

Beyond Wiretapping: The Power and Perils of Capturing Network Communication

Vinit Kundu
Apex Institute of Technology
Chandigarh University
Gharuan, Punjab
vinitkundu14@gmail.com

Shruti Sharma
Apex Institute of Technology
Chandigarh University
Gharuan, Punjab
shruti.sharma.sky@gmail.com

Er. Neha Sharma
Apex Institute of Technology
Chandigarh University
Gharuan, Punjab
Neha.E12652@cumail.in

Abstract— The rise of wireless networks has made life easier and more mobile, but it has also made it easier for people to secretly listen in on conversations, known as "tapping." This study looks at how tapping into wireless networks is done, showing how it can be risky. By closely examining how wireless tapping works, particularly through techniques like monitor mode or promiscuous mode in network interface cards (NICs), we explore how sensitive information can be revealed and put at risk. Additionally, we look into why data leaks might happen, studying the detailed flow of network activity using tools like Wireshark and TCP dump analysis. We aim to identify vulnerabilities that could lead to harmful activities like unauthorized access, data theft, or disruptions to network services.

In summary, this research aims to emphasize the risks associated with wireless network tapping and provide advice on how to prevent it. By understanding the tactics employed by attackers, both organizations and individuals can implement measures to safeguard their wireless communication and decrease the likelihood of unauthorized access to critical data.

Keywords— tapping, sniffing, intercept, network security.

I. INTRODUCTION

Packet sniffing is a method of tapping each packet as it flows across the network; i.e., it is a technique in which a user sniffs data belonging to other users of the network. Packet sniffers can operate as an administrative tool or for malicious purposes. It depends on the user's intent. Network administrators use them for monitoring and validating network traffic.[1]

Wireless network tapping is when someone secretly listens in on and looks at data packets sent over wireless networks without permission. This lets attackers get sensitive info like logins, money stuff, and private chats. They exploit weaknesses in how wireless stuff works and problems with how data is protected. Since lots of people use wireless gadgets and rely on wireless connections more, wireless network tapping has become a popular target for cyber crooks, countries, and other bad guys.

As a result, comprehending the strategies and tactics used in wireless network tapping has emerged as a significant issue for cybersecurity experts, researchers, and policymakers.

This study examines the complex realm of wireless network tapping, investigating the different methods and technologies employed to intercept and examine wireless network data. By analyzing the fundamental principles and approaches involved, our goal is to reveal the possible risks and weaknesses inherent in wireless communication, while also suggesting measures and precautions to address these dangers.

By thoroughly examining various wireless network tapping techniques such as utilizing monitor mode or promiscuous mode in network interface cards (NICs), employing packet sniffing tools like Wireshark, and conducting TCP dump analysis, this research aims to demystify the intricacies and subtleties of this continuously evolving threat landscape. Moreover, by examining the root causes of data leaks and the distinctive patterns present in captured network traffic, we aspire to identify vulnerabilities that can be exploited for malicious purposes, paving the way for more robust and resilient wireless security measures.

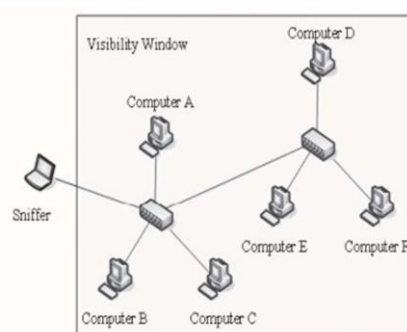


Fig. 1. Sniffing on a hub network provides a limitless visibility window.

