A Defence Strategy against Flooding Attack Using Puzzles by Game Theory

[1]Ch. V. N. Madhuri, [2]R. V. Krishnaiah

[1]M. Tech (CSE), B. Tech in CSE, Global Institute of Engineering & Technology, Moinabad, India

[2]PhD, M. Tech in CSE from JNTU Hyderabad, M. Tech in EIE from NIT, Warangal, India

Abstract: ***Security issues have become a major issue in recent years due to the advancement of technology in networking and its use in a destructive way. A number of Defence strategies have been devised to overcome the flooding attack which is prominent in the networking industry due to which depletion of resources Takes place. But these mechanism are not designed in an optimally and effectively and some of the issues have been unresolved. Hence in this paper we suggest a Game theory based strategy to create a series of Defence mechanisms using puzzles. Here the concept of Nash equilibrium is used to handle sophisticated flooding attack to defend distributed attacks from unknown number of sources***

Keywords: Dos Attacks, Game Theory, Puzzles

1. Introduction

The pace with which the technology is advancing is amazing. With the advancement in technology there has been a great advancement in networking too. Networking today has become inevitable and is a part and parcel in various aspects of our life. If we consider the present business and political scenario, there has been a rat-race going on which has made individuals not only upgrade their own resources but also degrade their competitor's resources by some malicious activities. Hence in recent years, security concerned issues has received enormous attention in networked system because of availability of services. Networked systems are vulnerable to DoS (Denial of Services) attack. A Denial-of-Service attack (Dos attack) is a type of attack on a network that is designed to bring network to its knees by flooding it with useless traffic. In this area, most researches are based on designing and verifying various Defence strategies against denial-of-service (DoS) attacks. A DoS attack characterizes a malicious behaviour preventing the legitimate users of a network from using the services provided by that network. Flooding attacks and Logic attacks are the two principal classes of DoS attack.

Flooding distributed denial of service attacks are the attacks launched by multiple attackers through the action of flooding, i.e. sending traffics in a quantity that is able to bring a network or a service down. Distributed denial of service (DDoS) flood attacks have been among the most frequently occurring attacks and badly threaten the reliability and usability of the services of the Internet. Hence, DDoS flood attacks (hereafter flood attacks) present severe threats to individuals, business organizations and even political entities such as a country. Reported impacts of DDoS floods include disgruntled customers, losses of business profits, disruption of critical infrastructures such as train operations and Internet disconnection of a country from the outside world .Using UDP for denial-of-service attacks is not as straightforward as with the Transmission control protocol (TCP). However, a UDP flood attack can be initiated by sending a large number of UDP packets to random ports on a remote host. As a result, the distant host will:

- Check for the application listening at that port;
- See that no application listens at that port;
- Reply with an ICMP destination unreachable packet.

Thus, for a large number of UDP packets, the victimized system will be forced into sending many ICMP packets, eventually leading it to be unreachable by other clients. The attacker may also spoof the IP address of the UDP packets, ensuring that the excessive ICMP return packets do not reach him, and anonym zing the attacker's network location(s). Most operating systems mitigate this part of the attack by limiting the rate at which ICMP responses are sent.

A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either simply not send the expected ACK, or by spoofing the source IP address in the SYN, causing the server to send the SYN-ACK to a falsified IP address - which will not send an ACK because it "knows" that it never sent a SYN. The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK, but in an attack increasingly large numbers of half-open connections will bind resources on the server until no new connections can be made, resulting in a denial of service to legitimate traffic. Some systems may also malfunction badly or even crash if other operating system functions are starved of resources in this way.

