Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 68A (2014) 22395-22400

ISSN: 2229-712X

Bayesian Game Theoretical Approach for TCP Syn Flooding

K.Gangadhara Rao[1,*] ,B.Basaveswara Rao[1] and K.Chandan[2]

[1]Department of Computer Science & Engineering, Acharya Nagajuna University, Guntur-522501, A.P India.

[2]Department of Statistics, Acharya Nagajuna University, Guntur-522501, A.P India.

ARTICLE INFO

Article history:

Received: 2 July 2013;

Received in revised form:

22 February 2014;

Accepted: 13 March 2014;

Keywords

Flooding,

Game theory,

Matrix.

ABSTRACT

In this paper Game Theory is applied to the context of SYN flooding and modeled the game as a two-person non-cooperative zero sum game between the defender (web server administrator) and attacker (any malicious client). This is basically a static Bayesian game model. The elements of the payoff matrix are computed based on Erlang loss queuing cost model. The numerical illustrations are also provided.

Introduction

The distributed nature of the contemporary networks and complexity of the underlying computing and communication environments prevent administrators and organizations from having absolute control on their networks. Furthermore, network boundaries are often vague, and administrators cannot exercise control outside their local domain, which leaves networked systems vulnerable to distant security attacks due to global connectivity. This results in a perpetual struggle between attackers who aim to intrude the deployed systems and security administrators trying to protect them. The current challenge is to invent and study appropriate theoretical models of cost effective security management in security attacks and defenses. Due to economic and performance reasons, the defender is only able to select a subset of security strengthening measures from a given defense strategy set. The attacks that are of important to the current context are DoS attacks which could be malicious DoS attacks or flash crowds in either of the cases though the intent is different the net effect is same.

A rich set of tools have been developed within the game theory to address the problems where one or more players with the same objectives would interact with a single target. These kinds of theories are successfully used in many disciplines including economics, decision theory and control. Therefore game theory is a strong candidate to provide the much needed mathematical frame work for analysis, modeling, decision, and control processes for information security. Furthermore, by using game theoretic tools, it is also possible to develop practical schemes which can be integrated with the existing solutions for DoS attacks in particular for SYN flooding. Because of these reasons, application of game theory to network security has been a recent topic of interest.

Katsunori et.al. (1999) used game theory to describe a distributed control method for the connection-oriented-type packet network in which they took two players, a connection player and a network player with the gaming mechanism based on mini-max principle. Haitel et.al. (2000) proposed a game theoretic framework for bandwidth allocation for elastic services in high-speed networks. They used Nash bargaining solution from cooperative game theory for characterization of rate allocation and a pricing policy. Yu Liu et.al. (2006) proposed analyzed game theoretic framework for the purpose of providing efficient defense strategies for network with multiple IDE's. They presented an attacker/defender game model in Zero sum game. They showed that in the zero-sum game, the minmax theorem provides an optimal solution for the game, for which defender's equilibrium strategy maximizes the attacker's minimum expected detection loss, and the attacker's equilibrium strategy minimizes the defender's maximum expected payoff of defense. Wei jiang et.al (2007) analyzed the attack prediction and active defense of computer network using the stochastic game theoretic approach. A Markov Chain for Privilege (MCP) model to predict attacker behavior and strategies were proposed. Wei Jiang et.al.(2007) presented a game theoretic method for analyzing the active defense of computer networks. They treated the interactions

Tele:

E-mail addresses: kancherlagangadhar@gmail.com

between an attacker and the defender as a two-player, non-cooperative, zero-sum finite game and formulate an attack-defense game (ADG) model for the game. An optimal active defensive strategy (OADSD) algorithm was developed using ADG and cost-sensitive model. Optimal defense strategies with minimizing costs are used to defend the attack and harden the network in advance. Rui guo et.al (2008) implemented and discussed a Differential Game Model (DGM) to complete with an attacker in case of DDOS attacks. The model was used to determine how a defender combat and protect the servers. Wei Jiang et.al.(2009) presented some models like defense graph model, attack-defense taxonomy and cost metrics, and Attack defense Game (ADG) model to help the system administrator how to select optimal security strengthening measures from a given defense strategy set. They formalized the ADG to solve the selection of optimal security strengthening measures. Yi Luo et.al.(2009) developed a multi-stage attacker defender algorithm(MAD) to help the administrator in defending against the multi-stage attacks. They considered some special scenarios which can be extended and generalized to other cases.