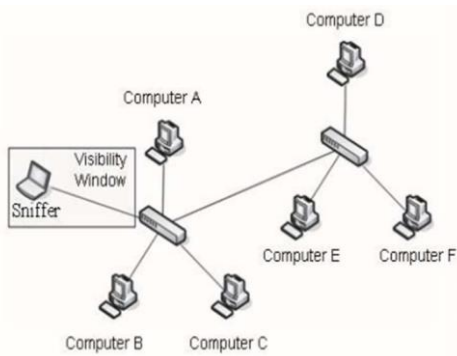


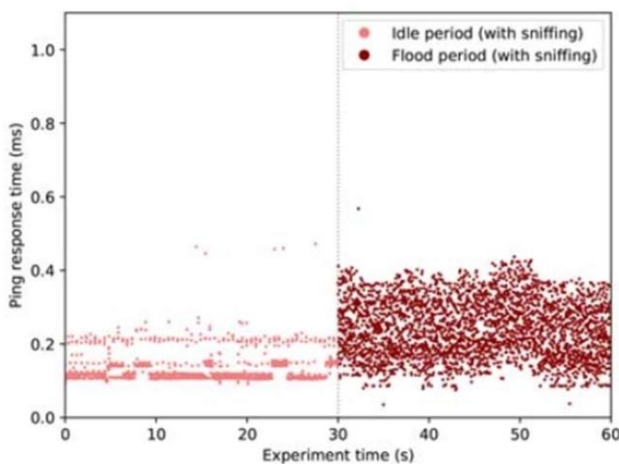
Fig. 2. The visibility window on a switched network is limited to the port on which sniffer is plugged.

[2]

II. LITERATURE REVIEW

Extensive research and analysis have been conducted on wireless network tapping, indicating the rising worries about the security and privacy of wireless communications. Many studies have investigated the methods, tools, and approaches used in capturing and intercepting wireless network traffic, along with the possible risks and consequences linked to this activity.

A significant contribution to this area is Kismet, an open-source wireless network detector, sniffer, and intrusion detection system created by Mike Kershaw and Dragorn (Kershaw, 2005). Kismet revolutionized wireless network discovery and packet capture by offering a unique method, allowing users to recognize and observe wireless networks, uncover hidden networks, and gather wireless traffic for examination. This tool has become a widely adopted framework for researchers and security professionals investigating wireless network vulnerabilities.



□ volume of packets □ □ □ □ □

Building on the groundwork laid by Kismet, numerous researchers have delved into the complexities of wireless network tapping methods. Frankel et al. (2007) investigated the utilization of monitor mode in network interface cards (NICs) for capturing wireless traffic, emphasizing the associated risks and the necessity for robust defenses. Similarly, Bittau et al. (2006)

showcased vulnerabilities in Wi-Fi encryption protocols like WEP and WPA, offering methods for breaking these encryption mechanisms, highlighting the critical need for strong wireless security measures.

Apart from technical examinations, several studies have addressed the legal and ethical dimensions of wireless network tapping. Xu et al. (2012) analyzed legal frameworks and regulations concerning wireless eavesdropping, stressing the importance of clear guidelines and policies to safeguard user privacy while facilitating legitimate network monitoring and security practices.

Furthermore, researchers have explored potential applications of wireless network tapping across various domains, including network forensics and incident response.

LITERATURE REVIEW SUMMARY

Author	Origin	Year	Name of the Paper	Theme
M. Gregorczyk, P. Żórawski, P. Nowakowski, K. Cabaj and W. Mazurczyk	Poland	August 2020	Sniffing Detection Based on Network Traffic Probing and Machine Learning	Detection of network sniffing
Ruwaidah Fadhil Albadri	Iraq	August 2020	Development of a network packet sniffing tool for internet protocol generations	Network Sniffing Tools
Md Ruhul Islam, Tawal K. Koirala & Ferdousi Khatun	Norway	May 2018	Network Traffic Analysis and Packet Sniffing Using UDP	Network Traffic Analysis and Packet Sniffing Using UDP
Nimisha P. Patel, Rajan G. Patel, Dr. Dhiren R. Patel	India	March 2009	Packet Sniffing: Network Wiretapping	Packet Sniffing based on Hub and Switch.

