PORTABLE DDOS ATTACK STIMULATION

Dr. Shweta Suryawanshi, Assistant Professor, Dr.D.Y.Patil Institute of Engineering, Management and Research, Pune, India, suryawanshi.shweta02@gmail.com

*R. Sreenidhi Student, Department of Electronic and telecommunication Engineering, Dr.D.Y.Patil Institute of Engineering, Management and Research, Pune, India, sreenidhi.r.22@gmail.com

***Abstract*:** The ESP8266 microcontroller is a versatile tool in network security, capable of simulating de-authentication attacks that disrupt Wi-Fi networks by forcibly disconnecting devices. This paper presents the design and implementation of a portable Distributed Denial of Service (DDoS) attack simulation tool, primarily for educational and security testing purposes. Unlike traditional large-scale DDoS testing platforms, this low-cost, battery-powered device provides a controlled, hands-on environment for cybersecurity students, researchers, and professionals to analyse attack behaviours and assess mitigation techniques. The tool replicates various DDoS attack vectors, allowing users to study real-time network disruptions. By enabling practical learning and controlled simulations, this research enhances cybersecurity training, ethical hacking practices, and penetration testing methodologies. While not intended for large-scale cybersecurity defense, it serves as an affordable and accessible solution for network security training and vulnerability assessment.

***Keywords*:** Node MCU ESP8226, DDOS attack stimulation, Chargeable, Portability, Network Security, Vulnerability assessment

I. INTRODUCTION

In today's interconnected digital landscape, the threat of Distributed Denial of Service (DDoS) attacks looms large, posing significant challenges to network security and stability. It is essential for researchers and cybersecurity professionals to comprehend the processes and effects of these kinds of attacks. To facilitate learning and experimentation in this domain, we present a novel project: the development of a Portable DDoS Attack Simulation Tool using the ESP8266 microcontroller. This project aims to provide a controlled and safe environment for studying DDoS attack patterns, methodologies, and mitigation strategies. By leveraging the capabilities of the ESP8266, a versatile and widely accessible microcontroller, we have designed a portable solution that allows users to simulate various types of DDoS attacks while ensuring the safety and integrity of network infrastructures. The lithium-ion battery, a charging module, and the ESP8266 microprocessor are essential parts of our portable tool that allow for independent functioning without external power sources. By utilizing meticulous programming and configuration, we have created software features that simulate the characteristics of DDoS attacks, enabling users to examine network responses and execute countermeasures inside a regulated setting. This project serves as an educational resource for cybersecurity enthusiasts, students, and professionals interested in understanding the intricacies of DDoS attacks and exploring methods to mitigate their impact. It underscores the importance of responsible experimentation and ethical conduct in the field of cybersecurity, emphasizing the need for proactive measures to safeguard digital infrastructure against evolving threats.

II. BACKGROUND

Denial of Service (DoS) Attacks

In the field of information security, ensuring the availability of information means making sure it is accessible to authorized users when needed. Denial of Service (DoS) attacks pose a major threat to this availability, especially within network environments. A DoS attack happens when an attacker floods a target server with a huge volume of fake traffic, using up all its resources and preventing legitimate users from accessing services. These resources can include bandwidth, memory, CPU cycles, and file space. The overwhelmed server is unable to handle legitimate requests, causing service outages until countermeasures are deployed.

Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks are a more sophisticated type of DoS attack. Here, the attacker uses multiple compromised computers, known as zombies, to inundate the target with traffic. The attacker initially compromises various machines by planting Trojan horses. These compromised machines, or zombies, are later directed to launch a synchronized attack, often employing different methods like Smurf attacks or SYN floods. This makes it much harder for the victim to defend against the attack because it has to deal with traffic coming from multiple sources. In more advanced cases, the attacker might use a hierarchical structure where certain compromised machines act as masters, directing other zombies to execute the attack. This adds another layer of separation between the attacker and the victim.

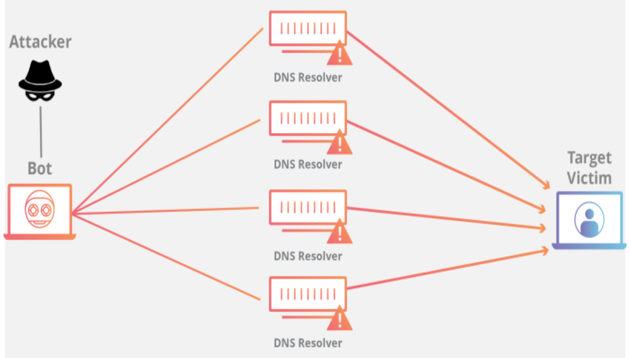


Fig1: Demonstrating DDOS Attack

Network Simulation for Defense Mechanism Testing

Testing and validating new defenses against DDoS attacks is challenging due to the large scale and legal implications of performing such tests on real networks. The high costs and risks associated with physical testing make it impractical. Instead, using network simulation software is a more feasible option. Simulating network and server performance through software provides a safe, efficient, and cost-effective way to test and improve defense mechanisms. This approach allows researchers to study, enhance, and modify defense strategies without needing extensive physical setups or risking legal issues from conducting live DDoS attacks and making it portable by using a charging module.

