IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 1, 2017, accepted April 21, 2017, date of publication May 9, 2017, date of current version June 28, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2702341

A Game Theoretical Based System Using Holt-Winters and Genetic Algorithm With Fuzzy Logic for DoS/DDoS Mitigation on SDN Networks

MARCOS V. O. DE ASSIS[1], ANDERSON H. HAMAMOTO[2], TAUFIK ABRÃO[3], (Senior Member, IEEE), AND MARIO LEMES PROENÇA JR.[2]

[1]Engineering and Exact Department, Federal University of Paraná, Palotina 85.950-000, Brazil
[2]Computer Science Department, State University of Londrina, Londrina 86.057-970, Brazil
[3]Department of Electrical Engineering, State University of Londrina, Londrina 86.057-970, Brazil

Corresponding author: Marcos V. O. de Assis (marcos.assis@ufpr.br)

This work was supported in part by the National Council for Scientific and Technological Development of Brazil under Grant 308348/2016-8 and Grant 304066/2015-0, in part by the Federal University of Paraná under Project Banpesq/2014016797 and in part by the SETI/Fundção Araucária for project 35987 under call 20/1012.

ABSTRACT The ever expanding the usage of cloud computing environments, connected applications and Internet of Things-based devices have progressively increased the amount of data that travels through our networks. Software-defined network (SDN) is an emergent paradigm that aims to support next-generation networks through its flexible and powerful management mechanisms. One of the biggest threats faced by these services nowadays is security management. Attacks based on the denial of service (DoS) are particularly efficient against this paradigm due to its centralized control characteristic. Once this controlling system receives a massive amount of malicious requests, the overall performance of the network operation is impaired. Although several researches propose to address this problem, most of them are reactive approaches, detecting the attacks and warning the network administrators, i.e., after the network is already compromised. This paper presents an autonomic DoS/DDoS defensive approach for SDNs called Game Theory (GT)-Holt-Winters for Digital Signature (HWDS), which unites the anomaly detection and identification provided by an HWDS system with an autonomous decision-making model based on GT. Real collected data and simulated attacks are used by the system to measure its effectiveness and efficiency. Furthermore, we also use a heuristic Fuzzy-GADS method for anomaly detection instead of HWDS, aiming to compare the achieved performance and evaluate the behavior of the presented game theoretical approaches a standalone mitigation module.

INDEX TERMS Game theory, HWDS, fuzzy logic, GADS, denial of service.

I. INTRODUCTION

As large-scale computer networks continuously grow in size and complexity, efficient and fast-responding management mechanisms are required now more than ever. The popularization of network technology is giving birth to a large number of useful online applications, such as Internet of Things (IoT) devices and Cloud Computing environments. As a result, the amount of relevant and valuable information traveling among large-scale networks has increased substantially in the last decade [1].

Therefore, people are increasingly dependent on online services to perform daily tasks. The advantage is that, as long as one has access to the service network, it is possible to generate and acquire information in a simple, ubiquitous and agile way. On the other hand, if the network services are unavailable, anenormous amount of end-users are negatively impacted. Thus, an efficient network management approach is needed to guarantee the availability and quality of the services provided by the network.

In that manner, Software-Defined Network (SDN) emerges as a powerful and flexible networking architecture. It was developed to simplify and improve the management process through better abstractions for network functions and more flexibility for controlling network devices. Ontraditional networks, both packet-forwarding (data plane) and routing tasks (control plane) are performed by routers and switches. The SDN basically separates the control plane from the data plane, *i.e.*, the network control process of the packet-forwarding plane is implemented in a software level by a centralized and programmable controller [2], [3], instead of being controlled by network's routers.

There are three main groups of anomalous events that may impair a SDN operation [3]: attacks directed to the control plane; compromising of the communication between data and control planes, and; threats to data plane's equipment.

In this paper, we address the first cited anomalous event, in which Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks'mitigation represent a major challenge for this network architecture. DDoS attacks usually use botnets as attacking hosts, which are a collection of several malware-infected machines remotely controlled by a malicious user [1]. This characteristic significantly improves the impact of these attacks, as the number of infected hosts inside botnets is usually massive. In these attacks, malicious requests overwhelm the central controlling system, consequently hindering the SDN operations. Recently, two large-scale DDoS attacks targeted the governments of the United States and South Korea, demonstrating that even though these attacks are widely addressed in the literature we still lack efficient mechanisms to detect, identify and mitigate them [4].

Computer network security is a well-addressed research area, with several different proposed approaches to detect [5], [6] and identify attacks [7]. For instance, the Holt-Winters for Digital Signature (HWDS) system [8], [9] is capable of detecting and identifying several different kinds of anomalies, such as DoS, DDoS and Port Scan attacks, through a seven-dimensional flow analysis and traffic characterization process. However, most of these works only detect and provide relevant information to the network administrator, who has to supervise the required counter-measures manually.

To mitigate the effects of these attacks, simple rules, such as blocking traffic from suspicious IP addresses [10] or the entire suspension of communication with the attacked service, may be defined at the network entry switch [11]. However, routing rules set by human operators usually impair end-users. It occurs due to their inflexibility and lack of adaptation regarding normal traffic behavior, as well as the low human response-time and error-prone actions. Thus, a new management approach known as Autonomic Management [12] is necessary as a result of demands for new automatic control mechanisms able to not only detect and identify network anomalies and attacks but also take countermeasures to mitigate their effect efficiently.

Thus, to develop an autonomic SDN defense system, an efficient and fast decision-making method must be used. One of the most promising methods in the area is the Game Theory (GT). Widely used in economics and resource allocation, it has been increasingly addressed in network management applications aiming to optimize responses and actions [13]–[15]. Briefly, a GT-based method consists of converting a problem with conflicting interests into a game, where different players can take actions trying to optimize the results of acquiring their objectives.

In this paper, we propose a set of procedure called Game Theoretical Based System for DoS/DDoS Mitigation using Holt-Winters (GT-HWDS) and Genetic Algorithm with Fuzzy Logic (GT-Fuzzy-GADS) directly applicable to a SDN network.Such a supervision system is capable of autonomously detect, identify and mitigate the occurrence of DoS and DDoS attacks to SDNs through the use of a game theorymodel. To measure the efficiency of the presented system, IP flow records are collected from a real environment similar to a SDN. This data is used alongside a Network Anomaly Simulator called Scorpius [16], which can inject anomalous flows into real ones to simulate attacks such as DoS and DDoS. Furthermore, we measure the results and evaluate the behavior of the proposed game theoretical approach as a standalone mitigation module using another base method instead of HWDS. For this purpose, we used the Fuzzy-GADS method, an approach based on Genetic Algorithm (GA) and Fuzzy Logic for network anomaly detection [17].

The remainder of this paper is composed of the following sections: Section II presents the related works; Section III introduces the proposed GT-HWDS system, as well as important Game Theory concepts; Section IV describes Fuzzy-GADS method, which is used instead of HWDS for comparison purpose and behavior analysis of the proposed game theoretical approach; Section Vanalyses the performed tests and numerical results; Finally, Section VIoffers the main conclusions of the paper and future work projects.

II. RELATED WORK

The evolution of network-based applications and data exchange is massively increasing the amount of traffic that computer networks transport. The conventional communication system, although it provides an easy-to-manage environment, it is becoming impractical due to its robust architecture. Thus, Software Defined Networks (SDNs) have been developed to provide a flexible and powerful architecture for next-generation networks, where it is possible to dynamically allocate the available bandwidth according to the current network necessity. Several works in the area have been developed, such as [18], where the authors propose a formal network model used to detect anomalies caused by the interference between two or more functions or policies of the network, which is called inter-function anomalies. Li *et al.* [19] propose a new control plane management method called CPMan, aiming to reduce the overhead caused by the management messages in large scale SDNs. Song *et al.* [20] propose and develop a control path management framework to enhance the reliability of SDN through the issues identified by extensive analysis. Poulios *et al.* [21] present a study of the relationship between Autonomic Network Management and SDN through the prism of Long Term Evolution (LTE) Self-Organizing Networks (SONs), highlighting how these different paradigms interact with and complement each other.