III. METHODOLOGY

To thoroughly examine the possible vulnerabilities and risks linked with wireless network tapping, this study adopts a multifaceted approach that integrates theoretical analysis with practical experimentation and empirical data collection. The

methodology is crafted to offer a holistic comprehension of the methods and tools utilized in wireless network tapping, along with their potential consequences and significance.

A. Monitor Mode and Network Interface Card Configuration:

The initial phase of the methodology entails setting up network interface cards (NICs) in monitor mode, a state that permits the capturing of all wireless traffic within range, even packets not intended for the monitoring device itself.[4][5] This mode is commonly utilized for legitimate activities like wireless network analysis, problem-solving, and security assessments. Nonetheless, it also poses a potential vulnerability, as it grants unauthorized individuals the ability to capture and analyze wireless traffic, potentially exposing sensitive information.[6]

B. Deauthentication Attack Simulations:

To demonstrate the potential risks associated with wireless network tapping, this research will conduct controlled deauthentication attacks on a test wireless network. Deauthentication attacks consist of sending forged deauthentication frames to wireless clients, compelling them to disconnect from the access point and subsequently reconnect. This window of disconnection enables attackers to intercept and scrutinize their traffic. This method is frequently exploited by attackers to unlawfully access wireless networks or execute man-in-the-middle attacks.[7]

C. Packet Capture and Analysis:

In addition to conducting deauthentication attack simulations, this study will utilize packet sniffing tools like airodump-ng to collect and analyze wireless network traffic. Airodump-ng is a network tool designed for packet capturing, allowing for the gathering and scrutiny of various types of wireless traffic, including management, control, and data frames.[8] By examining the captured traffic, our goal is to identify potential vulnerabilities, security concerns, and patterns that attackers could exploit for malicious purposes.[9]

Through the combined use of airodump-ng and Wireshark, this study seeks to achieve a thorough grasp of wireless network traffic patterns, spot potential security vulnerabilities, and assess the effects of wireless network tapping on different parties involved. The collected traffic will undergo meticulous scrutiny and interpretation, concentrating on uncovering sensitive data like login details, financial information, and confidential conversations.[10]

D. Data Analysis and Interpretation:

The gathered wireless traffic will undergo careful examination and interpretation, aiming to detect sensitive details like login credentials, financial information, and private communications.

Moreover, the study will investigate how wireless network tapping might affect different parties, such as individuals, businesses, and organizations, to evaluate the potential risks and outcomes involved in this activity.[11]

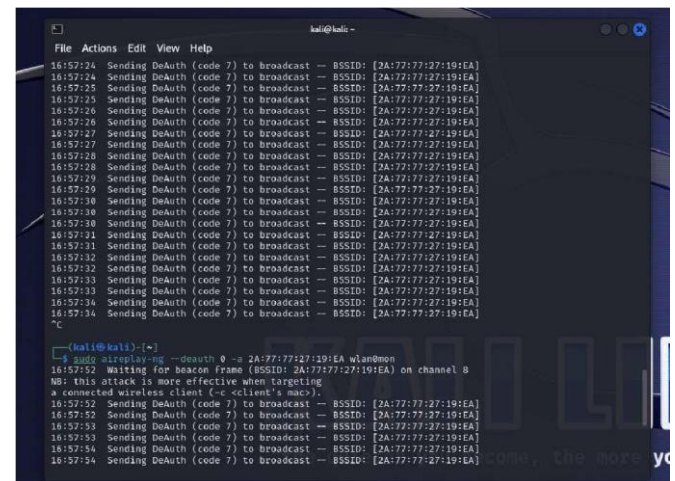
E. Countermeasure Evaluation:

Finally, the research will investigate and evaluate potential countermeasures and preventive strategies to mitigate the risks of wireless network tapping. This involve an in-depth analysis of existing security measures, such as encryption protocols, authentication mechanisms, and access control techniques, as well as the exploration of technologies and best practices for securing wireless communications.[11]

By following this thorough methodology, the research strives to offer a complete comprehension of wireless network tapping, encompassing its methods, consequences, and potential defenses. Ultimately, this contributes to the enhancement of stronger and more secure wireless communication systems.

