Jamming and Anti-Jamming Techniques on Wireless Networks (2024)

Qais Alqaissi

***Abstract*—Wireless Networks are an essential commodity in today's fast changing world and rapid development but with the rapid change and the way that communication works allows for attackers to be able to take advantage on the lack of relegation that needs time to be studied and passed and for the companies to adopt such strategies to be able to counter attacks that might happen and there is no other place lacking such research and development than Jamming Wireless networks, Thus the Objective of this Paper is to highlight such attacks and there effects on the IEEE 802.1X Wireless Networks and some techniques of counter such attacks.**

***Index Terms*— Jamming, Anti-Jamming, Wireless Networks, IEEE802.1X Networks.**

I. INTRODUCTION

Before diving into the Subject matter we must understand the basics, a **Wireless network** is a collection of networking standards that cover the physical and data link layer specifications for technologies such as Ethernet and Wireless, we also need to know what a Dos and Ddos are, **Dos(Denial Of Service)** is to stop a certain service for a period of time or indefinitely form being used by its intend purpose, While **Ddos(Distributed Denial Of Service)** is the use of Dos on a wider scale with more power to be able to cause damage to the target, What is **Jamming** in this case is the deliberate radiation or reflection of electromagnetic energy for the purpose of disrupting enemy use of electronic devices or systems, In today's world the use of Wireless networks cannot be downplayed since it is used in very critical communication channels such as military channels and any Disturbance would be considered an attack on such channels used for that purpose and these attacks can also come into play against companies when a Group of Rouge Employees in the United States of America used Jamming devices to disrupt GPS and cell communication in areas in the United States of America which highlights the immense danger that a greater attack might cause, like a great power using its power to disrupt another, which could hit not only military Channels but most certainly Civilian channels too.

II. Analyzing Attacks in context of Wireless networks

A. C.I.A Triad and passive, active attacks

In Communication Security we can apply the Cybersecurity triad (**C.I.A**), **Confidentiality**: The Maintenance of secrecy of a message, **Integrity**: Is keeping the message that is being sent unchanged, **Availability**: Keeping the link between the Host and the Receiver Connected or uninterrupted. Attacks are also classified into two categories which are Passive and Active attacks in which **Passive** attacks are attacks that only would Damage the Confidentiality of a message through either eavesdropping on a connection or by capturing traffic within a network and also other attacks that are of the same nature, an example of a Passive attack is the **Man In the Middle (MIM)** Attack in which an attacker would gain access to a network and instead of attacking the network and doing damage they would just lurk or wait for a conversation to start within the channel that they have access and collect any data that is being sent between the two nodes that could be IP address or even Passwords and the like, While **Active** attacks damage all three of the **C.I.A** Triad or Integrity or Availability, since an attack on Confidentiality would be considered most of the time a Passive attack, an example of an Active attack is Jamming in which an attacker would either pinpoint which channel they would like to disrupt or a broad attack in which it would target the whole area of the target, in which this would make it challenging for the defender to actual try to pinpoint the direction of the attack since everything is being actively jammed by the attacker While Passive attacker can be countered by using Cryptography techniques like RSA but for active attacker like Jammers are very hard to actually counter in a real world application since its increasing the noise levels within the channels of the target.

B. Types of Jamming Attacks

There are many types of Jamming attacks but they can be categorized into two section External attacks and Internal Attacks where **External Attacks** are attacks that come from outside of the targets scope or from outside the Wireless Network of the Target while **Internal Attacks** comes from a source within the Wireless network that is connected to the Target as in the jammer is within the Wireless network, These also must be know to understand how to Limit the Damage of Jamming on a Wireless network.

