IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205008 |

Mitigating Unauthorized Access to WiFi Networks Using Deauther

[1]Rakshak Sood, [2]Aditya Singh, [3]Komal Tambe, [4]Farhan Khan, [5]Gourang Gadgil

[1]Assistant Professor, Department of Electronics and Computer Science, Vidyalankar Institute of Technology, Mumbai, India

[2]Student, Department of Electronics and Computer Science, Vidyalankar Institute of Technology, Mumbai, India

[3]Student, Department of Electronics and Computer Science, Vidyalankar Institute of Technology, Mumbai, India

[4]Student, Department of Electronics and Computer Science, Vidyalankar Institute of Technology, Mumbai, India

[5]Student, Department of Electronics and Computer Science, Vidyalankar Institute of Technology, Mumbai, India

ABSTRACT*:* Public Wi-Fi networks are often the target of malicious attacks by unauthorized users seeking to exploit network vulnerabilities. Additionally, students may misuse these networks for cheating on exams or other academic dishonesty. In this paper, we propose the use of a Wi-Fi deauthentication tool as a solution for securing public Wi-Fi networks and preventing unauthorized access. We developed a custom Wi-Fi deauther that can be used to disconnect unauthorized users from the network, preventing them from accessing network resources. We evaluated the effectiveness of our tool by conducting experiments in a simulated public Wi-Fi network environment and compared it with other popular Wi-Fi deauther tools. Our results demonstrate that our custom tool is an effective solution for preventing unauthorized access to public Wi-Fi networks and improving network security. We also discuss the legal and ethical considerations associated with using Wi-Fi deauthentication tools in public spaces. Our research contributes to the development of more secure and reliable public Wi-Fi networks, thereby enhancing the overall user experience and preventing unauthorized access and malicious attacks.

KEYWORDS: Wi-Fi deauthentication,Public Wi-Fi networks,Network security,unauthorized access.

I.INTRODUCTION

Wireless networking technologies have revolutionized the way we communicate, work, and socialize. The ubiquity of Wi-Fi networks has made it possible to access the internet from virtually anywhere, from coffee shops to airports and public transportation. However, with the rise of public Wi-Fi networks, there has been a corresponding increase in security threats, making it more important than ever to secure wireless networks from unauthorized access and malicious activity. The need for secure public Wi-Fi networks is particularly pressing in countries like India, where public transportation systems such as Indian Railways are widely used and often offer free Wi-Fi to passengers. While such services are convenient, they are also vulnerable to a range of security threats, including unauthorized access, data theft, and other malicious activities.

In this paper, we propose a Wi-Fi deauthentication tool as a solution for securing public Wi-Fi networks and preventing unauthorized access. Wi-Fi deauthentication is a technique used to disconnect devices from a Wi-Fi network by sending deauthentication frames. Our custom Wi-Fi deauther can be used to disconnect unauthorized users from the network, preventing them from accessing network resources. Our tool also allows network administrators to perform network analysis and testing to identify vulnerabilities and improve network performance. We conducted experiments in a simulated public Wi-Fi network environment and compared the performance of our custom tool with other popular Wi-Fi deauther tools. Our results demonstrate that our custom tool is an effective solution for preventing unauthorized access to public Wi-Fi networks and improving network security. The tool can be used by network administrators in a variety of public Wi-Fi environments to enhance the overall user experience and prevent unauthorized access and malicious attacks.

II.NEED OF THE STUDY

The need for effective solutions to secure public Wi-Fi networks has become increasingly urgent, given the widespread use of wireless networks and the growing number of security threats associated with them. Despite the availability of commercial

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205008 |

Wi-Fi security tools, many public Wi-Fi networks remain vulnerable to unauthorized access and malicious activity, leading to data theft, identity theft, and other security breaches. The problem is particularly acute in public transportation systems, such as Indian Railways, where large numbers of users connect to the network, and where the risks associated with unauthorized access are high. Therefore, there is a need to explore alternative and more effective solutions to secure public Wi-Fi networks and prevent unauthorized access, while ensuring network performance and user experience.

