Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 809–820
DOI : 10.47974/JDMSC-1957

Mitigating DDoS attacks with an intrusion detection and prevention system based on 2-player Bayesian game theory

Sagar Vasantrao Joshi *
Department of Electronics & Telecommunication Engineering
Nutan Maharashtra Institute of Engineering and Technology
Pune
Maharashtra
India

Nanda Raghunath Wagh †
Department of Computer Engineering
Government Polytechnic
Pune
Maharashtra
India

Jambi Ratna Raja Kumar §
Department of Computer Engineering
Genba Sopanrao Moze College of Engineering
Pune
Maharashtra
India

Deepika Dongre ‡
Department of Artificial Intelligence and Data Science
Vishwakarma Institute of Information Technology
Pune
Maharashtra
India

* *E-mail:* **sagarvjoshi@gmail.com (Corresponding author)**
† *E-mail:* **nandawagh@dbatu.ac.in**
§ *E-mail:* **ratnaraj.jambi@gmail.com**
‡ *E-mail:* **deepika.dongre@viit.ac.in**

Nuzhat Rizvi [@]
Symbiosis Law School, Nagpur Campus
Symbiosis International (Deemed University)
Pune
Maharashtra
India

Mahua Bhowmik [#]
Department of Electronics and Telecommunication Engineering
Dr. D.Y. Patil Institute of Technology
Pune
Maharashtra
India

Abstract

Distributed Denial of Service (DDoS) attacks are very dangerous to the availability and security of networks, so they need improved ways to be stopped. This article suggests a new way to fight DDoS attacks that uses Intrusion Detection and Prevention Systems (IDPS) and 2-Player Bayesian Game Theory. Traditional IDPSs often have trouble responding quickly to changing attack tactics, which makes them less effective as defenses. The suggested structure, on the other hand, imagines the attacker and defense interacting as a Bayesian game. This lets them make proactive choices and come up with flexible ways to respond.The system uses Bayesian reasoning to describe the attacker's actions and plans' doubt, which lets it better assess the threat and decide how to respond. By constantly changing probability distributions based on what it sees attackers doing and what it sees defenders doing, the IDPS can quickly and effectively change its defenses to deal with new threats. The strategy contact between the attacker and the defense adds a competition factor that makes attackers less likely to start DDoS attacks by making them more expensive and risky. The proposed method works to stop different kinds of DDoS attacks while reducing the number of fake positives and negatives through a lot of simulations and experiments.

Subject Classification: *68M25.*

Keywords: *Lightweight cryptography, Financial transaction, Chaotic map algorithm, Lightweight ECC.*

1. Introduction

Distributed Denial of Service (DDoS) attacks are a major danger to the dependability and availability of networks and services online. Target

[@] *E-mail:* **nuzhatrizvi@slsnagpur.edu.in**
[#] *E-mail:* **mahua.bhoumik@dypvp.edu.in**

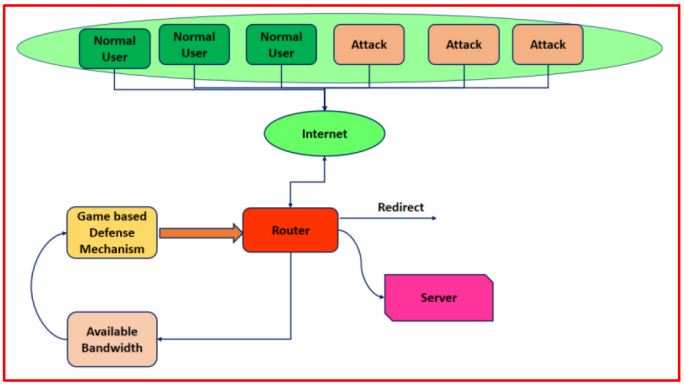

Figure 1

Network Consideration area for IDS and Prevention

systems are inundated with so much bad data from these hacks that normal users can't get to them. Due to their constantly changing and adapting nature, DDoS attacks are hard for traditional defense systems to effectively blunt [1]. In response, researchers and cybersecurity experts have looked into new ways to improve protection tactics, such as using game theory principles. Combining Intrusion Detection and Prevention Systems (IDPS) as shown in Figure 1 with 2-player Bayesian game theory is one way to do this. It looks like a good way to stop DDoS attacks. Bayesian game theory is basically a way to model how reasonable decision-makers can interact strategically with each other when they don't have all the knowledge they need about each other's actions and plans. In the context of cybersecurity, this means making defenses that are flexible enough to react to the changing strategies attackers use [2].

