**Journal on Education**
Volume 06, No. 01, September-Desember 2023, pp. 10789-10792
E-ISSN: 2654-5497, P-ISSN: 2655-1365
Website: http://jonedu.org/index.php/joe

# Game Theorical Concept for Denial of Services (DoS) Attacks

Puri Ratna Larasati[1], Bambang Suharjo[2], Richardus Eko Indrajit[3], H.A Danang Rimbawa[4]

[1,2,3,4]Universitas Pertahanan Indonesia, Kawasan IPSC Sentul, Kec. Citeureup, Kab. Bogor, Jawa Barat
larasatiratnapuri@gmail.com

***Abstract***

Information security is a crucial aspect in today's digital era, where increased connectivity and data exchange involves a high risk of denial of services attacks. Increasing cybersecurity and privacy issues require more effective defense mechanisms to counter these threats. This research was conducted through design formulation using game theory for denial of service attacks. First scheme , use Bayes' theorem to determine the probability of a DDoS attack. The probability is equal. The probability of attack and defense is 50-50. Second scheme, one of players is dominan. A game theoretic framework as an approach to find out the possibility of denial of services between pairs of attacking/defending nodes using a Bayesian formulation. Game modeling can propose for developing better mitigation and detection approaches.

**Keywords:** Denial of Services (DoS) Attack, Game Theory

**Abstrak**

Keamanan informasi merupakan aspek penting di era digital saat ini, di mana peningkatan konektivitas dan pertukaran data memiliki risiko tinggi terhadap serangan penolakan layanan. Meningkatnya masalah keamanan siber dan privasi memerlukan mekanisme pertahanan yang lebih efektif untuk melawan ancaman-ancaman ini. Penelitian ini dilakukan melalui formulasi desain menggunakan teori permainan untuk serangan penolakan layanan. Skema pertama, gunakan teorema Bayes untuk menentukan kemungkinan serangan DDoS. Kemungkinannya sama. Kemungkinan menyerang dan bertahan adalah 50-50. Skema kedua, salah satu pemain dominan. Kerangka teori permainan sebagai pendekatan untuk mengetahui kemungkinan terjadinya denial of services antara pasangan node penyerang/bertahan dengan menggunakan rumusan Bayesian. Pemodelan permainan dapat mengusulkan pengembangan pendekatan mitigasi dan deteksi yang lebih baik.

**Kata Kunci:** Serangan Denial of Services (DoS), Teori Permainan

✉ Corresponding author: Puri Ratna Larsati
Email Address: larasatiratnapuri@gmail.com (Kawasan IPSC Sentul, Kec. Citeureup, Kab. Bogor, Jawa Barat)

Received 16 Desember 2023, Accepted 23 Desember 2023, Published 30 Desember 2023

## INTRODUCTION

Information security is a crucial aspect in today's digital era, where increased connectivity and data exchange involves a high risk of denial of services attacks. Intrusions on computer systems can result in major losses, including the theft of sensitive data, fraud, or system damage. The increasing number of attacks taking place in cyberspace and the rise of identity theft have recently made the Internet seem like a scary place. Cyber attacks can pose a threat to society because economic and communication infrastructure is heavily dependent on computer networks and information technology. The target of this attack can be anyone from an individual, group, company or government agency. Increasing cybersecurity and privacy issues require more effective defense mechanisms to counter these threats (Do, Cuong et al 2017).

There are many types of attacks that occur on the use of computers and internet networks (computer and network services). The longer this type of attack occurs, the more difficult it is to detect or prevent. One of the cyber attacks that can occur when performing computer and network services is denial of services (DoS/DDos). Denial of services is an attack that aims to overwhelm existing internet network traffic on networks, systems and servers so as to make the website inaccessible. The resources hosted are usually bandwidth, RAM, cache memories, etc. (Indrajit, 2012).

Distributed Denial-of-Service (DDoS) attacks are attacks that crash servers and systems on a network by overwhelming packets or requests on the network increase. Identifying a DDoS attack becomes a more complex matter because there are different types of DDoS attack strategies. Several types of DDoS attacks are ICMP flood, SYN flood, IP packet flood, and others (Priya, S. et al 2016).

Thr effort to counter DoS attacks, information security researchers and practitioners continue to look for innovative solutions. One interesting and growing approach is game theory for understanding and addressing DoS attacks. This approach involves modeling the security situation as a game between interacting parties, namely the attacker and the system owner. The importance of this research lies in its ability to improve our understanding of DoS attacks and provide a more in-depth look at how to engage game theory principles in the context of information security.

Based on the background previously described, Denial of service (DoS) or distributed denial of service (DDoS) attacks remain a persistent threat to network security and have always been an important problem for the system to study, so this research is a game theory design approach for detecting denial of services attacks which hopefully can provide information and recommendations to audiences who need them in detecting and preventing denial of services attacks in cyber attacks.