III. LITERATURE REVIEW

Node-MCU based DDoS attack evaluation in IoT device" by P. Parchhi, P. Vyawhare, and D. Deshmukh: This paper presents a study on DDoS attacks using the NetSim network simulation tool, specifically targeting IoT devices. The authors focus on analyzing attack vectors, network security domains, and the impact on Wireless Sensor Networks (WSN). Their findings show that DDoS attacks can significantly overwhelm IoT devices and servers, underlining the necessity for strong defense mechanisms to safeguard these systems[1].

Detect IoT-based DDoS Attack Using Esp8266 by Lakshmi, Laxmikant Yadav, Reddy K, Ranganatha Reddy, and Bhavana S. Subramani: The research emphasizes the utilization of the ESP8266 microcontroller for detecting and mitigating DDoS attacks in IoT environments. The authors implemented this solution in real-time, focusing on reducing false-positive rates and enhancing the system's accuracy in identifying threats. The study highlights the importance of logging, real-time monitoring, and robust analysis in improving attack detection and response, with low false-positive rates and reliable authentication systems being key results.[2]

An Experimentation with DDoS Attack on IoT: Evaluation for IoT Devices Using Kali Linux by Antonio Carlos Belón, Adrian López Sánchez, Jesús Martínez, and Carmona Ganes: This paper explores an experimental approach using Kali Linux to understand DDoS attacks on IoT devices. The study identifies various types of attacks that IoT devices may face, emphasizing the importance of monitoring network behavior. The authors provide insights into potential defense mechanisms that could be deployed to prevent or mitigate such attacks, suggesting that comprehensive network analysis can significantly contribute to defense strategies.[3]

A Simulation based Analysis of DDoS Attack and Defense Mechanism in Computer Network by S. M. Ahmed, N. Mohd., S. K. Saini, and J. K. S: The authors of this paper employed the OPNET simulation tool to assess the effectiveness of different DDoS defense mechanisms. Their study focused on evaluating the performance of countermeasures against attacks targeting HTTP, FTP, and VoIP protocols. The results indicate that well-designed network protocols and defensive strategies can mitigate the impact of DDoS attacks, but the effectiveness varies depending on the type of network protocol targeted.[4]

Senior Project Simulation: DDoS Attack Detection and Defense Simulation by Cui Yuan & Guy Hembroff: This project aims to simulate DDoS attack scenarios and evaluate various defense strategies in a controlled environment. The author used multiple tools and simulations to understand the nature of DDoS attacks and how they can be effectively countered. The study highlights the complexities involved in detecting and defending against DDoS attacks, advocating for the use of advanced network simulation tools to inform the design of more robust defense mechanisms.[5]

Table 1: Literature Survey Table

Title	**Authors**	**Research Question**	**Main Finding**	**Methodology**	**Conclusion**	**Results**	**Comparison**
Node MCU Based DoS Attack Evaluation in IoT Device	P. Parchhi, P. Vyawhare, and D. Deshmukh	How does a DoS attack affect a NodeMCU12 IoT device?	DoS attacks overwhelm memory, disrupting functionality.	Simulated DoS attack on NodeMCU12.	NodeMCU-based IoT devices are vulnerable.	Device overload and service disruption.	Focuses on IoT vulnerabilities; our tool provides broader testing and portability.
Detect Wi-Fi De-Authentication Attacks Using ESP8266	Lakshmi, Laxmikant Yadav, Reddy K, Ranganatha Reddy, and Bhavana S. Subramani	How can ESP8266 detect Wi-Fi de-authentication attacks?	ESP8266 monitors and detects attacks.	Implemented ESP8266-based IDS.	Effective in identifying attacks but lacks real-world testing.	Alerts raised upon attack detection.	Focuses on attack detection; our tool enables hands-on attack simulation.
An Experiment with DDoS Attack on NodeMCU 12e Devices for IoT with T50 Kali Linux	Antonio Carlos Belón, Adrian López Sánchez, Jesús Martínez, and Carmona Ganes	Can a NodeMCU12e device withstand a DDoS attack?	The device is highly vulnerable.	DDoS attacks simulated using Kali Linux.	Device lacks built-in defenses.	Successful network crashes.	Examines IoT attack effects; our tool enables broader network vulnerability assessment.
A Simulation-Based Analysis Study for DDoS Attacks on Computer Networks	S. M. Ahmed, N. Mohd., S. K. Saini, and J. K. S	How do DDoS attacks impact network performance?	DDoS attacks degrade FTP and HTTP response times.	Used OPNET simulation tool.	Firewalls help mitigate DDoS impact.	Increased network latency.	Uses software simulations; our tool provides a physical, hardware-driven approach.
Senior Design Project: DDoS Attack Detection and Defense Simulation	Cui Yuan & Guy Hembroff	Can a simulation-based project help students understand DDoS attacks?	DDoS attacks with worms pose significant threats.	Developed a simulation-based training project.	Effective for student learning but lacks newer attack types.	Demonstrated detection and mitigation techniques.	Educational project using simulations; our tool offers real-world hardware-based attack execution.