Large number of Defences against flooding attack have been devised which may be reactive or preventive. Mechanisms such as pushback, trace back, or filtering are reactive mechanisms which alleviate the impact of flooding attack by detecting the attack on the victim, but they all have significant drawbacks that limit their practical utility in the current scenario. Whereas Preventive strategies make the victim able to tolerate the attack without the legitimate user's request getting denied. Preventive mechanism enforces restrictive policies such as use of client puzzles that limits the resource consumption. Generally reactive mechanisms have some drawbacks. It suffers from scalability and attack traffic identification problems. Dos can be effectively beaten by utilizing Client Puzzles. In client puzzle approach, the client needs to solve the puzzle produced by the defender (server) for getting services. The server produces computational puzzles to client before committing the resources. Once the sender solves the puzzle he is allocated the requested resources. The attacker who intends to use up the defender's resources by his repeated requests is deterred from perpetrating the attack, as solving a puzzle is resource consuming. To preserve the effectiveness and optimality of this mechanism, the difficulty level of puzzles should be adjusted in timely manner. Network puzzles and puzzle auctions tried to adjust difficulty level of puzzles but they are not much suitable in incorporating this trade-off. In this paper, we show that Puzzle-based mechanism can be effectively studied using game theory. This paper shows Puzzle-based defence mechanism modelled as two player game, one player as attacker who perpetrates a flooding attack and other as defender who counters the attack using client puzzles. Then Nash equilibrium is applied on game which leads to description of player's optimal strategy.

2. Strategic Game Of Client Puzzle

Using the client puzzle approach means that before engaging in any resource consuming operations, the server first generates a puzzle and sends its description to the client that is requesting service from the server. The client has to solve the puzzle and send the result back to the server. The server continues with processing the request of the client, only if the client's response to the puzzle is correct. This is summarized in the following abstract.

Protocol, where *C* and *S* denote the client and the server, respectively:

Step 1 *C* → *S:* sending service request
Step 2 *S:* generation of a puzzle
Step 3 *S* → *C:* sending description of the puzzle
Step 4 *C:* solving the puzzle
Step 5 *C* → *S:* sending solution to the puzzle
Step 6 *S:* verification of the solution
If the solution is correct:
Step 7 *S:* continue processing service request.

One can view the first six steps of the protocol as a preamble preceding the provision of the service, which is subsumed in a single step (step 7) in the above abstract description. The preamble provides a sort of algorithmic protection against DoS attacks. The server can set the complexity level of the puzzle according to the estimated strength (computational resources) of the attacker. If the server manages to set an appropriate complexity level, then solving the puzzle slows down the DoS attacker who will eventually abandon his activity.

2.1 Puzzle characteristics

To prevent DoS attacks, puzzles should have the following characteristics:

- The computational costs employed by the server in generating and verifying the puzzles must be significantly less expensive than the computational costs employed by the client in solving the puzzles.
- The puzzle difficulty, which depends on the server's resources availability, should be easily and dynamically adjusted during attacks.
- Clients have a limited amount of time to solve puzzles.
- Pre-computing puzzle solutions should be unfeasible.
- Having solved previous puzzles does not aid in solving new given puzzles.

Before a correct puzzle solution is submitted, the server does not keep a record of the connection's state. In addition, Feng [8] suggests three more factors to be taken into account when implementing client puzzles. First, the server's ability for generating puzzles must not be able to be flooded by the attacker; in other words, the server should be able to handle several concurrent requests from clients. Second, when a puzzle is delivered to a given client, the client must not be able to circumvent the puzzle mechanism. Third the concept of fairness is introduced which consists of making puzzles' difficulty dependable on the clients' hardware. More precisely, the author suggests that a "thin client" (cell-phone, PDA, etc.) should be given less difficult puzzles to solve. Nevertheless, we believe that this idea of puzzle fairness should be carefully handled otherwise it could open opportunities for DoS/ DDoS attacks.

3. Game History And Client-Puzzles

Game theory is the formal study of conflict and lead to exhaustion of defenders resources as the cooperation. Game theoretic concepts apply whenever the actions difficulty level of puzzles; random number generators of and other parameters are so adjusted to achieve the several agents are interdependent. These agents may be same, Individuals, groups, firms or any combination of these. The concepts of game theory provide a language to formulate structure, analyze, and understand strategic scenarios.

As a mathematical tool for the decision-maker the strength of game theory is the methodology it provides for structuring and analyzing problems of strategic choice. The process of formally modelling a situation as a game requires the decision-maker to enumerate explicitly the players and their strategic options, and to consider their preferences and reactions.