## METHOD

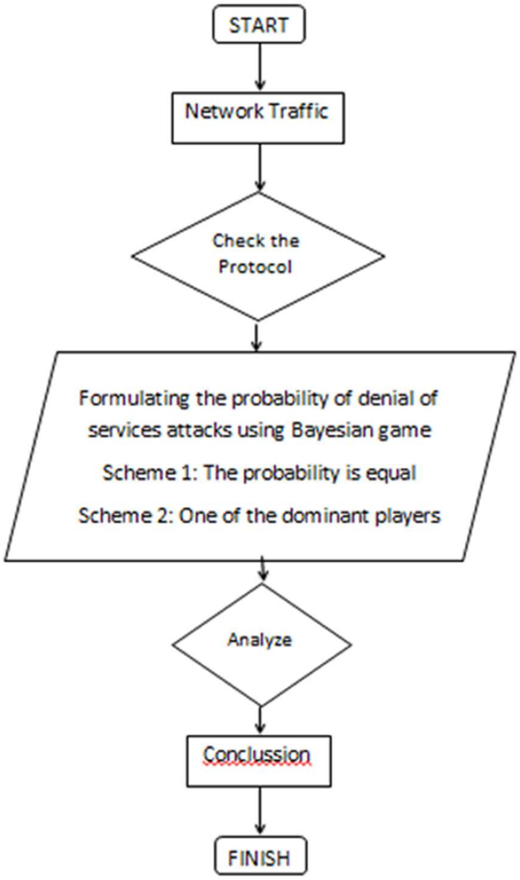
This research was conducted through design formulation using game theory for denial of service attacks. Research on game design the theoretical approach for denial of services attacks is compiled systematically by identifying problems, studying literature, methods and solutions, then making conclusions.

## RESULTS AND DISCUSSION

### *Design Game Theorical Approach for Denial of Services Attacks*

A game is a description of the strategic interaction between opposing, or co operating, interests where the constraints and payoff for actions are taken into consideration. On the other hand, a player is a basic entity in a game that is tasked with making choices for actions. A player can represent a person, machine, or group of persons within a game.

There are the design of theoretical approach is using a game model for DDoS attack


START
Network Traffic
Check the Protocol
Formulating the probability of denial of services attacks using Bayesian game
Scheme 1: The probability is equal
Scheme 2: One of the dominant players
Analyze
Conclussion
FINISH

According to the diagram of design game theoretical approach is using a bayesian model for DDoS attack is explained by scheme 1 and scheme 2.

**1$^{st}$Scheme**

Use Bayes' theorem to determine the probability of a DDoS attack. The probability is equal. The probability of attack and defense is 50-50. With conditions of the same probability, then one player can be assumed to have a stronger condition, and another player has a weaker condition. with this situation, the value of the probability is the same but the value is the opposite, the strong probability is ($\alpha$) and the weak probability is formulate by ($1 - \alpha$).

**2$^{nd}$ scheme**

In scheme 2, one of players is dominan,. As an assumption with the terms of the game as follows: player 1 attack the protocol, player 2 does not defense the protocol, and player 1 knows this latter fact. player 1 doesn‟t attack the protocol, player 2 defense the protocol, but player 1 does not know whether or not player 2 knows the attacks. Both of player 1 and 2 is attack and defense the protocol.

## CONCLUSSION

A game theoretic framework as an approach to find out the possibility of denial of services between pairs of attacking/defending nodes using a Bayesian formulation. In this scheme, the game is represented as a two-person with equal probability (50-50) and one of players is dominant. Some areas in game modeling can propose for future research work is application of operations research techniques in developing better mitigation and detection approaches.

## REFERENCE

Chukwudi, et al. 2017. Game Theory Basics and Its Application in Cyber Security. Advances 4, in Wireless Communications and Networks. Vol. 3, No. 2017, pp. 45-49. DOI:10.11648/j.awcn.20170304.13.

Do, Cuong et al. 2017. Game Theory for Cyber Security and Privacy. ACM Computing Surveys, Vol. 50, No. 2, Article 30, Publication date: May 2017.

Faried, Muhammad et al. 2021. Denial Of Service (Dos) Detection Analysis Using Fuzzy Logic Mamdani Method On Internet Of Things (Iot) Network. e Proceeding of Engineering : Vol.8, No.1 Februari 2021 ISSN : 2355-9365.

Huang, Liang et al. 2014. A Game Theory Based Approach to the Generation of Optimal DDoS Defending Strategy. ISBN: ©2014 SDIWC. 978-0-9891305-4-7.

Indrajit, richardus. 2012. Ragam serangan dunia siber. indrajit@post.harvard.edu post on 28 september 2012. No:20.

Priya, S.S., Yuvaraj., D., dan Sivaram, M., 2016. A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks, 20(4).

V. Zlomislić, K. Fertalj, and V. Sruk, "Denial of service attacks, defences and research challenges," Cluster Comput., vol. 20, no. 1, pp. 661–671, 2017

Zidane, Muamar. Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer Vol. 6, No. 1, Januari 2022, 172-180 e-ISSN: 2548-964X.