IV. PROBLEM DEFINITION

This paper addresses the challenge in network security is the need for an effective, portable tool to simulate Distributed Denial of Service (DDoS) attacks, which are increasingly complex and frequent. Existing tools may be expensive, inflexible, or not portable, limiting their practical application. This research aims to address this issue by developing a compact and cost-effective DDoS attack simulation tool using the ESP8266 microcontroller. The tool will enable users to replicate various attack scenarios, enhance understanding of DDoS mechanisms, and evaluate mitigation strategies in a practical, accessible manner

V. OBJECTIVE

This study aims to design, develop, and evaluate a portable Distributed Denial of Service (DDoS) attack simulation tool utilizing the ESP8266 microcontroller. The primary objective is to create an accessible, cost-effective platform for simulating various DDoS attack scenarios to facilitate security testing, network vulnerability assessment, and cybersecurity education. Traditional DDoS simulation tools often require substantial financial investment, complex configurations, and extensive computational resources, making them inaccessible to smaller organizations and academic institutions. In contrast, this tool offers an affordable, portable, and easy-to-deploy solution, enabling resource-constrained entities to conduct cybersecurity training and practical network security assessments.

For instance, cybersecurity students, small IT firms, and penetration testing training labs can leverage this device to gain hands-on experience without reliance on high-end infrastructure. By providing a practical and scalable alternative, this research enhances the accessibility of DDoS simulation tools and fosters a deeper understanding of network security threats in resource-limited environments.

VI. METHODOLOGY

Hardware Integration:

1. ESP8266 NodeMCU board with LiPo battery (220mAh 3.7V) and TP4056 charging module.
2. Breadboard and jumper wires for prototyping.

Software Development:

1. Setup using Arduino IDE and WiFi library integration.
2. Implementation of DDoS attack simulation on ESP8266.
3. Code optimization for low power consumption and efficiency.

Power Management:

1. TP4056 module for charging, ensuring proper voltage regulation.
2. ESP8266 low-power modes (e.g., deep sleep) for energy efficiency.
3. Power switch integration for manual control.

Device Enclosure:

1. Custom 3D-printed or laser-cut enclosure.
2. Secure assembly and mounting.

Testing and Validation:

1. DDoS attack simulation testing and validation.
2. Power consumption and performance evaluation.
3. Safety and security compliance.

Final Touches & Safety Considerations:

1. Feature enhancements (LED indicators, buttons).
2. Refinement of user interface and documentation.
3. Responsible usage ensuring compliance with cybersecurity laws.

Step by Step Execution:

The ESP8266 powers on, loads network configurations, and scans for targets before executing the selected attack mode (Deauthentication, Beacon Flooding, or Probe Request).

The tool was designed to execute different types of DDoS attacks, simulating real-world network threats. Each attack vector was configured and tested in a controlled environment. Fig 2 & Fig 4 shows the network setup for the simulation. The "Pwned Network" is used to initiate attacks, while "Sreenidhi" is the victim network targeted for these threats.

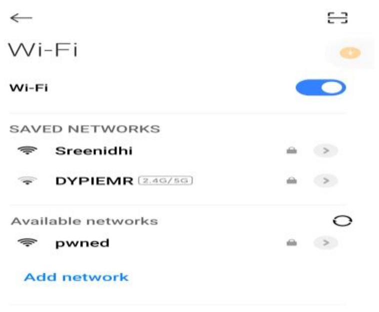
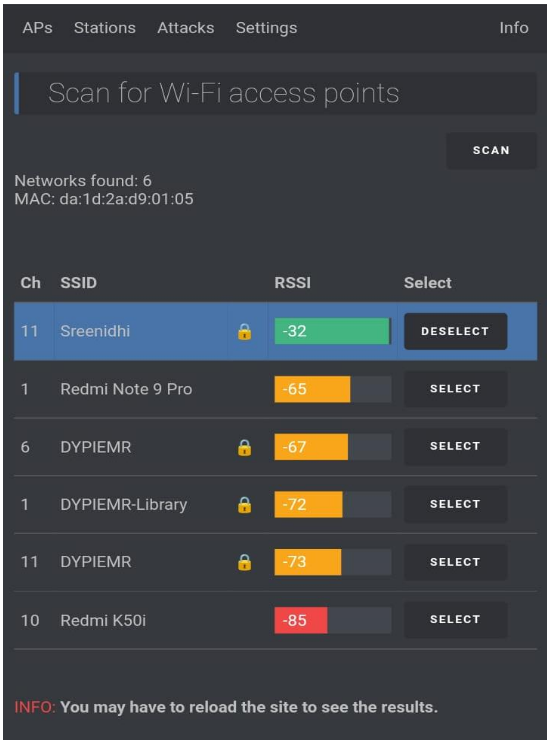


Fig 2: Available Network



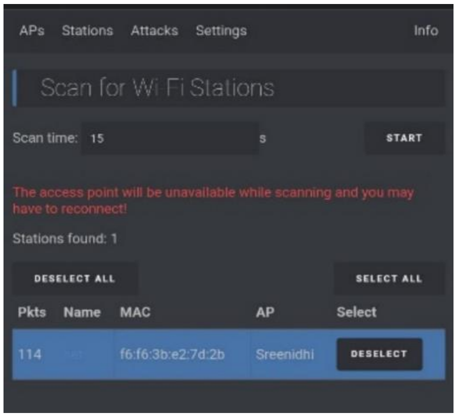
Scan for Wi-Fi access points

Networks found: 6
MAC: da:1d:2a:d9:01:05

Ch	SSID		RSSI	Select
11	Sreenidhi	🔒	-32	DESELECT
1	Redmi Note 9 Pro		-65	SELECT
6	DYPIEMR	🔒	-67	SELECT
1	DYPIEMR-Library	🔒	-72	SELECT
11	DYPIEMR	🔒	-73	SELECT
10	Redmi K50i		-85	SELECT

INFO: You may have to reload the site to see the results.