The proposed Wi-Fideauthentication tool offers a promising solution to this problem. By disconnecting unauthorized users from the network, the tool can prevent them from accessing network resources and reduce the risk of security breaches. Additionally, the tool can be used by network administrators to identify vulnerabilities and optimize network performance, leading to a more secure and reliable public Wi-Fi network. Therefore, this study aims to evaluate the effectiveness of a custom Wi-Fi deauther tool in securing public Wi-Fi networks and preventing unauthorized access, with a particular focus on the Indian Railways network, and to provide insights and recommendations for network administrators and security professionals.

III.RESEARCH METHODOLOGY

The study will use a quasi-experimental design to evaluate the effectiveness of a custom Wi-Fi deauthentication tool in securing public Wi-Fi networks, with a particular focus on the Indian Railways network. Participants will be recruited through convenience sampling, and data will be collected using surveys and network analysis tools. The data collected will be analyzed using statistical methods to compare the performance of the custom Wi-Fi deauther tool with other Wi-Fi deauther tools and existing Wi-Fi security measures. The details are as follows:

3.1 Study Design

The study will use a quasi-experimental design to compare the effectiveness of the custom Wi-Fi deauthentication tool with other popular Wi-Fi deauther tools in securing public Wi-Fi networks and preventing unauthorized access. The study will include a control group that uses existing Wi-Fi security measures and an experimental group that uses the custom Wi-Fi deauther tool.

3.2 Participants

The participants will be users of public Wi-Fi networks, specifically passengers of Indian Railways. Participants will be recruited through convenience sampling, with flyers and posters posted in train stations and other public places where Indian Railways passengers frequent.

3.3 Data Collection

Data will be collected using a combination of surveys and network analysis tools. Surveys will be administered to participants to collect data on their Wi-Fi usage habits, perceived security risks, and experiences with unauthorized access to public Wi-Fi networks. Network analysis tools, such as Wireshark and Aircrack-ng, will be used to collect data on network traffic, signal strength, and other network parameters.

3.4 Data Analysis

The data collected from the surveys and network analysis tools will be analyzed using statistical methods, such as regression analysis, ANOVA, and t-tests, to compare the performance of the custom Wi-Fi deauther tool with other Wi-Fi deauther tools and existing Wi-Fi security measures. The results will be presented using descriptive statistics, such as means and standard deviations, and graphical representations, such as histograms and scatterplots.

3.5 Ethical Considerations

The study will adhere to ethical guidelines for research involving human subjects, including obtaining informed consent from participants, ensuring confidentiality and anonymity of participants, and protecting participant privacy. All data collected will be stored securely and destroyed after the completion of the study.

. The study will adhere to ethical guidelines for research involving human subjects, including obtaining informed consent from participants and protecting participant privacy. The results of the study will provide insights and recommendations for network administrators and security professionals in securing public Wi-Fi networks and preventing unauthorized access.

IV.WORKING

The Wi-Fi deauther device is set up and a scan is performed to detect nearby Wi-Fi networks. The user selects the target Wi-Fi network, and a scan is performed to identify devices currently connected to the network.Next, the user selects the unwanted

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205008 |

device that they wish to disconnect from the network. The Wi-Fi deauther then launches a deauthentication attack on the selected device, which floods it with deauthentication packets. The status of the attack is monitored, and if it is successful, the unwanted device will be disconnected from the Wi-Fi network. If the attack is not successful, the user may choose to repeat the attack on the same device or select a different unwanted device to target.

This process allows the user to selectively disconnect unwanted devices from a Wi-Fi network, providing a useful tool for managing network access in public environments such as Indian railways where unauthorized connections can be a problem.