Thank you for all the colleagues who I used as references for this research paper

C. Classifications of Jamming Attacks

Jamming attacks can be classified into two which are Phy Jamming or RF Jamming and the second classification is MAC Layer or Virtual Jamming, In case of **Phy Jamming** it occurs in the Physical layer of a wireless network in which the jammer sends signals to over-saturate the channel in which the target is located in in which it would Lower the Quality of the SNR and increase the BER in a channel while **Mac Layer Jamming** occurs within the data link layer where it would saturate the targets RTS/CTS frames within the data frame an advantage for using Mac layer Jamming is that the Jamming Device would require less power that using a Phy Jamming Device since it is only sending Packets instead of Signals.

III. Types of Jammers

A. Proactive and Reactive Jammers

With understanding of Jamming attacks it is imperative that we also understand the devices that cause such disruption to Wireless networks and what there types are, Elementary and Advanced and each then create a there own Sub trees in which Elementary has within it Proactive and Reactive and Advanced has Function-Specific and Smart-Hybrid. **Proactive Jammers** are jammers that are able to only Jame one channel in a wireless Network and it also Doesn't differentiate between an empty or idle channel with no data and a channel with data in it and it will keep operating until power from the device is cut or powered off, While **Reactive Jammers** starts jamming only when the channel has data being transmitted within it and it only focuses on disrupting a message that is being sent in opposition of stopping the whole channel from functioning these are jammers within the Elementary Jammers Tree.

B. Function-Specific and Smart-Hybrid

Now onto the Advanced Jamming Devices house two more sub-trees which are Function-Specific and Smart-Hybrid, **Function-Specific** are jammers which have in mind a specific function in which they can be both Proactive and Reactive and jam one channel or multiple channels Depending on the Designer of the Jammer, and **Smart-Hybrid** Jammers are called smart in the sense that they automate most of its task and are energy efficient and can also magnify there jamming effect on networks and make large areas of it unusable both these types of Jammers can be either Reactive or Proactive.

C. Proactive Jammers types

Proactive jammers can also be divided into more sub-trees which are Constant, Deceptive and, Random Jammers each having there own functionality and purpose, **Constant Jammers** work by constantly sending signals without the CSMA protocol and its bits are also Random, While **Deceptive Jammers** Transmit regular packets instead of them being random, this can actually help the jammer to hide it self as a legitimate transmission occurring on the channel and thus it would force the real legitimate transmissions to stay in there receive state, and for **Random Jammers** they work by sending either random bits or regular bits and its goal is to conserve its energy and this jamming device also has Sleep state and Active state.

D. Reactive Jammers Types

Reactive Jammers have two types which are RTS/CTS Jammers and Data/Ack Jammers, **RTS/CTS Jammers** Work by sensing when the sender sends a RTS message the jammer will sense it and will start jamming thus stopping the Receiver from sending the CTS message, **While Data/Ack Jammers** Work by waiting for a transmission to start then it would corrupt the Transmission Data within the Channel its being transmitted in.

E. Function-Specific Jammer Types

These types of jammers can be classed into three types Follow-On Jammers, Channel Hopping Jammers and lastly Pulsed Noise Jammers. **Follow-On Jammers** These time of jammers can hop very frequently between channels, While **Channel Hopping Jammers** also hop between different channels but they also can Jam more than one channel at a time and Lastly **Pulsed Noise Jammers** This jammer is able to also jam different channels and hop between them but it can also change its Frequency at different periods of time these jammers are all a part of the Function-Specific Jammers.

F. File Formats for Graphics

Smart-Hybrid Jammers Has also three types Control Channel Jammer, Implicit Jammer and Flow Jammer, **Control Channel Jammer** This type of jammer is more advanced than its other counter parts in a sense since it works by Jamming the Control channel where all the channels used to coordinate the network, and **Implicit Jammers** work by Disabling the Functionality of the intend target thus causing a type of Dos on the target, and then we have **Flow Jammers** this works by using more than one jammer in an attack causing traffic to increase on the network, these are the types of Smart-Hybrid Jammers.