One of the most important aspects of SDN is security. Even though there are currently several different kinds of network attacks and exploits, the DoS and DDoS attacks are the most common due to their simplicity and power [22]. Furthermore, these attacks are particularly effective against SDNs due to its centralized architecture controller. Long *et al.* [23] analyze the impact caused by DoS attacks in remote controlled systems, also discussed mitigation methods. Hoque *et al.* [1], highlight that Botnet DDoS attacks are catastrophic to the victim network, and present a survey on the matter.

To secure network systems from these attacks, several approaches have been proposed. Tan *et al.* [22] propose a system to detect DoS attacks through Multivariate Correlation Analysis. Carvalho *et al.* [24] propose an anomaly detection and identification system based on IP flow analysis using a modification of the Ant Colony Optimization metaheuristic to improve the characterization process.

As SDN is a new network architecture, conventional security mechanisms mustadapt their operation to this new paradigm. This adaptation is not a simple task since most of the traditional defense systems use the measurement of the network behavior based on its static architecture. Röpke and Holz [25] propose a sandbox system that allows the restriction of SDN applications and internal Network Operating System (NOS) components to only access a configurable set of critical operations. According to the authors, this approach is necessary due to the danger of significant impairments and failures due to the power that NOS have over SDNs. Furthermore, Lara and Ramamurthy [26] propose OpenSec, a security framework based on OpenFlow that allows the network administrator to create and implement security policies in a human-readable language. The authors highlight that 95% of the tested attacks were detected through the usage of this framework and its policies.

One most desirable characteristic of network defense mechanisms is the capability to autonomously take decisions to mitigate the impact caused by attacks and anomalies. Mainly applied to economics, the Game Theory method is increasingly gaining space among network management approaches due to its power on decision-making processes and high efficiency on optimizing outcomes. Bruce [27] explains the basics of Game Theory and highlights the mechanisms used for its application to big data analytics and decision making of remote sensing and geosciences field. Hamdi and Abie [15] propose a game-based model for adaptive security in IoT paradigm, focusing on eHealth systems. In [28] and [29], Game theoretical models against DoS and DDoS attacks have been proposed, where the attacker aims to impair the network operation, and the defender counteracts to optimize the firewall configuration. Particularly Bedi *et al.* [29] present a defense framework called GIDA, which not only drop packages from potentially malicious hosts but also redirect a part of them to a honeypot for further analysis of the attack.

In this paper, we propose a supervising system capable of not only rapidly detecting and identifying network anomalies and attacks such as DoS and DDoS but also autonomously taking countermeasures to mitigate them. The framework of the presented system is similar to the one proposed by Bedi *et al.* [29]. However, unlike the work developed by the authors, this paper presents a system based on a deeper search over the characteristics of the attacks through the HWDS method, which provides a more precise detection and identification of DoS and DDoS attacks. Furthermore, DoS and DDoS attacks based on UDP protocol are analyzed, which represent a much stealthier kind of denial of service since the bandwidth of the network is barely impacted. Finally, we use IP flow records collected from a real large-scale network environment along with simulated attacks to evaluate the effectiveness and efficiency of the proposed supervising system, instead of using probability distributions to model the behavior of the legitimate network users.

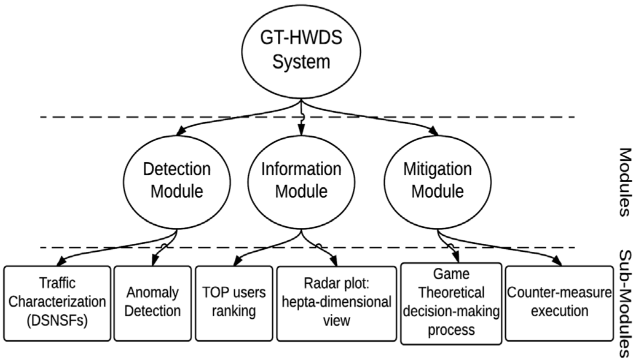
GT-HWDS System
Detection Module
Information Module
Mitigation Module
Modules
Traffic Characterization (DSNSFs)
Anomaly Detection
TOP users ranking
Radar plot: hepta-dimensional view
Game Theoretical decision-making process
Counter-measure execution
Sub-Modules

FIGURE 1. **GT-HWDS system.**

III. PROPOSED GT-HWDS SYSTEM

The attack detection and mitigation system presented in this paper aredesignedover two main approaches. The first of them is the HWDS system, responsible for the detection and identification of anomalies/attacks. This system is based on the analysis and characterization of seven IP flow dimensions. The second one is the GT-based method, responsible for the selection of the optimal countermeasure for an attack. Thus, the GT-HWDS system can be defined as the interaction of 3 modules: Detection, Information and Mitigation modules, as depicted in Fig. 1.

The proposed system aims to mitigate DoS and DDoS attacks that occur on Software-Defined Networks (SDNs). As previously discussed, this flexible architecture separates the data plane (packet-forwarding process) and the control plane (routing tasks) of the network. Thus, packet forwarding is implemented in a software level by a central controller. DDoS attacks target this central controller, overwhelming it with a huge amount of package transmission. Thus, in order to protect SDNs, incoming data must be analyzed before entering the network environment, *i.e.*, at the gateway connected to a border router.

The network topology considered is the same as the one analyzed by Bedi *et al.* in [29], which consists of a

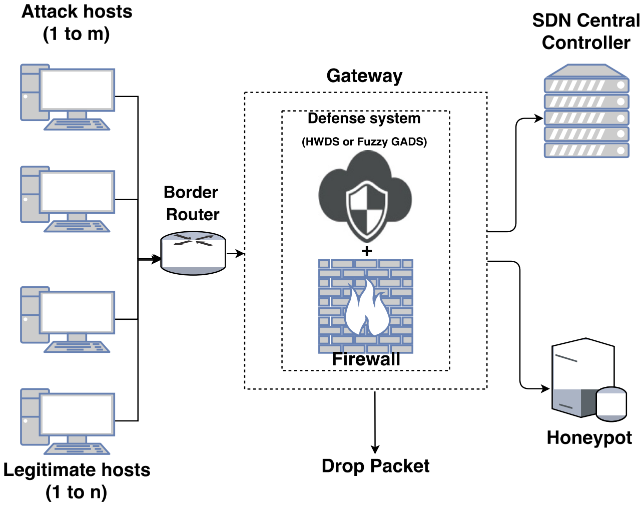

FIGURE 2. Network topology and defense system organization.

Gateway control using GT-HWDS System along with a Firewall to secure the connection between the Gateway controller with the SDN central controller. The Mitigation Module of GT-HWDS system decides, through a game theoretical approach, which packets should proceed to the SDN central controller, be redirected to a Honeypot or be dropped by the firewall. The network topology is represented in Fig. 2. It is important to highlight that the planes' construction, software and hardware requirements for the SDN architecture are not considered in this paper since the detection, identification and mitigation processes are performed before the entrance of data into the network. In other words, it is able to operate with any SDN configuration.

