize and eliminate different types of antigens. They are mainly rejection reactions conducted by external physical barriers such as skin or mucous membranes, and internal defensive elements like Natural Killer (NK) cells or phagocytes. They lack immune memory, and are only effective against pathogens known as priori.

On the other hand, the adaptive immunity presents specificity, i.e., after learning how to identify and reject an antigen, the knowledge gained allows it to react more firmly against the intruder, by generating new and stronger agents; but they can only act for mitigating the threat for which they were created. The most important cells involved in this process are lymphocytes and presenting cells, and the most important adaptive immune responses are humoral and cellular. In both of them take part agents responsible for antigen recognition and disposal. Given they pose a good example of this process, are briefly explained below.

- *Humoral response.* The antibodies detect and eliminate the threats by swallowing them. The remains of this process are captured by T_h lymphocytes, and these stimulate the T_b lymphocytes to generate an even greater amount of antibodies specialized in recognizing the threat. Antigens never seen before are identified by the antibodies that have suffered small mutations in their construction process, allowing them to recognize different antigenic determinants.
- *Cellular response.* The T_h detect the intrusions. Then they attract T_c cells for disposal. As in the previous case, the remains stimulate the generation of T_h and T_c, specializing them against the new threat. In addition, the recent T_c are often able to identify the antigen.

In both reactions, increasing defensive measures is temporary. After a quarantine period, the system is regulated by removing the excess of agents. These are programmed to die by apoptosis, also known as cell death.

Acquired immunity is the basis of the vaccination in human beings. When samples of an antigen are detected, the organisms deploy temporary and specific countermeasures for disposal. Therefore the response is faster and more effective than in the first contact.

2.3. Artificial immune systems

The adaptation of biological defenses towards information security is usually performed by deployment of multi-agent systems [50]. In pioneering approaches, such as [39,32], the main guidelines for the emulation of the activities carried out by immune cells were introduced. They often apply some of the four classical bio-inspired algorithms: negative selection, clonal selection, artificial immune networks and Danger Theory (DT), which are briefly described below.

Negative selection is the process by which the immune agents learn to distinguish antigens from the cells of the organism itself. In [71] there is a good example of its application for detection of anomalies. But as the authors suggest, it poses a methodology that tends to generate high false positive rates, a situation that often leads to its complementation by clonal selection algorithms [44]. These are based on the assumption that every lymphocyte at its growth stage must be able to react against a specific antigen before being released in the body. Clonal selection is an effective solution to problems of recognition and optimization [18]. In proposals like [57], it is also applied for identifying malware, often assuming an important refining step over negative selection.

The immune networks stem to the idea of extending clonal selection to networks. They are commonly implemented as a channel of interaction between the different actors of AIS. In [55] there is an example of an immune network for connecting different agents that perform negative selection. In [68] a similar deployment is adopted, but this time involving agents that apply Danger Theory.

The Danger Theory takes into account the latest advances in medical research. Consequently and unlike their predecessors, it rejects the idea that organisms have the capacity to distinguish between own cells and antigens. Instead it postulated that the triggering of immune reactions is originated by warning signals sent from tissues in direct contact with the threat. Because of its novelty, it is one of the most common algorithms in the bibliography of recent years. In [1] the bases for its adaptation to intrusion detection are defined. DT is applied to recognition of enumeration attacks in [29], and it is also considered for intrusion detection based on studying the system calls of the protected environment in [7].

Despite the predominance of these methods in the bibliography, not all AIS are based on such specific processes of the biological immune systems. Some approaches imitate the global behavior of the innate and adaptive immune responses on the vertebrate beings, without following predefined algorithms. This makes it easier to combine the defensive strategies used in each field, with the ideas provided by biological immune systems, by this way reaching solutions that best fit the real use cases. A good example of this is proposed in [13], where this idea is implemented to detect anomalies in network traffic. To do this, six main classes of agents are considered, among which are distributed sensing, communication and reaction tasks. Their adaptive immune response involves the cloning of a greater number of antibody agents in the threatened regions, by this way increasing their presence on the protected environment. In [19] antibodies are mobile agents that swarm the network looking for indicators of damage. Another example is [64], wherein when the immune agents identify a potentially harmful incidence, the adaptive reaction is triggered. This entails the increase of the weights of the monitored features, thus gaining restrictiveness and specificity. Finally, in [63] a solution to some of the attacks that affect mobile networks is proposed. As in previous approaches, its behavior is based on cloning the agents that have been able to recognize a specific threat.

3. Biological immune reactions against DDoS

To design a bio-inspired system for detecting and mitigating denial of service attacks requires being aware of certain aspects of both threats to be treated and features of the defensive deployment. In order to

establish the limitations and goals of this approach, the following describes the most relevant assumptions and requirements that have been taken into account throughout its development.

- The denial of service attacks to be treated may originate in one or more sources. In addition, they acquire the ability to take alternative routes to the victim, adapted to network conditions, such as filters that drop malicious traffic or congestion.
- Malicious traffic may harm the protected network in different places: proximities to victim nodes, intermediate network actors, or close to their source. Once a section is compromised, it is possible that a chain reaction leads to the compromise of the others.
- When a region on the protected environment is victim of a flooding attack, it must be quarantined until any hint of aggression disappears. In this way it is possible to provide proactive perimeter security.
- Although a region is in quarantine, the legitimate traffic should continue flowing through it practically in its normal rhythm. In other words, the quarantine should not block sections of the network nor prejudice their quality of service in a representative manner. Otherwise, the attacks achieve their goal.
- Mitigation actions should be performed as close as possible to the source of the threat. Thus the amount of network regions at risk is reduced, and the identification of the attacker is facilitated.
- Communications between the various immune agents must be performed through secure channels, in this way preventing that the attacker exploits them.
- Immune agents must be able to be activated/deactivated according to the state of the protected network.
- Defensive action must be proportionate to the risk to be treated. Thus the impact of the autoimmune reactions triggered by false positives is reduced.
- In order to enhance the alert correlation processes and the tasks performed by human operators, a record should exist which collects the current state of the network, the different immune reactions and their effectiveness. Nevertheless, it is out of the scope of this paper to deepen in how to manage this information, as well as how to associate incidences discovered by the proposed scheme with events related with threats of different nature (ex. link a mitigated DDoS attack with a botnet detected by other defensive elements). In the bibliography there are different approaches that address this problem from the perspective of the new generation networks, as is the case of [9,8].

As can be observed, these premises meet an important part of the needs of the current networks. However there are other aspects that have been set aside, highlighting among them the fight against the various evasion strategies. These contain methods for disguising the source of the attacks or hinder the tracking of the flooding path (Fast-Flux, Domain Generation Algorithms (DGA), exploitation of anonymous networks, etc.) [70,2]. On the other hand, there are algorithms designed for misleading the detection system and thus do not triggering countermeasures, such as those proposed in [51]. Their consideration involves adding a lot of complexity to the proposal, and because of this, it is out of the scope of the paper. Another important aspect that is also delegated to future work is to facilitate the interoperability with security protocols and data protection policies. We understand that analyzing obfuscated headers also means an important increment on its complexity, not being recommended for a first approach. Bearing this in mind, the architecture, behavior and properties of the proposal are described in depth below.

3.1. Architecture

The proposed system has distributed architecture and its different actors assume the various roles of the biological immune systems. Its success depends mainly on two types of agents spread along the protected network: H detectors (D_H) and A detectors (D_A). D_H are involved in the innate immune response and in the adaptive response. Consequently they are capable of recognizing and blocking new attacks, and they participate in the construction of the immunological memory. On the other hand, D_A have the ability to detect and mitigate the attacks previously identified by D_H assuming a very important role in the adaptive response.

In Fig. 1 an example of their deployment is shown. Apart from D_H and D_A, other important components take part in the immune process, which are defined below.

- *Protected network*. The protected network is defined as the network segment that connects the attacker with the victim, and where the AIS is operating. Therefore, it is the element to be protected and the main scenario of different immune reactions.
- *Intermediate nodes*. Every node on intermediate subnets between the attacker and the victim that is not capable of detecting, mitigating or taking part in the immune reactions is defined as intermediate node.
- *H detectors*. The immune system agents as nodes that perform innate reactions, and are capable of triggering adaptive reactions are defined as H detectors or D_H. In particular, they host VNFs with the detection/mitigation capabilities related with the innate responses.
- *A detectors*. The immune system agents as nodes that only perform adaptive reactions are defined as A detectors or D_A. They host VNFs with the detection/mitigation capabilities related with the adaptive response.
- *Orchestrator*. The Orchestrator performs the tasks of NFV M & O (Management and Orchestration) standardized by the ETSI, among them covering the orchestration and lifecycle management of physical and/or software resources that support the infrastructure virtualization, and the lifecycle management of the VNFs [24]. In addition, it acts as mediator between the immune agents, which includes the tasks of scope delimitation on the activation signals triggered at the immune responses, management of quarantine areas, separation of the AIS control data with respect to the protected network traffic and information gathering.
- *Protected connection*. Every connection between nodes on the protected network over which the proposed AIS acts is defined as protected connection.
- *Control channel*. The connections between the Orchestrator and immune agents are referred as control channel.

The distribution and cooperation of the various components of this architecture allows performing innate and adaptive responses to attacks. The deployment of an Orchestrator on a different data plane from the protected network connections provides autonomy, prevents that the traffic generated by the AIS penalize QoS, and facilitates the

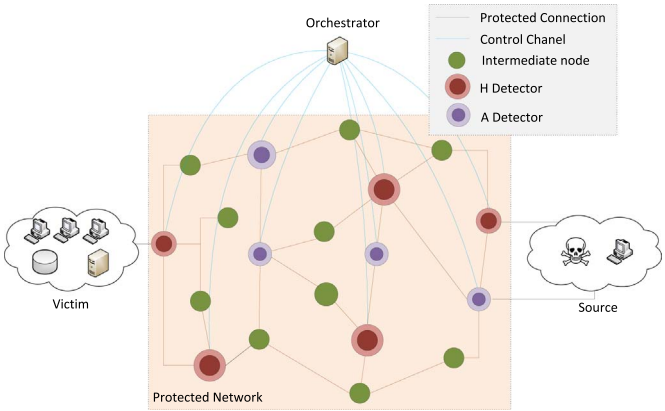

Fig. 1. Example of distribution of the different actors in the AIS.

adoption of security protocols, thus reducing the risk of packet poisoning or Man-in-the-Middle attacks. But despite its obvious benefits, it is optional, because in certain use cases it is not possible to have much control of the protected environment (law restrictions, privacy, etc.). In this situation, the immune agents may have sufficient autonomy to do without it, which involves: being in direct contact with agents over which it has influence, saving a log with the performed actions and determining whether it belongs to a region in quarantine or not (and the consequences that this entails). Usually these actions can be carried out easily, as for example by the implementation of tunneling between agents for their communication, the use of counters to determine the quarantine period, etc. but not with the global overview of the protected network and the advantages that the Orchestrator provides.

