# Poster: Mitigation of DDoS Attacks in 5G Networks: a Bio-inspired Approach

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)
Faculty of Computer Science and Engineering, Office 431, Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases s/n, Ciudad Universitaria, 28040 Madrid, Spain
E-mail: jmaestre@ucm.es, {asandoval, javiergv}@fdi.ucm.es

***Abstract*—Distributed Denial of Service (DDoS) attacks pose a threat in constant growth. This paper addresses their mitigation by introducing a novel Artificial Immune Systems (AIS) supported by new generation technologies. The approach is based on building networks of distributed sensors suited to the requirements of the monitored environment. These components are capable of identify threats and react 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. Experiments performed to date show promising results.**

***Index Terms*—Denial of Service, Intrusion Detection System, Artificial Immune System.**

## 1. Introduction

By definition, Denial of Service (DoS) attacks take as objective to disable 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 [1]. In addition, they emphasized that DDoS 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 or compromising anonymous networks, such as Tor or Freenet. Progress towards Self-Organizing Networks (SON) at fifth generation scenarios, as well as the different techniques involved in their development [2], such as Software-Defined Networking (SDN), Network-Function Virtualization (NFV), 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 [3]. Bearing in mind these technologies, a strategy for detection and counteraction against DDoS flooding attacks is proposed. Therein the deployment of a sensor network that integrates an Artificial Immune System (AIS) [4] inspired by the biological defense mechanisms of human beings is introduced. 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. The impact of the deployment of this approach is shown with preliminary experimental results.

## 2. Biological Immune Reactions Against DDoS

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 in relationship through an elaborate and dynamic network. The basic defense mechanisms compose the innate immunity, and usually are the first line of protection. 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 proposed system has distributed architecture and its different actors assume the various roles of these biological immune systems. Its success depends mainly on two types of agents spread along the protected network: $H$ detectors ($D_H$) and $A$ detectors ($D_A$), which are involved in the innate and adaptive immune responses, and orchestrated by Software-Defined Networking, implemented as Virtual Network Functions.

As in biological systems, the innate immunity on our 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 sensors 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 identified a threat, the innate mitigation measures consists mainly on the adoption of directives that restrict the communications with nodes, ports or services involved in the attack vector. The innate response provides quick and efficient countermeasures, requiring no communication with the orchestrator prior to their launch.

On the other hand, in the adaptive immunity the experience gained allows reacting more firmly against the intruder, by generating new and stronger agents based on the acquired knowledge; but they can only act for mitigating the threat for which they were created, which is commonly termed as specificity. The adaptive response is the next defensive step in our proposal. It is triggered every time a $D_H$ agent recognizes a new threat. Once the adaptive reaction is released, the $D_H$ that identified the attack sends activation signals to the $D_A$ agents in close proximity. Then the activated $D_A$ agents analyze traffic flowing through them. Unlike $D_H$, their detection engines increase restrictiveness in proportion to the flood of the attack, being usual that they act 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, becomes less noisy and hence more difficult to be detected. In order to prevent that this measure results in a substantial increase in the false positive rate, specificity is taken into account. To ensure specificity, they only are able to apply countermeasures against the threat that has activated them. Therefore, they can take action against several attacks only if they have been activated to mitigate each of them. Because all of this, and as in nature, the artificial adaptive immune response involves the increase of the amount of forces 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 activate; 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.

## 3. Preliminary Evaluation

To evaluate the effectiveness of our proposal, it was emulated via Mininet on different scenarios. A simulator capable of generating traffic distributions and different networks with different locations of $D_H$ and $D_A$ has been implemented. Detection is carried out by identifying anomalies in variations on the entropy of the traffic, and constructing adaptive thresholds based on their prediction. If the thresholds are exceeded, alerts occur. They are adjusted in the adaptive response to modify the level of detection restriction. In Fig. 1 the results of one of the performed test is shown. Particularly, it illustrated the amount of treats that reached their target depending on the number of nodes in their paths. When acting solely the innate response (as a conventional deployment of IPS), 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. But the adaptive response has the ability to spread rapidly over the network, thus increasing security measures in almost all available paths, and demonstrating its mitigation capabilities.

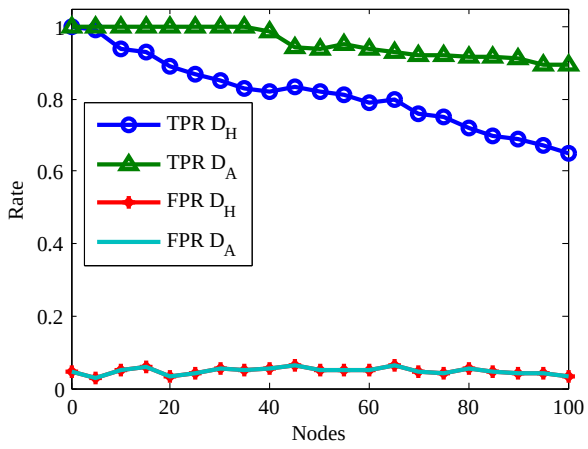


Figure 1. Mitigation of attacks based on the number of compromised nodes

## 4. Conclusion

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 preliminary results were satisfactory, empowering their collaboratively deployment. In view of these results, this proposal is promoting the initialization of new lines of research. The simplest of them are based on the improvement of metrics and implementation of different detection methods. Other are introducing the addition of novel immune agents, thus allowing the AIS to better performing in more complex use cases. But undoubtedly the most interesting are those that focus on its deployment at real uses cases, because at the moment, the evaluation of the AIS has been mostly performed in simulated test scenarios.

## Acknowledgments

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] ENISA (2016), “Threat Landscape 2015”. Available: https://www.enisa.europa.eu/

[2] N. Panwar, S. Sharma, A.K Singh, “A Survey on 5G: The Next Generation of Mobile Communication”, *Phy. Commun.*, 18(2) pp. 6484. 2016.

[3] L.I. Barona López, A.L. Valdivieso Caraguay, J. Maestre Vidal, M.A. Sotelo Monge, L.J. García Villalba, “Towards Incidence Management in 5G Based on Situational Awareness”, *Future Internet*, 9(1) 3, 2017.

[4] N. Bayar, S. Darmoul, S. Hajri-Gabouj, H. Pierreval, “Fault detection, diagnosis and recovery using Artificial Immune Systems: A review”, *Eng. App. of Artificial Intell.*, 46(A) pp. 4357, 2015