A DoS/DDoS cyber attacks defence framework base on the game theory

Harrison Stewart
Univeril Technology - Information Systems
Institute for Software Technology (IST), University of Koblenz-Landau

2016

ABSTRACT

Game theory models are often utilized in cybersecurity research to investigate the interaction between the attacker and the defender during a distributed denial-of-service (DDoS) attack. DDoS attacks are a continual challenge for industries and academic researchers due to the massive growth of cyber attacks in number, severity, and scope. This paper explores the relevance of the game theory hypothesis as an approach to mitigate DDoS security issues, with emphasis on dynamic bandwidth depletion attacks. Our work targeted the Financial Technology (FinTech) innovation industries where data are valuable assets in their businesss domain. The interactions between the attacker and the defender were modelled via a single-shot, non-unified, zero-sum game. The model was then consolidated with a larger set of attacker choices, building upon previous accomplishments. In this analysis, we considered the worst case scenario, where the attacker, a rational person, endeavors to locate the highest adequate transmitting rate or botnet size. Furthermore, we examined various factors regarding: the expense to carry out an attack; the quantity of attacking nodes; and the probability of malicious traffic conveyances and their parameters. In theory, our approach can be applied to every organization, however, controlling network topology utilizing game theory against a DDoS attack might not be effective due to its unrealistic approach, i.e. the defender has the possibility to redefine his or her configuration at each game. However, we modeled a static-game model to calculate the Nash Equilibrium, which portrayed the best procedure(s) of the defender. We then validated this model via simulations with the NS-3 simulator network.

Keywords; DoS attack, DDoS attack, Game theory, Defense mechanism, Cyber attack.

1.0 INTRODUCTION

Denial-of-service (DoS) attacks, classified as cyber-attacks, are becoming more widespread, and guarding against them is a vital issue in industrial processes, e.g., power plants, due to the usage of control tools during production. These threats can utilize different kinds of software, hardware and other application controls (Miyachi, 2012; Nawa, 2012; Takegami et al., 2013). According to the JPCERT Coordination Center (2008), common features between production control tools and data frameworks have allowed increased cyber-attacks against both data control frameworks and related production control frameworks.

Financial damages due to cyber-attacks

are difficult to estimate due to nonphysical resultant losses. A recent cyber-attack on the Sony© PlayStation Network™ and the Sony© Entertainment Network™ lowered the company's shares by "4.3 percent at $21.21 on the New York Stock Exchange" (Reuters, 2014). This is not an isolated incident, as many institutions, from the financial sector to the government sector, have experienced financial losses as a result of cyber-attacks. According to Wang & Rong (2008), such security breaches have often resulted in the collection of vital information by malicious individuals or groups. Researchers from the United States (U.S.) as well as those from Asian and European countries have conducted many studies that indicate that a country's industrial procedure plants are an essential part of its economy as well as an ongoing demand in infrastructure.

The general consensus is that security breaches due to cyber-attacks have been difficult to contain because of the approaches used in the attempt to solve the attacks. In recent decades, numerous technological advances have been adopted to facilitate advanced monitoring and threat detection; however, performing these tasks cannot be completely automated. Therefore, a human proactive approach rather than an anticipatory approach is a current major initiative in regards to these challenges (Wang *et al*., 2010).

1.1 Gap

Generally, traditional network security utilizes either defensive devices, e.g. firewalls, or a responsive apparatus, e.g. Intrusion Detection Systems (IDSs), or both used in conjunction (Shen et al., 2011). IDS calculations either distinguish an attack signature or recognize peculiar conduct in a framework. During an attack, the defender is informed of an attack by the IDS, which enables the administrator to prevent or alleviate the attack. However, IDSs still depend on ad-hoc plans and are not exceptionally refined. Current IDS innovation may be adequate in preventing occasional attackers that use well-understood procedures, but IDSs still lack outline instruments to fight clever and/or advanced attacks. Traditional and other standard security measures lack quantitative actions, which has caused us to investigate game framework methodologies (Shamshirband et al., 2013; Manshaei et al., 2013; Yan et al., 2012; Manshaei et al., 2010; Roy et al., 2010; Sun et al., 2008; Alpcan, 2006; Liu et al., 2005; You et al., 2003).

1.2 Aims

The research aims to utilize game theory framework ideas with the end goal of understanding a comprehensive attacker to defender approach in order to resolve DoS attack flooding in financial technology industries. This framework should enable us to facilitate and analyze the interactions between an attacker and a defender in a game form where: movements of the attacker embody the amount of nodes utilized and the total node transmission rate; and the movements of the defender embody the management of the flow rate threshold within defense mechanisms that permit the defense mechanism to block nodes of traffic with transmission rates higher than the threshold. The simulations will use the Network Simulators 3.0 (NS-3), an open-source, discrete-event network simulator, to help confirm the precision of the game theory framework as well as to uncover fluctuations during connectivity of data at the early stages of a simulated denial of-service attack.

1.3 Objectives

The main objectives of this research are:

1. investigate the relevance of game theory in DDoS issues and to analyze the shortcomings of traditional system security solutions caused by the absence of quantitative decision frameworks. It is hypothesized that the

model will enable us to both demonstrate and analyze a DDoS attack via a mathematical framework, since game theory regards issues where opponents compete.

2. diagnostically exhibit that there is a solitary, ideal methodology accessible to the defender and that by choosing this methodology, the defender defines a maximum threshold which intelligent attackers may achieve while non-rational attackers will not.

3. improve the model by using the NS-3 to conduct various simulations. The accuracy of the model can also be determined after the simulated environment has replicated the model's analytical parameters. It is hypothesized that the simulations generated in the NS-3 will help verify the game theory model and uncover data fluctuations during connectivity at the early stages of a simulated DoS/DDoS.

This paper is organized as follows. Section 2 is a related work of DoS/DDoS cyber-attack models. Section 3 is a review of game theory foundations and a presentation of all fundamental knowledge on game theory used in the current study. In Section 4, a game theory framework is presented in conjunction with logical processing and consequences of its application on an advanced network setup. In Section 5, we describe the outcome of the simulations in the NS-3 and how this substantiates the framework. Finally, Section 6 examines conclusions drawn from the previous sections.

2.0 RELATED WORK

Previous studies have proposed numerous defense mechanisms to mitigate DDoS attacks (Abliz, 2011). Most of the identified strategies were ultimately ineffective due to the concentration on the node-to-node approach rather than the (D)DoS issue itself. Even though the strategies addressed DoS attacks effectively, they still lacked effectiveness in DDoS attacks when the node-to-node approach is remodeled by attack dynamics into an attacker-to-defender approach. Therefore, conventional procedures may not be effective solutions as they neglect the conduct and choices of the attacker.

Yatagai et al. (2007) stated two basic proposals to distinguish cyber-attacks: (i) when attacks occur from numerous clients and use the same virus, the server cannot differentiate the order of browsed pages; and (ii) attackers spend less time browsing a web page compared to legitimate users, so a user who spends less time browsing a web page than an average threshold is likely to be an attacker. However, a single attacker might send requests via zombie machines for random pages, so the first proposal may be too simple to encompass the issue. The second theory is not a tenable threshold because, on the other hand, the longer the attacker browses a web page, the greater the chances to bypass the detection zone.

Recently, numerous studies have concentrated on selecting the ideal defense procedure to increase the level of security. Numerous hypotheses have been incorporated and game theory is one of the primary methodologies. Dingankar and Brooks (2007) observed that DDoS attacks are a game in which a defender tries, via optimum network topology, to prevent an attacker from placing zombies in the network. According to them, this is a fairly played game since each player is given the opportunity to make one step or decision at a time. In each phase the defender is forced to select one network topology for the network configuration. The defender initiates the game by choosing an optimum network

topology. This process enables the defender to locate the "loop" game, which enables him or her to return to the initial previous configuration. However, controlling network topology utilizing game theory against a DDoS attack might not be effective due to its unrealistic approach, i.e. the defender has the possibility to redefine his or her configuration at each game. Lack of overhead in movements is also another aspect, since cost is not involved.

The game theory was further utilized by Sun et al. (2008) to analyze and encourage technique recommendations for defender association and data security investment. They detailed the issue of two associations putting resources into security with parameters, e.g. for speculation, security hazard, and troubles and demonstrated a pay-off matrix. A Nash Equilibrium analysis was used to demonstrate consistency for both immaculate and blended strategy. Sun et al. (2008) maintained the contribution as rational by presenting a punishment parameter associated with non-investment. They then introduced a proposal to support organizations that venture into data security as well as used cryptographic puzzles according to the Merkle (1978) approach. However, Merkle (1978) utilized puzzles for key agreement, rather than control of access.

Juels and Brainard (1999) applied client puzzles to TCP SYN flooding while client puzzles were applied by Aura et al. (2001) to authentication protocols, in general. A client puzzle was introduced by Dwork and Naor (1992) as a general possibility to influence resource utility, particularly for managing garbage email. Their plans were based along a diverse axis that is fundamentally persuaded by the desire for the puzzles to obtain easy routes if a bit of vital information is recognized. A puzzle-based defense can be attacked if the attacker is aware of the defender's conceivable activities, e.g. if the defender adopts complicated puzzles, the attacker can react indiscriminately to them with false solutions. Along these lines, he or she (s/he) can potentially fume the defender resources involved in solution validity. However, if the administrator adopts uncomplicated puzzles, this makes it easier for the attacker to solve the puzzles and perform an exceptional attack due to the ineffective mechanism. Also, regardless of the fact that the administrator appreciates competent low-cost approaches for developing puzzles and confirming solutions, the puzzles s/he deploys need to be effective but with less complications, i.e. ideal puzzles with high quality of service for authorized users. Hence, puzzle difficulty should be precisely balanced to protect mechanism viability and excellency. Even though several mechanisms, e.g. those of Feng et al. (2005) or Wang & Reiter (2003), have endeavored to alter the difficult class of puzzles according to the loads of the victim, these mechanisms are not dependent on an appropriate protocol and fail to consolidate the above study and hence, those mechanisms' viability is still uncertain (Mehran & Fallah, 2010).