V. Real World Implementation of Jamming Attacks

In today's world there are many examples of real world Jamming attacks an example of such attacks are warring nation states jamming each other to limit the use of reconnaissance or drone warfare an example of such a battlefield is the large use of EW against drones in the Russo-Ukrainian war in which both sides use jammers to limit the use of drones against each others troops and an example of a nation using such attacks unhindered by jammers is the was between Israel and Hamas where the IDF has used there drones to attack civilian targets and since they have no access to jammers it has done massive damage against the civilian population, another example of EW attacks are attacks against Companies like the increasing amount of jammers used by rouge employees in the United States of America.

IV. Real World Implementation of Jamming Attacks

In today's world there are many examples of real world Jamming attacks an example of such attacks are warring nation

states jamming each other to limit the use of reconnaissance or drone warfare an example of such a battlefield is the large use of EW against drones in the Russo-Ukrainian war in which both sides use jammers to limit the use of drones against each others troops and an example of a nation using such attacks unhindered by jammers is the was between Israel and Hamas where the IDF has used there drones to attack civilian targets and since they have no access to jammers it has done massive damage against the civilian population, another example of EW attacks are attacks against Companies like the increasing amount of jammers used by rouge employees in the United States of America.

V. Implications of Jamming on Wireless Networks

Real World implications of a Jamming attack in 802.1X wireless networks can cause massive damage to the world wide web infrastructure since some jamming types of attacks can stay on for long periods of time and since most of the world now a days use wife and other mediums to communicate instead of wired communication it can stop most if not all mediums of modern communication, Jamming can also slow the channels of the 802.11 to a snails pace and since most of the devices used by the world never take into consideration an attack that might have jamming in mind since jamming does need a lot of technical knowledge and also hardware most of the time in which most of the threat actors in the world don't have but nation states do have those and thus we must strive to make our newer Wireless devices more immune to such attacks of jamming and to also train Cybersecurity professionals about such threats and how to counter or mitigate them since the world is lacking education about Jamming Devices and there effects on wireless networks.

VI. Anti-Jamming Techniques

Jammers have of-course there own defenses against since it is a damaging attack that might occur, thus we have more than one technique to defend against jamming, there are seven in total, Channel/Frequency hopping techniques, DSSS techniques, MIMO-based techniques, Coding techniques, MAC layer strategies, Learning based techniques, Firstly **Channel/Frequency hopping techniques** This technique works by channel hopping scheme for WiFi networks and also window dwelling and adaptive channel hopping, **DSSS techniques** This works by the 802.11b performance evaluation and then **MIMO-based techniques** works by mixing received signals projection onto the subspace orthogonal to the jamming signal and it can also work on MCR (Multi-Channel Ratio) decoding and **Coding techniques** LDPC and reed-Solomon code schemes analysis, **Mac-layer Strategies** this technique works using multiple mechanisms and **Detection mechanisms** uses Multi-factor learning-based algorithm, lastly **Learning-Based techniques** uses the Deep-WiFi: auto-encoding, feature extraction NN-based channel classification, RF fingerprinting.

VII. Detection of Jamming Techniques

Detection of the use of jamming is imperative since it would serve as a counter measure, since an attacker could try to jam a network for a brief moment to test the viability of such an attack on a wireless network thus we need to know what kind of techniques are there to detect Jamming, Since jamming causes a network to have a massive amount of interference thus causing a great amount of noise which renders it inoperable, We can try and detect a jammer when an attack is occurring by checking which device on the network has the most amount of transmission since a jammer needs to transmit a lot of packets or waves so that it will interfere on the network as a whole, Thus making the jammer a red target that can be easily Identified, In the survey on survival approaches in wireless network against jamming attack it is highlighted that there are five techniques to detected jamming, **Transmitter-Based Detection** is when the transmitter has to determine four metrics to detect jamming, **Receiver-Based Detection** works by checking the sequence number of each frame and determining if it is jamming or not, **Detected Detection** detects jamming by checking the Received Signal Strength Indication(RSSI) and the Physical Rate(Phy Rate) then it would make a decision and then informs the other nodes on the wireless network, **Cooperative Detection** This method Combines all three Techniques to try and reach an accurate conclusion, Lastly there is **Detection through RF Fingerprinting** uses RF fingerprinting enhances wireless security by using the unique transient signals emitted by radio transmitters during activation. These signals, influenced by manufacturing variations and aging, exhibit distinct patterns in frequency and amplitude, even among identical models. This unique behavior serves as an RF "fingerprint" to identify individual transmitters.