3.2. Artificial immune responses

Each response conducted by the proposal is subject to conditions and events that emulate the behavior of the biological immune systems. With this in mind, the behavior of the AIS is mainly conducted by two different artificial immune responses: innate and adaptive.

3.2.1. Innate response

As in biological systems, the innate immunity on the approach is the first line of the defense strategy. It aims to identify and mitigate new threats and protect H detectors of disablement by flooding. The process of innate immunity requires maintaining activated D_H agents along the protected network. These agents implement VNFs as IDS that monitor the entire traffic flowing through them looking for suspicious anomalies. Therefore, detected attacks must present certain evident characteristics related to considerable fluctuations in the analyzed traffic distribution. Once a threat is identified, the mitigation measures consist mainly on the adoption of directives that restrict the communications with nodes, ports or services involved in the attack vector. We are aware that more sophisticated mitigation actions could be implemented, but their decision and development are delegated to future studies in order to facilitate a better understanding of this first approach.

The innate response provides quick and efficient countermeasures, requiring no communication with the Orchestrator prior to their launch. By recognition and elimination of pathogens before they enter into the system, the proposal innate response emulates the behavior of the immune system of human beings. This is because it acts in the same way as the various external physical barriers or cells, and without specificity. In addition, it should be noted how agents involved in this task act coincide with those of most conventional Intrusion Prevention Systems (IPS), i.e. IDS with the ability to apply basic countermeasures.

3.2.2. Adaptive response

The adaptive response is the next defensive step in the proposal. It is triggered every time a D_H agent recognizes a new threat, which implies that they must hold at least a short memory capable of storing their latest decisions. In this context, determining when an attack is Non-Seen-Before (NSB) implies it is not presence in the immune memory. Because of this, that memory has a very important role in the AIS decision-making. Determination of how the immune memory will be implemented is not usually a trivial problem. With this purpose, the two more intuitive schemes to take into account are those centralized or distributed. When the immune memory is centralized, is sustained by the Orchestrator. In this case this component is responsible for determining whether an incidence is NSB, considering information provided by all the sensors. However, if it is distributed, each detector disposes only the information gathered for itself, or by a group of close sensors. Hence an attack tagged as NSB by an agent could not be new for other detectors. This second approach provides greater autonomy to the agents and allows some of them to trigger different adaptive reactions against the same pathogen. It also turns out to be a more efficient approach, where agents have the ability to make decisions based on information that they manage. In general terms it facilitates their design, and also eliminates the existence of a single point of failure in the system, which makes it stronger against disabling attempts. But it also has disadvantages: the VNFs that implement de immune capabilities demand the consumption of a greater amount of resources (memory, energy, hardware, etc.). On the other hand, since the Orchestrator no longer manages the memory, an information management strategy adapted to the needs of the agents must be established. Finally, the sensors ignore if the information encapsulated in the monitored packets belong to continuous data flows, hence limiting the decision making to the traffic only visible by the VNF, and being easier to deceive by evasion techniques; this could also worsen the accuracy of quarantine regions in time and space. Note that despite these disadvantages, and bearing in mind the efficiency of the distributed approach, it was implemented at the experimentation stage of this research.

Once the adaptive reaction is released, the D_H that identified the attack sends activation signals to the D_A agents in close proximity via the control/management plane of the Orchestrator. The scope of these signals can be determined in different ways. It may affect the surrounding neighbors, nodes on a certain region or network devices in specific routes previously established by the Orchestrator. This also enables the application of Artificial Intelligence and Data Mining in order to research their optimal propagation, giving many possibilities for future works. For simplicity the first of the previously mentioned alternatives was implemented.

Then the activated D_A agents instantiate VNFs that analyze traffic flowing through them. Unlike D_H, their detection engines increase restrictiveness in proportion to the flood of the attack, usually acting much more stricter than D_H. In this way it is prevented that the division of the attack flow reach the victim by alternative routes, assuming that when it is split, it becomes less noisy and hence more difficult to be detected. In order to prevent this measure resulting in a substantial increase in the false positive rate, specificity is taken into account. To ensure specificity, they are only able to apply countermeasures against the threat that has activated them, which imply that a specific VNF with analysis capabilities is instantiated for each discovered threat. Therefore, they can only take action against several attacks if they have been activated to mitigate each of them. The attacks are distinguished taking their source as main criterion, as is detailed in Section 4.4. Because of all of this, and as in nature, the artificial adaptive immune response involves the increase of the amount of effectives able to react against a certain triggering attack.

At the end, the deployed countermeasures are effective for a certain period of time. While the threat persists, the immune response remains activated. If it is no longer visible, a quarantine period is activated. The quarantine is interrupted only upon detection of replicas of the intrusion (implying back to the previous state), or when the countdown expires. The network segments covered by a set of D_A agents active against a specific threat and coordinated by the same D_H sensor, are their quarantine region.

3.3. Implementation

The behavior of the artificial immune responses is implemented in the following procedure:

1. At first, VNFs in D_H analyze all the traffic flowing through them. D_A remain on standby waiting to be activated.
2. When the D_H identify malicious traffic, the related connections will be blocked. This is an innate immune response. Then, the Orchestrator warns the D_A surrounding to proceed with the activation of countermeasures and the implementation of specific VNFs with the required analytical/mitigation capabilities. In this way the

adaptive immune response is triggered. The warnings contain information about their origin and the malicious flow characteristics.
3. When activated for a specific threat, the D_A analyze the traffic from their potentially harmful sources. Unlike in D_H, the level of restriction of their decision threshold are increased according to the characteristics of the triggering attacks. They also block the identified threats. Thus, if the attacks cross alternative paths, they are also mitigated.
4. In the case that different D_H emit activation signals for the same attack, the corresponding VNFs apply the most restrictive one.
5. The D_A deactivate the VNFs just in case a period of time without news of the attacker has passed, or triggering signals have not been received.
6. D_H remain vigilant to face new incoming threats.

An example of the behavior of the proposed AIS when dealing with DDoS flooding attacks is described in Fig. 2. It is part of the situation shown in Fig. 2a, where S is the source of the attack, T is the target, and each N_i is an intermediate node located at i. In the case that the sensor D_H is unable to recognize the threat, it is propagated along the protected network via different routes and according to the load balancing policies, as shown in Fig. 2b. But if the attack is successfully detected, the innate immune response is initiated. Thus the traffic from S is discarded, slowing the advance of the intrusion, as shown in Fig. 2c. As a legitimate flow trying to reach its destination when some network incident block its route, the malicious traffic will try to reach the victim for alternative paths. Fortunately, when the threat was detected the adaptive immune response was also triggered. As shown in Fig. 2d, this has led to the activation of the neighboring D_A agents. Consequently, the attack reaching the victim through the new connections is prevented. Fig. 3 summarizes as a flowchart the information processing stages of the proposed system and the relationship between the immune responses.

Despite its simplicity, this scheme has a large number of advantages. Firstly, it increases the defensive measures when a threat is recognized, proportional to the risk level. In addition, the specificity

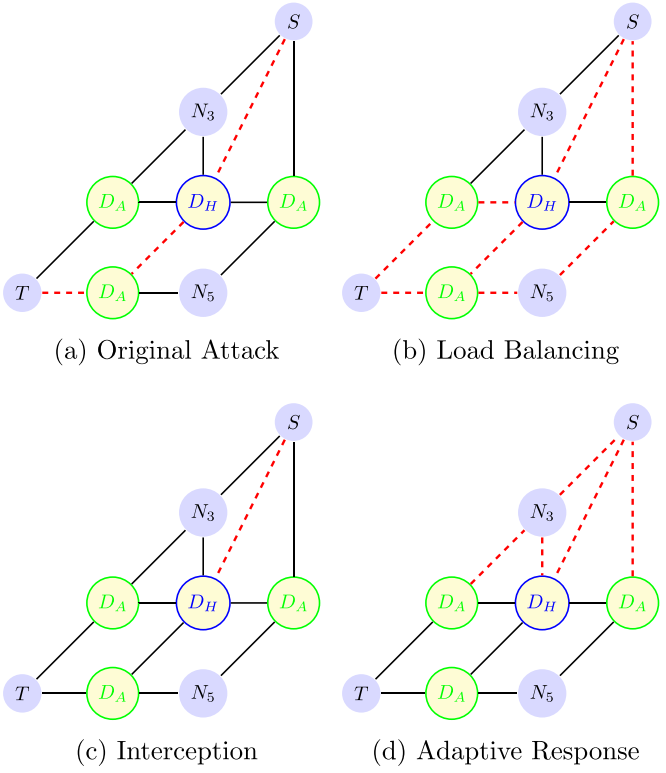

Fig. 2. Example of the AIS behavior.

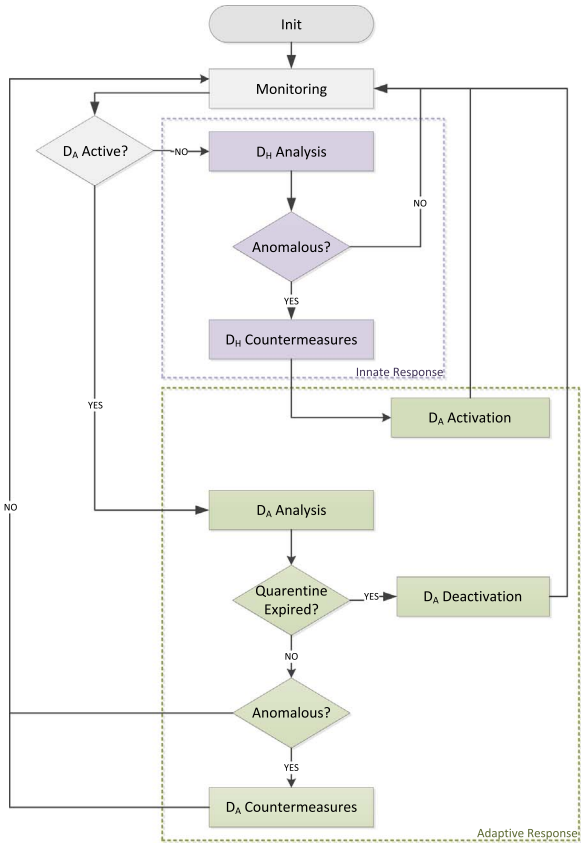

Fig. 3. Flowchart of the proposed AIS.

makes it only occur on specific connections, without affecting other traffic routes and reducing the impact of the false positives. Furthermore, the presence of two types of agents allows it to strategically adapt the defensive network to the monitoring environment. In this way the most powerful computers may act as D_H, and the rest assume the role of D_A. Note that a single node can assume both roles, or even deploy their own virtual network including several of them. On the other hand, the restriction level is self-regulated through deactivation of agents when the quarantine time passes, thus saving resources.