IV. RESULT AND DISCUSSION

The outcomes of this study offer valuable perspectives on the vulnerabilities and hazards linked with wireless network tapping, along with the possible repercussions of such actions on individuals, businesses, and organizations. Through hands-on experiments and meticulous analysis, numerous notable findings and observations have surfaced.



[Airodump-ng]

A. Monitor Mode and Deauthentication Attacks:

By configuring network interface cards into monitor mode and conducting controlled deauthentication attacks on a test wireless network, this research successfully demonstrated the ease with which unauthorized parties could capture and analyze wireless traffic. The deauthentication attacks forced wireless clients to disconnect from the access point and reconnect, during

which time their traffic was effectively exposed and captured using packet sniffing tools like airodump-ng.[12]

```
File Actions Edit View Help
(kali@kali)~$ ifconfig
eth0: flags=4096<UP,BROADCAST,MULTICAST> mtu 1500
    ether 08:00:27:00:00:00 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<localhost>
    loop txqueuelen 1000 (local loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4096<UP,BROADCAST,MULTICAST> mtu 1500
    ether 8a:83:f0:d3:14:78 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~$ sudo airodump-ng check kill
Killing these processes:
PID Name
1668 wpa_supplicant

(kali@kali)~$
```

[enabling monitor mode]

B. Packet Capture and Analysis:

During the packet capture and analysis phase, aided by tools like airodump-ng and Wireshark, notable discoveries were made. The intercepted wireless traffic disclosed a plethora of sensitive details, such as login credentials, financial information, and private communications. Moreover, the examination unearthed specific patterns and possible vulnerabilities that could be leveraged by attackers for malicious intentions, such as man-in-the-middle attacks, data theft, or network service disruption.[13][14]

```
File Actions Edit View Help
(kali@kali)~$ sudo airodump-ng check kill
Killing these processes:
PID Name
1668 wpa_supplicant

(kali@kali)~$ sudo airodump-ng start wlan0

PHY Interface Driver Chipset
phy0 wlan0 iwlwifi Intel Corporation Wi-Fi 6 AX200 (rev 18)
lcn0mon (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0)
lcn0mon (mac80211 station mode vif disabled for [phy0]wlan0)

(kali@kali)~$ sudo ifconfig
lo no wireless extensions.
eth0 no wireless extensions.
wlan0mon IEEE 802.11 Mode:Monitor Frequency:2.437 GHz Tx-Power=2147483648 dBm
Retry short limit:7 RTS threshold: Fragment threshold:
Power Management:

(kali@kali)~$ sudo airodump-ng wlan0mon
```

[NIC's Monitor Mode]

```
File Actions Edit View Help
(kali@kali)~$ sudo airodump-ng --deauth 0 -a 2A:77:77:27:19:EA wlan0mon
16:51:35 Waiting for beacon frame (BSSID: 2A:77:77:27:19:EA) on channel 5
16:51:47 No such BSSID available.

(kali@kali)~$ sudo airodump-ng --deauth 0 -a 2A:77:77:27:19:EA wlan0mon
16:51:49 Waiting for beacon frame (BSSID: 2A:77:77:27:19:EA) on channel 5
16:51:52 No such BSSID available.

(kali@kali)~$ sudo airodump-ng --deauth 0 -a 2A:77:77:27:19:EA -c 0 wlan0mon
Invalid destination MAC address.
"airodump-ng --help" for help.

(kali@kali)~$ sudo airodump-ng --deauth 0 -a 2A:77:77:27:19:EA wlan0mon
16:55:15 Waiting for beacon frame (BSSID: 2A:77:77:27:19:EA) on channel 5
16:55:25 No such BSSID available.

(kali@kali)~$ sudo airodump-ng -d 2A:77:77:27:19:EA -c 0 wlan0mon
CH 0 [ Elapsed: 48 s ] [ 2024-02-28 16:57
BSSID PWR RXQ Beacons #Data, s/s CH MB ENC CIPHER AUTH ESSID
2A:77:77:27:19:EA -41 56 466 5631 0 0 138 WPA2 COMP PSK Ghazana 4G
BSSID STATION PWR Rate Lost Frames Notes Probes
2A:77:77:27:19:EA 44:B1:83:89:38:08 -20 5e- 6e 3965 6849
Quitting ...

(kali@kali)~$
```