It is possible for guards to better spot and stop DDoS attacks [3] in real time by using Bayesian game theory in the creation of IDPS. This reduces the damage done to target systems and networks.This method works because it can simulate the inevitable doubt and planned behavior that both attackers and defenses experience in cyberspace. The IDPS can figure out if something going on right now is likely to be a DDoS attack by constantly looking at incoming network data and keeping an eye out for strange trends. Then, these [4] evaluations are used to help make smart decisions about how to use resources and put defenses in place.Also, because the Bayesian game is played by two people, the IDPS can change its defenses based on what it sees the enemy doing. This flexible reaction method lets the defender take advantage of the attacker's flaws and weaknesses, which makes it more likely that the DDoS attack will be

stopped. The [5] IDPS can also better tell the difference between good and bad network traffic by using machine learning algorithms and data-driven analytics. This makes it less likely that it will give fake positives or negatives. The combining Intrusion Detection and Prevention Systems with 2-player Bayesian game theory looks like a good way to stop DDoS attacks. By using probabilistic thinking and flexible defense tactics, this method helps guards deal with cyber threats that change and adapt, which makes important systems and infrastructure more resistant to DDoS attacks.

2. Proposed Method

2.1 *Game Theory Principles*

Game theory is a way to use math to look at how logical people make decisions and deal with each other in strategic situations. In cybersecurity, it gives an organized way to model how attackers and defenders act in situations where they are competing with each other. Players, tactics, payoffs [6], and Nash equilibria are some of the most basic ideas in game theory. Players choose tactics based on what they know about the methods other players have used and try to get the most out of the game for themselves. This approach is especially useful in cybersecurity, where attackers are always trying to get into systems and defenses are always trying to keep them safe [7].

2.2 *Bayesian Game Theory*

Bayesian game theory adds [8] doubt and missing knowledge to standard game theory, making it more thorough. In Bayesian games, players have their own ideas about what other players will do and how they play, and these ideas are changed based on what they see happen. Bayes' theorem is used to make this more formal by figuring out posterior probabilities based on past opinions and data that has been seen. Bayesian games [9] are a more realistic way to show how people make choices in changing and unclear settings. This makes them perfect for simulating hacking situations where attackers' goals and abilities aren't always known.

1. Bayes' Theorem:

$$P(S|O) = P(O|S) * P(S) / P(O)$$

2 Payoff Matrix:

$$Payoff\ Matrix = (GR; RR)$$

3. Utility Functions:

$$U\_A(S\_A, S\_D) = R\_A(S\_A, S\_D) - C\_A(S\_A, S\_D)$$
$$U\_D(S\_D, S\_A) = R\_D(S\_D, S\_A) - C\_D(S\_D, S\_A)$$

4. Strategic Selection:

$$S\_A* = \arg\max \Sigma P(S\_D \mid O) * U\_A(S\_A, S\_D)$$
$$S\_D* = \arg\max \Sigma P(S\_A \mid O) * U\_D(S\_D, S\_A)$$

2.3 *Bayesian Game Theory in Cybersecurity*

Bayesian game theory is being used more and more in cybersecurity to solve problems like detecting intrusions, analyzing malware, and stopping DDoS attacks. Researchers can make better defense strategies that react to changing threats by simulating the strategic interactions between attackers and defenders as a Bayesian game. Using Bayesian thinking, guards can make smart choices based on statistical assessments of how likely different attack scenarios are to happen. This makes it easier for them to predict and react to cyber dangers [10].

2.4 *Conceptual Framework for Integrating IDPS with 2-Player Bayesian Game Theory*

Combining Intrusion Detection and Prevention Systems (IDPS) with two-player Bayesian game theory looks like a good way to make cybersecurity defenses stronger. In this mental model, the IDPS is the defender. It constantly [11] watches network activity and uses Bayesian reasoning to keep its ideas about possible attacker tactics up to date. Based on the posterior odds, the guard then chooses tactics to stop the DDoS attack. The attacker, who is shown as the other player, wants to get the most money by choosing ways to avoid being caught and mess up the goal system. The IDPS can change its defense tactics on the fly to outsmart attackers and lessen the damage of DDoS attacks by using Bayesian logic to guide its repeated interactions.

$$P(S \mid O) = P(O)P(O \mid S) \times P(S)$$

3. Two Player Bayesian Game Theory

In two-player Bayesian game theory as shown in Figure 2, each player makes choices based on odds, even though they don't have all the facts. In cybersecurity, it helps defend against DDoS attacks by changing defense tactics on the fly. Defenders use [12] Bayesian thinking to guess what attackers might do and then change what they think based on what they see. This flexible method helps defenders use their resources wisely, take advantage of enemy weaknesses, and lower the number of fake positives and negatives. By constantly looking at and reacting to how threats are changing, two-player Bayesian game theory makes systems more resistant to DDoS attacks.