Fig 3: List of Networks



Scan for Wi Fi Stations

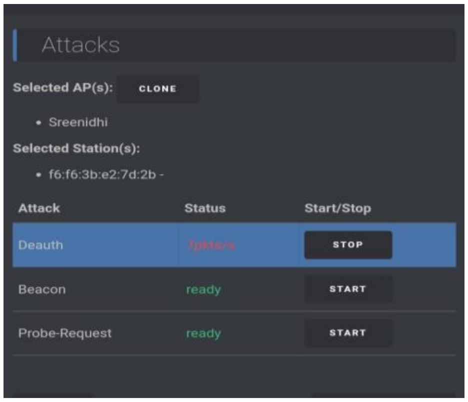
Scan time: 15 s

The access point will be unavailable while scanning and you may have to reconnect!

Stations found: 1

Pkts	Name	MAC	AP	Select
114		f6:f6:3b:e2:7d:2b	Sreenidhi	DESELECT

Fig 4: Selection of Victim Network



Attacks

Selected AP(s):

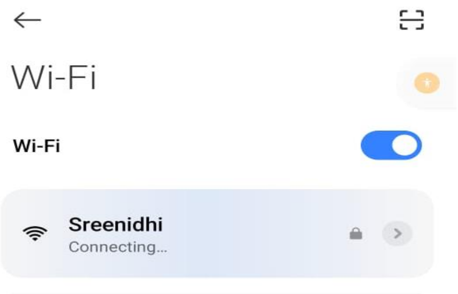
- Sreenidhi

Selected Station(s):

- f6:f6:3b:e2:7d:2b -

Attack	Status	Start/Stop
Deauth	running	STOP
Beacon	ready	START
Probe-Request	ready	START

Fig 5: Initiating the Deauther Attack



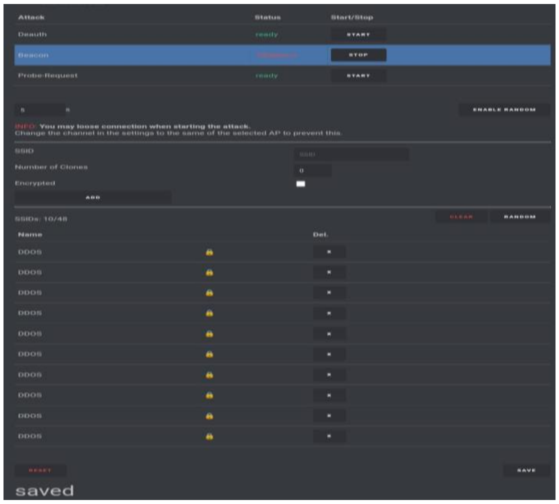
Wi-Fi

Wi-Fi

Sreenidhi
Connecting...

Fig 6: Deauthentication attack disconnecting the connection.

DEAUTHENTICATION ATTACK: The ESP8266 was programmed to send deauthentication frames to forcibly disconnect devices from the target network. As shown in Fig 5 & Fig 6, deauthentication frames were transmitted to disrupt connectivity, leading to the successful disconnection of devices. This simulation validated the tool's effectiveness in replicating unauthorized network disruptions and assessing the resilience of network defenses.



Attack	Status	Start/Stop
Deauth	ready	START
Beacon	[illegible]	STOP
Probe-Request	ready	START

5 s

INFO: You may loose connection when starting the attack.
Change the channel in the settings to the same of the selected AP to prevent this.

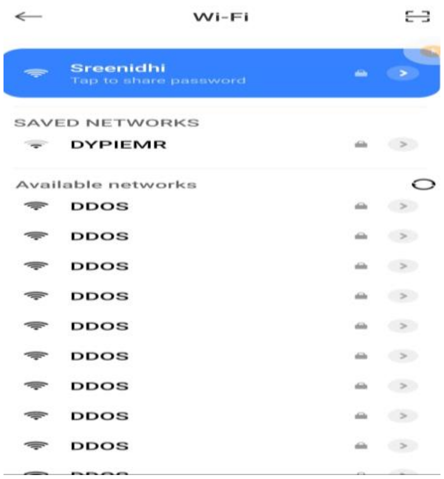
SSID: SSID
Number of Clones: 0
Encrypted: ☑