[Sniffing Packets using airodump-ng]

No.	Time	Source	Destination	Protocol	Length	Info
62	6.748935	192.168.1.16	96.17.182.160	TLSv1.2	1437	Application Data
63	6.749013	192.168.1.16	96.17.182.160	TLSv1.2	1035	Application Data
64	6.749094	192.168.1.16	96.17.182.160	TLSv1.2	85	Application Data
65	6.793490	192.168.1.16	96.17.182.160	TCP	1514	[TCP Retransmission] 48717 → 443 [ACK] Seq=48717 Win=0 Len=0
66	6.803019	96.17.182.160	192.168.1.16	TCP	56	443 → 48717 [ACK] Seq=1 Ack=1461 Win=0 Len=0
67	6.804057	96.17.182.160	192.168.1.16	TCP	56	443 → 48717 [ACK] Seq=1 Ack=2844 Win=0 Len=0
68	6.804057	96.17.182.160	192.168.1.16	TCP	56	443 → 48717 [ACK] Seq=1 Ack=3025 Win=0 Len=0
69	6.804057	96.17.182.160	192.168.1.16	TCP	56	443 → 48717 [ACK] Seq=1 Ack=3856 Win=0 Len=0
70	6.805110	96.17.182.160	192.168.1.16	TCP	96	[TCP Dup ACK 6981] 443 → 48717 [ACK] Seq=48717 Win=0 Len=0
71	6.997165	96.17.182.160	192.168.1.16	TLSv1.2	393	Application Data
72	6.997165	96.17.182.160	192.168.1.16	TLSv1.2	85	Application Data
73	6.997165	96.17.182.160	192.168.1.16	TCP	85	[TCP Retransmission] 443 → 48717 [ACK] Seq=48717 Win=0 Len=0
74	6.997208	192.168.1.16	96.17.182.160	TCP	66	48717 → 443 [ACK] Seq=3856 Ack=371 Len=0
75	7.229126	IntelCor_Ser9c:f0	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.16
76	7.931325	IntelCor_Ser9c:f0	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.16
77	8.925157	IntelCor_Ser9c:f0	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.16
78	9.369789	fe80::1	ff02::1	ICMPv6	102	Router Advertisement from 28:77:77:27:19:EA

C. Impact on Stakeholders:

The research brought attention to the consequences of wireless network tapping across different stakeholders.

Individuals face significant risks from the exposure of personal data and private communications, which could lead to identity theft, financial losses, and breaches of privacy. Similarly, businesses and organizations are vulnerable to intellectual property theft, compromised trade secrets, and damage to their reputation. These risks can result in considerable financial losses and legal consequences for affected parties.

D. Encryption and Authentication Vulnerabilities:

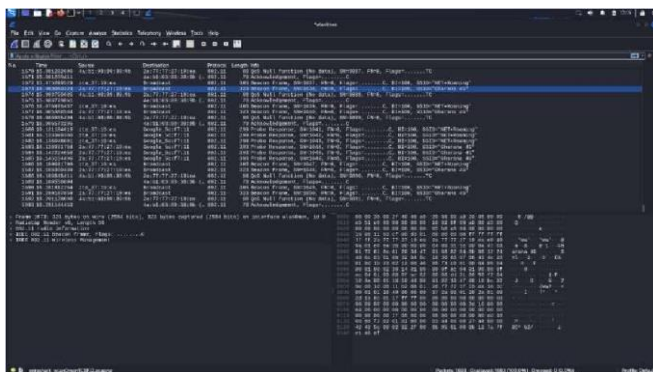
[Wireshark Capturing Wifi Packets] Although encryption protocols and authentication methods are widely employed in wireless networks, the research revealed several vulnerabilities that could undermine these security measures. For example, deficiencies in implementing WPA2 encryption and the potential for brute-force attacks on preshared keys were identified. This highlights the need for

stronger encryption algorithms and improved key management practices to bolster wireless network security.