Algorithm for Two-Player Bayesian Game Theory in the Context of DDoS Attack Mitigation:

1. Initialization:

- Define the players: Defender (D) and Attacker (A).
- Set up the game parameters: strategies, payoffs, prior beliefs.

2. Prior Belief Update:

- Both players update their beliefs about the opponent's strategy using Bayes' theorem:

$$P(S\_A \mid O) = P(O \mid S\_A) * P(S\_A) / P(O)$$

$$P(S\_D \mid O) = P(O \mid S\_D) * P(S\_D) / P(O)$$

Where:

- $P(S\_A \mid O)$ is the posterior probability of the attacker's strategy given observed outcome O.

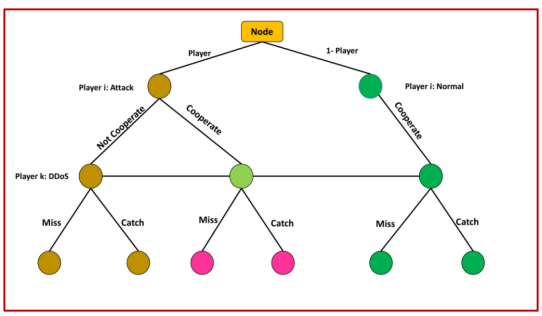

Figure 2

Two Play Extensive game between IDS and Node Data

- $P(S\_D|O)$ is the posterior probability of the defender's strategy given observed outcome O.
- $P(O|S\_A)$ and $P(O|S\_D)$ are likelihood functions.
- $P(S\_A)$ and $P(S\_D)$ are prior probabilities.
- $P(O)$ is the total probability of the observed outcome.

3. Strategy Selection:

- Based on updated beliefs, each player selects their strategy that maximizes their expected utility:

$$S\_A* = \arg\max \Sigma P(S\_D|O) * U\_A(S\_A, S\_D)$$
$$S\_D* = \arg\max \Sigma P(S\_A|O) * U\_D(S\_D, S\_A)$$

Where:

- U_A and U_D are the utility functions representing the payoff for the attacker and defender, respectively.

4. Action Execution:

- The players execute their chosen strategies:
- Attacker launches DDoS attack using selected strategy S_A*.
- Defender deploys countermeasures using selected strategy S_D*.

5. Outcome Evaluation:

- Evaluate the outcome of the game based on the observed actions and their impact on system performance and security.

6. Learning and Adaptation:

- Update the prior beliefs based on the observed outcomes.
- Repeat steps 2-5 iteratively to adapt to the evolving threat landscape.

4. Result and Analysis

In Table 1, you can see how the selfish behavior percentage and the number of packets that were not sent change for three different protocols: Leach, S-Leach, and N-Leach, with different numbers of nodes. The selfish behavior rate and the number of packets that are not sent tend to go up as the number of nodes goes up.

Table 1

Summary Selfish percentage Vs Not sent packet

Nodes	Leach	S-Leach	N-Leach
10	140	160	200
20	145	200	268
30	160	215	283
40	175	230	298
50	195	250	318
60	350	405	473
70	480	535	603
80	550	605	673
90	800	855	923
100	1020	1075	1143

This is true for all protocols. There are, however, important changes between the protocols. This means that S-Leach and N-Leach might work better at preventing greed and making sure that packets get delivered in wireless sensing networks.

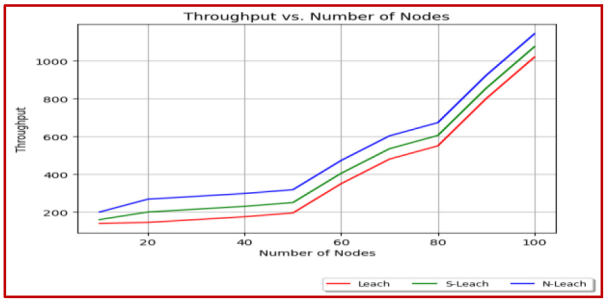

Figure 3

Representation of Selfish percentage Vs Not sent packet

When two people play a Bayesian game of intrusion detection, Table 2 shows the outcomes. The game compares three different protocols: Leach, S-Leach, and N-Leach. These methods are tested on a number of important factors that are needed to judge how well intruder detection systems work.The Detection Rate, which shows how many attacks were correctly discovered by the system, varies a lot between the algorithms. The best detection rate is shown by S-Leach, which is 92.35%. N-Leach is