This paper presents two player non-cooperative zero-sum game, i.e. Attacker and Defender Baseyian Game (ADBG) theoretical approach focuses on two main issues. The first one is that in the proposed ADBG, both the defender and the attacker have potentially three different strategies. The second one is that the payoffs for both the attacker and defender systematically relate to the gains computed based on the Erlang loss queuing cost model. In section 2 the formulation and definition of ADBG is presented along with the payoff matrix description. In section3 the computation of the payoff matrix entries using Erlang loss queuing cost model is presented. In section4 Numerical illustration is presented and in section 5 the conclusions and future scope of work are presented.

ADBG Formulation

ADBG is a Bayesian game because the attacker and the defender are with incomplete information, where the defender is assumed to know the intent of the opponent(malicious) however the defender would not know the strategies of the malicious opponent. Bayesian game formulation gives a framework for the defender to select his strategies based on his belief on the type of his opponent and both the players are non cooperative. Bayesian game can be played in two different ways ─ static and dynamic Bayesian game. Static Bayesian game doesn't take into account the game evolution where as the dynamic Bayesian game is a realistic game model, because the defender can dynamically update his beliefs based on new observations of the opponent's actions and the game history, and then he can accordingly adjust his monitoring strategies.

On the lines of Yu Liu et.al. (2006) and Wei Jiang et.al.(2007) the static ADBG game theoretic framework is formulated and the game value is also computed. The proposed ADBG is an illustrative model of SYN flooding in TCP layer where the traffic arriving at the Backlog queue may be malicious/legitimate, it would be exceedingly difficult to differentiate between both types of traffic. Attackers would typically attack the web server with flooding of requests which are to be serviced by the web server and the defender is the characteristic role of the administrator who would try to defend the web server from the traffic/requests that are coming from the attackers. Attacker has the full knowledge of which he is attacking where as the defender doesn't have any knowledge about the attacker, mainly because of IP spoofing.

In the proposed ADBG there are three strategies for the defender and the attacker respectively. The three strategies for the attacker are namely─ attack with variable attacking rate(q_1), attack with constant attacking rate(q_2) and not to attack(q_3). For protecting the system from defender's side to counter play with the attacker are the three strategies─ defend with variable effort (p_1), defend with constant effort (p_2) and not to defend (p_3). The probabilities of the strategies of the attacker are q_1, q_2, q_3 and $q_1+q_2+q_3=1$ and the probabilities of the strategies of the defender are p_1, p_2, p_3 and $p_1+p_2+p_3=1$.

The payoff matrix for the ADBG is as follows.

PAYOFF MATRIX

Attacker

Defender	q_1	q_2	q_3
p_1	gv_1-c_m	gc_1-c_m	$-c_m$
p_2	gv_2-c_c	gc_2-c_c	$-c_c$
p_3	$-gv_3$	$-gc_3$	0

The payoff matrix takes the form of 3x3 matrix, the entries of the matrix are the reward of the defender/attacker when the attacker playing any one of the three strategies combined with the defender's counter play for the respective strategies.

Let c_m is defender's variable effort to monitor and counter the attack by the attacker.

Let c_c is defender's constant effort to monitor and counter the attack by the attacker.

When the attacker is attacking with a probability q_1 ,the defender is defending with a probability p_1 for such a scenario the net gain value of the administrator would be gv_1-c_m .where gv_1 is defender's gain.

When the attacker is attacking with a probability q_1 the defender is defending with a probability p_2 for such a scenario the net gain value of the administrator would be gv_2-c_c .where gv_2 is defender's gain.

When the attacker is attacking with a probability q_1 ,the defender is not defending with a probability p_3 for such a scenario the net gain value of the administrator would be -gv_3 .where gv_3 is defender's loss .

When the attacker is attacking with a probability q_2 ,the defender is defending with a probability p_1 for such a scenario the net gain value of the administrator would be gc_1-c_m .where gc_1 is defender's gain.