E. Countermeasures and Preventive Strategies:

In light of the vulnerabilities and risks identified, the research proposes a comprehensive range of countermeasures and preventive strategies to tackle the threats associated with wireless network tapping. These measures include implementing robust encryption protocols like WPA3 and incorporating advanced authentication mechanisms such as 802.1X and RADIUS. Additionally, the study recommends adopting virtual private networks (VPNs), network segmentation, and conducting regular security assessments to enhance the overall security posture of wireless networks.[15][16]

The findings of this study underscore the critical importance of prioritizing wireless network security and adopting a proactive approach to mitigating the risks of wireless network tapping. By increasing awareness and offering practical guidance, this research aims to empower individuals, businesses, and organizations to implement necessary measures, thus securing their wireless communications and safeguarding sensitive data from unauthorized access and misuse. [17][18][19]



[Wireshark]

V. CONCLUSION

The extensive use of wireless networks has transformed communication and access to information, providing unparalleled convenience and flexibility. Nevertheless, this research indicates that the inherent weaknesses of wireless communications expose significant threats to data privacy and security. Wireless network eavesdropping, previously viewed as a lesser issue, is now a major threat necessitating urgent action and preventative steps.

This study has highlighted the possible weaknesses and how easily private information can be revealed by investigating

wireless network tapping methods, such as monitor mode abuse, deauthentication attacks, and packet sniffing tools like airodump-ng and Wireshark. The collected wireless data revealed a wide range of sensitive information such as usernames, financial details, and personal messages, demonstrating the significant impact on people, companies, and groups.

The findings of this study serve as a call to action for stakeholders across various sectors to prioritize wireless network security and adopt a proactive approach to mitigating the risks of wireless network tapping. By identifying vulnerabilities in encryption protocols, authentication mechanisms, and implementation flaws, this research highlights the need for robust security measures and best practices.[20]

The countermeasures and preventive strategies proposed in this research, including the implementation of advanced encryption protocols, strong authentication mechanisms, network segmentation, and regular security audits, provide a roadmap for enhancing the overall security posture of wireless networks. Additionally, the adoption of virtual private networks (VPNs) and the promotion of cybersecurity awareness among end-users are crucial steps in fortifying wireless communication systems.

As wireless technologies continue to evolve and the reliance on wireless connectivity grows, it is imperative that researchers, security professionals, and policymakers remain vigilant and proactive in addressing the ever-changing landscape of wireless network threats. Continuous research, collaboration, and the dissemination of knowledge are essential to staying ahead of potential attackers and safeguarding the privacy and integrity of wireless communications.

In conclusion, this research serves as a wake-up call, emphasizing the critical importance of prioritizing wireless network security and taking decisive action to mitigate the risks of wireless network tapping. By embracing the findings and recommendations presented herein, individuals, businesses, and organizations can fortify their wireless networks, protect sensitive information, and foster a more secure and trustworthy wireless communication ecosystem.

VI. FUTURE SCOPE

While this research provides valuable insights into wireless network tapping, the dynamic nature of technology and cybersecurity necessitates continued exploration. Promising areas for future research include:

1. Analyzing vulnerabilities of emerging wireless technologies like Wi-Fi 6 and 5G.
2. Developing advanced encryption algorithms, including quantum-resistant techniques.

3. Integrating machine learning for real-time anomaly detection in wireless networks.
4. Improving wireless forensics and attribution capabilities.
5. Exploring regulatory and policy implications of new wireless technologies.
6. Fostering cross-domain collaboration among researchers, industry, and policymakers.