The discipline involved in constructing such a model already has the potential of providing the decision-maker with a clearer and broader view of the situation. This is a "prescriptive" application of game theory, with the goal of improved strategic decision making. With this perspective in mind, this article explains basic principles of game theory, as an introduction to an interested reader without a background in economics.

3.1 Strategic and extensive form games

The strategic form (also called normal form) is the basic type of game studied in no cooperative game theory. A game in strategic form lists each player's strategies, and the outcomes that result from each possible combination of choices. An outcome is represented by a separate payoff for each player, which is a number (also called utility) that Measures how much the player likes the outcome. The extensive form, also called a *game tree*, is more detailed than the strategic form of a game. It is a complete description of how the game is played over time.

This includes The order in which players take actions, the information that players have at the time they must take those actions, and the times at which any uncertainty in the situation is resolved. A game in extensive form may be analyzed directly, or can be converted into an equivalent strategic form.

This paper uses the concept of Game theory with Nash equilibrium. Nash equilibrium is a solution concept that describes a steady state condition of the game; no player would prefer to change his strategy as that would lower his payoffs given that all other players are adhering to the prescribed strategy.

This paper uses the concept of Nash equilibrium in a prescriptive way rather than only in descriptive way. Use of Nash equilibrium in prescriptive way does not.

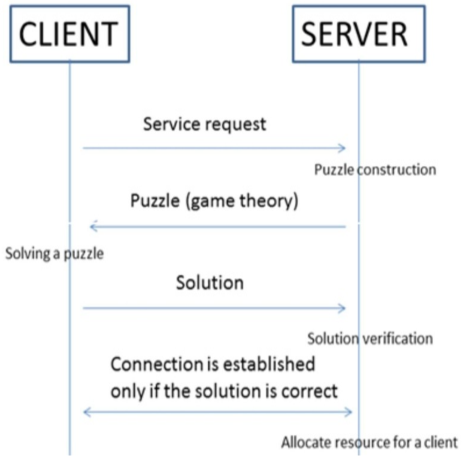

Figure 1: Client Puzzle Approach

Here we calculate each player's payoff using game theory concepts. We calculate defender's payoff and attacker's payoff. The payoff is considered through actions QT, RA, and CA, which stand for quitting (no answer), random answer to puzzle, and correct answer to the puzzle. It is assumed that a legitimate user always solves the puzzles and returns correct answers.

Assume that the defender uses an easy puzzle P1 and a difficult puzzle P2 to defend him.

αm -> time spend by defender in providing the service.
αpp -> time taken by defender to produce a puzzle.
αVp ->time taken by defender to verify the solution.
$\alpha SP1$-> expected time of attacker to spend to solve P1.

Defender chooses the puzzles P1 and P2 such that
$\alpha SP1 < \alpha m < \alpha SP2$

On receiving a puzzle, the attacker may choose from one among the following actions:

When attacker selects CA for puzzle Pi
Pi: $CA = \alpha m + \alpha PP + \alpha V P - \alpha SPi$
When attacker selects RA for puzzle Pi
Pi: $RA = \alpha m + \alpha PP + \alpha V P$

Defender's Time:
Pi: $X = -\alpha PP - \alpha V P - \alpha m + \alpha SPi$

We are using four Puzzle-based Defence Mechanism based on Nash equilibrium. They are Open-Loop Solutions: Open-loop is history independent solution. PDM1 (Puzzle-based Defence Mechanism) is derived from the open-loop defender chooses his actions regardless of what happened in the game history. The second is Closed-Loop Solutions: Closed loop is history dependent solution.PDM2 resolves PDM1problems by using the closed-loop solution concepts, but it can only defeat a single-source attack. PDM3 extends PDM2 and deals with distributed attacks. This defence is based on the assumption that the defender knows the size of the attack Coalition. PDM4, the ultimate defence mechanism is proposed in which the size of the attack coalition is assumed unknown [34].