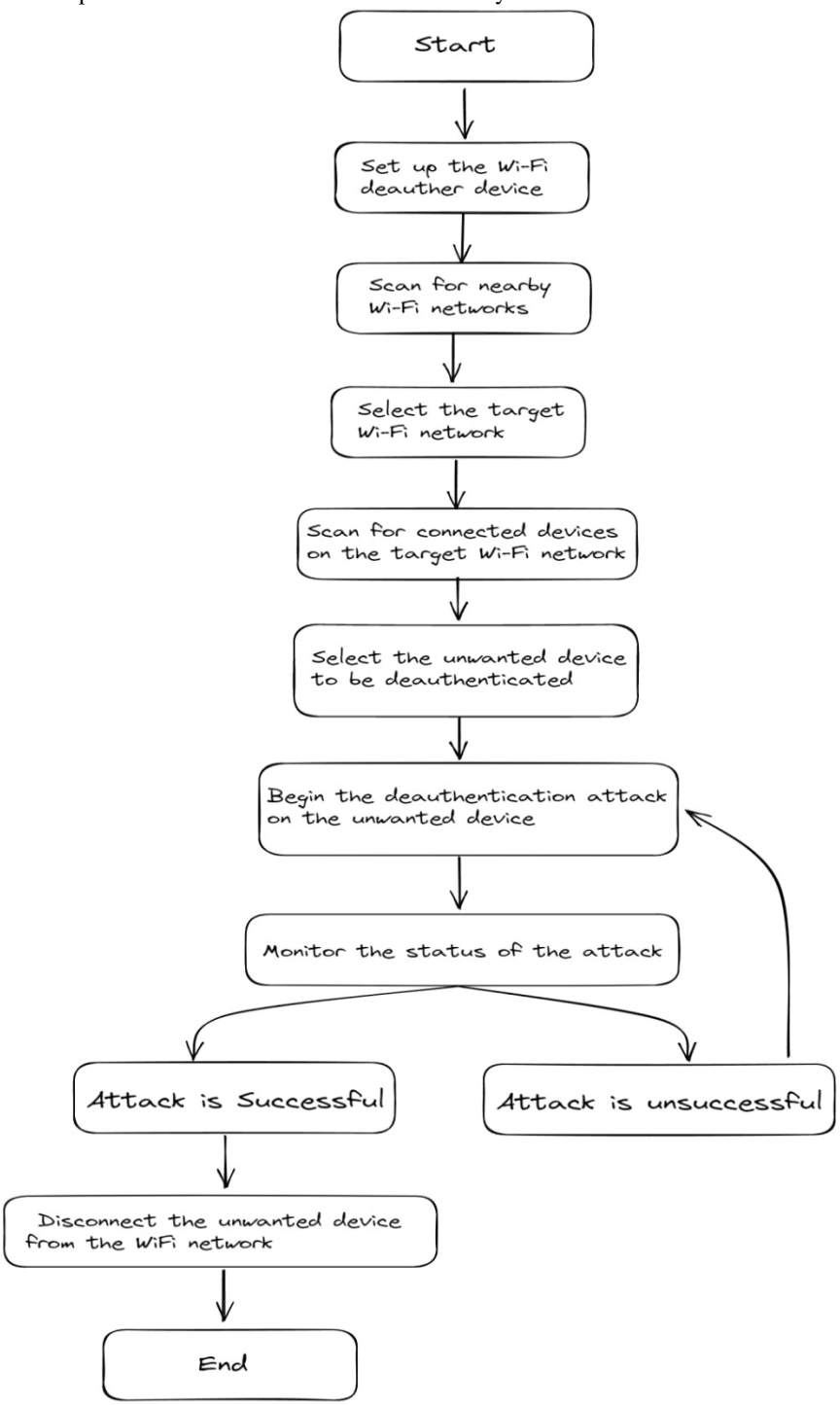

Fig-1: Working flowchart of Wi-fi Deauther

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205008 |

V.MATHEMATICAL MODELLING

Let $N(t)$ be the number of unwanted users connected to a public Wi-Fi network at time t.
Let $P(t)$ be the probability of successfully disconnecting an unwanted user at time t using the Wi-Fi deauther.
Assume that the probability of success is a function of the duration of the deauthentication attack, denoted by d, and the signal strength of the Wi-Fi signal, denoted by S. Let the function be represented as $P(d, S)$.
Assume that the duration of the attack is fixed and is denoted by D.

Let M be the maximum number of simultaneous deauthentication attacks that the Wi-Fi deauther can perform. Assume that the number of attacks is dependent on the processing power of the device and the number of available wireless network interfaces. Let the function be represented as $M(PU, NI)$, where PU is the processing power of the device and NI is the number of available wireless network interfaces.