When the attacker is attacking with a probability q_2 the defender is defending with a probability p_2 for such a scenario the net gain value of the administrator would be gc_2-c_c .where gc_2 is defender's gain.

When the attacker is attacking with a probability q_2 ,the defender is not defending with a probability p_3 for such a scenario the net gain value of the administrator would be -gc_3 .where gc_3 is defender's loss .

When the attacker is not attacking with a probability q_3 ,the defender is defending with a probability p_1 for such a scenario the net gain value of the administrator would be -c_m .

When the attacker is not attacking with a probability q_3 the defender is defending with a probability p_2 for such a scenario the net gain value of the administrator would be -c_c .

When the attacker is not attacking with a probability q_3 the defender is defending with a probability p_3 for such a scenario the net gain value of the administrator would be 0.

Analysis of ADBG

If one takes a close look at the payoff matrix, maxmin is not equal to the minmax, so that the above payoff matrix doesn't have a saddle point. Hence the calculation of the optimal game value for the mixed strategy is as follows.

If the game value is V an optimal strategy for the defender is characterized by the property that defender's average payoff is at least with the corresponding column of the attacker that is.

$$p_1(gv_1-c_m)+p_2(gv_2-c_c)+p_3(-gv_3)=V \quad (1.1)$$

$$p_1(gc_1-c_m)+p_2(gc_2-c_c)+p_3(-gc_3)=V \quad (1.2)$$

$$p_1(-c_m)+p_2(-c_c)=V \quad (1.3)$$

Solving these three equations one can arrive at the values of p_1, p_2, p_3 and V.

$$p_1 = \frac{V(-gv_2gc_3 + gc_2gv_3)}{(c_mgv_2gc_3 - gc_2gv_3c_m - gv_1gc_3c_c + gc_1gv_3c_c)} \quad (1.4)$$

$$p_2 = \frac{V(gv_1gc_3 - gc_1gv_3)}{(c_mgv_2gc_3 - gc_2gv_3c_m - gv_1gc_3c_c + gc_1gv_3c_c)} \quad (1.5)$$

$$p_3 = \frac{V(gc_2\,gv_1 - gc_1gv_2)}{(c_mgv_2gc_3 - gc_2gv_3c_m - gv_1gc_3c_c + gc_1gv_3c_c)} \quad (1.6)$$

$$V = \frac{(gv_3gc_1c_c - gv_1c_cgc_3 - gv_3gc_2c_m + gc_3gv_2c_m)}{}$$

$$(gv_3gc_2-gc_3gv_2+gv_1gc_3+gv_1gc_2-gc_1gv_3-gc_1gv_2) \quad (1.7)$$

If the game value is V an optimal strategy for the attacker is characterized by the property that attacker's average payoff is at least with the corresponding row of the defender that is

$$q_1(gv_1-c_m)+q_2(gc_1-c_m)-q_3c_m = V \quad (1.8)$$

$$q_1(gv_2-c_c)+q_2(gc_2-c_c)-q_3c_c = V \quad (1.9)$$

$$q_1(-g\,v_3)+q_2(-gc_3) = V \quad (1.10)$$

Solving these three equations for q_1, q_2, q_3 and V one can arrive at the following values

$$q_1 = \frac{V(-gc_1c_c-gc_3\,c_c+gc_2c_m+gc_3\,c_m)}{(gv_3gc_1c_c-gv_1c_cgc_3-gv_3gc_2c_m+gc_3gv_2c_m)} \quad (1.11)$$

$$q_2 = \frac{V(gv_1c_c-gv_2c_m+gv_3c_c-gv_3c_m)}{(gv_3gc_1c_c-gv_1c_cgc_3-gv_3gc_2c_m+gc_3gv_2c_m)} \quad (1.12)$$

$$q_3 = \frac{V(gv_3gc_2-gc_3gv_2+gv_1gc_2+gv_1gc_3+gc_1c_c+gc_3c_c-gc_2c_m-gc_3c_m-gc_1gv_2-gc_1gv_3-gv_1c_c+c_mgv_2-gv_3c_c+c_mgv_3)}{(gv_3gc_1c_c-gv_1c_cgc_3-gv_3gc_2c_m+gc_3gv_2c_m)} \quad (1.13)$$

In order to quantify the gains in payoff matrix, Erlang loss queuing cost model has to be applied to website under DoS attack.