The largest duty in the game hypothetical model is the abnormally-based Wireless Sensor Network (WSN). This is caused by the conveyed ways of various players in Wireless Sensor Networks (WSNs). A substantial sum of players adds more difficulties in achieving equilibrium. Naserian and Tepe (2009) adopted game theory to control attacks in WSN. For example, they added the non-cooperative, non-zero, and two-player concept into their game theory. In this game, excellent options are made in accordance to the laws governing the circumstances of the payoff. Shen et al. (2011) converted the conveying game into an IDPS game that determined and displayed the interactions between an attacker and a WSN cluster head. The basis for their model was a combination of a Bayesian Nash Equilibrium (BNE) strategy and blended techniques for extraordinary recognition guidelines. Thus, a

perfect crucial defense strategy was developed to ensure the accomplishment of WSNs, whereby the probability of distinguishing attacks was simultaneously significantly improved. The notoriety defense mechanism accomplishes an active role by considering the three limitations of bootstrap time, energy, and reputation. This methodology ousts profoundly non-collaborative and harmful nodes from the server (Misra & Vaish, 2011).

Sallhammar (2006) utilized a probability game to evaluate the behavior of the attacker. A two-person, zero-sum Markov game was suggested by Alpcan (2006) for grabbing interactions between enemies and an IDS. A straightforward queuing model for the SYN-flooding attack was suggested by Chang (2002), and Khirwadkar (2011) utilized a repetitive game to model attacker interactions. To obtain the probability of packet loss, Gligor (1983, 1988) argued on the need to take serious action to define DoS. Gligor proposed that the Maximum Waiting Time (MWT) needs to be designated to every service provided. Wang (2007) assessed DoS attacks on PC systems utilizing a lining model. Crosby (2003) introduced a sample of a bandwidth attack, but the sample lacked attack detection and DoS attack prevention and had a low vulnerability algorithm. Warrender and Forrest (1999) exhibited a model that can distinguish DoS attacks. In their model, one program needs to complete running before a new one can be executed, assuming the program utilizes more than one source.

In computer networks, game theory is another application for network security, e.g. equilibrium examination and defense mechanism models are compiled (Manshaei et al., 2010; Roy et al., 2010; You et al., 2003). Walfish et al. (2006) proposed a hostile technique against DoS attacks by proposing the utilization of offense as defense. In their work, the defender supports the network legal nodes to expand their rate of transmission when the attacker attempts to carry out a DoS attack, under the presumption that the entire bandwidth capacity of the attacker is being utilized rather than legitimate clients. This enables authorized clients to seize a larger proportion of the resources on the server being attacked, beating out the attacker. This methodology is thought to be viable under certain conditions, but the primary hindrance is that, in the event that a few clients increase their sending rate, they are obstructed due to congestion. Furthermore, the bandwidth can only be shared fairly among the legitimate clients if they all set practically indistinguishable sending rates.

The areas of game theory which are significant to information warfare were illustrated by Hamilton et al. (2002). This study analyzed situations requiring various courses of actions (COA) including anticipated results and what/if sequences. The algorithm of hill-climbing was recommended to detect adversary moves in advance and ideal weights were discovered by deploying a linear programming strategy utilizing pattern recognition. Both the automatic tuning of assessment capacities and Deep-Blue were recommended. Hamilton et al. (2002) concluded with conjecture regarding the incredible conceivable outcomes in the application of a game theory hypothesis to information warfare. Their work focused on a persuading illustration to show the utilization of game theory in network security issues, while our work focus on a defense mechanism to solve DoS/DDoS attack scenarios.

Yan et al. (2012) designed a game-theoretical framework for assessing DDoS attack and defense. This work examined the circumstances that influence the decision of both the attacker and the defender when a multi-layer barrier is constructed. Liu et al. (2005) assembled models for attacker expectations, objectives and techniques. The attacker cases are classified into nine types from

measurements of agility and precision in interruption detection, and connection among attack activities. Liu et al. (2005) concluded that the utilization of game theory could be deployed to surmise attacker aim, targets, and methods, thereby enhancing cybersecurity. The consolidation of the defense graph by Jiang et al. (2009) enabled the calculation of strategy expense. A game theory model was then deployed to choose the ideal defending strategy. Bedi et al. (2011) modeled a bandwidth depletion attack which focused on the probabilities of permitting, diverting, and dropping incoming traffic. The ideal estimations of the probabilities were determined with game theory methodology.

Wu et al. (2010) realized how the utilization of firewalls as defense mechanisms in the game theory can enhance cyber-security and decrease communication overheads. In their experiment, the defender deployed various firewall regulations to prevent malicious traffic and allow authorized users, while the attacker deployed a persuasive botnet to compromise the network. The model is a static game involving single-shot and two players, with each player adapting their own strategy from the initial stage. Even though this model seems to be a large interaction between both players, it can be rendered untenable due to the restriction of options for both players. This work was expanded by Bedi et al. (2011) who incorporated the use of honeypot and defense mechanisms against DDoS attacks on TCP-Friendly Rate Control (TFRC) to detect attacker intention(s). However, their work was also limited by restrictions. Unlike the other forms of attack, Leguay et al. (2007) took into account the challenges inflicted when the defense mechanisms are enhanced.

The research in this dissertation concentrates on data bandwidth consumption DoS or DDoS attacks, where attacker conduct is demonstrated by the decision of the amount of zombie nodes and their stream frequencies received from a random value. The increments in attacker move difficulty are hypothesized to enhance the dependability and proficiency of the initial model.

3.0 BACKGROUND OF GAME THEORY

Game theory is a concept whereby every player picks a strategy that derives the highest conceivable reward while simultaneously foreseeing the intelligent strategies from the opponent. A chosen strategy is abided to by each player throughout the game, no matter how situations change. The steadiness of the game is depicted using the Nash Equilibrium, i.e. a change in a player's strategy will decrease the payoff of each opponent, assuming that all players are to abide to their chosen strategy.
Game theory can be used in different models such as *static game* or *dynamic game*. The *static game* is a single-shot game in which strategies which have been picked by each opponent are made *simultaneously*. The *dynamic model* involves multiple stages in which strategies can be changed at any time and where each opponent can always reconsider the arrangement of activities at the start of the game and at any other time point (Alpcan & Basar, 2009). The point equilibrium under this model can shift such as the initial strategy chosen by the player *(rZ, m, M)* as seen in Figure 1. Focusing on the Nash Equilibrium in the *dynamic* model involves complexity in contrast to the *static* model. Due to space restriction, we abide to the *static game* theory concept our work.

The game theory hypothesis regards conflict and interaction between different competing rational entities, i.e. cases where different players battle one another. This type of interaction furnishes the logical architecture of the current work in the analysis and demonstration of network system security cases. For illustration, defender and attacker can be

considered as contending players taking an interest in a game. Utilizing game theory will allow us to examine a large number of conceivable situations prior to making the best move. Consequently, this can allow network analysts to make sophisticated choice procedures. Thus, several game theory methodologies have recently been proposed to address network security issues (Yan et al.,2012; Manshaei et al., 2010; Roy et al., 2010; You et al., 2003; Sun et al., 2008; Liu et al., 2005).

4.0 METHODOLOGY

We based our work on the *static game* by which each opponent picks and abides to a chosen strategy. The model includes more choices by the attacker's side and permits us to elaborate the interaction between the attacker and the defender.
This study concentrates on the design and methods of data bandwidth consumption DoS/DDoS attacks where each flow rate and number of zombie nodes received from a random value distribution demonstrates the attacker conduct (Bedi et al., 2011). The game steadiness is depicted using the Nash Equilibrium as studied by Alpcan et al. (2009), which is the focal idea in the speculation of games and the most generally used framework for reckoning the payoff of a key relationship in the Social Sciences (Nash, 1950). This concept was first demonstrated by John Nash (Nash 1951), wherein each player maintains his or her strategy till the end of the game. Simply put, if one player changes his or her strategy during the game, there is no benefit increase or extra score for this player, supposing both players are to abide to a constant strategy policy. The Nash Equilibrium concept is a solution that will elaborate a fixed condition (strategy) for the game in which each participator gets the best marks. However, there could be multiple occurrences of Nash Equilibrium in a game, but with this concept, each player keeps his or her strategy no matter what action the other player undertakes. The current author focuses on the node-to-node approach due to its effectiveness (e.g. as in Yan et al. (2012)) rather than the (D)DoS issue.

We utilized two opposite players (attacker and defender) in a non-cooperative, single shot, and zero-aggregate game where the attacker's aim was to deploy the ideal setup parameters for the attack and interrupt service with no cost or as little cost as possible (e.g. as in Naserian and Tepe (2009)). The defender deploys the ideal firewall setup parameters so as to repulse the attacker and win the highest payoff (e.g. as in Wu et al. (2010)).

In this study, the worst scenario was taken into higher consideration in the model by considering the attacker as a reasonable opponent who attempts to win the highest score in the game (e.g. as in Wu et al. (2010)). We regarded the model as a single-shot game strategy, since each player picks his or her methodology which s/he needs to abide to until the end of the game. Due to the lack of collaboration between the two players, we regarded the game as non-collaborative (e.g. as in Naserian and Tepe (2009)).

Ultimately, as per Lin et al. (2009) information warfare games involve an attacker and a defender, and most of the time, one player's gain is at the loss of the other player. Therefore, we regarded the game as a zero-aggregate, i.e. the payoff of the defender is equal to the attacker payoff. To identify the Nash Equilibrium of the model, we incorporated the saddle point theorem to deliver the most favorable strategies for both parties (e.g. as in Wu et al. (2010)). The saddle point theorem is in the form of a game matrix. For illustration, suppose (a and b) are both fixed equilibrium strategies in a matrix game M, then the entry (ma,b) of M will become a saddle point. Assuming G represents our game theory,

then the attacker and defender become fixed equilibrium strategies in the game G. We used the NS-3 for simulation instead of the NS-2 due to the NS-3 improvements in the core architecture, models, software integration and educational components from the NS-2 (Riley, 2010; NSNAM, 2015).