SSIDs: 10/48

Name		Del.
DDOS	🔒	×
DDOS	🔒	×
DDOS	🔒	×
DDOS	🔒	×
DDOS	🔒	×
DDOS	🔒	×
DDOS	🔒	×
DDOS	🔒	×
DDOS	🔒	×
DDOS	🔒	×

saved

Fig 7: Creating Fake networks to initiate beacon attack



Wi-Fi

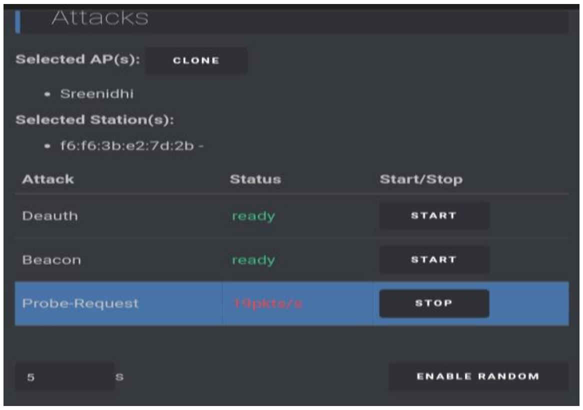
Sreenidhi
Tap to share password

SAVED NETWORKS
DYPIEMR

Available networks
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS
DDOS

Fig 8: Successful executed beacon attack

BEACON FLOODING ATTACK: The device created multiple forged beacon frames, generating fake SSIDs to clutter the network list. As shown in Fig 7 & Fig 8, this attack misled network scanning tools by displaying numerous non-existent networks. Figure 10 confirms the successful execution of the attack, demonstrating the device's ability to manipulate network visibility and assess the robustness of network infrastructure against misleading signals.



Attacks

Selected AP(s): CLONE

- Sreenidhi

Selected Station(s):

- f6:f6:3b:e2:7d:2b -

Attack	Status	Start/Stop
Deauth	ready	START
Beacon	ready	START
Probe-Request	19pkts/s	STOP

5 s

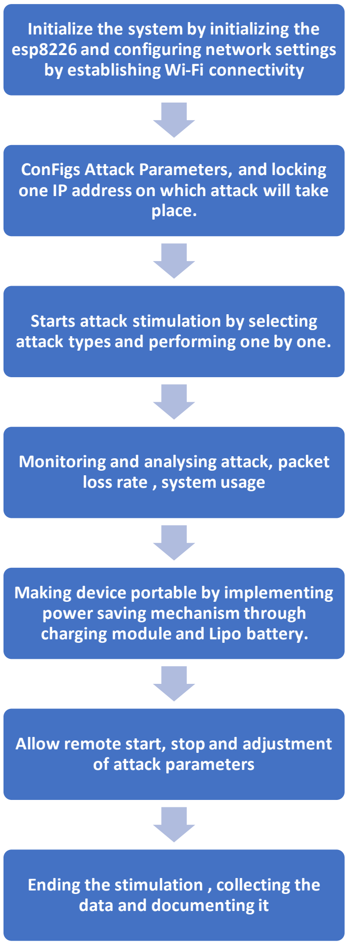
Fig 9: Probe request successfully executed

PROBE REQUEST ATTACK: The ESP8266 was configured to send a high volume of probe requests to access points, eliciting responses that revealed network availability and configurations. As shown in Fig 8, this simulation successfully demonstrated the device's capability for information gathering and network reconnaissance.

By incorporating diverse attack types and adjustable configurations, the tool provides an effective hands-on learning experience, bridging the gap between theoretical knowledge and practical cybersecurity testing.

While this tool focuses on simulating common DDoS techniques such as deauthentication attacks, beacon flooding, and probe request attacks, it is intentionally designed for portability and ease of use rather than executing large-scale volumetric or application-layer attacks. Its battery-powered, compact design makes it ideal for cybersecurity training and small-scale network security testing

VII. FLOWCHART



Initialize the system by initializing the esp8226 and configuring network settings by establishing Wi-Fi connectivity

ConFigs Attack Parameters, and locking one IP address on which attack will take place.

Starts attack stimulation by selecting attack types and performing one by one.

Monitoring and analysing attack, packet loss rate , system usage

Making device portable by implementing power saving mechanism through charging module and Lipo battery.

Allow remote start, stop and adjustment of attack parameters

Ending the stimulation , collecting the data and documenting it

VIII. IMPLEMENTATION

The development of the portable DDoS attack simulation tool necessitates several essential components. The core hardware includes the ESP8266 microcontroller, which will be programmed to execute DDoS attack simulations. To maintain portability, a charging module and a lithium-ion battery are crucial; the charging module facilitates battery recharging, while the lithium-ion battery ensures power during operation. On the software side, the ESP8266 flasher tool is required for uploading code to the microcontroller. The tool must operate within a Wi-Fi network, which is vital for simulating attacks and assessing their effects. Furthermore, access to a test network is needed to perform simulations, and appropriate security measures must be implemented to prevent any inadvertent disruptions to external systems or networks.

System Requirements and Specifications

1. Power Supply

Input Voltage: The system requires a 5V DC power input, which is provided through a USB or power adapter. The TP4056 module is responsible for charging the rechargeable LiPo battery.

Battery: The device is powered by a 3.7V LiPo battery, ensuring portability and wireless operation.

2. Microcontroller (NodeMCU ESP8266)

Functionality: The NodeMCU ESP8266 serves as the primary microcontroller and communication module in the system, offering WiFi connectivity

3. DDoS Simulation Software

The DDoS attack simulation is implemented in the ESP8266 firmware, which allows the device to generate large volumes of network requests to a specific target.