3.4. Properties

One of the main properties of the proposed strategy is its ability to self-calibrate the protection adjustment. In general terms, the implementation of security elements involves a penalty in the protected environment, either in terms of resource consumption, information processing capabilities, scalability, interoperability or quality of service decrease (the latter is directly related to classification errors and the impact of triggering countermeasures) [10]. In order to deploy effective information security strategies, it is necessary to analyze in depth the scenarios to be protected (organization goals, policies, asset identification, assessment, etc.), as well as identifying and evaluating their potential threats. From their analysis, security operators decide the best defensive measures, which must be proportionate to the value of the safeguarded assets [49]. This sets up the main features of the defensive deployment; among them, amount of sensors and their scope, limitations, decision thresholds or straightening against evasion methods.

Consequently, the novel defensive schemes must provide different adjustment options, from which it is possible to adapt them to the information security management guidelines. Because of this, the proposed approach distinguishes two types of defensive elements:

one in charge of providing quick defensive actions (innate response) and if necessary, capable of modifying the security deployment (adaptive response), and other which temporarily extends the defensive measures and adapt its level of restrictiveness to the state of the system; the first are referred as D_H nodes and the second as D_A nodes. This scheme offers among other advantages: low resource consumption and bandwidth penalty when the system is not at risk, self-tuning of defensive measures based on the intensity of the threats, accommodation of the defensive elements deployed to the regions of the network which are most affected by the attacks, and real time recalibration of decision thresholds according to the characteristics of the monitored traffic; which aligns them more closely with the real needs of the information security management strategies. This is an important difference from most of the related work, which mainly consider deployments based on static features. Furthermore, and unlike most of the proposals in the bibliography, this scheme allows to perform in the same strategy: prevention, detection, mitigation and identification of attack sources actions, which make it a much more complete solution.

In addition, the main characteristics of the biological immune systems have been assumed and adapted to the fight against DDoS in the following ways:

- *Innate and adaptive responses*. At the innate response, the proposal has the capacity to react against threats which were not previously recognized. Once detected, it strengthens the defensive measures against future replies as occurs in biological adaptive immune reactions. From the networking point of view, this implies that D_H capabilities are VNFs that act as IDS initially deployed on the protected environment. When the adaptive response is triggered, the Orchestrator distributes the activation signals to the corresponding D_A nodes through the control/management plane. Once activated, the adaptive capabilities of the D_A nodes are temporally deployed via VNFs.
- *Specificity*. In nature each adaptive immune cell reacts against only one type of antigen (unlike the case with innate responses). Bearing this in mind, in this approach the innate response is common to any type of detected threat. However, the immune response affects only the triggering flooding attack. This behavior is achieved through only allowing VNFs related with D_A capabilities act on traffic from the source of the attacks reported by D_H nodes, whether as detection or mitigation countermeasures.
- *Clonality*. When unknown antigens are detected, the adaptive biological response clones the cells that have been able to be recognized. This increases the chance of identifying their replicas. The AIS behaves in a similar way when activating agents after the adaptive response is released. In particular, the activation signals provided by D_H nodes are distributed through their associated D_A nodes by the Orchestrator via control/management plane. The information related with the transmitted information includes adjustments of detection thresholds and the scope of the sensor, which allows the newly incorporated IDS reconfigure to operate with analogy to the sensor that triggered the adaptive response.
- *Immune memory*. Both in nature and this approach, the deployed countermeasures remain active for a period of time. This enables them to react more effectively against future replicates. In order to prevent similar threats, the proposed AIS relies on the Orchestrator or VNFs to maintain this deployment.
- *Self-Regulation*. Once the adaptive response is triggered, the human immune system is regulated by the apoptosis of most of the new cells. In the AIS, defensive measures are also reduced when a certain period of time is exceeded and no replications of the triggering threat are detected, i.e. the Orchestrator send deactivation signals to the VNFs that implement the D_A capabilities via control/management plane.
- *Autonomy*. In both cases, once the entities of the defensive deployment are activated, they operate with complete autonomy. Because of this, the Orchestrator only is able to activate/deactivate the deployed VNFs, hence managing the instantiation of sensors and stabilizing their initial configuration, but without intervening in the rest of their activities.
- *Diversity*. In nature, the set of immune agents must be able to detect any antigen. The same thing happens in the AIS, where specificity is applied only in the deployment of countermeasures. This is possible because the detection strategy is based on the recognition of anomalous behaviors, and not on collections of signatures of previously known attacks.

4. Detection of flooding attacks

The following describes the most important aspects of detection of threats and identification of sources on the approach, which involves metrics, forecasting, thresholding and recognition of compromised nodes.

4.1. Metric

The monitored traffic is analyzed by studying the entropy of its distribution. In particular, entropy fluctuations are analyzed looking for discordant behaviors. Hence the sensors act as anomaly-based intrusion detection systems, which are characterized for allowing identifying unknown threats [70]. This led to satisfy the biological property of *diversity* (see Section 3.4), where immune agents are able to detect any antigen, including those NSB. The decision to use entropy variations over other detection methods proposed in the bibliography is that, as demonstrated in [51], is much more effective. This is principally because its accuracy depends less than those of the others on how the protected network is used. The traditional entropy was first adapted to the information theory by Shannon in 1948 [56]. It was considered as a measure of fluctuations on qualitative variables, and it is often defined as the degree of unpredictability on their behavior. Given the qualitative variable X, the finite set $\{x_1, x_2, \ldots, x_n\}$ and their probabilities $p_1, p_2, \ldots, p_n$, the Shannon entropy was described by the following expression:

$$H(X) = \sum_{i=1}^{n} p_i \log_a \frac{1}{p_i} = -\sum_{i=1}^{n} p_i \log_a p_i \tag{1}$$

where $\log_a b \times \log_b x = \log_a x$. In addition, if the variable is deterministic then $H(x) = 0$ must be satisfied. This means that all the p_i probabilities are 0, except for one, which has value 1. There are different generalizations of this entropy, adapted to the different use cases. The AIS applies that proposed by Rènyi. This decision was made considering studies like [12], where its effectiveness stands out from the rest of variations when applied on the detection of DDoS flooding attacks. Rènyi entropy is defined as follows:

$$H(X) = \frac{1}{1-\alpha} \log_2 \sum_{i=1}^{n} p_i^{\alpha} \tag{2}$$

where the parameter α indicates its order, such as $\alpha \geq 0$ and $\alpha \neq 1$. Note that the Shannon entropy is the particularly case proposed by Rènyi when $\alpha = 1$.

In our approach, the variable X is defined as the volume of traffic flowing between two network nodes A and B, destined to port C. The P probability implies that every p_i represents the frequency of occurrence in the monitored traffic of packets with certain source, destination and that are addressed to a specific port. Therefore it is fulfilled that:

$$p_i = \frac{a_i}{No.\ packets} \tag{3}$$

where a_i is the total amount of packets that met the previously described condition. In this proposal the entropy variations are treated as univariate time series of N observations, expressed a:

$$H_\alpha(X)_{t=0}, H_\alpha(X)_{t=1}, \ldots, H_\alpha(X)_{t=N}; (H_\alpha(X)_{t=0}^{N}) \tag{4}$$

4.2. Forecasting entropy variations

When estimating the entropy of future observations it is taken into account that $H_\alpha(X)_{t=0}^{N}$ series may experiment changes in trend and seasonality over time. Additionally, the forecasting methods to consider should be effective with few observations, and able to run efficiently in real time. For this reasons, to model the network behavior the triple exponential smoothing proposed by Holt-Winters has been chosen. This election is supported by publications like [27,30], where it is shown that considering the trend and seasonality of series in which they are unrepresentative, leads to insignificant prediction errors. Furthermore, the time required to calculate their forecasts is considerably lower than in the autoregressive models. Note that in order to avoid confusion between the α range on Rènyi entropy and the α parameter on Holt-Winters, henceforth $H_\alpha(X)$ is summarized as $H(X)$, and the coming α symbols will refer only to the forecasting adjustment.

The Holt-Winters model allows performing the prediction of the next observation $H(X)_{t+1}$ by analyzing three different components B, T and S. These are defined in the following recursive expression:

$$B_t = \alpha(H_i - S_{t-N}) + (1-\alpha)(B_{t-1} + T_{t-1}) \tag{5}$$

$$T_t = \beta(B_t - B_{t-1}) + (1-\beta)T_{t-1} \tag{6}$$

$$S_t = \gamma(H_t - B_t) + (1-\gamma)B_{t-n} \tag{7}$$

where B_t is the base estimation at t, the estimation of the trend is T_t and the estimation of the seasonal factor is S_t. The forecasting parameters α, β and γ fall in the range $0 < \alpha, \beta, \gamma < 1$, and facilitate the adjustment of the smoothing. The prediction H_{t+1} is usually calculated by additive or multiplicative operations. This approach considers the additive version, since it is assumed that the seasonal pattern of the series is independent of its trend. Consequently the forecast is calculated as follows:

$$H(X)_{t+1} = B_t + T_t + S_t \tag{8}$$

Another important aspect to keep in mind is the initialization method of B_0, T_0 and S_0 estimators. It is assumed that when no trend or seasonality is expected on the time series, the initialization of estimators based on the latest observations is preferable over the use of global measures. The implemented method is described in [47], which has proven to behave particularly well in similar use cases. Namely, the last twenty-four observations are considered. The calculations performed are the following:

$$B_0 = \overline{M_1} \tag{9}$$

$$T_0 = \frac{\overline{M_2} - \overline{M_1}}{12} \tag{10}$$

$$S_{t-12} = \frac{p_t}{M_1} \tag{11}$$

where M_1 summarizes the first twelve observations and M_2 the last dozen. The adjustment of parameters α, β, γ is obtained by calculating the values minimizing the function Sum of the Squared Errors of prediction (SSE), defined as:

$$SSE(\alpha, \beta, \gamma) = \sum_{t=1}^{N} (H(X)_t - \widehat{H(X)}_{t|t-1})^2 \tag{12}$$

4.3. Definition of prediction intervals

For the evaluation of the variation of entropy according with X in the observation t, two thresholds are constructed: an upper threshold Th_t and a lower threshold Tl_t. From these the prediction interval of the sensor is defined in the same way as is usually performed when implementing Holt-Winters [34]. They are expressed as follows:

$$Th_t(t) = p_0 + K \times \sqrt{var(E_t)} \tag{13}$$

$$Tl_t(t) = p_0 - K \times \sqrt{var(E_t)} \tag{14}$$

where E_t is the prediction error in t and p_0 is the prediction of the last observation. The prediction error is given by the difference between the forecast and the t observation. The variance $Var(E_t)$ is calculated considering the prediction error of the last t observations. In addition, the thresholds include a parameter K, from which it is possible to adjust the sensitivity of the detector. In the case of D_H agents, the default value $Z = \frac{\alpha}{2}$ is assigned to K, thus relating the thresholds with the normal distribution of the series. Note that this is not a wrong decision considering publications as [47], where it has shown that when the time series does not approach the normal distribution, the error is unrepresentative. Moreover the margin rate of both intervals is in the order $100(1-\alpha)$.