4.1 Network Topology

As shown in Figure 1, we utilized the dumbbell system topology, a successful method for displaying a DoS/DDoS attack (Shevtekar and Ansari, 2009; Floyd and Kohler, 2003; Wu et al., 2010). The right-end corner is signified with a server (S), and the switch on the other side was indicated with SW. Closer to the switch is the firewall (FW) that hosts the defense mechanism. The network bottleneck is between the pipe *P1* and *P2* located between the firewall and the switch (SW), and this is vulnerable to a DoS/DDoS attack where the attacker tries to devour all the accessible data transfer bandwidth by entering revolt action so as to make the server inaccessible for its legitimate clients. A perimeter router (PR) to transmit traffic is on the left of the firewall.

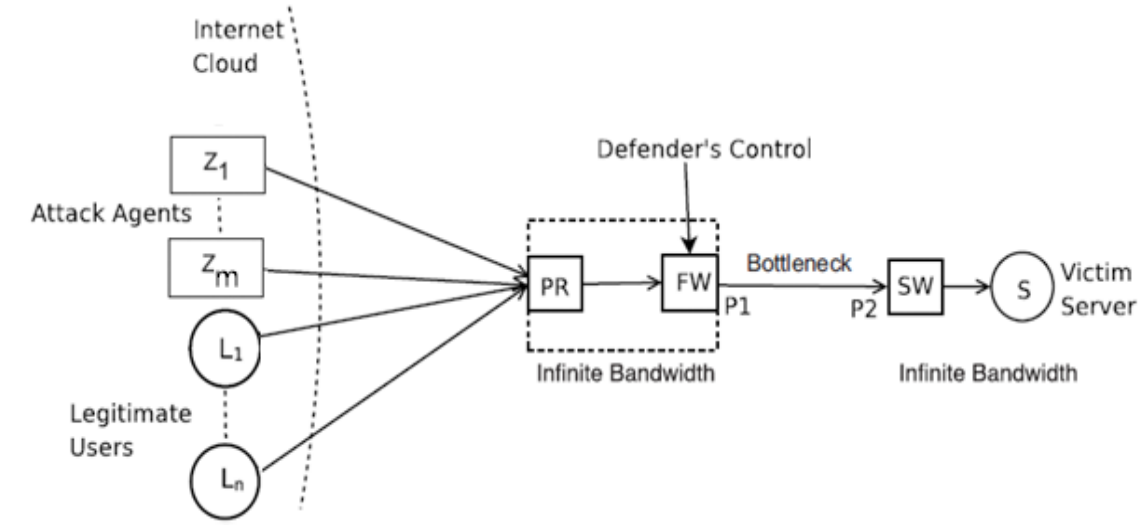

Figure 1. Dumbbell network topology.

To keep the model simple, we assumed that the transmission between the perimeter router and the firewall, alongside the data transfer capacity between the switch and the server, to be boundless (e.g. as in Wu et al. (2010)). As seen in Figure 1, the internet, comprised of legitimate clients, is signified by $L_i, i \in [1,n]$ and located on the left side of the network topology. The *n* indicates the legitimate clients willing to interact with the server S. The main action accessible to the attacker is to determine the flow rate and to pick the *m* number of attacking nodes. We assumeed a flow rate equal to all attacking flows, which is indicated with *m*, near *rA*. The attacking nodes are indicated by $Z_j, j \in [1,m]$, where *m* indicates the number of nodes under the attacker's control. The attacker was assumed to carry on a DDoS attack to consume the pipe's $(P1, P2)$ highest bandwidth. Both legitimate and attack nodes were considered to generate User Datagram Protocol (UDP) traffic. By setting $m = 1$, we were able to present a DoS attack by a basic version of the DDoS framework. The attacker, Z, manages *m* attacking nodes that can transfer fake packages. A DoS attack is an exceptional instance of a DDoS attack when $m = 1$. Dependable modeling of the flow of internet is an essential issue for network simulation; therefore, it is vital to model the movements of

UDP traffic as arbitrary numbers obtained from a particular law of distribution or blended distribution of laws, e.g. Exponential, Normal, Constant, Pareto, etc. (Bedi et al., 2011). For the study of the model, we adopted the Wu et al. (2010) methodology, in which each authentic client transmits its traffic to the network at a particular consistent flow rate displayed as an irregular variable that pursues the normal distribution of law. Table A illustrates the tabulation of all documentations utilized in the mathematical models.

Table A. Notations and abbreviations used in the model.

Symbols	Meaning
S	Server of the victim
PR	Perimeter router
FW	Firewall
SW	Switch
P1	Going out point from the firewall (FW)
P2	Coming point to the switch (SW)
B	Bandwidth of both pipes (P_1P_2)
n	Number of legitimate clients
m	Number of assaulting nodes
r_l	Bit rate expected
σ_l	the standard deviation of a legitimate flow rate
r_A	the bit rate of an attack flow
γ	the minimum bit rate for a flow to be considered alive

4.2. Legitimate Client Profile

Aware of the importance of network simulation when modeling internet flow, we abided to good practice by modeling UDP traffic flow as arbitrary numbers obtained from approved laws of distribution or combined laws, e.g. Exponential, Normal, Constant, etc. (Bedi et al., 2011). However, in this study, traffic was sent by each legitimate client to the server at a particular consistent flow rate demonstrated as an arbitrary variable that pursues the Normal distribution as in the work of Wu et al. (2010), i.e. $X_i \sim \mathcal{N}(r_l, \sigma_l^2), i = 1,2,...,n$ where $\boldsymbol{Xi}$ signifies the transmission rate of the ***i*-th** client, and the mean estimation of an authentic client's transmission rate is $\mathbf{r_l}$, and the standard deviation is s_l. The bit rate of an attack flow is r_A. The σ_l also represents the standard deviation for legitimate clients' flow rate. Along these lines, the aggregate approaching flow rate with no attack is $T^{na} = X_1 + X_2 .... + X_n$. Based in basic probability laws, we generated: $T^{na} \sim \mathcal{N}(n \cdot r_l, n \cdot \sigma_l^2)$. The pipe bandwidth B is picked such that $\boldsymbol{T^{na}}$ **< B** maintains a high probability. The bandwidth of the bottleneck is

constantly larger than the bandwidth consumed by legitimate client. This helps to prevent package loss caused by legitimate clients, which could cause bottleneck congestion.

4.3 Without Defense Mechanisms

In the initial stage, we determined the attacker result when the defender is not utilizing the firewall (e.g. as in Fallah (2010)). In doing so, the aggregate result for the attacker will rely on: i) normal transfer speed utilized by the nodes of zombie; ii) total number of authentic clients lost due to the zombie nodes bandwidth consumption; and iii) quantity of zombie nodes utilized by the attacker. The final part offers a negative outcome because the more zombie nodes the attacker utilizes, the bigger the expense s/he pays. This expense is based on the exertion that the attacker needs to make for specific end goal of transforming authentic clients into zombie nodes. The expenses increase if the threshold is higher. It is therefore obvious that the absence of the defense mechanism enables all packages to pass the firewall. Still, only a small fraction is able to pass through the pipe **(P1, P2)** if ***T > B***. In the model, α signifies this fraction for each flow. We assumed that the fraction $(1-\alpha)$ of each flow will decline at ***P1***. Supposing **r** is the flow of the bit rate or rate, and then only an αr bit rate or rate will reach the network. Still basing this on a zero-sum game theory, we estimated that attacker and defender bandwidth resource is shared equally, that is $\alpha = \frac{B}{T}$ (e.g. as in Wu et al. (2010)). It is assumed that we can only consider a flow to be a flow if γ is the minimum flow rate and n_g is the normal number of legitimate flows, which have the capacity to reach the server. This scenario results in the Equation: $n_g = n \cdot P[X_i > \frac{\gamma}{\alpha}]$, where n signifies the aggregate authentic flows and **P[X > x]** constitutes the likelihood that the estimation of the arbitrary variable **X** is greater than **x**. There is also a decrease in the α fraction of every attack movement at **P1**. Therefore, the attacker normal transfer speed utilization rate is indicated in Equation (1) below:

$$= \frac{m \cdot \alpha \cdot r_a}{B} = \frac{m \cdot r_A}{n \cdot r_l + m \cdot r_A}.$$

Whereas the average rate of lost clients compared to the aggregate number of clients is calculated via:

$$\begin{aligned} &= \frac{n - n_g}{n} \\ &= P[X_i < \frac{\gamma}{\alpha}] \\ &= P[X_i < \frac{\gamma(n \cdot r_l + m \cdot r_A)}{B}]. \end{aligned}$$

Thus, the attacker's total payoff was:

$$: w_b^a \cdot v_b^{nd} + w_n^a \cdot v_n^{nd} - w_c^a \cdot v_c,$$

Where w_b^a , w_n^a and w_c^a were the attacker's consumption-related weight coefficients.

Subsequently, the payoff of the defender was modelled as a weighted aggregate and defined as:

$$: -w_b^d \cdot v_b^{nd} - w_n^d \cdot v_n^{nd} + w_c^d \cdot v_c,$$

Where w_b^d , w_n^d and w_c^d are the defender's consumption-related weight coefficients.

4.4 Utilizing Defense Mechanisms

There are four elements comprised in the attacker's technique: i) quantity of zombies utilized; ii) distribution type of flow rate that will be followed by every zombie node; iii) custom deviation; and iv) the mean value of the flow rate, if appropriate for the type of distribution utilized. As argued by Matusitz (2009), wetake the defender's overheads into major consideration by utilizing the firewall to represent the defender's defense mechanism. This firewall will eliminate all pertinent overheads (e.g. as in Fallah (2010)). The rate restriction of User Datagram Protocol movement might reduce a substantial rate of UDP flood attacks (e.g. as in Gill (2009)). The dropping rate of the firewall utilizing a sigmoid function as shown in Equation (5), was modeled by Wu et al. (2010):

$$F(x) = \frac{1}{(1+e^{-\beta\frac{(x-M)}{B}})},$$

In Equation (5), β represents a scaling parameter and M is the parameter indicating the transmitting rate for which the fall rate is 0.5. A sigmoid function is illustrated in Figure 2 where $\mathbf{B} = 100$ units and $\beta = 20$. The firewall drops the package of a flow of rate r with likelihood $F(r)$. It is vital to recognize that some legitimate packages will also get dropped at the firewall. If we increase the threshold of the scaling parameter, then the firewall will function differently by dropping all the packages of a flow with flow rate more prominent than M while permitting all flow packages with flow rate (*rate*) less than M to go through. Thus, Figure 2 illustrates how the firewall has been modelled to allow the defender to reset the value M which is the threshold for packages drops in a flow.