A. DETECTION AND INFORMATION MODULES

The HWDS system executes both detection and information modules. In this section, we briefly discuss the operation of the HWDS system. For detailed information, please refer to our previous works [8], [9]. The detection module is an approach that analyses seven IP flow dimensions in parallel to create a traffic characterization schema. The IP Flow dimensions analyzed are bits, packets and flows per second and the Shannon Entropy of the source and destination IP addresses and ports. To characterize the behavior of these dimensions, the system uses a modification of the statistical forecasting method Holt-Winters, namely Holt-Winters for Digital Signature (HWDS). Through the utilization of this procedure, the system generates a signature, specifically a Digital Signature of Network Segment using Flow analysis(DSNSF) for every analyzed dimension.

By a parallel analysis of the seven created DSNSFs, the HWDS system compares real collected IP flows with the signature generated every minute. If the observed traffic differs from the DSNSFs generated, then the system compares the current signature with the signature of known attacks, such as DoS and DDoS. At this point, the Information and the Mitigation Module are triggered.

The Information module provides relevant information about the anomaly detected to the network administrator and the mitigation module. It provides the TOP 3 (most relevant) elements of the dimensions: source and destination IP addresses, source and destination ports, and protocols, alongside a "Global View," a radar-plot of the network state at the detection moment, *i.e.*, the graphical signature of the attack/anomaly. Furthermore, this module stores the source IP addresses of the previous 5 minutes the analyzed time interval, to help differentiate legitimate users from malicious ones.

B. MITIGATION MODULE

The mitigation module is responsible for autonomously taking countermeasures to mitigate the impact of the DoS/DDoS attack. Through the use of a GT approach, the system analyzes a set of possible actions for both attacker and defense system, calculates the rewards and costs of every action and executes the optimal countermeasure.

Before we proceed to describe our GT approach, it is important to define some terms. According to [30], "Game Theory describes multi-person decision scenarios as games where each player chooses actions which results in the best possible reward for itself, while anticipating the rational actions from other players." In other words, it is a method for translating a real world problem into a game, where two or more players are trying to win. In our GT approach, two players play the game: the attacker (malicious user) and the defense mechanism. The objectives of the game are different for each player, but they complement each other. As the attacker tries to maximize the damage caused to the network and reduce its chance of being detected, the defense aims to reduce the impact posed by the attacker and preserve the network's normal operation.

The GT approach that composes the Mitigation Module of the presented system can be defined as a 4-tuple vector:

$$G = (A_{att}, A_{def}, P_{att}, P_{def}) \tag{1}$$

The elements of the vector G are detailed as follows.

The A_{att} element stands for the set of possible actions that the attacker can perform, *i.e.*, all the possible attacker's strategy. Two actions compose this set:

- Change the intensity (u) of the attack, *i.e.*, the number of packets per second directed to the network by each attacking node;
- Modify the number of attacking nodes (m).

Similarly, the A_{def} element stands for the set of possible actions that the defense can perform, *i.e.*, all the possible defense's strategy. Three actions compose this set:

- Allow packets to pass to the SDN central controller;
- Drop packets at the firewall to protect the SDN central controller through a particular dropping rate (D);
- Redirect packets to the Honeypot for further analysis of the attack behavior, motivation, and source.

It is important to highlight that only new users (new source IP addresses) are dropped or redirected to the Honeypot. New hosts can be identified due to the Information Module, which keeps a historical database of the last five minutes containing the source IP addresses of the hosts that used the network in this period. Thus, users that were accessing the network's service before the attack began do not have their packets dropped.

The elements P_{att} and P_{def} are the Payoffs or Utility Functions for the attacker and the defense, respectively. According to [30], Payoff is the positive or negative reward to a player for a given action within the game. The Payoffs of attacker and defense are usually represented by (2):

$$P = Reward - Cost \tag{2}$$

Thus, the Payoffs for the attacker and the defense mechanism can be respectively represented as (3) and (4):

$$P_{atk} = w_1^{atk} \cdot E - w_2^{atk} \cdot BC - w_3^{atk} \cdot AC + w_4^{atk} \cdot PL \tag{3}$$

$$P_{def} = -w_1^{def} \cdot E + w_2^{def} \cdot BC + w_3^{def} \cdot AC - w_4^{def} \cdot PL \tag{4}$$

where w^{atk} and w^{def} are weight parameters for each metric for the attacker and defense mechanism, respectively. Furthermore, the remaining variables stand for: E represents the normalized error between the expected network behavior and the current network state; BC is the average Bandwidth Consumption of the legitimate users in comparison to malicious ones; $AC$is the attack cost for the attacker, and; PL is the estimated Packet Loss of legitimate users through the packetdropping during the mitigation process.

The metric of normalizer Error E is defined in (5) and it is calculated by comparing the number of packages that was expectedPkt_{exp} at the current time interval (Signature or DSNSF of the Packets/s dimensions, calculated by the HWDS method) with the number of packets observed after the mitigation process. Furthermore, the resulting value should be normalizedby the maximum between expected and observed packets aimingto normalize the metric to interact with the other cost/reward functions. Finally, the absolute value of the normalized error is considered to ease the error minimization problem, since dropping an excessive number of packets will also negatively impact the network operation (optimal value achieved when $E = 0$).

$$E = \left| \frac{Pkt_{end} - Pkt_{\exp}}{\max(Pkt_{end}, Pkt_{\exp})} \right| \tag{5}$$

where the packets observed after the mitigation process is provided by:

$$Pkt_{end} = Pkt_{leg} + Pkt_{new} * (1 - D) \tag{6}$$

withPkt_{leg} being the number of packets of legitimate users, known through the analysis performed by the Information Module, as previously described. Pkt_{new} is the number of packets from new users, which merges new legitimate users and malicious users. Finally, D is the dropping rate of new packages, varying from 0 to 100%.

The average Bandwidth Consumption (BC) can be calculated using data provided by the Information Module and observed at the current time interval. First of all, the bandwidth difference (7) between the expected number of bits and the observed number of bits can be expressed by:

$$d_{bits} = B_{\exp} - B_{obs}, \quad where \tag{7}$$

$$B_{obs} = B_{leg} + B_{new} \tag{8}$$

With the difference d_{bits} calculated, the proportion Pb_{leg} (9) of bits from legitimate users among the total bits of new users can be determined:

$$Pb_{leg} = \frac{(B_{new} - d_{bits})}{B_{new}} \tag{9}$$

Finally, the average bandwidth consumption BC, measured in bits/s, can be calculated considering the drop rate of new packets D, the number of attacking hosts m and the intensity of the attack u:

$$BC = \frac{B_{leg} + D\left[B_{new} \cdot Pb_{leg} - m \cdot u \cdot (1 - Pb_{leg})\right]}{B_{leg} + D\,(B_{new} + m \cdot u)} \tag{10}$$

The Attack Cost AC is considered linear to the number of hosts m controlled by the attacker, as proposed by [20]. This number is normalized to ease the interaction with the other metrics. Thus, this parameter can be obtained through:

$$AC = \frac{m}{\max(m)} \tag{11}$$

Finally, the estimated Packet Loss ratePL can be achieved considering the expected and observed packets along with the attack parameters, including the number of attacking hosts m and intensity of the attack u, herein measured in packets/s), and the defense parameter D (dropping rate of new packages).First of all, the distance d_{pkt} is calculated through:

$$d_{pkt} = (Pkt_{leg} + Pkt_{new}) - Pkt_{\exp} \tag{12}$$

Then, we apply the result achieved by (12) to calculate the estimated packet proportion of legitimate users among the new packets:

$$Pp_{leg} = \frac{Pkt_{new} - d_{pkt}}{Pkt_{new}} \tag{13}$$

Thus, the result obtained through (13) can be applied in (14) to calculate the PL rate:

$$PL = 1 - \frac{Pkt_{leg} + (1 - D)Pkt_{new} \cdot Pp_{leg}}{Pkt_{\exp}} \tag{14}$$

At the end of the payoff's calculation, given by (3) and (4), the GT method generates a matrix containing the calculated payoffs of each different attack possibility (combination of different m and u values) with each defense strategy available (each possible value for D). The cells of this matrix are organized as a pair of information (P_{att}, P_{def}).