On the other hand, as part of the adaptive response, the D_A agents acquire the ability to increase their level of restriction based on the anomalous activities detected by D_H. Hence the parameter k is determined by the following expression:

$$K(t) = K_{prev}\left(1 - \frac{Vol_{atk}}{Vol_{leg}}\right) \tag{15}$$

Where K_{prev} is the last setting of K, V_{atk} is the total volume of traffic monitored during the attack and V_{leg} is the total volume of traffic monitored at the previous legitimate situation.

As an example, in Fig. 4, the time series associated with the entropy of the monitored traffic in part of one of the experiment and its prediction are shown. Legitimate traffic passes through the sensor until the observation at t=56; then the injection of a large volume of traffic is observed. In Fig. 5, the prediction intervals of the sensor under the same circumstances are shown. When the attack is launched, both thresholds are exceeded. Then the agent reports of the incidence and drops the malicious packets, so the entropy back to their original values.

4.4. Identification of sources

Before the deployment of mitigation measures, and in order to

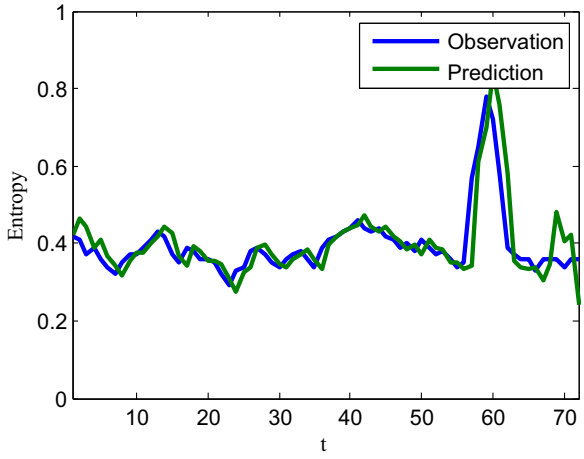

Fig. 4. Example of forecasting of the entropy.

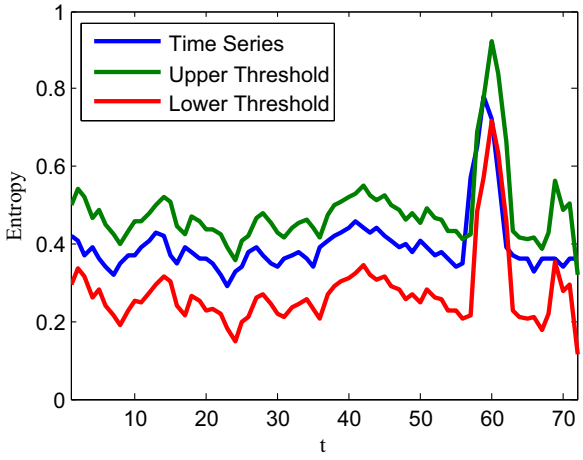

Fig. 5. Example of variations on the thresholds of prediction.

allow specificity, it is important to identify the possible origins of the detected threat. With this purpose, the different p probabilities observed at t are studied. The following assumptions are taken into account:

- Attacks could be originated from different IP addresses.
- Attacks may be directed against different destination IP addresses and ports.
- The routes Source, Destination, Port with higher p are more likely to be involved in the attack

On this basis, the various instances of X are grouped in function of their p. Given the nature of the information to be processed, the implemented algorithm must be unsupervised. Of the many options available, k-means algorithm has been chosen and the K value has been adjusted by the *elbow* method. K-means was selected because is well known and it is especially resilient regarding the presence of outliers and errors in distance measurements. The *elbow* method compensates its main drawback: the need to previously specify the number of clusters to be generated. This method launches k-means with different K values, until unrepresentative variations in the sum of the squared error between each member of the clusters with its central value occurs. Alternatives to this decision can be found in [54]. At the end of the identification of sources, nodes grouped in the cluster with greater p area tagged as suspicious, and therefore are quarantined. It is worth stressing that in order to provide an easy to understand framework, as well as stated when describing the assumptions and requirements of the proposed AIS, the recognition of disguised attackers is not contemplated in this source identification method. The latter would require deploying specific tracking capabilities at Orchestrator level, or even have the support of ISPs to study the activities on the backbone network [69], which falls outside the scope of this research. But it is to be expected that these threats may be detected and mitigated regardless of the disguising strategy (as a conventional DDoS flooding attack) by assuming as sources the compromised nodes.

5. Experimentation

In the implementation of the sensors, the observations are delimited by a fixed number of packets whose order of arrival is consecutive. A common alternative to this is their delimitation by considering time intervals. Both pose advantages and disadvantages, with the first choice being more efficient in the analysis of collections of previously captured traces, as is the case of most of the datasets analyzed [51]. In addition, a sliding window of size N that gathers the observations involved in the calculation of the entropy was applied. This boundedness is important to ensure that the implemented algorithms are computable, avoiding the case where $N \to \infty$. The proposal has been evaluated in two stages. Firstly, the accuracy of the various agents when dealing with DDoS flooding attacks was measured. On the other hand, several features related to the effectiveness of the deployment of the AIS were studied. The following describes each of them in detail.

5.1. Assessment of accuracy of the immune agents

Given the controversy relating to the evaluation methods of the effectiveness of intrusion detection system for identification of DDoS attacks, the scheme proposed in [40] was applied. This involves the use of two well-known datasets: KDD'99 [37] and CAIDA'07 [15]; and the generation of flooding attacks with the tool DDoSIM [22] in a real use case. The first two are collections of old samples that have served over the years for the comparison of DDoS detection approaches. Nowadays their use still common, so they allow the comparison of the proposed AIS with the related works in the bibliography. On the other hand, the analysis of current traffic traces provides a much more realistic assessment of the detection capabilities of the sensors, but the obtained results are not directly comparable with those of previous publications. The following describes the principal characteristics of each test and their application.

5.1.1. KDD'99

The KDD'99 [37] is one of the most referenced methodologies in the bibliography, and according to [11], possibly the only one that presents a dataset with reliable labeling. It was created in 1999, under the KDD Cup competition, and from captures of traffic provided by DARPA'98. The competition task was to build a network intrusion detector, a predictive model capable of distinguishing between "bad" connections, called intrusions or attacks, and "good" normal connections. It provides 41 different features of legitimate and malicious traffic samples. The attacks fall into four main categories: DoS (Denial of Service, e.g. *syn flood*), R2L (unauthorized access from a remote machine, e.g. *guessing password*), U2R (unauthorized access to local superuser (root) privileges, e.g., *buffer overflow* attacks) and probing (surveillance and other probing, e.g., *port scanning*). Originally it separates a subset of the datasets for the training stages of expert intrusion detection systems, and the rest for their evaluation. Since the proposed system requires no training, all samples have been applied in the evaluation process, with the exception of the first observations, necessary for initialization of the predictive models. It is noteworthy that the antiquity of the dataset and the discovery of irregularities in its content have led to its discrediting. An important part of the research community considers KDD'99 unrepresentative, mainly due to lack of heterogeneity in comparison with current networks, old class of intrusions, errors when data gathering, etc. As is discussed in [65], this leads to the mistake of consider that the experimental results are scalable to real monitoring environments. But despite this, it remains one of the most used methodologies, mainly due to the administrative difficulties associated with the publication of new datasets and the fact that it was implemented in most of the previous proposals.

5.1.2. CAIDA'07/08

The CAIDA'07 dataset [15] provided samples of traffic traces containing DDoS flooding attacks (mainly ICMP, SYN and HTTP) monitored in August 2007. They are divided into files with extension pcap and spaced at time intervals of five minutes. As described in their documentation, after the capture, most of the non-malicious contents were removed. Therefore it provides a good battery of tests to evaluate the effectiveness of the detection systems when analyzing flooding attacks, thus allowing their hit rates to be calculated. However, it is also necessary to determine their behavior when processing legitimate traffic, thereby calculating the false positive rates. Consequently, the use of CAIDA'07 is often complemented with the passive collection of traffic traces CAIDA'08 [16], as described in [40]. The latter compiles

usual and legitimate traffic monitored at the data centers *Equinix* of San Jose and Chicago (the same networks as CAIDA'07). Both represent the traditional evaluation scheme with greater similitude to recent networks, allowing the contrast of the results, and involving a more current context. In the evaluation of the proposal, were separated into traces of 15,000 packets, and the distinction of the class of flooding attacks has not been taken into account.

5.1.3. DDoSIM and UCM traffic

This test scenario is a real use case. It combines the study of the habitual traffic on the subnet corresponding with the Faculty of Computer Science of the Complutense University of Madrid (UCM), with the analysis of flooding attacks injected by the tool DDoSIM [22]. The generated attacks act at application layer, and are based on the massive send of different HTTP and TCP requests. During its course, DDoSIM simulates the behavior of various zombie computers using random assignment of IP addresses, which are able to log into the victim servers. Once established, it proceeds to the flooding of requests. The captured traffic has been divided into two classes: legitimate and malicious. Both contain samples with traces of 40,000 packets in format pcap. The first one is applied to calculate the false positive rate of the approach. The other is to determine the hit rate.