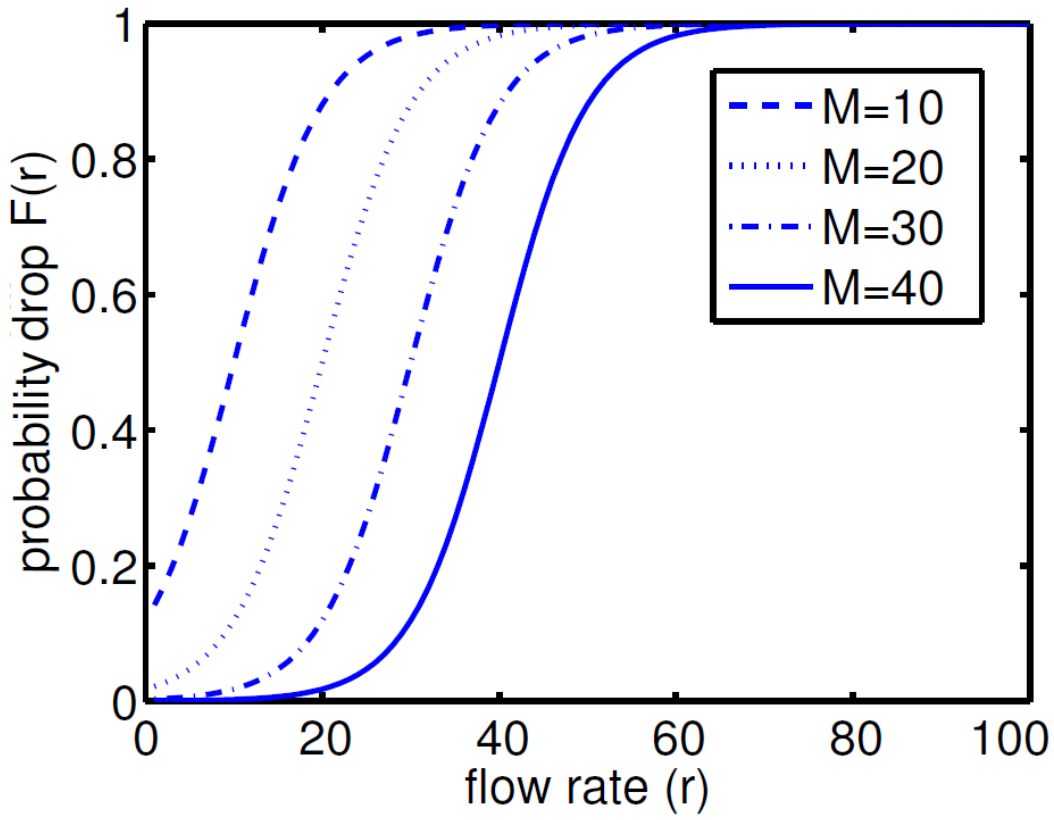

Figure 2. Schemes of a few example S curves. The S curve displays the drop rate of a flow at the firewall. The flow rate is the X-axis, while the Y-axis is the drop probability. The parameter M represents the flow rate when the rate drops to 0.5.

In this case, the r_l signifies the rate of legitimate flow. We also signified the average rate of authentic flow past the firewall with $\mathbf{r'_l}$, allowing: $\mathbf{r'_l = r_l \cdot (1-F(rl))}$, while the average rate of attacking flows going past the firewall becomes: $\mathbf{r'_A = r_A \cdot (1-F(r_A))}$. We then acquired the attacker's rate of average bandwidth utilization if r_A and r_l are substituted by r'_A and r'_l, respectively in Equations (1) and (2):

$$v_b = \frac{m \cdot r'_A}{n \cdot r'_l + m \cdot r'_A}, \quad (1)$$

And, the average lost client ratio to the aggregate number of clients is:

$$v_n = P[X_i < \frac{\gamma(n \cdot r'_l + m \cdot r'_A)}{B}]. \quad (2)$$

Due to the firewall and the blockage, the right-hand side of Equation (7) considers the losses. We could process the attacker's and defender's outcomes V^a and V^d from Equations (3) and (4), sequentially, by supplanting $V^{ad}{}_b$ by V_b and $V^{ad}{}_n$ by V_n.

4.5 *Nash Equilibrium computing and alternative-games*

We utilized the Nash Equilibrium to focus the best strategy profile of both players. The objective was to expand the payoff for each player. The attacker is required to pick ideal values for m and r_A, and in the sigmoid function the defender is required to pick the ideal values for M to be utilized by the firewall. In this game, the Nash Equilibrium was characterized as be a blend of procedures (r^* A, m^*, M^*), which at the same time fulfill the following Equations:

$$V^a_{(r^*_A,\, m^*,\, M^*)} \geq V^a_{(r_A,\, m,\, M^*)} \quad \forall\, r_A,\, m$$

$$V^d_{(r^*_A,\, m^*,\, M^*)} \geq V^d_{(r^*_A,\, m^*,\, M)} \quad \forall\, M$$

At this point we could calculate the Nash Equilibrium strategy profile (r^* A, m^*, M^*), which could have also been obtained via an algorithmic calculation for specific game settings. We used Matlab to diagnostically ascertain the Nash Equilibrium for algorithmic calculation. It was assumed that there were $n = 80$ authentic clients with flow rates received from the normal distribution type and a *mean* $f_l = 50$ kbps and standard deviation $a^2 = 20$. Regarding the network, we assumed 5Mb to be the bottleneck threshold and the base flow rate to be γ = 10Kbps, utilized by the application protocol. Finally, we set the accompanying values for the weight coefficients: $w_b = w_u = 1000$ and $w_z = 5$.

The accompanying analysis demonstrates an intriguing scenario in which the aggregate bytes transmitted by the attacker stayed steady, i.e. no change in $m \cdot r_A$, which implies that the attacker was only required to determine the estimation of m. We will broaden this analysis scenario in future work. For the case of illustration, we assumed that the weight coefficients for both the attacker and the defender were equal: *($w^a{}_b = w^d{}_b$, $w^a{}_n = w^d{}_n$, and $w^a{}_c = w^d{}_c$)*, i.e., $V^a = -V^d$ (in a zero-aggregate game). The attacker's payoff, V^a, for diverse numbers m of attack flows, and distinctive estimations of M with $w^a{}_b$ =1000 and $w^a{}_n$= 1000 as well as $w^a{}_c$= 10, B = 2000, n = 20, r_l = 60, s_l = 20, γ = 10, and $m \cdot r_A = 5000$ is illustrated in Figure 3. We noted a saddle point at at m^* = 22, M^* = 220, representing the Nash Equilibrium and the rate of attacker flow r^*_A = 227.27 relating to m^* =22.

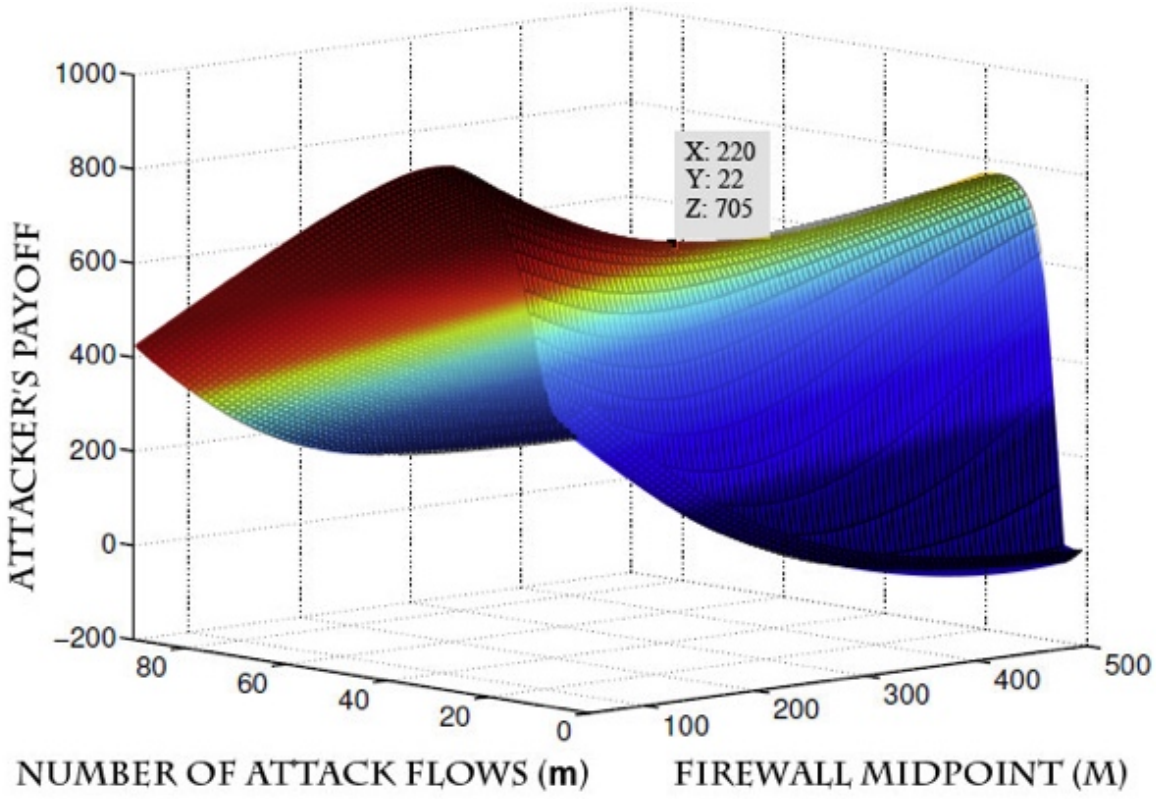

Figure 3. The payoff of the attacker Va for diverse numbers m of attack flows and diverse values of M (the firewall midpoint) m∗= 22, M∗= 220 is the attacker saddle point of observation indicating the Nash Equilibrium.