The optimal defense strategy must be a Nash Equilibrium obtained through the payoff matrix. Nash Equilibrium is a steady situation where no rational player would choose to modify its strategy since any possible action would decrease its utility function. As described by Equations (3) and (4), the reward of a player is the cost of another. If the weight parameters w_i^{atk} and w_i^{def} are equal for all values of i, then the problem is configured as a zero-sum game [28]. According to [31], the Nash equilibrium of zero-sum games existsand can be achieved by transforming the problem into a linear optimization problem, which is solved by the Minimax theorem. For proof of the existence and the number of Nash Equilibrium on the analyzed problem, refer to Appendix I.

Finally, with the optimal defense strategy calculated, the GT-HWDS system performs the dropping and redirecting processes along with the network's Firewall. A certain percentage of the dropped flows may be redirected to a Honeypot for further analysis but, since the redirect rate does not influence the optimal defense strategy, this rate is out of the scope of this research, and will be addressed in future works.

The defense strategy is performed for one hour, and the network comes back to a normal state after that. This time interval was chosen because, even though the attack stops within a few minutes, the impact suffered by the network is small, as shown on Section V. If a new attack is detected within this period, the Mitigation Module will be triggered again, and a new optimal defense strategy will be calculated updating the defense parameters of the network server.

IV. FUZZY-GADS METHOD

To test the effectiveness of the proposed game theoretical approach as a standalone mitigation module for other anomaly detection mechanisms besides HWDS, we use it along with the Fuzzy-GADS method, a two-phase system, which is described in this section. The Genetic Algorithm (GA) is applied to generate the network characterization, namely DSNSF, and a Fuzzy Logic approach is used to determine if an anomaly is present in a given time interval.In this method, a six-dimensional analysis of IP flows is employed, instead of seven as described in the HWDS approach.

A. GA FOR DIGITAL SIGNATURE

The concept of Genetic Algorithm (GA) was first proposed by Holland [32] in 1972. GA is a meta-heuristic search approach successfully applied to optimization problems,mimicking the steps observed in Darwin's theory of evolution. This algorithm starts with an initial set of solutions and optimizes them through genetic operations (selection, crossover, mutation) until an acceptable solution is reached.

The presented GA for DSNSF generation [17] uses the network's flows records of the past four weeks. As an example, to generate the DSNSF of a given Monday, the previous four Mondays are analyzed and used as input to the GA to create the DSNSF. Using the information available through IP flows, a six-dimensional analysis is performed, and these dimensions are: bits per second; packets per second; IP source entropy; IP destination entropy; port source entropy, and; port destination entropy.

When a GA is designed to solve a problem, the implementation of the genetic operators are not the only fundamental parameters to be defined. There is also the chromosome encoding and the fitness function. In the deployed GA, a numerical encoding is used, as the DSNSF is a real value containing the expected behavior of the computer network in a time period. The fitness function defines how appropriate the solution is to the problem in question. In this case, the Euclidian Distance was used, represented by:

$$f = \sqrt{\sum_{i=0}^{n} (y - x_i)^2} \tag{15}$$

where y is the value of the chromosome, x_i represents each element of the input data i of that time interval and n is the number of inputs.

In most cases, the population generation is random and uses the scope of the problem as the parameter. The DSNSF generated deploying the GA strategy uses a lower and an upper boundary values, randomly generatedin that interval. It ensures that the values of the solutions are neither too low or too high.

To increase the diversity and chances to produce fitter solutions to the problem, the genetic operations are applied iteratively to the initial set of solutions. The selection methods widely used are roulette wheel and tournament [33]. Roulette wheel uses the fitness value of the chromosome as the parameter to determine the likelihood of selection. The tournament selection method compares the fitness of two or more chromosomes chosen at random, selecting the one with the best fitness. In the proposed GA, the tournament selection is applied, which has a lower computational cost.

The crossover operation uses the chromosomes chosen through selection to create new chromosomes. As the DSNSF is a value that best represents the network behavior in a given time interval, the crossover methods used is the mean between the selected chromosomes. After the crossover operation, the new chromosome has a chance to suffer mutation, which can increase or decrease a small value to itself. After a certain number of generations, the algorithm stops and returns the fittest solution, which is the DSNSF.

B. ANOMALY DETECTION USING FUZZY LOGIC

The application of Fuzzy Logic for network anomaly detection is justified for two main reasons, as observed by Wu and Banzhaf [34]. First, the information of network traffic is collected and measured through statistics, which includes some level of uncertainty and errors. Second, there is no clear boundary between what is a normal behavior from abnormal, adding another layer of uncertainty to the problem. Due to these reasons, Fuzzy Logic is appropriate for the context of network anomaly detection, which is a method known for its performance involving uncertainty and partial truths, as stated by Zadeh [35].

In set theory, the membership value represents the set to which a certain element belongs. In Boolean Logic, an element either belongs or not to a set (0 or 1). On the other hand, Fuzzy Logic uses membership values that usually range from 0 to 1, indicating degrees of membership. The membership degrees in Fuzzy Logic are assigned using a membership function, such as Gaussian, Generalized Bell, triangular and trapezoidal. In this work, the membership degree measures the anomaly score of each network attribute, used to decide if a time interval is anomalous.

The DSNSF and a threshold are used to calculate the anomaly scores. The thresholds indicate normal fluctuations of the normal behavior from the predicted. This approach assigns different weights to the data used to generate the DSNSF; the further it is from the date to be analyzed the less it will affect the threshold. The threshold defined as ϕ is calculated by:

$$\varphi_k = DSNSF_k \pm L\sigma_k\sqrt{\frac{\lambda}{(2-\lambda)}} \tag{16}$$

in which k is network dimension indexer, L is the width of the threshold, σ is the standard deviation of the input data and λ is the weight. The values used for L and λ are 3.0 and 0.25 respectively, as suggested by Montgomery [37].

The DSNSF value is generated as outputs for the GA,while the threshold is calculated through EWMA, a membership function is used to determine the anomaly score of each dimension in a time interval. The anomaly scorecan be calculated by:

$$\zeta_k = 1 - e^{\frac{-(x_k - DSNSF_k)^2}{x\varphi_k^2}} \tag{17}$$

where k is network attribute indexer, x is the real traffic value, DSNSF is the prediction and ϕ is the threshold.

The anomaly score of every attribute is aggregated using a sum, and an alarm is generated if the total score is higher than a cutoff value. It is important to highlight that the Fuzzy-GADS method uses a six-dimensional analysis of IP flows for DSNSFs generation, unlike the seven-dimensional analysis of the HWDS.The rules for alarm generation are given by:

$$\begin{aligned} &Rule_1 : IF \rightarrow \sum_{k=1}^{6} \zeta_k \geq \Gamma, \quad THEN \rightarrow \text{“}anomalous''\\ &Rule_2 : IF \rightarrow \sum_{k=1}^{6} \zeta_k < \Gamma, \quad THEN \rightarrow \text{“}normal'' \end{aligned} \tag{18}$$

where the cutoff value Γ was defined using a precision-recall curve, with a dataset with five weekdays with injected anomalies, as depicted in Fig. 3. This curve varies the cutoff values and calculated the precision and recall for each of these values. The optimal cutoff value is defined as $argmax(P\Gamma + R\Gamma)$, where $P\Gamma$ is the precision and $R\Gamma$ is the recall for value Γ. In the test performed to determine Γ, the value achieved is 3.9644, which is used in the experiments shown in Section V. The network environment in which this test was conducted is also described in the following section.