5.2. Evaluation of the artificial immune system

To evaluate the effectiveness of the deployment of the AIS, a simulator capable of generating traffic distributions and different networks with different locations of D_H and D_A has been implemented. This is because none of the functional standards for the evaluation of similar systems provides a complete knowledge of the organization of various networks. In the generation of new networks, several parameters had been taken into account: number of nodes, bandwidth, link density, and cyclic component. The last two determine the number of connections associated with each node and the number of cycles in the network when it is plotted as a graph of finite dimensions. Note that in the bibliography there are a lot of approaches to the problem of generating random network topologies. The proposed methodology considers those based on the Erdõs-Rényi model [21], and hence assumes as main property the graph density (i.e. the amount of links per node). In this model, the density p of the new graphs and the amount of nodes is randomly selected at the beginning of their construction, so each pair of nodes is connected with an independent probability p. As stated by [23], the constructed graphs are expressed as $G(n, p)$ where n is the number of nodes connected according to p; if the amount of generated closed walks exceeds the cyclic component, the graph is discarded and a new one is built. When a new graph meets this requirement, the available bandwidth for each link is specified. On the other hand a tool for simulating flooding attacks has been developed. Given a network built by the previously described scheme, the tool emulates the injection of a certain amount of packets from a source node to a victim side, according with [11].

In Fig. 6 a summary of the tasks involved in the creation of each of the networks in the experiments is shown. In a first step, the network topology and the distribution of agents are defined. The network is built according to the previously described parameters, and is represented by a graph where the vertices are its nodes, and the edges are its connections. Then the origin and the destination of the attacks are defined. The location of immune agents is defined by greedy graph coloring [26], where the two most frequent calculated colors represent the class of actors. Thus the amount of D_A sensors dependent of each D_H is regulated. The second level defined how the traffic is generated. The legitimate communications are randomly decided by taking into account the simulation parameters. The injection of traffic is carried out by the tool hping3. In the case of clean traffic, various protocols (FTP, HTTP, ICMP, etc.) and actions (transfer of files, requests, session maintenance, etc.) are performed. With all of this, a script that allows

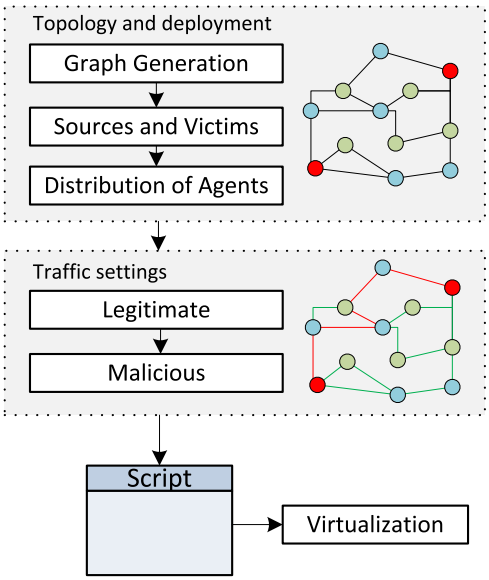

Fig. 6. Construction of virtual networks for testing.

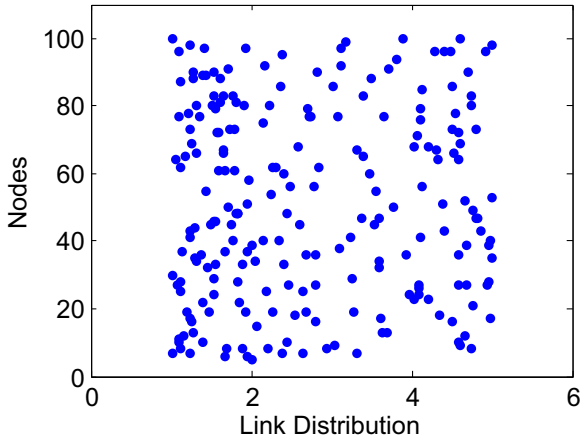

Fig. 7. Network topologies in the experimentation.

the deployment of the network in a virtualized environment is built. Through its execution it is possible to assess the effectiveness of the AIS in the test. In the experiments, 220 different networks have been considered. Their topology features are summarized in Fig. 7, where the X axis indicates the link distribution per node and the Y axis the amount of nodes. Link distributions range between 1 and 5 (average: 2.74, median: 2.42, variance: 1.29), and the number of nodes between 5 and 100 (average: 50.8, median: 48, variance: 28.26). For each of them, the behavior of denial of service attacks with different power, directed between each possible pair of source and destination nodes had been studied. Different features of the proposal have been evaluated in function of the location of the immune agents, the flooding power of the attacks, the congestion of the network, or the malicious traffic mitigated.

6. Results

The results obtained when assessing the behavior of the agents separately and in the study of their capacity of collaboration according with the proposed AIS, are described below.

6.1. Detection of threats

At the evaluation of the effectiveness of the artificial immune agents

when detecting threats, the adjustment parameters of the detectors are the variable α that defines the order of the traffic entropy, and the number of packets per observation. Variations on the first of them have a similar result with the three benchmarks: When higher is the value, the higher the level of restriction of the sensor. In such a way that when $\alpha > 3$, the deployment of the AIS is counterproductive because the false positive rate becomes excessively high (exceeding 20%). In general terms, the smaller the value of α, the lower the rate of false positives. For this reason it was considered $\alpha = 1$ along the experimentation. Bearing this in mind, the following describes and discusses the results obtained by analyzing KDD'99, CAIDA'07/08 and DDoSIM injection against habitual UCM traffic.

6.1.1. KDD'99

In Fig. 8 the results obtained by analyzing the collection KDD'99 are shown. The X axis displays the number of packets per observation, whereas the Y axis indicates the True Positive Rate (TPR) and False Positive Rate (FPR). The hit rate has remained nearly unchanged in all the tests. However, the amount of errors in analyzing legitimate traffic is especially sensitive to the position in X; with fewer packets per sample, the system behaves more restrictively. Its ability in detection ceases to depend on it from 2000 observations, at which it operates in saturation mode. This reason has led to study in more detail the two class of flooding attacks contained in more than 100,000 packages within the dataset: *smurf* and *neptune*. The first aim to deploy the victim resources by flooding ICMP echo requests via broadcast to computer networks using IP broadcast addresses. On the other hand, *neptune* attacks are also known as SYN Flood attacks, and hence based on the transmission of a huge amount of SYN request to the victim systems in order to hinder their handling of legitimate traffic. The rest (*back*, *teardrop*, *pod* and *land*) are not taken into account because KDD'99 does not provide enough information to initialize the predictive models in the cases where there are lots of packages per observation. The true positive rates in saturation are 98.66% (*neptune*) and 100% (*smurf*), with a false positive rate of 1.42%. Assuming that the distribution of samples is 72.3% (*neptune*) and 27.7% (*smurf*), the average hit rate is 99.03%. Their performance in the ROC (Receiver Operating Characteristic) space is illustrated in Fig. 9. The accuracy of the sensors is validated by comparing them with some of the most representative publications of the state of the art, as illustrated in Table 1. For both *neptune* and *smurf*, the obtained hit rate and false positive rate are similar, and sometimes better than those of their predecessors. However, it is important to note that these results have been obtained when analyzing a dataset composed by obsolete traffic samples which are far from representative of the current networks, so their contrast with more recent evaluation schemes is required.

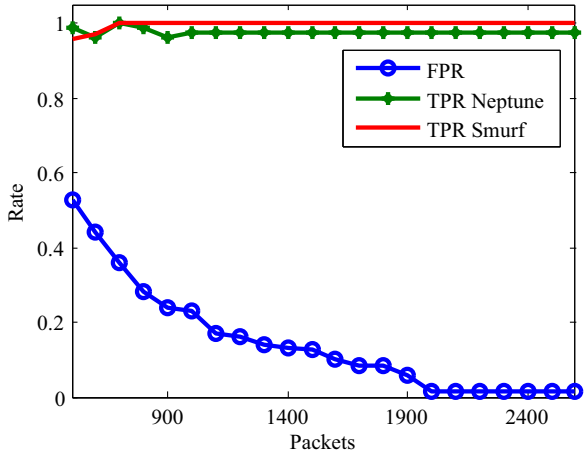

Fig. 8. Results when analyzing KDD'99.

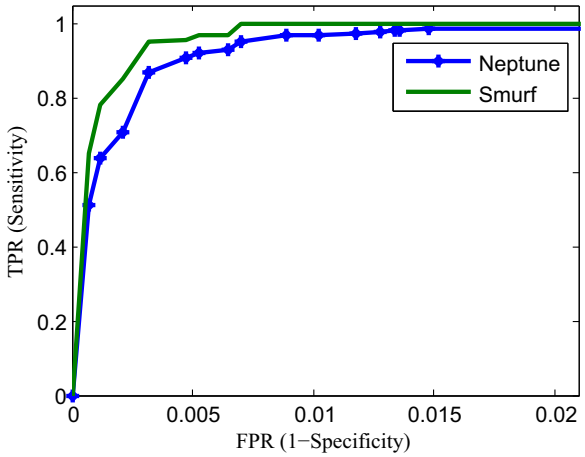

Fig. 9. Performance in ROC space when analyzing KDD'99.

Table 1
Accuracy of the various approaches that implement KDD'99.

Proposal	Method	TPR (%)	FPR (%)
[3]	SVM+ELM	99.79	2.13
[31]	Two level hybrid	97.32	0.78
[43]	Neuro-Fuzzy	99.5	1.9
[40]	Bagging	91.8	6.7
[40]	NFBoost	96.1	2.8
[40]	NFBoost+cost minimization	98.2	1.7
[5]	Multiclass SVM	96.8	0.43
The proposed sensors (Neptune)	Entropy variations	98.66	1.42
The proposed sensors (Smurf)	Entropy variations	100	1.42
The proposed sensors (Average)	Entropy variations	99.03	1.42

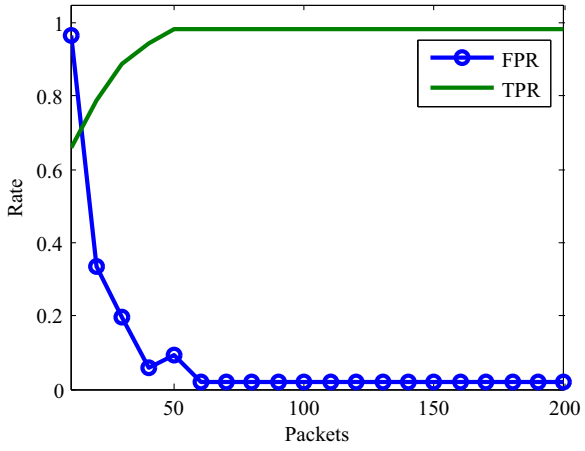

Fig. 10. Results when analyzing CAIDA'07 and CAIDA'08.