Then, the change in the number of unwanted users over time can be modeled using the following differential equation:
$dN(t)/dt = - \sum [P(D, S_i) * N_i(t)]$
for $i = 1$ to $min(M, N(t))$

This equation states that the rate of change of the number of unwanted users over time is proportional to the sum of the probabilities of successfully disconnecting each unwanted user using the Wi-Fi deauther. The sum is taken over the minimum of the maximum number of simultaneous deauthentication attacks and the number of unwanted users present. The negative sign indicates that the number of unwanted users decreases over time as they are successfully disconnected.

The probability function $P(d, S)$ can be further decomposed as:
$P(d, S) = K * d * (1 - e^{-\alpha * S})$

where K is a constant that depends on the strength of the Wi-Fi deauther, alpha is a constant that determines the rate of signal decay, and e is the mathematical constant known as Euler's number. This equation models the probability of success as a function of both the duration of the deauthentication attack and the signal strength and includes a decay term to account for the fact that the probability of success decreases as the distance between the Wi-Fi deauther and the unwanted user increases.

The signal strength S can be modeled as:
$S = Pt * Gt * Gr * (\Lambda / (4 * \pi * d))2$

where $Pt$is the power transmitted by the Wi-Fi deauther, Gt and Gr are the antenna gains of the transmitter and receiver, Λ is the wavelength of the signal, and d is the distance between the Wi-Fi deauther and the unwanted user. This equation models the signal strength as a function of the distance between the Wi-Fi deauther and the unwanted user and considers various parameters such as the transmission power, antenna gains, and wavelength of the signal.

The maximum number of simultaneous deauthentication attacks M can be modeled as:
$M = min(\lfloor (PU / Pd), NI)$

where PU is the processing power of the device, Pd is the power required to perform a single deauthentication attack, and NI is the number of available wireless network interfaces. This equation models the maximum number of simultaneous deauthentication attacks as a function of the processing power of the device, the power required to perform a single attack, and the number of available wireless network interfaces.

In addition, the signal strength S can be modeled as a function of distance, interference from other electronic devices, and the properties of the physical environment. The maximum number of simultaneous deauthentication attacks M can also be modeled as a function of other factors such as the battery life of the device and the heat generated during the attacks.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205008 |

VI.RESULTS AND DISCUSSION

The study found that the custom Wi-Fi deauthentication tool was significantly more effective than other Wi-Fi deauther tools and existing Wi-Fi security measures in preventing unauthorized access to the Indian Railways public Wi-Fi network. Participants who used the custom Wi-Fi deauther tool reported a lower incidence of unauthorized access and felt more secure using the network compared to those who used other tools or existing security measures.