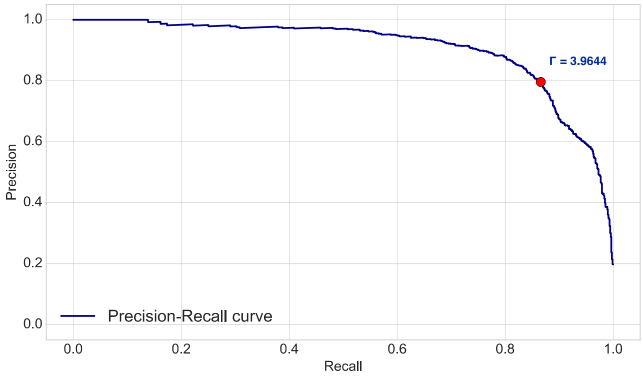

FIGURE 3. Precision-Recall curve for the estimation of Γ.

V. RESULTS AND ANALYSIS

To execute a performance analysis of the proposed system, we collected real IP flow data from the State University of Londrina (Brazil), which is a large-scale network composed of about 7000 different active hosts. The flows are collected by the usage of the sFlow protocol through a packet sampling scale of 1:512 due to the high data traffic volume. As the presented defense system operates directly at the network's gateway, the fact that the tested network is not a real SDN is not relevant for the results since the mitigation process occurs before any packet arrives at the SDN central controller.

The collected days are related to the Wednesdays of August 2015. These days represent a state of normal behavior of the network and were chosen arbitrarily due to the fact that this behavior was detected on all other collected days. Furthermore, HWDS and Fuzzy-GADS models need only three days of history to generate the DSNSFs that represent the network's normal behavior. Since, during the collection period, no DoS or DDoS attacks occurred on the analyzed network, we used an anomaly simulator called Scorpius [16] to inject the anomalous behavior of these attacks into real IP flow data.UDP-based denial of service attacks are harder to detect and less common than TCP-based DoS/DDoS. Given that the goal of our work is to detect and mitigate anomalous behaviors, we focused on a common threat to network security using a stealthier approach, *i.e.*, UDP-based denial of services.

The attacks were performed to simulate a denial process over a DNS/Cache server, the most accessed address into this network. For the DDoS tests, several intensities were discussed, using 512, 1024, 2560 and 5120 different hosts simultaneously attacking the selected target with UDP packets (experiments 1 to 4). For the DoS test, a single IP address of origin transmits a high amount of UDP packets over the selected target (experiment 5). All the attacks began at 14:00 and were finished at 14:30, to test the impact of the filters over non-anomalous hosts (from 14:30 to 15:00).

Before proceeding to the complete system analysis using both HWDS and Fuzzy-GADS, we carried out a detection performance analysis of the methods using Accuracy and Precision metrics. In classification problems, Accuracy measures

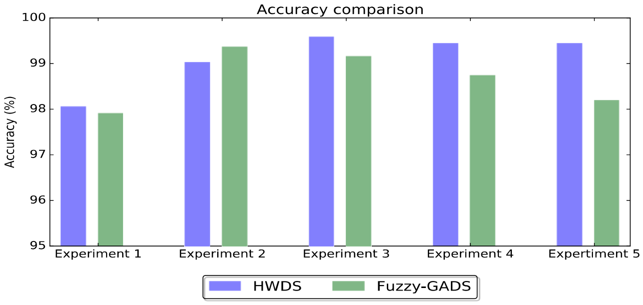

FIGURE 4. Accuracy rates for anomaly detection of HWDS and Fuzzy-GADS.

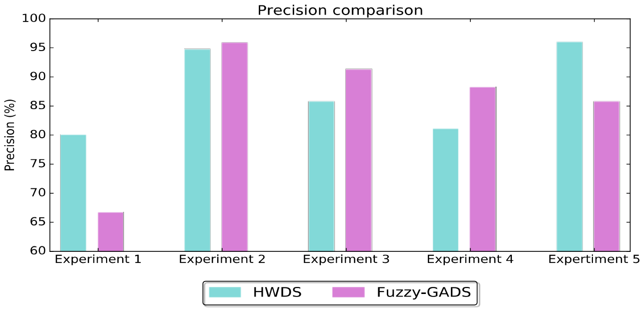

FIGURE 5. Precision rates for anomaly detection of HWDS and Fuzzy-GADS.

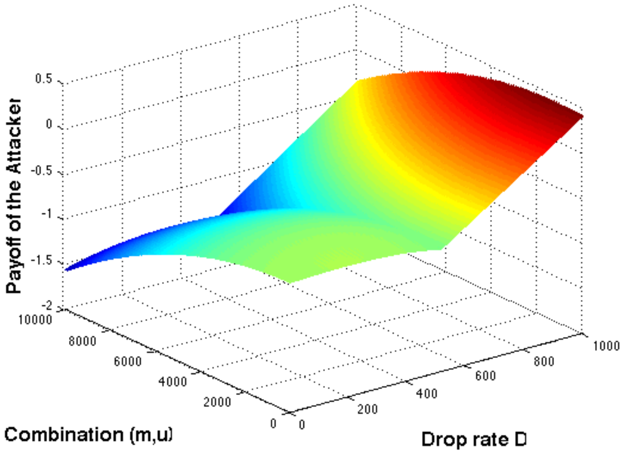

FIGURE 6. An example of Mesh plot for the variables *D*, *m*, *u* and P_{atk} used for Nash Equilibrium calculation.

the overall capability for correctlyclassifying the samples in the test set, both anomalous and normal behaviors. On the otherhand, Precision measures the percentage of samples classified as anomalies (alarmsgenerated by the system) are in fact anomalous. The results achieved byboth methods are shown in Fig. 4 and 5.

As observed, both methods achieved good results for both Accuracy and Precision metrics. Regarding Accuracy, HWDS and Fuzzy-GADS attained Accuracy higher than 98% for most of the experiments. Concerning Precision, Fuzzy-GADS presented an inferior performance in comparison with HWDS, especially for Experiments 1 and 5. In contrast, Fuzzy-GADS obtained better Precision for Experiments 3 and 4, with similar results in Experiment 2. In general, both methods displayed good results for anomaly detection concerning Accuracy and Precision metrics.

To demonstrate the presented Game Theoretical approach for decision-making process, we will discuss in detail one of the result tests, namely the DDoS attack using 2560 different attacking hosts (Experiment 3).

As previously mentioned, the attacks were performed at 14:00. The Detection and Information Modules of the GT-HWDS system, as well as the Detection Module provided by the Fuzzy-GADS model, triggered an alarm on the 841-minute of the day, *i.e.*, at 14:01. As the GT-HWDS can identify the attack as a DDoS, itprovides relevant information to the Mitigation Module, while GT-Fuzzy-GADS only trigger an alarm pointing out the occurrence of an anomaly. The information received by the Mitigation Module through its parameters,using HWDS, include:

- the DSNSFs (expected behavior) for bits and packets per second;
- a list of legitimate hosts (source IP addresses of flows from 5 minutes before the alarm triggering) that cannot be dropped on the mitigation process;
- the number of packets and bits belonging to legitimate hosts on the analyzed time interval (members of the previous list);
- the number of packets and bits belonging to unknown hosts (legitimate and potentially malicious hosts) on the analyzed time interval;

Since Fuzzy-GADS method does not use an Information Module, it provides the Mitigation Module with:

- the DSNSFs (expected behavior) for bits and packets per second;
- the number of packets and bits belonging to unknown hosts (legitimate and potentially malicious hosts) on the analyzed time interval;

Once the parameters are sent to the Mitigation Module, it triggers the GT-based decision-making sub-module. As discussed in Section III, the game is modeled as a one-shot game where the Defense System needs to choose a Dropping rate D based on the number of attacking hosts m and the intensity u of these attacks. For implementation purposes, we set the ranges for $D_{\%}$ from 0 to 100% with a step size of 0.1%, for m from 1 to 100 and for $u_{\%}$ from 1 to 100%. For the variable m, we consider its value representing the number of different attacking hosts per minute on the average, and, for variable $u_{\%}$, its value represents the intensity of the attack from 1 to 100% of the hosts' transmission capacity. The possible values for D are stored in an array with 1000 elements. Since both variables m and u interact with each other in the game, we stored them into an array with 10000 elements containing the combinatorial of them in the form (m, u).