6.1.2. CAIDA'07/08

In Fig. 10 the results obtained when analyzing the traces of CAIDA'07 and CAIDA'08 are shown. The behavior of the agents is very similar to the previous test. But this time, the detectors operate in saturation with fewer packets per observation; in particular, around 160. In this case the hit rate is 98.11% and false positive is almost 1.91%. The difference between the results obtained in KDD'99 and CAIDA'07/08 is mainly due to the variations in the homogeneity of samples. In KDD'99 the traffic is older, and the scenario where the samples were gathered is more limited. Consequently, the legitimate samples are more like each other, thus reducing the tendency of the system to issue false positives. Their performance in the ROC (Receiver

Operating Characteristic) space is illustrated in Fig. 11. Note that this trend is also visible in the bibliography, where the different contributions usually are less accurate. The proposed sensors are compared with the previous works in Table 2, where can be observed that the obtained true positive rate is among the best solutions, and the rate of false positives is similar to many of them. The test has facilitated its comparison with another important set of previous publications, but as in the previous case, the results obtained separately may not be extrapolated to every real monitoring environment.

6.1.3. DDoSIM and UCM traffic

In Fig. 12 the results obtained in the experimentation with UCM traffic and DDoSIM are shown. They remain the behavior of the previous tests, reaching saturation in 2000 packets per observation. However, the accuracy obtained is considerably worse: the hit rate is 92.3% and the false positive rate is 8.3%. The difference precision achieved demonstrates that the good results obtained when applying the evaluation functional standards are not scalable to real networks. This is because the homogeneity of the traffic analyzed is much higher, according to the current usage models. But despite the high false positive rate, the quality of service of the protected environment will not be affected. The proportional increase in the rigor with which act the agents of the adaptive immune response and the specificity of the approach, allow that most of the legitimate traffic involved in the emission of false positives reach their destination by alternative ways; this will be unusual when dealing with malicious traffic.

The experimentation also emphasizes another important feature of the proposed method: most of the identified attacks have triggered alerts with proximity to the beginning and end of the malicious flooding. These are the observations where variations of entropy differ most from the legitimate traffic. When the attack is constant (as example, due to high rate attacks), the entropy tends to stabilize again, becoming invisible to the detector. Such behavior is illustrated more clearly in Figs. 14 and 13. It shows the impact on the traffic entropy of a distributed attack generated by DDoSIM against the UCM network. The X axis displays the observations and the Y axis indicates the value of the normalized entropy. The attack starts from the observation 60. Entropy anomalies are particularly visible on the following 15–20 observations, where the forecast exceeds the prediction thresholds, and thus the sensor reports an incidence. If mitigation measures (such as the packet drop applied in Fig. 2) are not adopted, the entropy is stabilized, albeit with much higher values. Most likely the attack will not be visible again until completion. At that time 15–20 observations reveal the descent of the entropy to their usual values. In view of this behavior, and in order to prevent evasion strategies, the combination of detection and mitigation measures is required, as is driven by the proposed AIS .

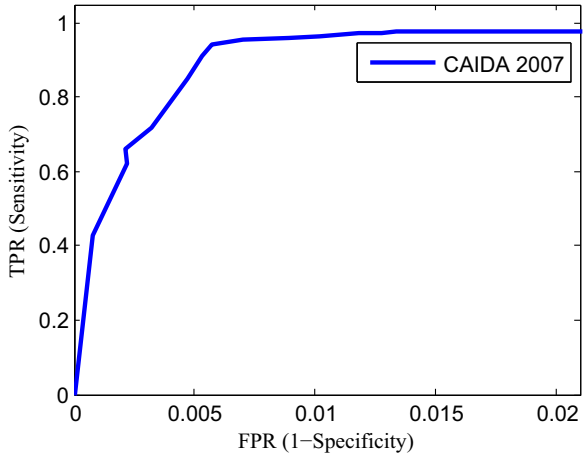

Fig. 11. Performance in ROC space when analyzing CAIDA'07 and CAIDA'08.

Table 2
Accuracy of the various approaches that implement CAIDA'07 and CAIDA'08.

Proposal	Method	TPR (%)	FPR (%)
[59]	Artificial Neural Network	99.62	5.61
[42]	Synchronous Long Flows	93.3	1.1
[53]	Decision Tree J48	95.5	0.1
[53]	Decision Tree IBK	97.5	0.5
[46]	Identifier/Locator separation	94.87	3.85
[40]	Bagging	90.4	8.1
[40]	NFBoost	97.2	4.6
[40]	NFBoost+cost minimization	98.8	1.9
[45]	TrustGuard	97.68	1.0
The proposed sensors	Entropy variations	98.66	1.42

6.2. Artificial immune reactions

The behavior of the proposed systems taking into account the location of the agents, the flooding power of the attack, the legitimate congestion of the protected network and the mitigation capacity of the AIS are described below.

6.2.1. Location of the immune agents

In Fig. 15 the results when D_H and D_A are triggered in different placements are shown. Y axis indicates the TPR/FPR and the X axis the location of the agents. Note that this test considers as location, the position of the sensor in each path crossed by each flooding threat between the source and the victim. It is a normalized value, where 0 is

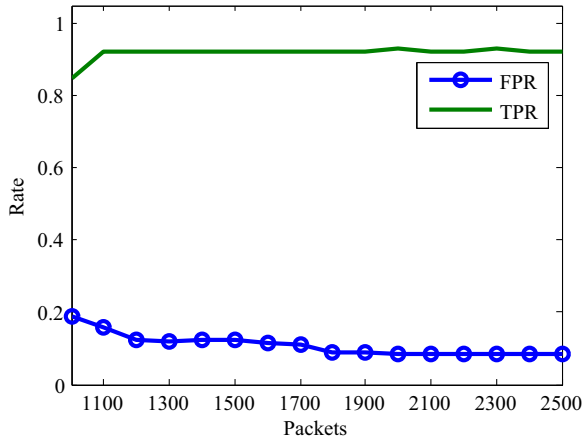

Fig. 12. Results when analyzing traffic from DDOSIM and UCM.

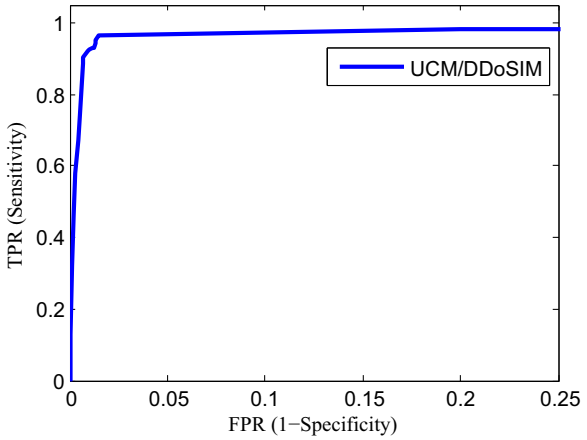

Fig. 13. Performance in ROC space when analyzing traffic from DDOSIM and UCM.

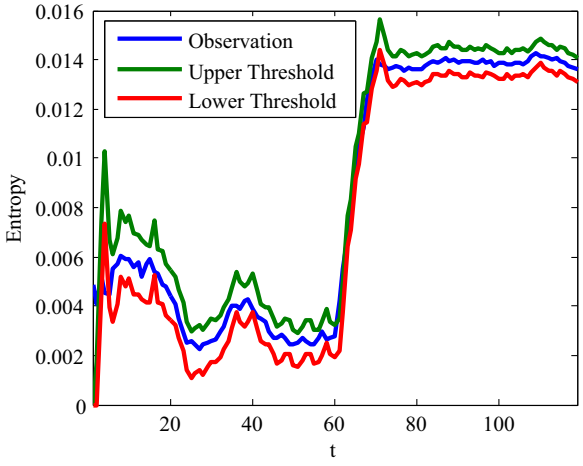

Fig. 14. Evolution of the entropy with DDOSIM and UCM.

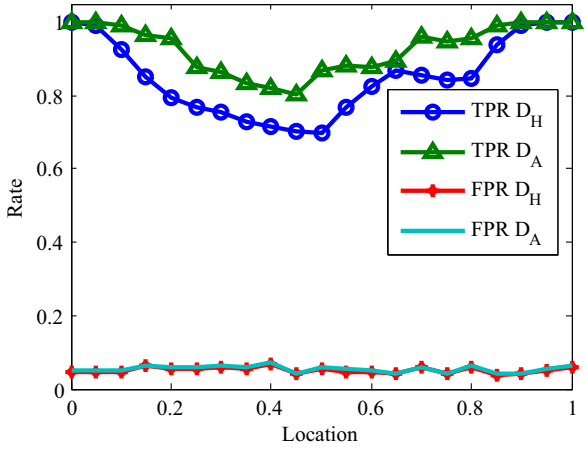

Fig. 15. Results based on the location of the immune agents.

the source of the attack and 1 is the victim system. When the attack has different sources, the threats are studied separately, hence considering different origins but a same destination. On the other hand, it is important to highlight that in a real network the length of the attack paths may vary; however, at the performed experimentation the network topologies are static, so the impact of these variations has not been contemplated, which poses an interesting line of future research.

When new attacks are launched, the average TPR is 0.85 and the FPR is 0.072. There is a trend: near the ends, the TPR value approaches 1. However, at intermediate points the accuracy is reduced by up TPR is 0.70. This occurs in the points closest to the equidistant location between the ends. When the D_A agents are activated by the immune adaptive response, the trend is repeated. Nevertheless the average TPR was increased by 7%. The greatest improvement is observed at intermediate distances. The worst TPR value is 0.82, which implies the improvement of 12%. The adaptive immunity response has low impact on the FPR, i.e., it increased 0.6% at the worst case.

In view of these results, and assuming that most of the conventional IPS behave similarly to the innate response, it can be stated that the proposed AIS poses a significant improvement in the cases where they find more difficulties to operate adequately. This occurs at the nodes above halfway between the attacker and the victim, mainly because the malicious traffic can spread over a larger number of alternative paths; near the ends they tend to converge (close to the victim) or diverge (close to the attacker).