Erlang loss queuing cost model for ADBG

In this section the computation of the different elements of the payoff matrix is considered based on the Erlang loss queuing cost model. For the computation of gains for both attacker and administrator the website that has only one web server is considered. The clients without any consideration for their intent will normally access the information, do a transaction or conduct the business electronically based on the nature of the website. The commercial website administrator has to generate the revenue by providing the services requested by the clients of the website and simultaneously he has to protect the assets of the website. The responsibility of the administrator further extends to maximizing the revenue beyond just generating the revenue. To fulfill this responsibility the administrator must ensure that the legitimate connection would never gets rejected/failed by simultaneously protecting the server from the attacks.

The gains of the defender would depend upon the successful completion of legitimate connections. Based on Erlang loss model, SYN flooding is modeled (explained in 2.2). Daniel Boteanu et.al.(2007) and BBRao et.al.(2009) modeling server under DoS attack as m/m/N/N queuing model, where N is maximum number of half-open connections that can be served at the same time. Based on this analytical model, first the connection failed probability of legitimate connections is computed for various values attack rates and timeout values. Based on that, the gains are computed.

Let a connection expire with probability p_e, μ_c is the legitimate connections service rate and taken the value from the tcpdump data referred in 2.2.3. the value is 0.33333. Let c_e be the connection expired probability (the server tried to serve the connection but not succeeded within a timeout value , then the connection is dropped). The connection failure occurs, when the connection is either rejected or expired. The connection failed probability (c_f) is defined as a sum of the connection rejected probability B(ρ,N) equation (2.1) and connection expired probability.

$$c_f = B(\rho,N) + c_e = B(\rho,N)+ p_e\,(1 - B(\rho,N)).$$

where $p_e = e^{-(t_{out}*\mu_c)}$ (1.14)

$$g = (1-c_f)*\lambda_l * r. \quad (1.15)$$

Where r is defined as revenue for each legitimate connection.

The gains of the defender are calculated by the present Backlog Queue status parameters (λ_m and μ_m). The ADBG game is modeled as a static game. Hence the values of λ_m and μ_m are collected for each strategy with a meaningful gain in k different discrete instants of time with a gap of unit time spread over fixed quantum of time.

In ADBG model, the gain values are computed on the basis of loss queuing model according to the dynamics of parameters and status of the Backlog Queue. For the computation of the gains the following algorithm is developed (BB Rao 2010).

Step-1 : Initialization.

t_{out}, μ_c , λ_l, λ_m,k and N are initialized.

Step- 2 : Perform the step 3 and step 4 for

all the elements of the payoff matrix with gain.

Select the element of the payoff matrix for the computation of gain.

Step- 3 : Repeat upto K.

Decide the λ_m, t_{out} values as per the chosen strategies of the attacker and the defender.

Compute p_e and $\mu_l = \mu_c / (1 - p_e)$.

Compute

$\mu = (\mu_l \mu_m(\lambda_m \mu_l + \lambda_l \mu_m)) / (\lambda_m\mu_l^2 + \lambda_l \mu_m^2)$.

Daniel Boteanu et. al. (2007).

Compute $\rho = (\lambda_l + \lambda_m)/ \mu$.

Calculate B(ρ,N) as per equation (2.1).

Compute g(k) as per equations (1.14) and (1.15).

Go to step 3.

Step- 4 :

Gain of the element in the payoff matrix = $\sum_{s=0}^{k} g(s)/k$.

Go to step-2.

Numerical Illustration

The Numerical illustration follows the phenomenon discussed in section 4.3. For implementation of this algorithm the following initial values are taken for different parameters. The configured Backlog Queue size of the web server is N =1024 and the timeout value t_{out} = 75 sec. Legitimate connections arrival rate λ_l=4 con/sec and service rate μ_c =0.33333 con/sec. These two values are collected from the tcpdump of the original website (Section 2.2.3).

If the algorithm is implemented for a period of 1 minute with the equal intervals of 4 seconds by changing the values of λ_m , μ_m according to different strategies already defined in ADBG.