By setting the weight parameters w^{atk} and w^{def} from (3) and (4) with the value 1, we assure that all the Reward and

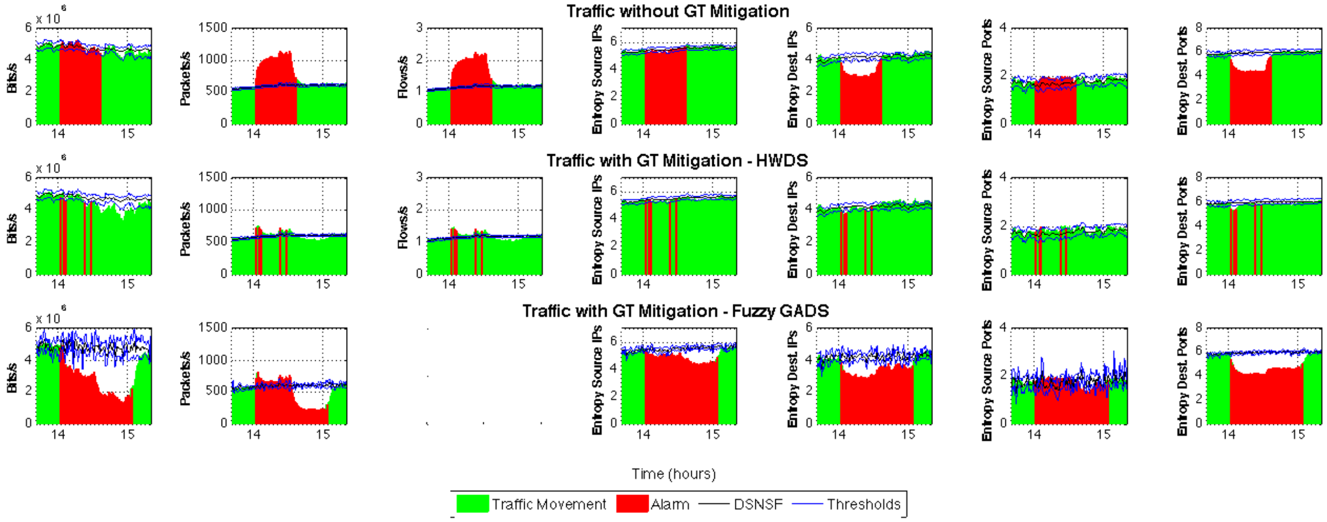

FIGURE 7. **Comparison between Traffic Movement and Alarms with and without the presented GT-based decision-making approach for HWDS and Fuzzy-GADS after the second played game in Experiment 3 (DDoS 2560 attacking hosts).**

Cost functions have the same weight. One can change these values to favor a certain function according to the need of aparticular network. Besides, by setting w^{atk} and w^{def} the same value, the problem turns into a zero-sum game. This specific kind of game can be solved through a minimax theorem, achieving a Nash Equilibrium (steady state or optimal solution) when the Defense system minimizes the maximum payoff of the Attacker [31].

Thus, a matrix of 10000x1000 elements is generated relating the Attacker optimization variables m and u with the Defense System's optimization variable D, and the Payoffs of the Attacker (3) and Defense system (4) are calculated as described in Section III. Fig. 6 illustrates an example of mesh plot for the variables D, m, u and the Attacker's Payoff P_{atk} used to calculate the Nash Equilibrium of the problem.

At this stage, the Mitigation Module found the solution of the problem with $D_{\%} = 40.6\%$ packets (30 flows per minute), $m = 8$ and $u_{\%} = 100\%$ for the HWDS, and with $D_{\%} = 20.6\%$ packets (18 flows per minute), $m = 14$ and $u_{\%} = 100\%$ for the Fuzzy-GADS. The difference between the methods' results occurs due to the difference of the provided information to the Mitigation Module. Furthermore, the variable u selected for both methods was defined as 100% because it is an UDP DDoS attack and, thus, the intensity of the attack has small influence over the available bandwidth.

As a one-shot game, this is the final result, and the dropping process can now be performed. The dropping process is performed by the Firewall controlled by the Mitigation Module. For the HWDS, this module selects, through data collection conducted by the Information Module [9], the flows directed to the attacked server and, excluding legitimate flows from known hosts, randomly drops flows until the limit of 30 flows per minute is achieved. For the Fuzzy-GADS, as the Mitigation Module does not have any additional information about the attack, a random drop process is performed until the limit of 18 flows per minute is achieved.

This process is performed every minute for 1 hour. This period was chosen in order to test the influence of the dropping process over legitimate hostssince the injected attacks last only 30 minutes.

At this point, the Defense system continues to monitor through the Detection Module the behavior of the network through the generated DSNSFs. If a new anomaly is detected, a new game is played between Attacker and Defense system, and a new Dropping rate is chosen. In our analysis of experiment 3, new alarms were triggered by the HWDS at 14:04 and by Fuzzy-GADS at 14:03. Thus, a new game was played, and the Mitigation Module found the Nash Equilibrium of the problem when $D_{\%} = 30.6\%$ packets (20 flows per minute), $m = 7$ and $u_{\%} = 100\%$ for the HWDS, and when $D_{\%} = 27.9\%$ packets (27 flows per minute), $m = 13$ and $u_{\%} = 100\%$ for the Fuzzy-GADS.

After that, no more alarms were triggered, and the comparison results are shown in Fig. 7. As observed, the random dropping process performed by the GT-Fuzzy-GADS significantly impacts legitimate users, since a considerable volume losscan be observed in the "Bits/s" plot. The information provided by HWDS greatly improves de mitigation process, directly impacting into the GT-HWDS outcomes.

Fig. 8 and 9 depict the complete achieved results for GT-HWDS and GT-Fuzzy-GADS, respectively. As observed, GT-HWDS fared better due to the information provided to the Mitigation Module. However, both approaches successfully mitigated the attacks performed from experiments 1 to 5, guaranteeing the operation of the SDN central controller. The GT-Fuzzy-GADS, however, have a disadvantage of impacting a higher number of legitimate users. Furthermore, it is important to highlight that HWDS can identify the source