6.2.2. *Flooding power*

In Fig. 16 the accuracy of the system depending on the flooding potency is observed. The Y axis details the TPR/FPR and the X axis indicates the power of the attacks. Note that in this test, the flooding power is defined as the bandwidth rate of the victim system that is depleted by the attack. It is represented in values in range of 0–1, with 0 being no traffic injection and 1 means the complete saturation of the connections. As shown, when the attack is more powerful than 0.5, the accuracy in both responses is similar and close to 1. Therefore, changes are irrelevant. However, when less noisy attacks, they are more difficult to be detected. These cases are where the adaptive response improves the performance of the system. At the best case, the TPR has increased by 26.5% in the power range 0.3–0.4. In summary, the higher the power of the attacks, the greater the noise caused, and therefore the threats are easier to detect. When attacks are less visible, a more significant improvement of the proposed AIS on the conventional IPS is observed.

6.2.3. *Network congestion*

In Fig. 17 the detection capability in function of the volume of legitimate traffic flowing through the networks is shown. The X axis details the TPR/FPF, and the Y axis indicated the legitimate traffic volume. In this test, the network congestion is defined as the bandwidth rate of the connections involved in the attack occupied by legitimate traffic, and therefore prior to the injection of malicious traffic. As is the case of the flooding power of the threats, it is represented in values in range of 0–1, with 0 being no traffic and 1 means the complete saturation of the connections by legitimate traffic.

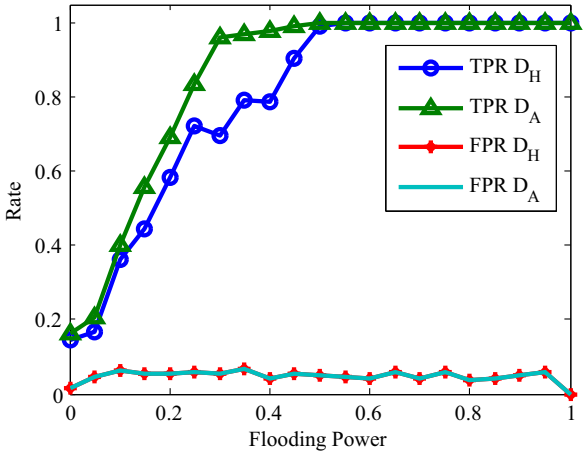

Fig. 16. Results based on the flooding attack.

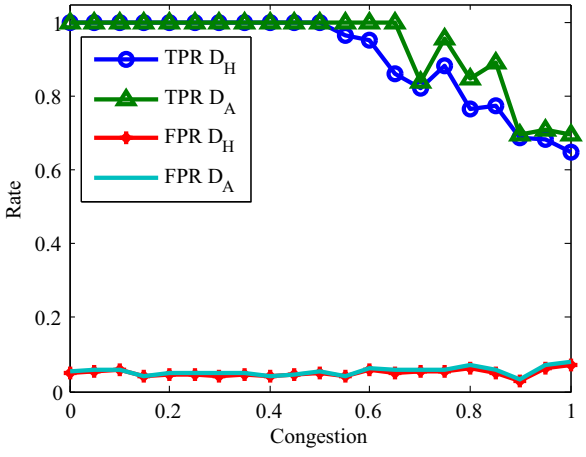

Fig. 17. Results based on the legitimate network congestion.

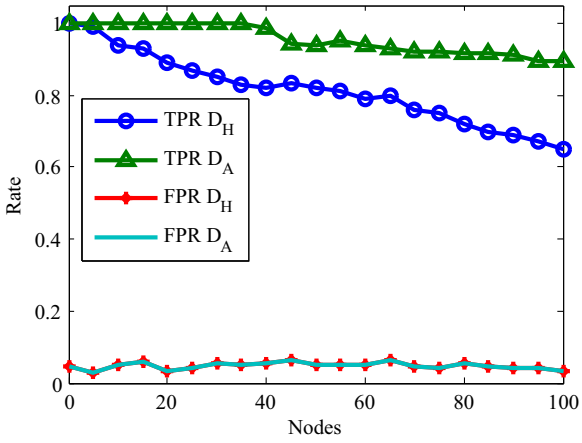

Fig. 18. Mitigation of attacks based on the number of compromised nodes.

Results are very similar to those in Fig. 16. When the traffic density is low, the proposed strategy is very accurate, as is the case of the conventional schemes. This is because the attacks are much more visible, taking a larger share of bandwidth. However, when congestion is high, especially above 0.7, the hit rate decreases, and the false positive rate increases. In the same way as in the previous tests, this problem is reduced by the activation of the adaptive response. Particularly, this strategy results in an improvement of the TPR of 13.7% when greatest slope (congestion between 0.6 and 0.7).

6.2.4. Mitigation

In Fig. 18 the mitigation capabilities of the proposed AIS depending on the number of nodes in their paths, is observed. In this test, the mitigated threats are considered as the rate of attacks that have not reached their destinations, and therefore have been neutralized by the deployed immune agents. When acting solely the innate response, 81.4% of the threats had been blocked at the worst case. However, the adaptive response was able to prevent 95.5% of them, i.e., has improved accuracy by 14.1%. From the figure it also follows that the longer the path, the greater the probability of success. This is because the load of the attack can be distributed more effectively. Bearing this in mind, it is possible to state that the larger the protected network, more relevant is the improvement obtained with this proposal. This is because the attacks that traverse larger networks often flow from greater amounts of nodes. A great effect is not achieved by avoiding their pass through few connections if there are many other routes available, as occur in the conventional IPS. But the adaptive response has the ability to spread rapidly over the network, thus increasing security measures in almost all available paths.

7. Conclusions

In this paper a novel approach for detecting and mitigating DoS flooding attacks based on the emulation of the behavior of the immune system of the human beings has been proposed. It implied the design of different artificial immune agents and their distribution throw the protected network.

The system has been evaluated in two stages. Firstly, the accuracy of the detection methods was measured taking into account the functional standards KDD'99, CAIDA'07 and recent traffic of the UCM network compromised by the tool DDoSIM. The results obtained were satisfactory, empowering their collaboratively deployment. On the other hand, their efficiency as AIS has been evaluated. This has entailed its implementation on different virtualized networks and the assessment of their effectiveness based on different parameters. Regardless of the criteria from which the behavior of the AIS has been evaluated (location of the immune agents, flooding power, network congestion or mitigation), the adaptive response has always shown more effectiveness than the innate response. This results in a significant improvement in their ability to detect and mitigate attacks, without penalization in their error rates when processing legitimate traffic. The innate response behaves in the same way as the conventional IPS, so in the adaptive reactions it is possible to study the raw effectiveness of the approach over the conventional mitigation schemes. Bearing these in mind, it is possible to confirm that the emulation of the biological immune responses is a very good way to enhance the classical countermeasures against DoS attacks.

In view of these results, this proposal is promoting the initialization of new lines of research. The simplest of them is based on the improvement of metrics and forecasting methods. Others are introducing the addition of novel immune agents, thus allowing the AIS to better perform in more complex use cases. But undoubtedly the most interesting are those that focus on its deployment at real uses cases. Any work in this regard will be especially interesting, given that the evaluation of the AIS has been mostly performed in simulated test scenarios. In particular, our research group is progressing towards its implementation on Software Defined Networks, and in adaptation to the anonymous network Tor.

Acknowledgements

This work was funded by the European Commission Horizon 2020 Programme under Grant Agreement number H2020-ICT-2014-2/671672 SELFNET (A Framework for Self-Organized Network Management in Virtualized and Software Defined Networks).

References

[1] U. Aickelin, P. Bentley, S. Cayzer, J. Kim, J. McLeod, Danger Theory: The Link between AIS and IDS, in: Proceedings of the 2nd International Conference on Artificial Immune Systems (ICARIS). Edinburgh, United Kingdom, 2003, pp. 147–155.
[2] B. Al-Duwairi, A. Al-Hammouri, Fast flux watch: a mechanism for online detection of fast flux networks, J. Adv. Res. 5 (4) (2014) 473–479.
[3] W. Al-Yaseen, Z. Othman, M. Nazri, Real-time multi-agent system for an adaptive intrusion detection system, Pattern Recognit. Lett. 85 (2017) 56–64.
[4] N. Alenezi, M. Reed, Uniform DoS traceback, Comput. Secur. 45 (1) (2014) 17–26.
[5] T. Ambwani, Multi class support vector machine implementation to intrusion detection, in: Proceedings of the International Joint Conference on Neural Networks 2003. Portland, OR, US, 2003, pp. 1–6.
[6] M. Anagnostopoulos, G. Kambourakis, P. Kopanos, G. Louloudakis, D. Gritzalis, DNS amplification attack revisited, Comput. Secur. 39 (B) (2013) 475–485.
[7] R. Azmi, B. Pishgoo, SHADuDT: secure hypervisor-based anomaly detection based on danger theory, Comput. Secur. 39 (B) (2013) 268–288.
[8] L. Barona López, J. Maestre Vidal, L. García Villalba, An approach to data analysis in 5G networks, Entropy 19 (2) (2017) 74.
[9] L. Barona López, A. Valdivieso Caraguay, J. Maestre Vidal, M. Sotelo Monge, L. García Villalba, Towards incidence management in 5G based on situational awareness, Future Internet 9 (1) (2017) 3.
[10] N. Ben-Asher, C. Gonzalez, Effects of cyber security knowledge on attack detection, Comput. Human. Behav. 48 (2015) 51–61.
[11] S. Bhatia, D. Schmidt, G. Mohay, A framework for generating realistic traffic for distributed Denial-of-service attacks and Flash Events, Comput. Secur. 40 (1) (2014) 95–107.
[12] M. Bhuyan, D. Bhattacharyya, J. Kalita, An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection, Pattern Recognit. Lett. 51 (1) (2015) 1–7.
[13] A. Boukerche, R. Machado, K. Juca, J. Sobral, M. Notare, An agent based and biological inspired real-time intrusion detection and security model for computer network operations, Int. J. Comput. Commun. 30 (2007) 2649–2660.
[14] Y. Cai, R. Franco, M. García-Herranz, Visual latency-based interactive visualization for digital forensics, J. Comput. Sci. 1 (2) (2010) 115–120.
[15] CAIDA UCSD. DDoS Attack 2007 Dataset. ⟨http://www.caida.org/data/passive/ddos-20070804_dataset.xml⟩, 2007.
[16] CAIDA UCSD. Anonymized Internet Traces 2008. ⟨http://www.caida.org/data/passive/passive_2008_dataset.xml⟩, 2008.
[17] C. Callegari, S. Giordano, M. Pagano, T. Pepe, Wave-cusum: improving cusum performance in network anomaly detection by means of wavelet analysis, Comput.