4. Discussion

The defence mechanism proposed in this paper largely depends on the quality of the puzzles i.e. how the PDM levels are used and differentiated using puzzles at application layer. Moreover the security and maintenance of database consisting of puzzles at the defenders side is an important issue which should be considered. In the game theory approach both the attacker and defender will try to increase their pay-off and at the same tries to gain more by reducing the counterpart's pay-off. The attempt of a defender will be considered optimum if the pay-off of a defender; legitimate user is maximum and is minimum for the attacker. Some other important concepts have been discussed below: 6.1 Pushback Let us discuss some issues that may affect the way Pushback [35] could be deployed. First off, it is fairly obvious that the pushback is most effective when an attack is non-isotropic; in other words, there will be routers fairly close to the target where most of the attack traffic will be arriving from a subset of the input links. That is a fairly safe assumption; even the biggest attacks do not involve more than a few thousand compromised machines, and there are many millions of machine on the Internet. It would be particularly hard for an attacker to ensure that the attack slaves are evenly distributed with respect to the target.

In a Password Cracking [36] attack an attacker tries to gain unauthorized access to some machine by making repeated guesses at possible usernames and passwords. Password guessing can be done remotely with many services; telnet, ftp, pop, rlogin, and imp are the most prominent services that support authentication using usernames and passwords. Dictionary attack is one such type of attack. A Dictionary attack uses a targeted technique of successively trying all the words in an exhaustive list called a dictionary which is a pre-arranged list of values. In contrast with a brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed typically derived from a list of words for example a dictionary or a bible etc. Dictionary attacks succeed because many people have a tendency to choose passwords which are short (7 characters or fewer), single words found in dictionaries or simple, easily-predicted variations on words, such as appending a digit.

5. Conclusion

Game theory has been used in this paper to provide defence mechanisms for flooding attacks using puzzles. The interaction between the defender and attacker is considered as an infinitely repeated game of discounted payoffs. The mechanism has been divided into different levels. This paper has also described the architecture of a client puzzle protocol. The algorithm selected for the client puzzle can be implemented on almost any platform. For the scenario in which an attacker carries out a DDoS attack, we modelled the actions of the attacker as intensities or data rates employed in carrying out the attack. And to develop a trace back system that can trace a single packet so that the data of the whole message is saved and to reduced eavesdropping risks.

References

[1] E. Bursztein and J. Goubalt-Larrecq. A logical framework for evaluating network resilience against faults and attacks. Lecture Notes in Computer Science; Vol. 4846, 2007

[2] 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.

[3] T. Aura and P. Nikander. Stateless protocols. In Proceedings of the ICICS'97 Conference, Springer-Verlag, LNCS volume 1334, 1997.

[4] B. Bencsath and I. Vajda. Protection against DoS attacks based on traffic level measurements. Submitted for publication, April 2003.

[5] CERT Coordination Center, "Denial of Service Attacks," Tech Tips, June 4, 2001.

[6] CERT Coordination Center, "TCP SYN Flooding and IP Spoofing Attacks," Tech Tips, November 29, 2000.

[7] Dean, D., and Stubblefield, A., Using Client Puzzles to Protect TLS. In Proceedings of the l0th USENIX Security Symposium, August 2001.

[8] D. Song and A. Perrig, "Advanced and Authenticated Marking Schemes for IP Trace back," Proc. IEEE INFOCOM '01, pp. 878-886, 2001.

[9] ShibiaoLin, Tzi-ckerChiueh A Survey on Solutions to Distributed Denial of Service Attacks

[10] John Ioannidis, Steven M. Bellovin, Implementing Pushback: Router-Based Defence against DDoS Attacks.

Author Profile

CH. V. N. Madhuri, M. Tech from JNTUH and B. Tech from Global Institute of Engineering & Technology, Moinabad, India

Dr. R. V. Krishnaiah has received Ph. D from JNTU Ananthapur, M. Tech in CSE from JNTU Hyderabad, M. Tech in EIE from NIT (former REC) Warangal and B. Tech in ECE from Bapatla Engineering College. He has published more than 50 papers in various journals. His interest includes Data Mining, Software Engineering, and Image Processing.