It is obvious from this game model that a player has no opportunity to alter a chosen strategy. The attacker was not allowed to modify the flow rate r_A value nor the total m of attacking nodes during the game. Additionally, the defender wass not allowed to manipulate the M (firewall midpoint). In this case, the attacker was able to pick the number of zombies for the technique while the M limit was controlled by the defender. It is apparent that the attacker's payoff increases in the lower values of M due to the increase in the likelihood of declining authentic traffic as M approaches the mean value. Then again, the attacker's payoff decreases when the defender expands the firewall threshold. This is normal because less authentic clients are dropped due to the presence of the firewall when M values are high. Nonetheless, the bandwidth utilized by the attacker and the authentic flows that are declined due to the blockage in the bottleneck prevents the payoff from reaching zero. Furthermore, we note that an increase in attacker's attacking nodes results in a lower payoff due to the weight coefficient that the zombie nodes utilize. In this game, the Nash Equilibrium is discovered when 22 zombie nodes are utilized by the attacker and the limit value is set at 220 by the defender. The current payoff is $V_{total} = 705$ as seen in Figure 3.

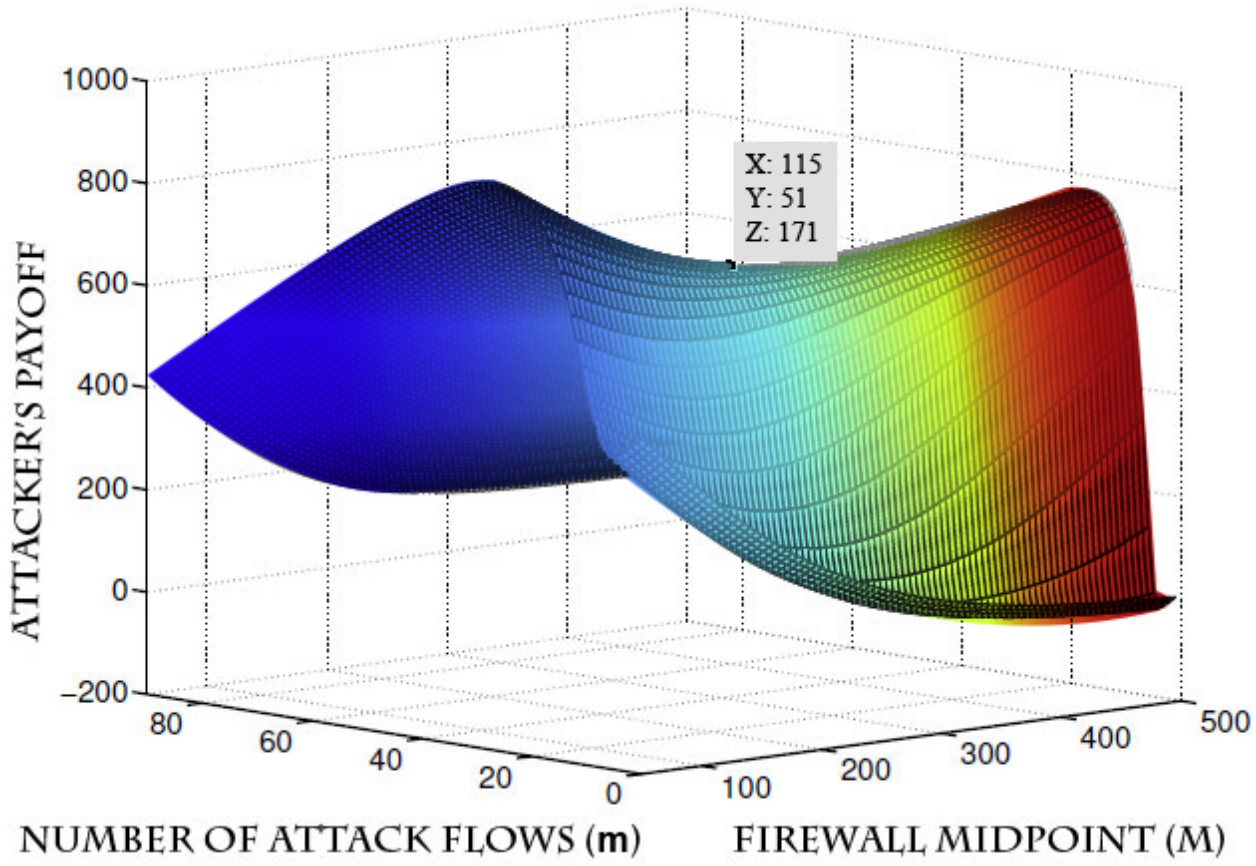

Figure 4. The payoffs for exponential distribution.

In Figure 4 we utilized the same configuration with a single change: an exponential distribution utilized by the attacker. The exponential distribution is seen as the probability of dispersion that portrays the period between events that occurs during a Poisson process. This could be understood as a process where event happen consistently and autonomously at a steady normal rate. In this scenario, the player's payoff is less than the previous when s/he abides to the Nash Equilibrium model. $V_{total} = 171$ is discovered when 51 zombie nodes are utilized by the attacker and the limit value is set at 115 by the defender. Likewise, the attacker's payoff is illustrated in Figure 5 when the Poisson distribution is utilized. Here, at the Nash Equilibrium tip, the payoff is equivalent to the payoff of the normal distribution, $V_{total} = 705$, yet it can be fulfilled when 22 zombie nodes are utilized by the attacker and the limit value is assigned at 260 by the defender, i.e. a greater than normal distribution.

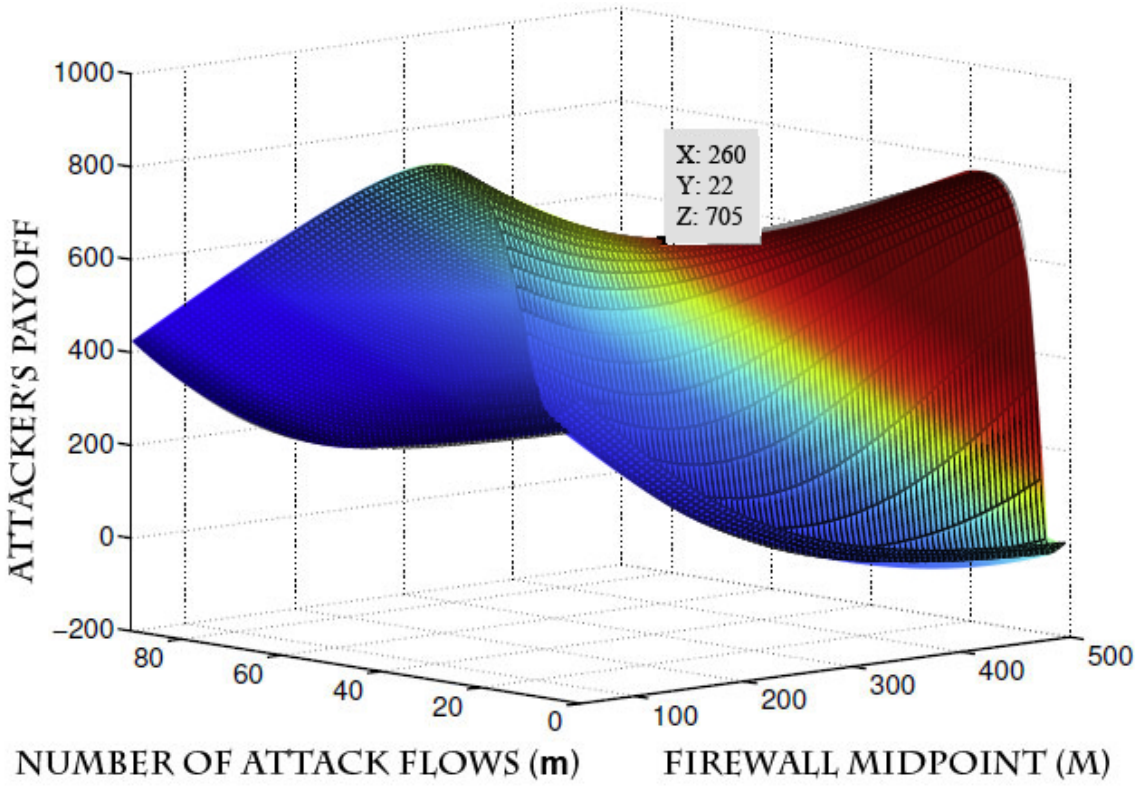

Figure 5. Poisson Distribution payoffs.

At this point we discovered the Nash Equilibrium of the framework by considering the previous case as a sub-game, and by figuring the Equilibria of rehashed sub-games for distinctive estimations of *fz* and diverse sort of distributions and comparing them. Since the attacker controls the *fz* value and the type of distribution, the general Nash Equilibrium was selected in accordance with the attacker's requirements. As such, all the Nash Equilibrium of sub-games with the biggest payoff will be the general Nash Equilibrium.

4.5 *Simulation*

NS-3 is written in C++ and is more advanced than the NS-2. There have been many recent developments based on the FlowMonitor model (Carneiro et al., 2009) to develop applications to monitor package flows. However, this model was unrealistic in the current analysis as it relies completely on the traced output of package data and not the current navigation status in the NS-3's protocol stack. Based on game theory, it was vital for us to design a package-filtering module and gather statistics on it. We then implemented a unique network hook for the package-filtering module, enabling the observation of the package movement information as these certainly travel across area the stack and not at the simulation end.

4.6 *Developing New Modules in NS-3*

We were able to maneuver the normal package-handling schedules in NS-3 with the NetPointFilter module developed. This idea has been generally utilized as a part of Linux for filtering package, mutilating, NAT (system address conversion) and lining packages for client-land survey. Linux's NetFilter creates conceivable associations via the utilization of different hook codes in the network kernel, where those hooks replace the code of a kernel statically fabricated, or as a stacked module able to enroll activities to-be defined for

particular network occasions based on areas inside the protocol stack.