Secur. 31 (5) (2012) 727–735.
[18] L. Castro, F. Zuben, Learning and optimization using the clonal selection principle, IEEE Trans. Evolut. Comput. 6 (3) (2002) 239–251.
[19] B. Chen, Agent-based artificial immune system approach for adaptive damage detection in monitoring networks, J. Netw. Comput. Appl. 33 (6) (2010) 633–645.
[20] Y. Chen, X. Ma, X. Wu, DDoS detection algorithm based on preprocessing network traffic predicted method and chaos theory, IEEE Commun. Lett. 17 (5) (2013) 1052–1054.
[21] J. Daudin, F. Picard, S. Robin, A mixture model for random graphs, Stat. Comput. 18 (2) (2008) 173–183.
[22] DDoSIM. DDoSIM Layer 7 DDoS Simulator. ⟨http://http://sourceforge.net/projects/ddosim/⟩, 2013.
[23] P. Erdős, A. Rényi, On the evolution of random graphs, Publ. Math. Inst. Hung. Acad. Sci. 5 (1) (1960) 17–60.
[24] ETSI. GS NFV 002 V1.2.1: Network Functions Virtualisation (NFV); Architectural Framework, 2014a 2014.
[25] Europol. The Internet Organised Crime Threat Assessment (iOCTA). ⟨http://www.europol.europa.eu⟩, 2015.
[26] P. Galinier, A. Hertz, A survey of local search methods for graph coloring, Comput. Oper. Res. 33 (9) (2006) 2547–2562.
[27] E. Gardner, D. Dannenbring, Forecasting with exponential smoothing: some guidelines for model selection, Decis. Sci. 11 (2) (1980) 370–383.
[28] D. Gkounis, V. Kotronis, C. Liaskos, X. Dimitropoulos, On the interplay of link-flooding attacks and traffic engineering, ACM SIGCOMM Comput. Commun. Rev. 46 (2) (2016) 5–11.
[29] J. Greensmith, U. Aickelin, G. Tedesco, Information fusion for anomaly detection with the dendritic cell algorithm, Inf. Fusion 11 (1) (2010) 21–34.
[30] G. Groff, Empirical comparison of models for short-range forecasting, Manag. Sci. 20 (1) (1973) 22–31.
[31] C. Guo, Y. Ping, S. Luo, A two-level hybrid approach for intrusion detection, Neurocomputing (C) (2016) 391–400.
[32] P. Harmer, P. Williams, G. Gunsch, G. Lamont, An artificial immune system architecture for computer security applications, IEEE Trans. Evolut. Comput. 6 (3) (2002) 250–280.
[33] K. Heckman, M. Walsh, F. Stech, T. O'Boyle, S. DiCato, A. Herber, Active cyber defense with denial and deception: a cyber-wargame experiment, Comput. Secur. 37 (2013) 72–77.
[34] R. Hyndman, A. Koehler, J. Ord, R. Snyder, Prediction intervals for exponential smoothing state space models, J. Forecast. 24 (2005) 17–37.
[35] R. Jansen, F. Tschorsch, A. Johnson, B. Scheuermann, The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network, in: Proceedings of the 18th Symposium on Network and Distributed System Security (NDSS). San Diego, Ca, US, 2014.
[36] E. Jeong, B. Lee, I.P. An, Traceback protocol using a compressed hash table, a sinkhole router and data mining based on network forensics against network attacks, Future Gener. Comput. Syst. 33 (1) (2014) 42–52.
[37] KDD cup. KDD Cup Dataset 1999. ⟨http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html⟩, 1999.
[38] S. Khanna, S. Venkatesh, O. Fatemieh, F. Khan, C. Gunter, Adaptive selective verification: an efficient adaptive countermeasure to thwart DoS attacks, IEEE/ACM Trans. Netw. 20 (3) (2012) 715–728.
[39] R. King, S. Russ, A. Lambert, D. Reese, An artificial immune system model for intelligent agents, Future Gener. Comput. Syst. 17 (4) (2001) 335–343.
[40] P. Kumar, S. Selvakumar, Detection of Distributed Denial of Service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems, Comput. Commun. 36 (3) (2013) 303–319.
[41] S. Lee, D. Kim, J. Lee, J. Park, Detection of DDoS attacks using optimized traffic matrix, Comput. Math. Appl. 63 (2) (2012) 501–510.
[42] C. Li, J. Yang, Z. Wang, F. Li, Y. Yang, A Lightweight DDoS Flooding Attack Detection Algorithm Based on Synchronous Long Flows, in: Proceedings of the IEEE Global Communications Conference (GLOBECOM), San Diego, CA, US, 2015.
[43] H. Liang, An improved intrusion detection based on neural network and fuzzy algorithm, J. Netw. 9 (5) (2014) 1274–1280.
[44] R. Ligeiro, Monitoring applications: an immune inspired algorithm for software-fault detection, Appl. Soft Comput. 24 (2014) 1095–1104.
[45] H. Liu, Y. Sun, V. Valgenti, M. Kim, TrustGuard: A flow-level reputation-based DDoS defense system, in: Proceedings of the IEEE Consumer Communications and Networking Conference (CCNC). Las Vegas, NV, US, 2011, pp. 287–291.
[46] H. Luo, Y. Lin, H. Zhang, M. Zukerman, Preventing DDoS attacks by identifier/locator separation, IEEE Netw. 27 (6) (2013) 60–65.
[47] S. Makridakis, S. Wheelwright, R. Hyndman, Forecasting: Methods and Applications, John Wiley and Sons, New York, 1998.
[48] L. Marinos, A. Sfakianakis, Threat Landscape, 2014, ⟨http://www.enisa.europa.eu/⟩, 2014.
[49] R. Oliveira Albuquerque, L. García Villalba, A. Sandoval Orozco, R. Timóteo de Sousa, T. Kim, Leveraging information security and computational trust for cybersecurity, J. Supercomput. 72 (10) (2016) 3729–3763.
[50] C. Ou, Host-based intrusion detection systems adapted from agent-based artificial immune systems, Neurocomputing 88 (1) (2012) 78–86.
[51] I. Ozcelik, R. Brooks, Deceiving entropy based DoS detection, Comput. Secur. 48 (1) (2015) 234–245.
[52] B. Pfahringer, Winning the KDD99 classification cup: bagged boosting, ACM SIGKDD Explor. Newsl. 1 (2) (2000) 65–66.
[53] R. Robinson, C. Thomas, Ranking of machine learning algorithms based on the performance in classifying DDoS attacks, in: Proceedings of the IEEE Recent Advances in Intelligent Computational Systems (RAICS). Trivandrum, India, 2015, pp. 185–190.
[54] X. Rui, D. Wunsch, Survey of clustering algorithms, IEEE Trans. Neural Netw. 16 (3) (2005) 645–678.
[55] N. Seresht, R. Azmi, MAIS-IDS: a distributed intrusion detection system using multi-agent AIS approach, Eng. Appl. Artif. Intell. 25 (2014) 286–298.
[56] C. Shannon, A mathematical theory of communication, Bell Syst. Tech. J. 27 (3) (1948) 379–423.
[57] K. Sheshtawi, H. Abdul-Kader, N. Ismail, Artificial immune clonal selection classification algorithms for classifying malware and benign processes using API call sequences, Int. J. Comput. Sci. Netw. Secur. 10 (4) (2010) 31–39.
[58] S. Shin, S. Lee, H. Kim, S. Kim, Advanced probabilistic approach for network intrusion forecasting and detection, Expert Syst. Appl. 40 (1) (2013) 315–322.
[59] K. Singh, K. Thongam, T. De, Entropy-based application layer ddos attack detection using artificial neural networks, Entropy 18 (10) (2016) 350.
[60] Sophos, Security Threat Report 2014. ⟨http://www.sophos.com⟩, 2014.
[61] Symantec, Internet Security Threat Report 2014, 19, ⟨http://www.symantec.com⟩, 2014.
[62] Y. Tang, X. Luo, Q. Hui, R. Chang, Modeling the vulnerability of feedback-control based internet services to low-rate DoS attacks, IEEE Trans. Inf. Forensics Secur. 9 (3) (2014) 339–353.
[63] S. Venkatesan, R. Baskaran, C. Chellappan, A. Vaish, P. Dhavachelvan, Artificial immune system based mobile agent platform protection, Comput. Stand. Interfaces 34 (4) (2013) 365–373.
[64] A. Visconti, H. Tahayori, Artificial immune system based on interval type-2 fuzzy set paradigm, Appl. Soft Comput. 11 (6) (2011) 4055–4063.
[65] A. Viswanathan, K. Tan, C. Neuman, Deconstructing the Assessment of Anomaly-based Intrusion Detectors, in: Proceedings of the 16th International Symposium on Research in Attacks, Intrusions and Defenses (RAID). Rodney Bay, St. Lucia, 2013, pp. 286–306.
[66] L. Wang, Q. Li, Y. Jiang, J. Wu, Towards mitigating Link Flooding Attack via incremental SDN deployment, in: Proceedings of the IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 2016, pp. 27–30.
[67] W. Wei, F. Chen, Y. Xia, G. Jin, A rank correlation based detection against distributed reflection DoS attacks, IEEE Commun. Lett. 17 (1) (2013) 173–175.
[68] H. Yang, J. Guo, F. Deng, Collaborative RFID intrusion detection with an artificial immune system, J. Intell. Inf. Syst. 36 (1) (2011) 1–26.
[69] G. Yao, J. Bi, A. Vasilakos, I.P. Passive, Traceback: disclosing the locations of IP spoofers from path backscatter, IEEE Trans. Inf. Forensics Secur. 10 (3) (2015) 471–484.
[70] S. Zargar, J. Joshi, D. Tipper, A survey of defense mechanisms against re (DDoS) flooding attacks, IEEE Commun. Surv. Tutor. 15 (4) (2013) 2046–2069.
[71] L. Zhaowen, L. Shan, M. Yan, A Negative Selection Approach to Intrusion Detection, in: Proceedings of the 11th International Conference on Artificial Immune Systems (ICARIS). Taormina, Italy, 2012, pp. 178–190.
[72] W. Zhou, W. Jia, S. Wen, Y. Xiang, W. Zhou, Detection and defense of application-layer DDoS attacks in backbone web traffic, Future Gener. Comput. Syst. 38 (2014) 36–46.
[73] B. Zhu, J. Yan, G. Bao, M. Yang, N. Xu, Captcha as graphical passwords-a new security primitive based on hard AI problems, IEEE Trans. Inf. Forensics Secur. 9 (6) (2014) 891–904.