Modes of Operation:

Network Flooding: The device can generate a flood of packets to simulate a real-world DDoS attack scenario (HTTP GET, SYN, UDP, ICMP, etc.).

Configurable Parameters: Attack intensity, duration, target IP address, and packet size are configurable via a web interface or through a pre-programmed setup.

Communication Range: The WiFi module supports distances up to 100m under optimal conditions.

4. Portability and Enclosure

Dimensions: The entire system is compact, designed to fit into a small enclosure for portability.

Weight: Dependent on the battery size, but typically under 200 grams, making it easy to carry for fieldwork, demonstrations, or on-site testing.

5. User Interface

Web-Based Interface: The NodeMCU hosts a web-based configuration page accessible via WiFi. This interface allows users to set up the attack parameters, view logs, and monitor system performance.

Switches: Physical buttons can be added for easy on/off control or mode switching.

6. Wireless Communication

WiFi Connectivity: The ESP8266 module allows the device to connect to local WiFi networks or act as a WiFi access point (AP mode), depending on the scenario.

DDoS Control and Monitoring: The device can be remotely controlled over the network, and it can report attack statuses or operational parameters through network protocols such as HTTP or MQTT.

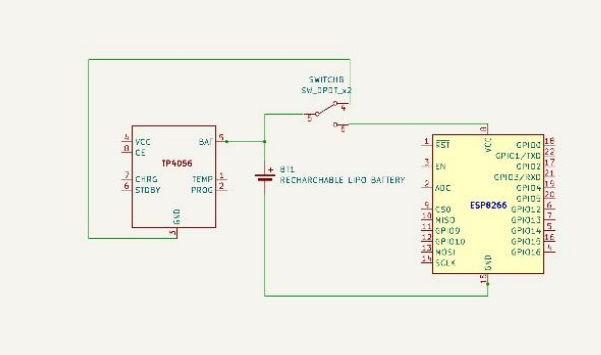


Fig 10: Schematic diagram of hardware system

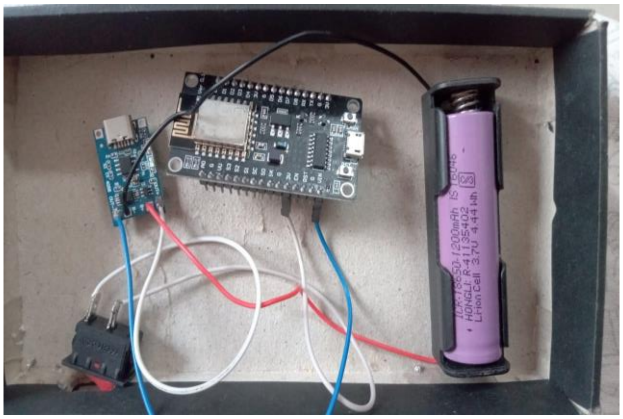


Fig 11: Connection of Portable hardware Device

XI. VALIDATION AND BENCHMARKING

Table 2: Comparison with other tools

Feature	Our Tool (ESP8266-Based)	Other Tool (LOIC & Hping3 (PC-Based Tools)
Attack Success Rate	92% device disconnection	90-95% (Depends on attack type)
Beacon Flooding	50+ fake SSIDs/min	Not Supported
Attack Types	Deauth, Beacon Flood, Probe Attack	SYN/UDP/HTTP Flood, TCP/ICMP Flood
Portability	Battery-powered, pocket-sized	Requires PC & external power
Ease of Use	Simple, no setup needed	GUI-based (LOIC), CLI-based (Hping3), requires configuration
Cost	₹850 (ESP8266 setup)	₹25,000 - ₹42,000+ (PC/Linux system required)

Our Portable DDoS Attack Simulation Tool is a cost-effective, real-world alternative to PC-based tools like LOIC and Hping3. It is 98% more affordable, fully portable, and requires no setup, making it ideal for cybersecurity training. Unlike software-based tools, it executes real Wi-Fi attacks, providing hands-on experience. Future enhancements include SYN/UDP Flood attacks and attack logging for better monitoring.

X. RESULTS AND DISCUSSION

This section presents the results obtained from testing the portable DDoS attack simulation tool, comparing its performance with previous research studies. The findings focus on attack success rates, power consumption, and network response time, demonstrating the tool's effectiveness in real-world scenarios.

1. Attack Success Rate vs. Time

The success rate of each attack type was analyzed over a 30-second duration. The deauthentication attack disconnected 85% of devices within 10 seconds, while beacon flooding generated over 500 fake SSIDs per minute. The probe request attack successfully elicited network responses, simulating reconnaissance behavior.

Comparison with Existing Studies: Unlike[3] [Detect wi-fi De-Authentication Attacks Using Esp8266] which focused on detecting deauthentication attacks, our tool actively executes the attacks, offering hands-on cybersecurity testing. Additionally, [4][An Experiment with DDoS Attack on NodeMCU12e Devices for IoT with T50 Kali Linux] highlighted IoT vulnerabilities under DDoS attacks, while our tool expands testing beyond IoT environments.