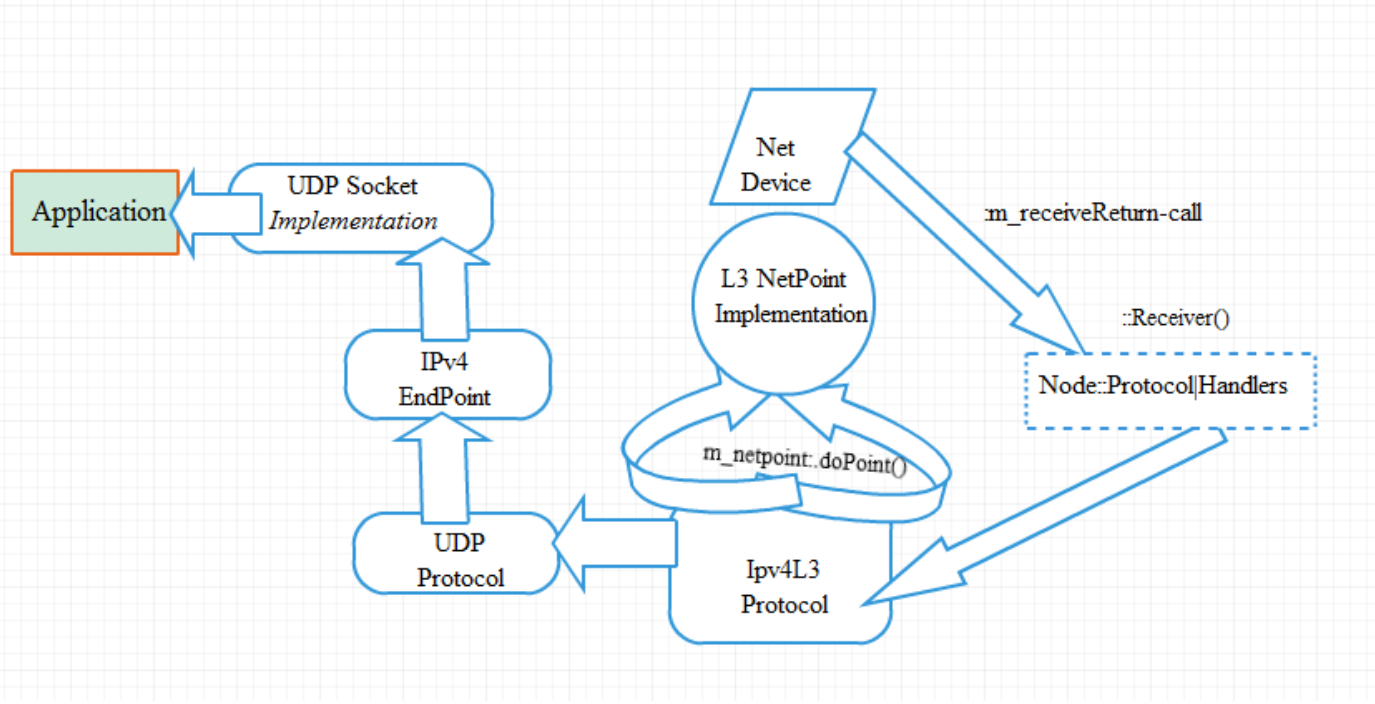

Figure 6. NetPoint implementation. The doPoint() is a function that enables NetPoint, and returns a Boolean value that determines if the package should be refused.

As indicated in Figure 6, the NS-3 NetPoint is conducted via a requested rundown of return-calls related by return-call type with a priority value. The list of the NetPoint return-call was initiated via a call coming inside the current NS-3 code through the procedure doPoint(), and has the capability to execute all random figure of hooks proving the suitable hook sort. The current NetPoint is not restricted to the standard NetFilter in terms of local-in, local-out, forward, pre-routing and post-routing, but instead it provides the adaptability for a NS-3 engineer to actualize an examination return-call at an unspecified area desired inside the NS-3 network framework. The engineer can then decide on the hook point for NetPoint by executing the function-call, including the total NetPoint-object, that suits a particular node inside the topology.

5.0 VALIDATION (Experimental Setup)

We validated the game theoretic defense mechanisms by conducting several stages of experiments in NS-3 to analyze any constraints on the model in a real world scenario network. We then utilized the dumbbell network topology indicated in Figure 1 for simulation. The main aim of this was to observe the influence of control traffic, i.e. if the game theory framework can be employed to data-intensive transactions, e.g. example package filtering, or to determine if the framework is useful in any sense. As shown in Figure 1, our internet world is indicated on the left-hand side embodying $_{L}$ legitimate nodes and $_{Z}$ attack nodes. Both nodes generate UDP traffic at a steady rate as the transport protocol so as to abstain from utilizing an altered TCP stack and re-transmission storms that influence simulation outcomes. Figure 7 demonstrates the core infrastructure (i.e. firewall, edge switch, and perimeter router) relationship and the package-filtering usefulness.

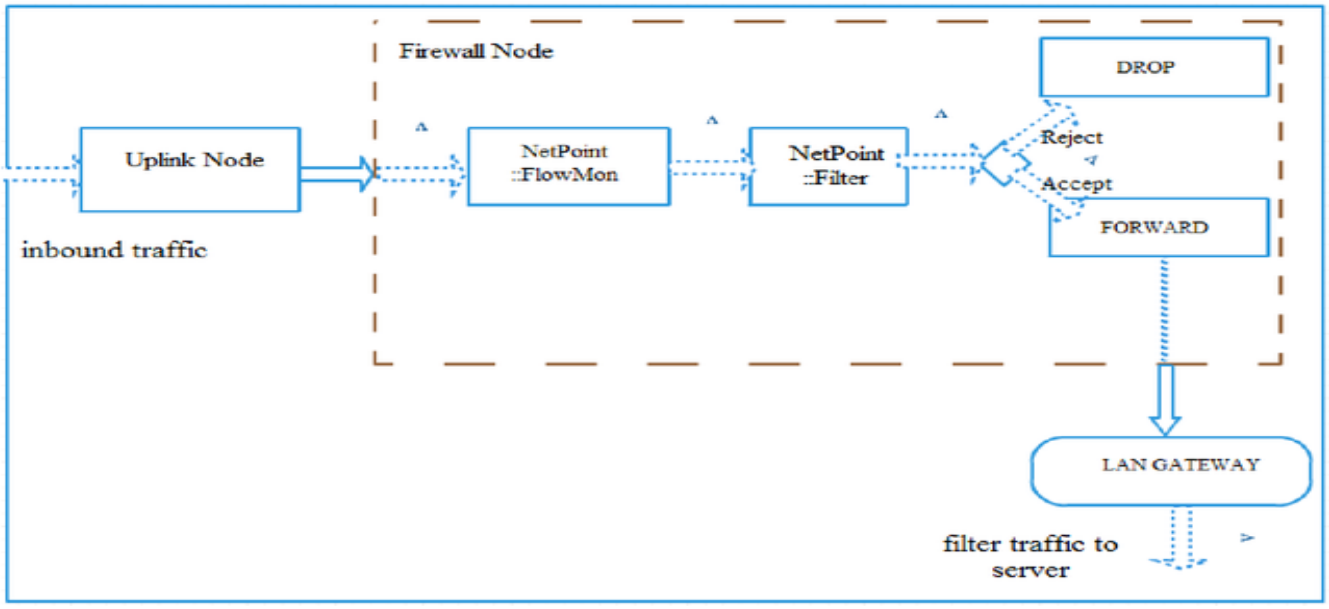

Figure 7. NetPoint Filter joining into trial topology.

The dumbbell network utilized consists of three nodes. The uplink, where both authentic and attacker nodes are joined, is seen on the furthest left node. The package-filter is implemented at the center node of the dumbbell core. The local area network (LAN), which provides connectivity for our server node, can be observed on the far right. Point-to-Point channels were utilized to clarify the simulation topology setup. Both the left- and right-side of the topology consisted of 1.5Gbps of transmission capacity, each accessible with the traffic at the firewall knot. Both authentic users and malicious nodes are setup through the command line with random altercations for the package size, bit rates, and quantity of nodes sent so as to reinforce numerous runs with distinctive setups. We utilized a consistent bitrate generator accessible in NS-3, i.e. the On-Off Application, to produce packages bound to a server.

Our experiment was executed in ten cycles with 60 legitimate nodes consisting of 512 bytes' package size, with a transmission rate of 15Kbps. The first phase consisted of six attack nodes that transmitted at an average sum of 6Mbps, partitioned equitably between every attack node, plus the quantity of attack nodes incremented by six for every round. The filter midpoint was changed three times during each cycle, e.g. 250Kbpps, 520Kbps and 700Kbps accordingly. In total, 100 runs were comprised in each cycle while each midpoint consisted of 40 runs with a constant simulation quantity of attack nodes. Every execution ran for 900 seconds, transferring authentic nodes at a steady rate. In addition, the attacks nodes started from 60 seconds with a maximum executive time of 600 seconds. Literal scenarios without package filtering had the same settings in order to obtain a minimum execution contrast.

We simulated the executions on an Intel® Core™ i5 system with 8Gb of RAM and a speed of 14.04.2 LTS with Linux kernel version 4.0.5. Each execution took five to ten minutes to complete depending on the quantity of nodes present. To ensure the independent replication of the simulation results, there was an increase in the arbitrary number generator of seed value estimation in every run.

5.1 Simulation Results

As previously discussed, we based player payoff upon three components. However, the simulation center of interest was the initial rate of data transmission consumption by authentic and attacking nodes. Our future studies will focus on the second component, and they will examine the fraction of active authentic nodes transmitting at distinctive bit rates. Furthermore, the third segment, which is the attacker payoff, is not within the scope of the current study. Figure 8 shows the adequacy of the current game framework defense system in preventing a DoS/DDoS attack. Figure 9 illustrates the ideal setting possibilities of the attacker, while Figure 10 demonstrates that there is a possibility to decrease the viability of the attack if a suitable midpoint configuration is selected. The indications in these experimental results demonstrate that the attacker can boost the attacking nodes and decrease the bit rate of each node simultaneously, so as to avoid the filter. Alternately, the defender should choose a suitable S-curve midpoint to permit authentic traffic while rejecting the attack traffic. A huge amount of the attack transmission will pass when the S-curve midpoint is set high. These are illustrated in the Figure 3 results where we recognized that there is an ideal configuration for both players.