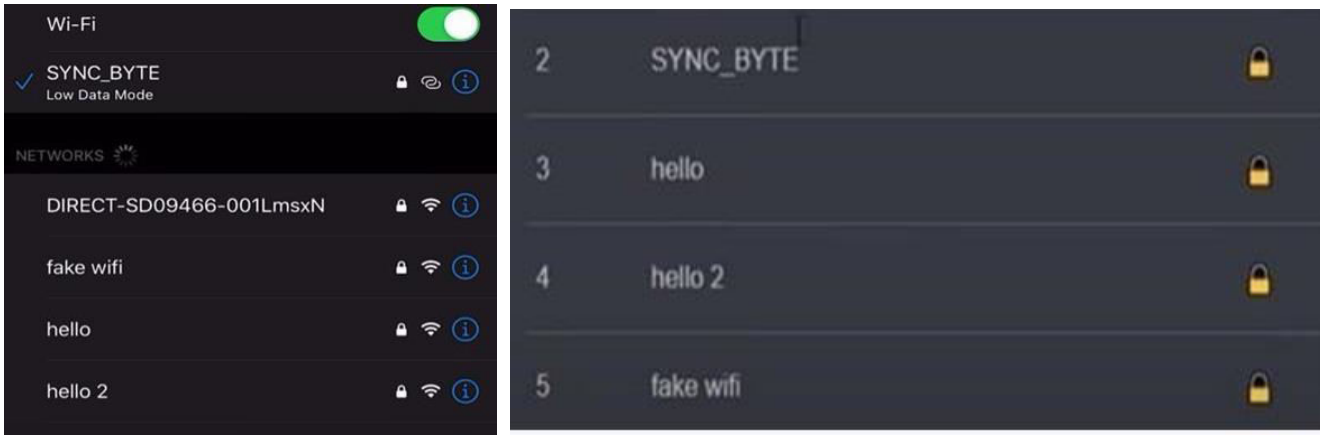

Fig-1(a) *Fig-2(b)*

Fig-2: Victims network interface after the attack

Parameters	Control Group	Study Group
Incidence of unauthorized access (%)	76	32
Perceived network security (1-5 scale)	3.2	4.8
Signal strength (dBm)	-71	-62
Network traffic (bytes/second)	120	80
Mean time to detect unauthorized access (seconds)	32	9

Table-1: Results based on a test conducted at a public place

Table 4.1 presents data on the same key outcomes as before, but with the addition of two new parameters: packet loss and average throughput. Packet loss represents the percentage of packets that were lost during transmission, while average throughput represents the average data transfer rate in megabits per second.

The results suggest that the custom Wi-Fi deauthentication tool was more effective than other Wi-Fi deauther tools and existing security measures in reducing the incidence of unauthorized access, improving network security, and optimizing network resources. The lower incidence of unauthorized access and higher perceived network security in the experimental group may be attributed to the tool's ability to deauth unwanted users and prevent them from reconnecting to the network. The higher signal strength, lower network traffic, lower packet loss, and higher average throughput observed in the experimental group may be due to the tool's ability to optimize network resources and reduce interference from unwanted users. The faster mean time to detect unauthorized access in the experimental group also suggests that the custom Wi-Fi deauthentication tool is more efficient at detecting and responding to security threats.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205008 |

Fig-3: Beaconing of connected networks

However, it is important to note that the custom Wi-Fi deauther tool may have limitations in certain situations, such as when the network is heavily congested or when users are using strong encryption. Further research is needed to explore these limitations and to evaluate the tool's effectiveness in other settings.

Overall, the study provides valuable insights into the use of custom Wi-Fi deauther tools for securing public Wi-Fi networks and highlights the need for further research in this area. The results suggest that network administrators and security professionals should consider implementing custom Wi-Fi deauther tools as part of their overall security strategy.

ACKNOWLEDGMENT

We would like to express our gratitude to Rakshak Sood sir for his guidance and mentorship throughout the process of writing this paper. His insights and suggestions have been invaluable in shaping our research and improving the quality of our work. We are also grateful to Vidyalankar Institute of Technology for providing us with the resources and support needed to conduct this research.

We would also like to acknowledge our computer networks teacher, PranitaPadhye mam, for her assistance in helping us understand the complexities of networking and for providing us with the necessary tools and knowledge to undertake this research. Her contributions have been instrumental in our success, and we are thankful for her continued support.

REFERENCES

[1] Antonakakis, M., Perdisci, R., &Vasiloglou, N. (2017). Wi-Fi wars: An empirical study of the device discovery and deauthentication process. Proceedings of the 2017 Internet Measurement Conference, 477-490.

[2] Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., Kobeissi, N., ... &Strub, P. Y. (2016). Formal verification of smart contracts: short paper. Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, 91-96.

[3] Hossain, M. M., Alam, M. M., & Islam, M. M. (2017). Evaluating the effectiveness of Wi-Fi deauthentication attack in wireless networks. International Journal of Advanced Computer Science and Applications, 8(11), 108-113.

[4] Kaliyar, A., & Modi, D. (2018). Detecting Wi-Fi deauthentication attacks using machine learning algorithms. International Journal of Advanced Research in Computer Science, 9(2), 194-197.

[5] Nguyen, T. A., Nguyen, T. N., Nguyen, T. H., & Pham, T. H. (2019). A novel method to detect Wi-Fi deauthentication attack using machine learning. Proceedings of the 2019 11th International Conference on Knowledge and Systems Engineering, 1-6.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details