The number of discrete intervals of time instants is k=60/4=15. The value of c_m=2 units, c_c=1 unit and revenue for each legitimate connection r=5 units. The 3x3 payoff matrix of ADBG is as follows.

	q_1	q_2	q_3
p_1	11.54	9.22	-2
p_2	10.01	2.55	-1
p_3	-7.54	-2.48	0

If one takes a close look at the payoff matrix presented above the following observations can be made:

(i) Defender has the highest payoff among all the strategies when both the defender and the attacker decides to play the game with variable attacking and variable effort.

(ii) While the attacker is attacking with variable effort and if the defender chooses to defend with constant effort then he has higher payoff.

(iii) There doesn't exist a saddle point for the payoff matrix .

From the above equations of section 4.2.2, the game value V is -0.41013, it is always beneficial game to the attacker. The mixed equilibrium strategy probabilities are p_1=0.00423**,** p_2= 0.40166**,** p_3= 0.59410 q_1=0.01291, q_2= 0.12611 and q_3= 0.86097.

The 3x3 payoff matrix of ADBG after the deployment of the admission control mechanism i.e. SACM is as follows.

	q_1	q_2	q_3
p_1	11.54	9.32	-2
p_2	10.21	2.5	-1
p_3	-8.81	-3.5	0

The payoff matrix after deployment of SACM has close resemblance to that of without SACM.

The game value V is -0.49298, it is always beneficial game to the attacker. The mixed equilibrium strategy probabilities are p_1= 0.05986, p_2= 0.37319, p_3= 0.566911, q_1= 0.005847, q_2= 0.126135 and q_3= 0.868018.

Conclusions

It can be observed from the values of the mixed equilibrium strategies without SACM, the defender 60% of the time decides not to defend any kind of attack by the attacker and for the rest 40% of the time he decides to defend with constant effort. After deployment of SACM, the defender 56% of the time decides not to defend any kind of attack by the attacker and for 37% of the time he decides to defend with constant effort. For the attacker either with SACM or without SACM 86% of the time he decides not to attack. Expected payoff of the defender with SACM is less than the expected payoff of the defender without SACM by a factor of 10%. The implementation of the SACM would obviously ensure that the server will be in the survival zone .The administrator is at the liberty whether to deploy SACM or not, however if SACM is implemented the sever would continue to be in the survival zone.

There are two basic ways for the administrator to defend against SYN flooding Admission control of SYN arrivals or tuning the timeout value. In this paper Zero-sum game is formulated by combining the effect of admission control(SACM) in order to arrive at the expected payoff of the defender. Next paper focuses on Non zero-sum game formulation by combining the effect of tuning the timeout value (AITS). This knowledge serves as a guide for the defender.

References

1. Andrew M. Ross and J George Shanthi Kumar (2005), " Estimating Effective Capacity in Erlang Loss Systems under Competition", Journal Queueing Systems: Theory and Applications , Volume 49 Issue 1.

2. B.Basaveswara Rao, (2010), "Analysis of TCP connection establishment mechanism of a web server under normal and attack modes", Thesis presented to Department of Computer Science and Engineering, Acharya Nagarjuna University.

3. Daniel Boteanu Edouard Reich Jose M. Fernandez and John McHugh (2007), "Implementing and Testing Dynamic Timeout Adjustment as a DoS Counter-measure"-http://www. professeurs.polymtl.ca/jose.fernandez/QueueDosExp.p df.

4. Robert B. Cooper Introduction to queuing theory Macmillan 1972.

5. Wei Xie, Hairong Sun, Yonghuan Cao and Kishor S. Trivedi (2002), "Optimal Webserver Session Timeout Settings For Web Users", http://people.ee.duke.edu/~kst/netpaper/WeiXie_cmg-final.pdf.

6. Zakaria Al-Qudah, Michael Rabinovich and Mark Allman (2010), "Web Timeouts and Their Implications"- http://vorlon.case.edu /~zma/pubs/web_timeouts.pdf.

7. Zhaotong Lian and Jian Lin (2007), "Simulation analysis of the DoS Attack in Internet Service", International Conference on Wireless Communications, Networking and Mobile Computing (WiCom 2007), pp. 6298 – 630.