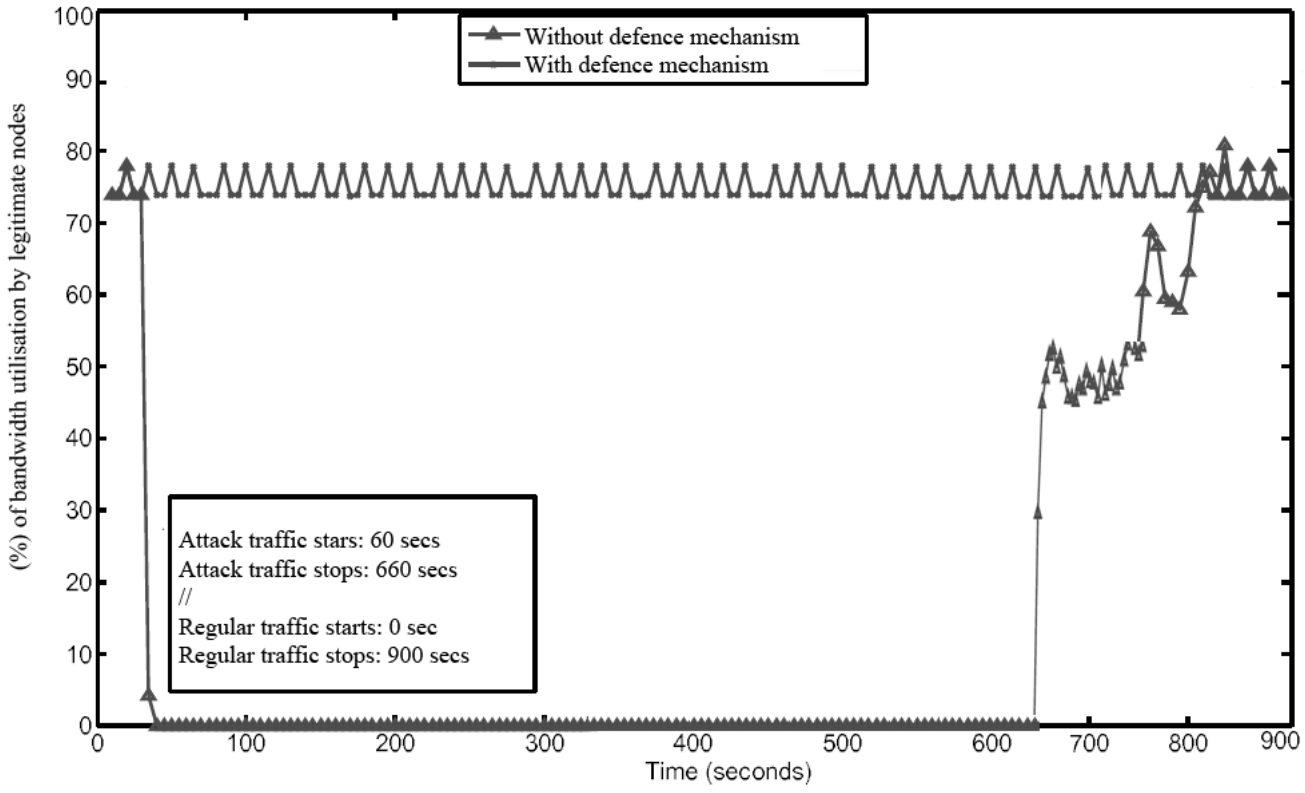

Figure 8. Effect of a DDoS attack on authentic data transmission utilization. Six attacking nodes transferred at 1Mbps (aggregate 6Mbps), 60 authentic nodes transferred at 15Kbps (aggregate 900Kbps), and 600Kbps determined the S-curve midpoint.

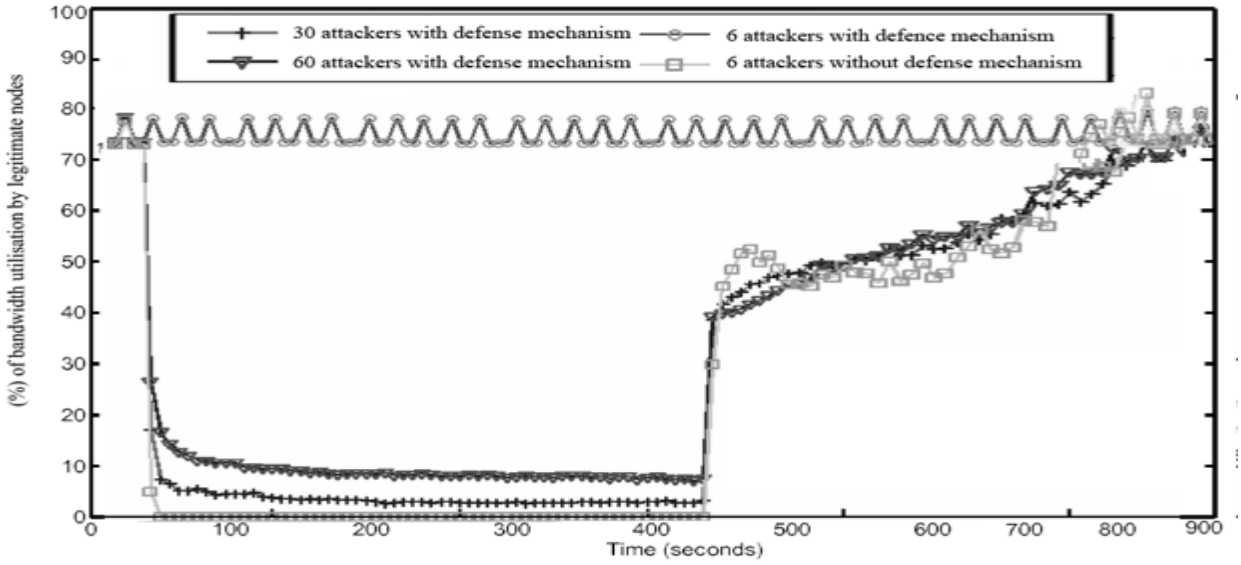

Figure 9. Data transfer capacity utilized by authentic nodes when diversifying the quantity of attack nodes. The aggregate attack bit rate stays at 6Mbps.

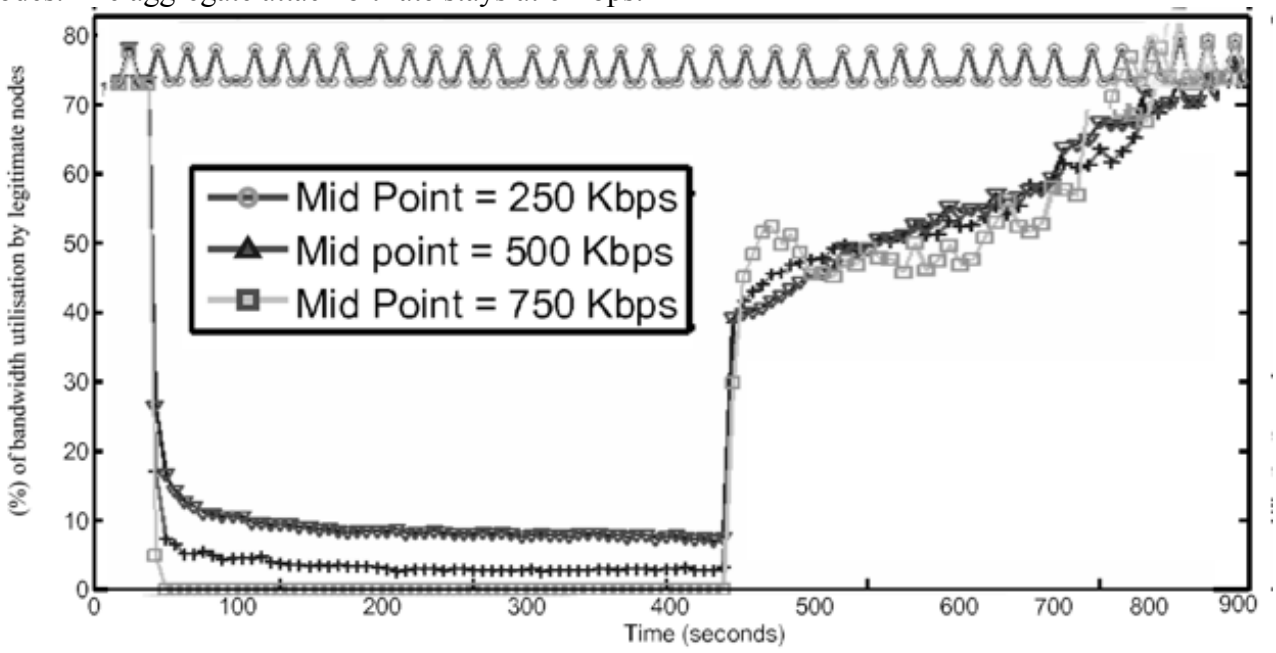

Figure 10. Data transfer capacity utilized by authentic nodes when diversifying the S-curve midpoint. A total of 15 attacking nodes with a constant total attack bit rate stays at 6Mbps.

6.0 CONCLUSION & FUTURE

This study focused on a game theory model as a defense mechanism against DoS/DDoS attacks to depict the interaction between defender and attacker, and provided a holistic methodology for resistance against DDoS attacks. We utilized the NS-3 to validate the analytic results and specifically inspected suggestions for firewall settings and efficiency. This was based upon assumptions regarding activity modeling, different parameters, and host exploitation rate. There is cost involvement for the movement of both parties, classifying the situation to be a form of a game, in which both parties perform to increase achievement. The detailed insight of the player's behaviors was obvious due to the variety of parameters utilized in the model. These data demonstrate that, assuming that the attacker has major concerns regarding attack cost, the defender can embrace an exact firewall layout to decrease expense with little respect in regards to attacker moves.