VIII. Conclusion

That is why it is very imperative that we understand expand our understanding of Jamming Attacks and also detection methods so that we are equipped with the tools and knowledge that is required to counter such attacks that might occur on wireless networks, and hopefully this paper is able to help in gathering all other sources so that we can reach the conclusion that Jamming attacks aren't reserved to nation states only or unique attacks but can also be used by low level threat actors.

REFERENCES

[1] "Jamming." *Vocabulary.com Dictionary,* Vocabulary.com, https://www.vocabulary.com/dictionary/jamming. Accessed 03 Dec. 2024.

[2] Mike Brunker, "GPS Under Attack as Crooks, Rogue Workers Wage Electronic War",NBC news

[3] RajaRatna, R.Ravi Ramaraj, "Survey on Jamming Wireless Networks: AttacksandPreventionStrategies" https://www.researchgate.net/publication/362044124_Survey_on_Jamming_Wireless_Networks_Attacks_and_Prevention_Strategies

[4] “Jamming and Anti-Jamming Techniques in Wireless Networks: A survey”https://scholarworks.montana.edu/server/api/core/bitstreams/b1d9de32-0aa5-4aa9-b6e1-9dde2aee188c/content

[5] Abderrahim Benslimane, Mohammed Bouhorma, Abdelouahid el yakoubi”Anaylysis of Jamming effects on IEEE 802.11 Wireless Networks”https://www.researchgate.net/publication/224249602_Analysis_of_Jamming_Effects_on_IEEE_80211_Wireless_Networks

[6] Hossein Pirayesh and Huacheng Zeng, Senior Member, IEEE. ”Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey”https://ieeexplore.ieee.org/ielaam/9739/9779264/9733393-aam.pdf

[7] Faraz Ahsan, Ali Zahir, Sajjad Mohsin, Khalid Hussain, “Survey on survival approaches in wireless networks against jamming attacks”https://www.researchgate.net/publication/228834097_Survey_on_survival_approaches_in_wireless_network_against_jamming_attack

[8] IEEE 802 Wireless Standards “Wireless Networks”

[9] IEEE “Dos and Ddos IEEE Distributed Denial Of Service: Attack techniques and mitigation “

BIOGRAPHY

QAIS MOHAMMAD ALQAISSI

I am a passionate **Cybersecurity specialist in training**, currently pursuing a Bachelor’s degree in **Cybersecurity** at **Amman Arab University** in Jordan. I am a third-year student, maintaining a **GPA of 3.8**, which reflects my dedication to academic excellence and my deep interest in mastering the field of Cybersecurity.

I have gained hands-on experience through my professional roles at **Amazon** (August 2023 – January 2024) and **C.S.C Beyond** (April 2023 – August 2023), where I worked in customer support and telemarketing. These roles enhanced my **problem-solving abilities**, **communication skills**, and **time management**, which are vital for addressing challenges in both customer-facing roles and technical domains.

To deepen my technical knowledge, I have earned several certifications, including being **Certified in Cybersecurity (ISC2)**. I have also completed specialized training in networking, cloud computing, SQL, data analysis, and Cybersecurity through programs from **Microsoft**, **Coursera**, and the **National Cybersecurity Center of Jordan**. Additionally, I regularly participate in **Capture the Flag (CTF)** competitions, which have helped sharpen my analytical thinking and practical problem-solving under time constraints.

My ultimate goal is to bridge the gap between **technical solutions** and **real-world security challenges**, contributing to a safer digital world. I am committed to continuous learning and innovation, striving to become a leader in the field of Cybersecurity.