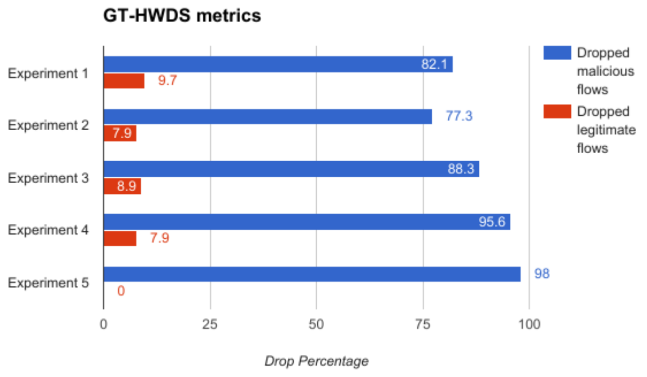

FIGURE 8. **Results achieved for GT-HWDS system.**

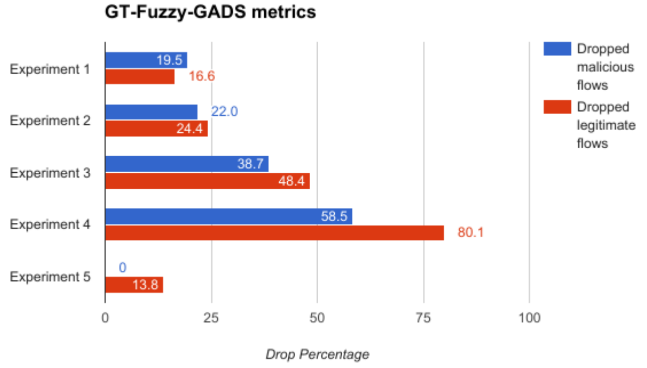

FIGURE 9. **Results achieved for GT-Fuzzy-GADS system.**

of a DoS attack. Thus, in experiment 5 for HWDS, there was no need to play the game since a directed dropping process solves the problem, which reflects on the numerical outcomes. Finally, even though GT-HWDS fared better in most performance tests, GT-Fuzzy-GADS triggered alarms faster on Experiments 1 and 2, demonstrating its efficiency on detecting the occurrence of anomalies even when they are starting, a criticalperiod where abnormalities tend to be stealthier.

VI. CONCLUSION

In this paper, we presented GT-HWDS, an autonomous supervising system able to detect, identify and mitigate the impact caused by DoS and DDoS attacks on SDNs. The system deploys the HWDS method to detect and identify anomalies based on a seven-dimensional traffic characterization process. After this step, the system triggers a Mitigation Module based on a GT decision-making approach to choose the best defense strategy, which is autonomously applied to the network as an immediate countermeasure. To evaluate the performance of the proposed system, we used five different test scenarios, characterized by one DoS and four DDoS attacks with different intensities. Furthermore, we used the Fuzzy-GADS method instead of HWDS to verify the applicability of the presented game theoretical approach as a standalone Mitigation Module. The obtained results corroborated the effectiveness of both methods, which achieved similar outcomes from anomaly detection metrics, butGT-HWDS fared better for most of the performance tests. Such performanceresults are due to the availability of the Information Module as part of the HWDS method, which provides relevant information about the attack and the SDN to the Mitigation Module. Thus, we conclude that GT-HWDS system is an efficient and powerful defense mechanism for SDNs, avoiding congestion over its central controller by precise mitigation actions. Furthermore, it is possible to conclude that the presented GT-based decision-making approach can be used as a standalone Mitigation Module able to guarantee the proper operation of a SDN, even though it may directly impact on the user experience of legitimate hosts depending on the attack intensity.

For future works, we intend to analyze an adaptable period for the mitigation process to be applied at the SDN while evaluate the game theoretical approach as a standalone mitigation module coupled with different anomaly detection and identification methods. Furthermore, we intend to model different games to enable the mitigation module to counteract different kinds of network anomalies, such as Port Scans and Worms.

APPENDIX

PROOF OF NASH EQUILIBRIUM EXISTENCE

As stated by Nash [38], there always exist Equilibrium points in N-person games. Specifically, on the problem reported in this paper, which is defined as a zero-sumtwo-person game (also known as matrix game), one or more equilibrium points may exist. However, all equilibrium points yield the same payoff for the players, *i.e.*, a Nash Equilibria of the problem is always the optimal outcome. Formally:

Theorem 1: Let G be a two-player zero-sum game defined by $G = (A_{att}, A_{def}, P)$*. Let* (η_{att}, η_{def}) *and* $(\kappa_{att}, \kappa_{def})$ *be two Nash Equilibria of G, then:*

1. *P is the general Payoff since the attacker's payoff is the opposite of the defender's.*
2. $P(\eta_{att}, \eta_{def})=P(\kappa_{att}, \kappa_{def})$

Proof: The first part of the Theorem 1 is achieved by the definition of zero-sum games, where:

$$P_{att} + P_{def} = 0 \tag{19}$$

As (η_{att}, η_{def}) is one of Nash Equilibria, the attacker player, who tries to maximize P, cannot change its strategy without reducing P, *i.e.*:

$$P(\eta_{att}, \eta_{def}) \geq P(\kappa_{atk}, \eta_{def}) \tag{20}$$

However, $(\kappa_{att}, \kappa_{def})$ is another Nash Equilibrium of the problem, and the defense system player, who aims to minimize P, cannot change its strategy without increasing P:

$$P(\kappa_{atk}, \eta_{def}) \geq P(\kappa_{atk}, \kappa_{def}) \tag{21}$$

Combining these two inequalities we achieve:

$$P\left(\eta_{atk}, \eta_{def}\right) \geq P\left(\kappa_{atk}, \eta_{def}\right) \geq P\left(\kappa_{atk}, \kappa_{def}\right) \tag{22}$$

which proves the part 2 of the Theorem.

Thus, although we only found one of the Nash Equilibria on all performed games through the tests of our proposed decision-making system, there may be two or more equilibrium points [38]. However, as the game described in this paper is a zero-sum two-player game, all Nash Equilibria points have the same Payoff value, i.e., it is irrelevant which one is chosen as the game answer.

REFERENCES

[1] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS attacks: Trends and challenges," *IEEE Commun. Surveys. Tuts.*, vol. 17, no. 4, pp. 2242–2270, 4th Quart., 2015.

[2] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 602–622, 1st Quart., 2016.

[3] W. Li, W. Meng, and L. F. Kwok, "A survey on OpenFlow-based software defined networks: Security challenges and countermeasures," *J. Netw. Comput. Appl.*, vol. 68, pp. 126–139, Jun. 2016.

[4] S.-S. Seo, Y. J. Won, and J. W.-K. Hong, "Witnessing distributed denial-of-service traffic from an attacker's network," in *Proc. 7th Int. Conf. Netw. Ser. Manage. (CNSM)*, Oct. 2011, pp. 1–7.

[5] A. Kind, M. P. Stoecklin, and X. Dimitropoulos, "Histogram-based traffic anomaly detection," *IEEE Trans. Netw. Ser. Manage.*, vol. 6, no. 2, pp. 110–121, Jun. 2009.

[6] M. H. A. C. Adaniya, M. F. Lima, J. J. P. C. Rodrigues, T. Abrão, M. L. Proença, Jr., "Anomaly detection using DSNS and firefly harmonic clustering algorithm," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 1183–1187.

[7] Q. Guan and S. Fu, "Wavelet-based multi-scale anomaly identification in cloud computing systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 1379–1384.

[8] M. V. O. de Assis, J. J. P. C. Rodrigues, and M. L. Proença, Jr., "A novel anomaly detection system based on seven-dimensional flow analysis," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2013, pp. 735–740.

[9] M. V. O. de Assis, J. J. P. C. Rodrigues, and M. L. Proença, Jr., "A seven-dimensional flow analysis to help autonomous network management," *Inf. Sci.*, vol. 278, pp. 900–913, Sep. 2014.

[10] Y. Cui *et al.*, "SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks," *J. Netw. Comput. Appl.*, vol. 68, pp. 65–79, Jun. 2016.

[11] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, and V. Maglaris, "Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments," *Comput. Netw.*, vol. 62, pp. 122–136, Apr. 2014.

[12] M. Lee, X. Ye, D. Marconett, S. Johnson, R. Vemuri, and S. J. B. Yoo, "Autonomous network management using cooperative learning for network-wide load balancing in heterogeneous networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Nov. 2008, pp. 1–5.

[13] J. Gao, S. A. Vorobyov, and H. Jiang, "Game theoretic solutions for precoding strategies over the interference channel," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Nov. 2008, pp. 1–5.