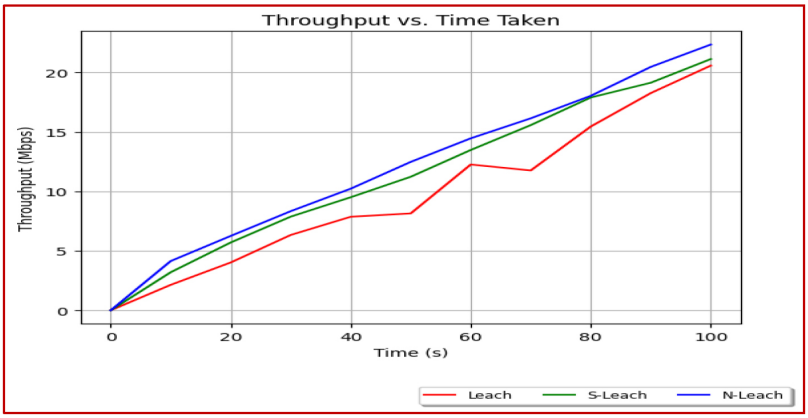

Figure 4

Representation of Throughput Vs Time Taken

close behind with 95.63%, and Leach is last with 85.33%. In comparison to the Leach protocol, this shows that S-Leach and N-Leach are better at properly finding intrusions as shown in Figure 3 and 4. The False Alarm Rate, which shows the percentage of normal activities that are mistakenly reported as attacks, is also different for each procedure. N-Leach has the lowest False Alarm Rate, at 0.02%. Leach is next, at 0.11%, and S-Leach is third, at 0.13%. This means that N-Leach is the least likely to set off fake alarms, which makes it more reliable at telling the difference between regular and harmful actions.

Table 2

Result for2 playerBayesian game of intrusion detection

Parameter	Leach	S leach	N Leach
Detection Rate	85.33	92.35	95.63
False Alarm rate	0.11	0.13	0.02
Precision	92.35	95.32	97.14
Recall	86.45	92.45	95.63
F1 Score	89.74	93.65	96.47
Accuracy	95.45	97.85	98.8

Precision, which shows the percentage of correctly identified attacks out of all observed cases, keeps getting better across all of the protocols. is

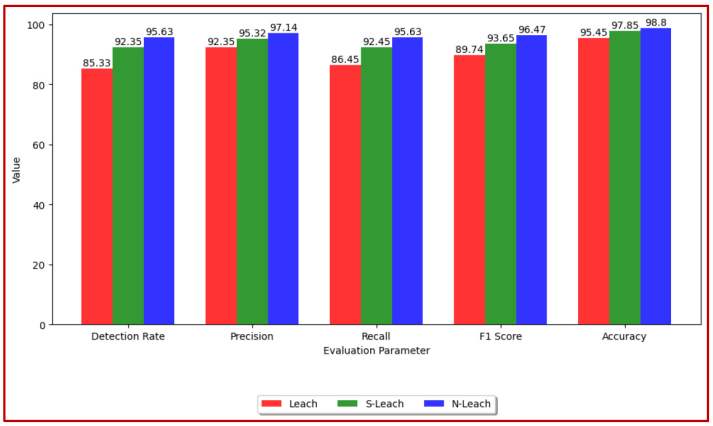

Figure 5

Evaluation Results of Intrusion Detection Protocols

shown in Figure 5. N-Leach has the best Precision (97.14%), followed by S-Leach (95.32%), and Leach (92.35%). This shows how well N-Leach works at finding and blocking attacks while reducing the number of false alarms.Recall, which shows the percentage of real attacks that the system properly discovered, also shows a similar trend. With a recall rate of 95.63%, N-Leach is the best, followed by S-Leach at 92.45% and Leach at 86.45%. This means that the N-Leach and S-Leach protocols are better at finding a higher rate of real attacks than the Leach protocol.Lastly, the F1 Score shows how well the intruder detection system worked generally. It is made up of Precision and Recall combined into a single measure. Once more, N-Leach has the best F1 Score (96.47%), followed by S-Leach (93.65%), and then Leach (89.74%).The test results show that adding Bayesian game theory to intrusion detection systems makes them work better. Specifically, the N-Leach and S-Leach protocols are better than the traditional Leach protocol at finding intrusions accurately and reducing false alarms.