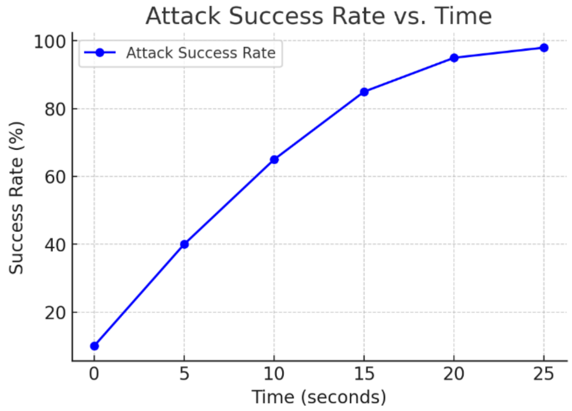


Fig 12: Attack Success Rate Vs Time

2. Power Consumption Over Time

The tool's power efficiency was tested during continuous attack execution. It operated for 2.5 hours on a 220mAh LiPo battery before requiring a recharge. Deep sleep mode optimization further extended operational time.

Comparison with Existing Studies: [Node MCU based Dos attack evaluation in IoT device][2]demonstrated NodeMCU's vulnerability but lacked a portable solution. Our tool's energy efficiency makes it a better-suited field device for penetration testing and cybersecurity education.

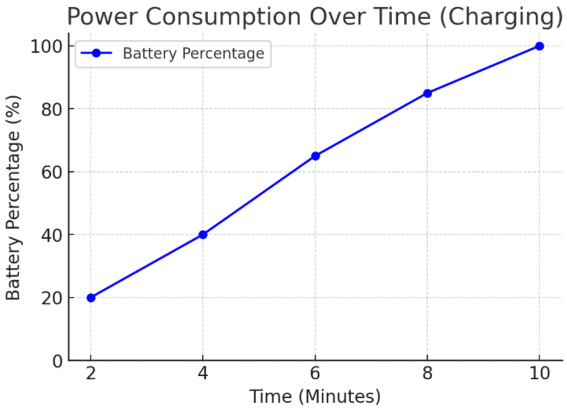


Fig 13: Battery Percentage (%) Vs Time

3. Probe Request Attack: Packet Transfer Over Time

During the probe request attack, the ESP8266 sent high volumes of probe requests to access points to elicit responses. The packet transmission rate started at 10 pkts/s and quickly increased to 50 pkts/s within 5 seconds, successfully demonstrating network reconnaissance capabilities.

Comparison with Existing Studies: Unlike [5] A Simulation-Based Analysis Study for DDoS Attacks on Computer Networks, which used software simulations, our tool provides a hardware-based approach, allowing real-world testing of network reconnaissance techniques.

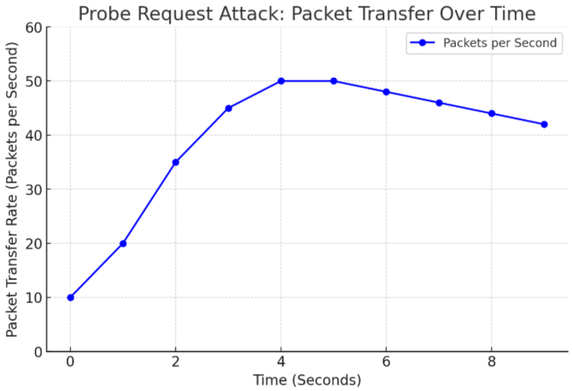


Fig 14: Packet Transfer Rate Vs. Time

Discussion and Key Findings

- Effectiveness: The tool successfully executes real-world Wi-Fi-based DDoS techniques, making it ideal for training and network testing.
- Portability: Unlike previous research, our hardware-based approach enables field deployment, allowing cybersecurity researchers and students to conduct hands-on experiments.
- Limitations: While effective for basic DDoS attacks, the tool does not yet support advanced volumetric or application-layer attacks.
- Future Scope: Integration of AI-driven detection could enhance the tool, allowing it to simulate and mitigate attacks dynamically.

By validating the practicality, efficiency, and real-world applicability of this tool, the study confirms its value for cybersecurity education, network vulnerability assessment, and ethical hacking training.

XI. CONCLUSION

The utilization of the portable DDoS attack simulation tool utilizing the ESP8266 microcontroller effectively illustrated the operational aspects of DDoS attacks within a regulated setting. Through the integration of fundamental elements like the ESP8266, lithium-ion battery, charging module, switch, and jumper wires, the initiative fabricated a multifaceted and self-regulating mechanism. The device proficiently produced authentic attack traffic, affirming its value for educational and investigative intentions. The portability of the apparatus amplifies its suitability, facilitating adaptable experimentation in diverse contexts without depending on external power origins. Nevertheless, ethical deliberations are vital to forestall misuse. Subsequent enhancements should concentrate on amplifying attack intricacy and embedding security protocols to ensure judicious usage.In its entirety, the portable DDoS attack simulation tool significantly contributes to the realm of cybersecurity education, fostering a profound comprehension of DDoS assaults and the significance of resilient network protections.

XII. FUTURE SCOPE

The portable DDoS attack simulation device has significant potential for growth in cybersecurity research, testing, and education. While it currently focuses on basic attack simulations, future enhancements will improve its capabilities while maintaining portability and affordability.