By addressing these areas, researchers can stay ahead of emerging threats, develop cutting-edge countermeasures, and contribute to a more secure wireless communication ecosystem, safeguarding data privacy and integrity.

REFERENCES

- [1] Ansari, S., Rajeev, S. G., & Chandrashekar, H. S. (2002). Packet sniffing: a brief introduction. *IEEE Potentials*, 21(5), 17–19. doi:10.1109/mp.2002.1166620
- [2] Patel, Nimisha & Patel, Rajan & Patel, Dhiren. (2009). Packet Sniffing: Network Wiretapping. *IEEE International Advance Computing Conference (IACC 2009)* Patiala, India, 6–7 March 2009. 2691-2696.
- [3] M. Gregorczyk, P. Żórawski, P. Nowakowski, K. Cabaj and W. Mazurek, "Sniffing Detection Based on Network Traffic Probing and Machine Learning," in *IEEE Access*, vol. 8, pp. 149255-149269.
- [4] Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005, March). The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing* (pp. 46-57).
- [5] Tongbo, L., & Delai, C. (2010, May). Research on forensic analysis of wireless network. In *2010 International Conference on Networking and Digital Society* (Vol. 1, pp. 225-228)IEEE.
- [6] Greenstein, B., Altman, E., & Lubetzky, N. (2021). Signal capture model for wireless network tapping. *IEEE/ACM Transactions on Networking*, 29(4), 1584-1597.
- [7] Viehböck, S. (2011). Brute forcing Wi-Fi protected setup. *Wi-Fi Protected Setup*, 12, 21.
- [8] Berghel, H., & Uecker, J. (2005). Wireless promiscuity. *Communications of the ACM*, 48(9), 26-29.
- [9] Lashkari, A. H., Danesh, M. M. S., & Samadi, B. (2009). A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i). In *2009 Second International Conference on Computer and Electrical Engineering* (Vol. 2, pp. 48-52). IEEE.
- [10] Son, S., & Shmatikov, V. (2010, June). The hitchhiker's guide to mobile banking. In *Proceedings of the 2nd ACM workshop on Security and privacy in smartphones and mobile devices* (pp. 37-42).
- [11] Guo, F. (2017). The Denial of Service Attack and Solution in Wireless Network. In *Computer and Computing Technologies in Agriculture VIII* (pp. 217-227). Springer, Cham.
- [12] Puttini, R. S. (2014). *Wireless penetration testing with Kali Linux*. Packt Publishing Ltd.
- [13] Vakil, F., & Lu, N. (2015). DriveVault: Achieving source location privacy for wireless networks through traffic anonymity. *Computers & Security*, 48, 40-58.
- [14] Ghosh, S., & Thapa, R. S. (2020). Wireless network security: A look into the future. *IEEE Potentials*, 39(5), 31-36.
- [15] Xu, W., Wood, T., Trappe, W., & Zhang, Y. (2004, March). Channel surfing and spatial retreats: defenses against wireless denial of service. In *Proceedings of the 3rd ACM workshop on Wireless security* (pp. 80-89).
- [16] Shafiee, K., Atakhorrami, M., Subbalakshmi, K. P., & Senjian, J. G. (2018). Detection of rogue access point attack using statistical characteristics of network traffic. In *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1-6). IEEE.
- [17] Jover, R. P. (2015). The defcon wireless village. *IEEE Potentials*, 34(4), 24-31.
- [18] Babu, P. S., & Suresh, A. (2022). Detection and mitigation of wireless network tapping using machine learning techniques. *Journal of Ambient Intelligence and Humanized Computing*, 1-17.
- [19] Yıldırım, A., & Camtepe, S. A. (2022). Wireless network tapping with adversarial machine learning. *IEEE Transactions on Information Forensics and Security*, 17, 2363-2377.
- [20] Souppaya, M., & Scarfone, K. (2012). Guidelines for securing wireless local area networks (WLANs). *NIST Special Publication*, 800(153).