RESEARCH PAPER ON "PREVENTION OF INTENTIONAL INTEREFERENCE ATTACK ON WIRELESS NETWORK"

Karan Sakunde

Student, Institute of industrial and computer Management and Research (IICMR), Savitribai Phule University

Karansakunde5@gmail.com

Jeevan Lembe

Student, Institute of industrial and computer Management and Research (IICMR), Savitribai Phule University

Jeevanlembe2001@gmail.com

Komal Neware

Student, Institute of industrial and computer Management and Research (IICMR), Savitribai Phule University

Komalneware@gmail.com

Abstract:

An intentional interference attack in a wireless network is when a third party intentionally creates interference to disrupt the normal functioning of the network. This can be done to deny eavesdropping capability. Interference can decrease coverage, capacity and limit the effectiveness of both new and existing systems. Interfering devices can act like a DoS attack that prevents an 80 radio from transmitting. Interference is difficult to avoid because wireless communication systems must coexist in complex signal environments consisting of multiple operating wireless networks. Interference has a direct correlation with the Quality of Service (QoS). The zone where a transmitting node can be interrupted by a third node during transmission is called the interference range. Interference ranges can intensely affect the throughput in wireless sensor networks due to collisions leading to outage

Keyword:

Firewall, Updating Firmware, Monitoring Network, Intrusion Detection System, Access Points

Introduction:

Wireless networks are becoming increasingly popular, as they offer a convenient and cost-effective way to connect devices. However, wireless networks are also vulnerable to a variety of attacks, including intentional interference attacks (IAAs). This can prevent legitimate users from accessing the network or make it difficult for them to do so. There are several different techniques that can be used to prevent IAAs. IAAs are attacks that disrupt the normal operation of a wireless network by flooding the network with noise or jamming signals. There are several different techniques that can be used to prevent IAAs. These techniques include: Spread spectrum techniques spread the signal over a wider frequency range, making it more difficult for an attacker to jam the signal. Frequency chopping techniques change the frequency of the signal at regular intervals, making it more difficult for an attacker to jam the frequency signal. Channel coding techniques add redundant information to the signal, which can help to correct errors that are introduced by noise or jamming Anti-jamming techniques: Anti-jamming techniques can be used to detect and mitigate jamming attacks.

Related Work:

Several studies have been conducted on the prevention of IAAs in wireless networks. These studies have proposed a variety of techniques for preventing IAAs, including the techniques listed above. The authors propose a frequency hopping technique for preventing IAAs in wireless networks. The proposed technique changes the frequency of the signal at regular intervals, making it more difficult for an attacker to jam the signal. The authors propose a spread spectrum technique for preventing IAAs in wireless networks. The proposed technique spreads the signal over a wider frequency range, making it more difficult for an attacker to jam the signal. The authors propose a channel coding technique for preventing IAAs in wireless networks. The proposed technique adds redundant information to the signal, which can help to correct errors that are introduced by noise or jamming. The authors propose an anti-jamming technique for preventing IAAs in wireless networks. The proposed technique detects and mitigates jamming attacks by using a combination of signal processing techniques and machine learning algorithms.

Prevention:

The techniques listed above can be used to prevent IAAs in wireless networks. However, it is important to note that no single technique is perfect. It is therefore important to use

combination of techniques to provide Intentional interference attacks (IAAs) are a serious threat to the security and reliability of wireless networks. Jamming is the intentional transmission of radio signals that interfere with the operation of legitimate wireless devices. Spoofing is the act of impersonating a legitimate wireless device to gain unauthorized access to the network. IAAs can be carried out by a variety of means, including jamming, spoofing, and denial-of-service (DoS) attacks. DoS attacks are designed to disrupt the normal operation of a wireless network by flooding it with traffic or by preventing legitimate users from accessing the network. In some cases, IAAs can even be used to completely disable a wireless network. The prevention of IAAs is a challenging problem. There is no single solution that can be used to protect against all types of IAAs. However, several techniques can be used to mitigate the impact of IAAs.

These techniques include:

Anti-jamming techniques: These techniques are designed to prevent or mitigate the effects of jamming attacks. Spread spectrum techniques spread the signal over a wider frequency range, which makes it more difficult for jammers to block the signal. One common anti-jamming technique is to use spread spectrum techniques.

DoS prevention techniques: These techniques are designed to prevent or mitigate the effects of DoS attacks. Traffic filtering allows legitimate traffic to pass through the network while blocking malicious traffic. One common DoS prevention technique is to use traffic filtering.

The most effective way to secure your wireless network from intruders is to encrypt, or scramble, communications over the network. Most wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router doesn't have an encryption feature, consider getting one that does. Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on.

Performance Evaluation:

The performance of these algorithms is verified and validated using metrics such as probability of detection, probability of false alarm, and accuracy. The paper discusses the use of deep learning techniques to detect jamming and interference attacks in wireless networks. The authors analyze the usefulness of many deep learning models in detecting jamming and interference signals. They investigate the types of signal features that could be used to diagnose jamming and interference signals, and create a large dataset using these parameters. Deep learning algorithms such as logistic regression and naïve bayes are tested using this dataset.

Conclusion:

In summary, the major security requirements for the wireless network which should be regarded as a guiding principle to come up with the solutions to the security issues in the Wireless Network are studied and analyzed. The security related features of heterogeneous wireless networks such as sensor networks, WMNs, ad hoc networks, cellular networks WLAN and are briefly discussed. Then we come up with a heterogeneous wireless network integration mode reference that clarifies and integrates the security points at the boundaries between heterogeneous network. Our network integration model provides workable framework for wireless security concerns for challenges in the realization of open wireless architecture. In addition to this, various security attacks that mainly threaten the Wireless Network are discusses

References:

1) “Mitigation of jamming attacks in wireless networks - ResearchGate.” [Online]: This article discusses the use of an Intrusion Detection System to mitigate and prevent jamming attacks, as well as the addition of cryptographic primitives to preserve the integrity of packets.

https://www.researchgate.net/publication/261019407_Mitigation_of_jamming_attacks_in_wireless_networks

2) “12 types of wireless network attacks and how to prevent them | TechTarget.” [Online]: This article provides an overview of common wireless network attacks and how to prevent them.

https://www.techtarget.com/searchsecurity/feature/A-list-of-wireless-network-attacks

3) “Mitigation of jamming attacks in wireless networks | IEEE Conference Publication | IEEE Xplore.” [Online]. This article proposes a mechanism for preventing jamming attacks on wireless networks using proactive and reactive protocols. The RSA algorithm is used for providing data packet integrity information during wireless transmission.

https://ieeexplore.ieee.org/document/6528486

4) “Most Common Wireless Network Attacks - WebTitan DNS Filter.” [Online].: This article discusses common wireless network attacks and suggests upgrading to more secure encryption standards such as WPA2 or WPA3 to improve security and prevent WLAN attacks.

https://www.webtitan.com/blog/most-common-wireless-network-attacks/

5) “Common Wireless Network Security Threats | Pluralsight.” [Online]. Available: This article discusses common wireless network security threats and suggests methods for preventing them.

https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats

6)Multimedia, Computer Vision and machine learning, volume 13, Number 1, january-june2022

Research Science press

New Delhi (India)