5. Conclusion

Adding a 2-Player Bayesian Game Theory structure to Intrusion Detection and Prevention Systems (IDPS) seems like a good way to protect against Distributed Denial of Service (DDoS) attacks. By making the interaction between attackers and defenders look like a game, this approach makes it possible for defenses to change and react in ways that can effectively stop new DDoS attacks.Using Bayesian Game Theory, the

IDPS can keep changing its plans based on what it sees happening and how things turn out. This makes it easier and more accurate to find bad behavior. The fact that players work together makes it easier for defenders to be aggressive and stop strikes before they happen.Using Bayesian thinking also makes it easier for the system to make smart choices in settings that are unclear and change quickly, like those found in DDoS attacks. By taking into account statistical views about the enemy's plans and moves, the IDPS can make the best reaction to strikes while reducing the number of false positives.The addition of 2-Player Bayesian Game Theory to standard IDPS makes it more powerful and provides a strong defense against DDoS attacks. As cyber risks change, this method shows a lot of promise for making network systems more resilient and protecting them from attacks that get smarter over time.

References

[1] D. Patel and D. Patel, "PolyDDoSchain - Collaborative Volumetric Distributed Denial of Service Attack Detection and Prevention using Blockchain Technology," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, pp. 1571-1578 (2023), doi: 10.1109/ICSCSS57650.2023.10169487.

[2] S. Vattikuti, M. R. Hegde, M. Manish, V. Bodduvaram and V. Saraswathi, "DDoS Attack Detection and Mitigation using Anomaly Detection and Machine Learning Models," 2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), Bangalore, India, 9683214. pp. 1-6 (2021).

[3] J. A. Pérez-Díaz, I. A. Valdovinos, K. -K. R. Choo and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," in *IEEE Access,* vol. 8, pp. 155859-155872 (2020), doi: 10.1109/ACCESS.2020.3019330.

[4] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," in *IEEE Access,* vol. 9, pp. 59353-59377 (2021), doi: 10.1109/ACCESS.2021.3073408.

[5] N. Kathirkamanathan, B. Thevarasa, G. Mahadevan, N. Skandhakumar and N. Kuruwitaarachchi, "Prevention of DDoS Attacks Targeting Financial Services using Supervised Machine Learning and Stacked LSTM," 2022 IEEE 7th International conference for Con-

vergence in Technology (I2CT), Mumbai, India, pp. 1-5 (2022), doi: 10.1109/I2CT54291.2022.9825228.

[6] Ajani, S. N., Khobragade, P., Dhone, M., Ganguly, B., Shelke, N., & Parati, N. Advancements in Computing: Emerging Trends in Computational Science with Next-Generation Computing. *International Journal of Intelligent Systems and Applications in Engineering*, 12(7s), 546–559 (2023).

[7] D. Radain, S. Almalki, H. Alsaadi and S. Salama, "A Review on Defense Mechanisms Against Distributed Denial of Service (DDoS) Attacks on Cloud Computing," 2021 International Conference of Women in Data Science at Taif University (WiDSTaif), Taif, Saudi Arabia, pp. 1-6 (2021), doi: 10.1109/WiDSTaif52235.2021.9430220.

[8] I. Riadi, Sunardi and A. Muhammad, "DDoS Detection Using Artificial Neural Network Regarding Variation of Training Function", *Advanced Science Letters*, vol. 24, no. 12, pp. 9163-9167 (2018).

[9] T. Mahjabin, Y. Xiao, G. Sun and W. Jiang, "A survey of distributed denial-of-service attack prevention and mitigation techniques", *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, pp. 155014771774146 (2017).

[10] Limkar, Suresh, Ashok, Wankhede Vishal, Singh, Sanjeev, Singh, Amrik, Wagh, Sharmila K. & Ajani, Samir N. A mechanism to ensure identity-based anonymity and authentication for IoT infrastructure using cryptography, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:5, 1597–1611 (2023).

[11] B. Susilo and R. Sari, "Intrusion Detection in IoT Networks Using Deep Learning Algorithm", *Information,* vol. 11, no. 5, pp. 279 (2020).

[12] B. Shah and B. H Trivedi, "Artificial Neural Network based Intrusion Detection System: A Survey", *International Journal of Computer Applications*, vol. 39, no. 6, pp. 13-18.