We tentatively approved the theoretical model outcomes by means of simulations and showed a solid match of the hypothetically calculated qualities and the related simulated information. Nevertheless, we plan to pursue further validations in real world scenarios to guarantee that the model can be useful in any organization. He has planned to extend the work by considering the presence of multiple equilibria in future scenarios. It is also our intent to expand the simulation to integrate a normal distribution, which will enable him to choose the dispatching rate of an authentic movement and explore the relevance of the game hypothesis defense mechanism in situations where the attacker plans to abuse a particular protocol mechanism to enable attacking possibilities.

Additional tasks may incorporate the blend of a framework similar to the one in the current study to investigate a conventional context of internal attackers with insider risk expectation models, as in Kandias et al. (2010). Such joined methodologies may provide exhaustive methods for dissecting the dangers posed by both external and internal sources.

We also plan to stimulate a game in which the attacker and defender are able to adjust strategies during the attack. These outcomes could be utilized by system supervisors and security overseers to improve firewall achievement and organize efficient crosswise defenses over infrastructures that might be vulnerable to DDoS assaults. Due to future developments, the NetPoint module will be contributed to the NS-3 code base to make it accessible to other researchers.

ACKNOWLEDGEMENT

We express immense gratitude towards Mr. Leon Stewart and Ms. Hannah Boateng of Univeril Median and Communication Concern for their valuable opinions regarding the advancement of the present study.

REFERENCES

A. Juels and J. Brainard. "Client Puzzles: A cryptographic defense against connection depletion attacks," In Proceedings of NDSS '99 (Networks and Distributed Systems Security), 1999, pages 151-165.

Abliz M. Internet denial of service attacks and defense mechanisms 2011.

Alpcan T, Basar T. An intrusion detection game with limited observations. 12th International Symposium on

Dynamic Games and Applications; 2006; Sophia Antipolis, France.

Aura, T. ; Nikander, P. & Leiwo, J. (2001). DoS- resistant authentication with client puzzles. Proceedings of the 8th International Workshop on Security Protocols , pp. 170-177, Springer-Verlag, Germany.

Bedi, H.S., S. Roy, and S. Shiva. Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows. in 2011 IEEE Symposium on Computational Intelligence in Cyber Security (CICS). 2011.

Becker, G.: Crime and punishment: An economic approach. Journal of Political Economy76(2) (March - April 1968) 169 - 217

B. Dwork and M. Naor. "Pricing via Processing or Combating Junk Mail," In Advances in Cryptology–Crypto '92. Spring-Verlag, LNCS volume 740, pp. 129-147, August 1992

Chang R. Defending against flooding-based distributed denial-of-service attacks: a tutorial. IEEE Communications Magazine. 2002; 40(10):42–51.

Chen, Y., Hwang, K., 2006. Collaborative detection and filtering of shrew DDoS attacks using spectral analysis. J. Parallel Distrib. Comput. 66, 1137–1151.

Crosby A, Wallach D. Denial of Service via Algorithmic Complexity Attacks. Proceeding of the 12th USENIX Security Symposium. 2003; 29–44.

Dingankar C, Brooks RR. Denial of service games. In: Proceedings of the third annual cyber security and information infrastructure research workshop. p. 7e17.

Floyd S, Kohler E. Internet research needs better models. SIGCOMM e Computer Communication Review 2003; 33:29e34.

G. Riley. (2010) http://www.nps.edu/Academics/Institutes/Cebrowski/Docs/RileyNPS-2010.pdf
(Accessed June, 2015).

Gill S. Maximizing firewall availability. Retrieved July 14 2009.

Gligor V. A note on the denial-of-service problem. IEEE Symposium on Security and Privacy. 1983; 139–49.

J. Wang, X. Liu and A.A. Chien, Empirical study of tolerating denial-of-service attacks with a proxy network, in: *Proceedings of the 14th USENIX Security Symposium*, August 2005, pp. 51–64.

Jiang, W., et al. Optimal Network Security Strengthening Using Attack-Defense Game Model. in Sixth International Conference on Information Technology: New Generations, 2009. ITNG '09. 2009.

Khirwadkar T. Defense against network attacks using game theory [Master's thesis]. University of Illinois at Urbana-Champaign, Urbana, Illinois, 2011.

Leguay, J. et al. 2007, Describing and simulating internet routes, *Computer Networks, Vol.* 51, no. 8, pp. 2067.

Liu, P., W. Zang, and M. Yu, Incentive-based Modeling and Inference of Attacker Intent, Objectives, and Strategies. ACM Trans. Inf. Syst. Secur., 2005. 8(1): p. 78-118.

Manshaei, M., Zhu, Q., Alpcan, T., Bacsar, T., Hubaux, J.P.: Game theory meets network security and privacy. ACM Computing Surveys45(3) (July 2013) 25:1- 25:39

Manshaei M, et al. Game Theory Meets Network Security and Privacy. Technical report. EPFL, Lausanne; 2010.

Miyachi, T. (2012). Protecting the control systems of organizations and firms. Journal of the Institute of Electrical Engineers of Japan, 132(6), 354–358.

Mehran S. Fallah, A Puzzle-Based Defense Strategy Against Flooding Attacks Using Game Theory, IEEE transactions on dependable and secure computing, vol. 7, no.1, pg. 5-19.

Misra, S., Vaish, A., 2011. Reputation-based role assignment for role-based access control in wireless sensor networks. Comput. Commun. 34, 281–294.

John Forbes Nash: Non-cooperative games, Dissertation, Princeton University 1950 – 1951

JPCERT Coordination Center (2008), <https://www.jpcert.or.jp/english/at/2008.html> [Accessed April 2015]

Naserian, M., Tepe, K., 2009. Game theoretic approach in routing protocol for wireless ad hoc networks. Ad Hoc Networks 7 (3), 569–578.

Nawa, Toshio (2012). Protecting organizations and firms from cyber-attacks. Journal of the Institute of Electrical Engineers of Japan, 132(6), 349–353.

NSNAM. (2015). http://www.nsnam.org (Accessed June, 2015).

R. C. Merkle. “Secure Communications Over Insecure Channels,” In Communications of the ACM. April, 1978.

Reuter 2014, *Sony's PlayStation store back online after cyber attack*. Available from: <http://www.reuters.com/article/2014/12/08/us-sony-cybercrime-playstation-idUSKBN0JM1D120141208>. [Accessed April 2015]

Roy S, et al. A Survey of Game Theory as Applied to Network Security. Hawaii International Conference on System Sciences; 2010 Jan 4–7; USA.

S. N. Hamilton, W. L. Miller, A. Ott, and O. S. Saydjari. Challenges in applying game theory to the domain of information warfare. *Proceedings of the 4th Information survivability workshop (ISW-2001/2002)*, 2002.

Sallhammar K, Helvik B, Knapskog S. On stochastic modeling for integrated security and dependability evaluation. Journal of Networks. 2006; 1(5):31–42.

Shamshirband, S., Anuar, N.B., Kiah, M.L.M., Patel, A., 2013. An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique. Eng. Appl. Artif. Intell. 26, 2105–2127.

Shen, S., Li, Y., Xu, H., Cao, Q., 2011. Signaling game based strategy of intrusion detection in wireless sensor networks. Comput. Math. Appl. 62, 2404–2416.

Shevtekar A, Ansari N. Is it congestion or a DDoS attack? IEEE Communications Letters 2009; 13:546e8.

T. Alpcan and L. Pavel. Nash equilibrium design and optimization. *International Conference on Game Theory for Networks, GameNets,* 2009.

T. Yatagai, T. Isohara, I. Sasase, Detection of HTTP-GET flood attack based on analysis of page access behavior, in: Proceedings of IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, Victoria, Canada, 2007, pp. 232–235.

Takegami, M., & Nawa, T. (2013). Business risk management with control system protecting companies from cyber-attacks. In: Abstract presented at the 27th national conference of the Japan Society of Security Management, 85–90, and published materials.

W. Sun, X. Kong, D. He, and X. You. Information security problem research based on game theory. International Symposium on Publication Electronic Commerce and Security, 2008

W. Feng, E. Kaiser, W. Feng, and A. Luu, “The Design and Implementation of Network Puzzles,” Proc. 24th Ann. Joint Conf. IEEE Computer and Comm. Societies, pp. 2372-2382, 2005

Walfish M, Vutukuru M, Balakrishnan H, Karger D, Shenker S. DDoS defense by offence. In: Proceedings of the 2006 conference on applications, technologies, architectures, and protocols for computer communications, SIGCOMM ’06. New York, NY, USA: ACM; 2006. p. 303e14.

Wang, H., Jin, C., Shin, K.G., 2007. Defense against spoofed IP traffic using hop-count filtering. IEEE/ACM Trans. Netw. 15, 40–53.

Wang, J. W. and Rong, L.L. 2008, Effect attack on scale-free networks due to cascading failures, *Chinese Physics Letters, Vol.* 25, no. 10, pp. 3826-3829.

Warrender B, Forrest S. Detecting intrusions using system calls: Alternative data models. IEEE Symposium on Security and Privacy. 1999.

Wu, Q., Shiva, S., Roy, S., Ellis, C., Datla, V.: On modeling and simulation of game theory-based defense mechanisms against dos and ddos attacks. In: *Proceedings of the 2010 Spring* Simulation Multi conference. (2010) 159:1 - 159:8

X. Wang and M. Reiter, “Defending Against Denial-of-Service Attacks with Puzzle Auctions,” Proc. IEEE Security and Privacy, pp. 78-92, 2003.

Yan, G., et al. Towards a Bayesian Network Game Framework for Evaluating DDoS Attacks and Defense. Proceedings of the 19th ACM conference on Computer and communications security - CCS '12, 2012: p. 553-566.

You ZX, Shiyong Z. A Kind of network security behavior model Based on game theory. Proceedings of the Fourth International Conference on Parallel and Distributed Computing Applications and Technologies. 2003.