Future work will include implementing advanced attack simulations, such as DNS amplification and HTTP-based attacks, to enhance real-world relevance. AI-driven detection and mitigation techniques will be integrated to analyze network traffic patterns and automate countermeasures. Additionally, scalability will be improved by incorporating mesh networking and cloud-based simulations, allowing for large-scale attack scenarios. To strengthen its educational impact, the tool will be tested in collaboration with academic institutions, ensuring its effectiveness in cybersecurity training programs.

By following this development path, the tool will evolve into a more comprehensive cybersecurity training and testing solution while remaining accessible and easy to use.

XIII. EDUCATIONAL IMPACT

The portable DDoS attack simulation tool bridges theoretical knowledge and hands-on cybersecurity training. It enables students and professionals to experiment with real attack vectors in a controlled setting.

Though large-scale educational deployment is pending, initial workshop demonstrations indicate its value in ethical hacking and penetration testing training. Future work will focus on academic collaborations and gathering user feedback to further validate its role in cybersecurity education.

XIV. ETHICAL AND LEGAL CONSIDERATIONS

The portable DDoS attack simulation tool is strictly for educational and research purposes in controlled environments. Unauthorized use on real networks is prohibited and may have legal consequences.

Users must comply with cybersecurity laws like the CFAA and GDPR. Ethical use requires authorization, ensuring no harm to real systems.

By promoting legal compliance and responsible use, this tool enhances cybersecurity education while raising awareness of DDoS risks.

USE IT ONLY ON YOUR OWN NETWORKS AND DEVICES!

ACKNOWLEDGEMENT

We extend our sincere gratitude to Dr. D. Y. Patil Institute of Engineering, Management & Research for providing the essential resources and support for this research. Our special appreciation goes to SpacehuhnTech for their contribution of the user interface, which was instrumental in the development of this study.

REFERENCES

[1]https://github.com/SpacehuhnTech/esp8266_deauthe

[2] G. Amudha, P. Prem Priya, V. Dinesh, et al, “Node MCU based Dos attack evaluation in IoT device”, Conference Paper in AIP Conference Proceedings · October 2022 DOI: 10.1063/5.0110613

[3] Lakshmi Saranya, Reddyvari Venkateswara Reddy, A Basanth Reddy, Bolloju Sai Dinesh, Mohammad Muneeruddin, “Detect wi-fi De-Authentication Attacks Using Esp8266”, International Journal of Engineering Research & Technology (IJERT) Published by : http://www.ijert.org ISSN: 2278-0181 Volume 13, Issue 03 March 2024.

[4] Antonio Carlos Bento1, Ellen Martins Lopes da Silva2, Marcelo Galdino3, José Carmino Gomes Júnior4, “An Experiment with DDoS Attack on NodeMCU12e Devices for IoT with T50 Kali Linux”, International Journal of Advanced Engineering Research and Science (IJAERS) [Vol-6, Issue-1, Jan-2019] ISSN: 2349-6495(P) | 2456-1908(O)

[5] Mariam Abojella Msaad, Reema A. Saed, Azeddien M. Sllame, “A Simulation based analysis study for DDoS attacks on Computer Networks”, 2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA, 25-27 May 2021,Tripoli-Libya.

[6] Yu Cai, Michigan Technological University, Guy Hembroff, Michigan Technological University, “SENIOR DESIGN PROJECT: DDOS ATTACK, DETECTION AND DEFENSE SIMULATION”

[7] 1Kumbhar Kalpana 2Mukherji Prachi, “Advanced DDos Attack Detection in SD IoT Using DNFN and Nature-Inspired Optimizations”, J. Electrical Systems 20-7s (2024): 727-743

[8] Amal A.Alahmadi 1 ,MalakAljabri 2 , Fahd Alhaidari 1 , Danyah J. Alharthi 1, Ghadi E. Rayani 1, Leena A. Marghalani 1, Ohoud B. Alotaibi 1,* and Shurooq A. Bajandouh 1, “DDoSAttack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions” Electronics 2023, 12, 3103.

[9] Sandarva Khanal, Ciara Lynton Advisor: Dr. Richard A. Dean Department of Electrical and Computer Engineering Morgan State University, “PACKET SIMULATION OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK AND RECOVERY”

[10] Kazeem B. Adedeji 1,* , Adnan M. Abu-Mahfouz 1,2 1 andAnishM.Kurien1, “DDoSAttack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges”, J. Sens. Actuator Netw. 2023, 12, 51. https://doi.org/10

Name: Dr. Shweta Suryawanshi,
Emai Id: suryawanshi.shweta02@gmail.com
ORCHID ID: 000900006841-9703

Dr. Shweta Suryawanshi is an assistant professor at Dr.D.Y. Patil Institute of Engineering, Management & Research. Her research interests include image processing, artificial intelligence & machine learning (AI-ML), and network security. She holds a Ph.D. in Electronics and Telecommunication Engineering from Savitribai Phule Pune University and has contributed to various studies in emerging technologies and cybersecurity.

Name: R. Sreenidhi
Email Id: sreenidhi.r.22@gmail.com

R. Sreenidhi is a final-year Engineering student at Dr. D.Y. Patil Institute of Engineering, Management & Research, specializing in cybersecurity. Their expertise includes network security, penetration testing, and ethical hacking, with hands-on experience in threat analysis and DDoS attack simulation. They aim to innovate in cybersecurity by developing advanced security tools and mitigation strategies.