[14] O. E. Ferkouss and W. Ajib, "Game theory based resource allocation for cognitive radio networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 1174–1179.

[15] M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 920–925.

[16] M. V. O. de Assis and M. L. Proença, Jr., "Scorpius: sFlow network anomaly simulator," *J. Comput. Sci.*, vol. 11, no. 4, pp. 662–674, Apr. 2015.

[17] A. H. Hamamoto, L. F. Carvalho, and M. L. Proença, Jr., "ACO and GA metaheuristics for anomaly detection," in *Proc. 34th Int. Conf. Chilean Comput. Sci. Soc. (SCCC)*, Nov. 2015, pp. 1–6.

[18] C. Basile, D. Canavese, A. Lioy, C. Pitscheider, and F. Valenza, "Inter-function anomaly analysis for correct SDN/NFV deployment," *Int. J. Netw. Manage.*, vol. 26, no. 1, pp. 25–43, Jan. 2016.

[19] J. Li, J.-H. Yoo, and J. W.-K. Hong, "Dynamic control plane management for software-defined networks," *Int. J. Netw. Manage.*, vol. 26, no. 2, pp. 111–130, Mar. 2016.

[20] S. Song, H. Park, B.-Y. Choi, T. Choi, and H. Zhu, "Control path management framework for enhancing software-defined network (SDN) reliability," *IEEE Trans. Netw. Ser. Manage.*, to be published, doi: 10.1109/TNSM.2017.2669082.

[21] G. Poulios, K. Tsagkaris, P. Demestichas, A. Tall, Z. Altman, and C. Destré, "Autonomics and SDN for self-organizing networks," in *Proc. 11th Int. Symp. Wireless Commun. Syst. (ISWCS)*, Aug. 2014, pp. 830–835.

[22] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 447–456, Feb. 2014.

[23] M. Long, C.-H. Wu, and J. Y. Hung, "Denial of service attacks on network-based control systems: Impact and mitigation," *IEEE Trans Ind. Informat.*, vol. 1, no. 2, pp. 85–96, May 2005.

[24] L. F. Carvalho, S. Barbon, Jr., L. S. de Mendes, and M. L. Proença, Jr., "Unsupervised learning clustering and self-organized agents applied to help network management," *Expert Syst. Appl.*, vol. 54, pp. 29–47, Jul. 2016.

[25] C. Röpke and T. Holz, "On network operating system security," *Networks*, vol. 26, no. 1, pp. 6–24, Jan. 2016.

[26] A. Lara and B. Ramamurthy, "OpenSec: Policy-based security using software-defined networking," *IEEE Trans. Netw. Ser. Manage.*, vol. 13, no. 1, pp. 30–42, Mar. 2016.

[27] L. M. Bruce, "Game theory applied to big data analytics in geosciences and remote sensing," in *Proc. IEEE Int. Geosci. Remote Sens. Symp. (IGARSS)*, Jul. 2013, pp. 4094–4097.

[28] Q. Wu, S. Shiva, S. Roy, C. Ellis, and V. Datla, "On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks," in *Proc. Spring Simul. Multiconf.*, San Diego, CA, USA, 2010, pp. 159:1–159:8.

[29] H. S. Bedi, S. Roy, and S. Shiva, "Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows," in *Proc. IEEE Symp. Comput. Intell. Cyber Secur. (CICS)*, Apr. 2011, pp. 129–136.

[30] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2010, pp. 1–10.

[31] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*, 1st ed. Cambridge, MA, USA: MIT Press, 1994.

[32] J. H. Holland, *Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control and Artificial Intelligence*. Cambridge, MA, USA: MIT Press, 1992.

[33] R. L. Haupt and S. E. Haupt, *Practical Genetic Algorithms*, 2nd ed. Hoboken, NJ, USA: Wiley, 2004.

[34] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," *Appl. Soft Comput.*, vol. 10, no. 1, pp. 1–35, Jan. 2010.

[35] L. A. Zadeh, "Is there a need for fuzzy logic?" in *Proc. Annu. Meeting North Amer. Fuzzy Inf. Process. Soc. (NAFIPS)*, May 2008, pp. 1–3.

[36] R. Matias, A. M. M. Carvalho, L. B. Araujo, and P. R. M. Maciel, "Comparison analysis of statistical control charts for quality monitoring of network traffic forecasts," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Oct. 2011, pp. 404–409.

[37] D. C. Montgomery, *Introduction to Statistical Quality Control*, 6th ed. Hoboken, NJ, USA: Wiley, 2008.

[38] J. F. Nash, Jr., "Equilibrium points in n-person games," *Proc. Nat. Acad. Sci. USA*, vol. 36, no. 1, pp. 48–49, 1950.

MARCOS V. O. DE ASSIS received the master's degree in computer science from the State University of Londrina, Brazil, where he is currently pursuing the Ph.D. degree with the Electrical Engineering Department. He is currently a Professor with the Engineering and Exact Department, Federal University of Paraná, Brazil. He is part of the research group Computer Networks and Data Communication. His research interest is in the management and security of large-scale computer networks.

ANDERSON H. HAMAMOTO received the M.Sc. degree in computer science from the State University of Londrina in 2017, where is currently pursuing the Ph.D. degree in electrical engineering. He has experience in computer science with an emphasis in computer networks. He is part of the research group Computer Networks and Data Communication. His main research interests are the management and security of computer networks.

TAUFIK ABRÃO (M'97–SM'12) received the B.S., M.Sc., and Ph.D. degrees in electrical engineering from the Polytechnic School, University of São Paulo, São Paulo, Brazil, in 1992, 1996, and 2001, respectively. Since 1997, he has been with the Communications Group, Department of Electrical Engineering, State University of Londrina, Paraná, Brazil, where he is currently an Associate Professor of Telecommunications and the Head of the Telecomm and Signal Processing Laboratory. From 2007 to 2008, he was a Post-Doctoral Researcher with the Department of Signal Theory and Communications, Polytechnic University of Catalonia, Barcelona, Spain. In 2012, he was an Academic Visitor with the Southampton Wireless Research Group, University of Southampton, Southampton, U.K. He has participated in several projects funded by government agencies and industrial companies. He is involved in editorial board activities of six journals in the telecommunications area and has served as a TPC Member in several symposiums and conferences. He has supervised 21 M.Sc., six Ph.D., and three post-doctoral students, and coauthored ten book chapters on mobile radio communications and over 180 research papers published in specialized/international journals and conferences. His current research interests include communications and signal processing, especially massive MIMO and OFDM/OFDMA systems, detection and estimation methods, cooperative communication and relaying, resource allocation, and heuristic and convex optimization aspects of 4G and 5G wireless communication systems. He is a Senior Member of the Brazilian Telecommunication Society. He has also served as an Editor of the IEEE Communications Surveys and Tutorials since 2013, the IEEE Access since 2016, and the *IET Journal of Engineering* since 2014.

MARIO LEMES PROENÇA JR. received the M.Sc. degree in computer science from the Informatics Institute, Federal University of Rio Grande do Sul, in 1998, and the Ph.D. degree in electrical engineering and telecommunications from the State University of Campinas in 2005. He is currently an Associate Professor and the Leader of the research group that studies computer's network in the Computer Science Department with the State University of Londrina (UEL), Brazil. He has supervised 12 M.Sc. and two Ph.D. students. He has been a master's supervisor of computer science with the State University of Londrina and Ph.D. supervisor with the Department of Electrical Engineering, UEL. He has authored or coauthored over 90 papers in refereed international journals and conferences, books chapters, and one software register patent. His current research interests include computer network, network operations, management and security, and IT governance.