Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 9
September 2023

Defence Mechanism for Data Security and Fraud Detection in Wireless Network

[1]Ashutosh, [2]Dr. Harmeet Singh
[1]Research Scholar School of Engineering & Technology CT University, LUDHIANA (PUNJAB)
[2] (Deputy Director-IPR Cell) Department of Computer Application CT University, LUDHIANA (PUNJAB)

Abstract: The paper is a survey of defence mechanisms for data security and fraud detection in wireless networks. It covers various techniques used to protect wireless networks from security threats and to detect fraudulent activities. The paper also examines various fraud detection techniques that can be used to detect fraudulent activities in wireless networks. The survey includes a comparison of different defence mechanisms in terms of their effectiveness, efficiency, and applicability. The paper also identifies the limitations of the existing defence mechanisms and suggests future research directions for improving the security of wireless networks. Overall, the paper provides a comprehensive overview of defence mechanisms for data security and fraud detection in wireless networks, which can be useful for researchers, practitioners, and policymakers in the field of wireless network security.

Keywords: Data Security, Fraud Detection, Security Threats, Intrusion Detection Systems, IPS

I. Introduction

Wireless networks are widely used in various applications, including communication, entertainment, and information sharing. However, wireless networks are vulnerable to security threats, including data breaches, unauthorized access, and fraud. These security threats pose a significant risk to the confidentiality, integrity, and availability of data in wireless networks. Therefore, it is essential to implement defence mechanisms for data security and fraud detection in wireless networks. This essay will explore various defence mechanisms that can be used to secure data and detect fraud in wireless networks.

One of the most commonly used defence mechanisms for data security in wireless networks is encryption. Encryption is the process of converting plain text into ciphertext using an encryption algorithm and a secret key. The ciphertext is sent over the wireless network and decrypted at the receiving end using the secret key.

Access control can be implemented using authentication and authorization mechanisms. Authentication ensures that only authorized users can access the wireless network by requiring them to provide credentials such as usernames and passwords. Authorization ensures that authorized users can only access the resources they are authorized to access.

Firewalls are another defence mechanism for data security in wireless networks. Firewalls are devices or software that monitor and control the traffic entering and leaving the wireless network. Firewalls use predefined rules to filter out malicious traffic and allow only legitimate traffic to pass through. Firewalls can be implemented as hardware devices or software running on servers or clients.

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are other defence mechanisms for data security in wireless networks. IDS are systems that monitor the wireless network for signs of intrusion or attack and alert the system administrator when such signs are detected. IPS are systems that not only detect but also prevent intrusions and attacks by blocking or filtering out malicious traffic.

Fraud detection in wireless networks can be achieved using various defence mechanisms. One such mechanism is behavior analysis. Behavior analysis involves monitoring user behavior and detecting any anomalies or deviations from normal behavior. Behavior analysis can be achieved using machine learning algorithms that learn the normal behavior of users and detect any unusual behavior.

Wireless Network

Wireless networks have become increasingly popular due to their convenience and flexibility. They allow devices to communicate without the need for physical connections and enable mobility and portability.Wireless networks can be classified into several types, depending on the technology used and the coverage area. WLANs are the most popular type of wireless network and are used in homes, offices, and public places such as cafes and airports. WLANs are based on the IEEE 802.11 standard and use radio waves to transmit data between devices within a limited coverage area, typically up to 100 meters. WLANs can be either infrastructure-based, where a central wireless access point (AP) is used to connect devices, or ad-hoc, where devices communicate directly with each other without a central AP.WWANs are used to provide wireless connectivity over a larger coverage area, typically covering an entire city or even a country. WPANs are used for short-range wireless communication between devices within a few meters of each other, typically within a single room. WPANs are based on the Bluetooth standard and are commonly used for connecting peripherals such as keyboards, mice, and headphones to computers and mobile devices.

Defence Mechanism for Data Security

Defence mechanism for data security is a critical aspect of information technology. With the increasing amount of data that organizations and individuals generate, store, and share, there is a growing need to protect sensitive information from unauthorized access, theft, or misuse. Data security measures are essential to ensure confidentiality, integrity, and availability of data. In this article, we will discuss various defence mechanisms for data security.

- **Encryption:** Encryption is one of the most effective defence mechanisms for data security. It involves the conversion of plain text into a secret code, making it unreadable to anyone who does not have the key to decrypt it. Encryption helps to protect sensitive data such as personal information, financial data, and passwords. There are different types of encryption algorithms such as symmetric key encryption and asymmetric key encryption.
- **Firewall:** A firewall is a network security system that monitors and controls incoming and outgoing traffic based on predefined security rules. It acts as a barrier between the internal network and the internet, preventing unauthorized access and attacks. Firewalls are commonly used in both home and enterprise networks to protect against threats such as malware, viruses, and hackers.
- **Antivirus Software:** Antivirus software is a computer program that is designed to detect, prevent, and remove malware, viruses, and other malicious software from a computer system. Antivirus software is an essential defence mechanism for data security as it can identify and eliminate threats before they cause harm to the system.
- **Two-factor authentication:** The first authentication factor is usually a password, while the second factor could be a fingerprint scan, facial recognition, or a security token. Two-factor authentication helps to prevent unauthorized access to sensitive data.
- **Access Control:** Access control is a security technique that restricts access to data, applications, and systems based on user roles and permissions. Access control helps to ensure that only authorized users can access sensitive information, reducing the risk of data breaches and cyberattacks.
- **Data Masking:** Data masking is a technique that involves replacing sensitive data with fictional data to protect the original data from unauthorized access. For example, a credit card number could be replaced with a fake number that has the same format as a credit card number but does not reveal any sensitive information. Data masking helps to protect sensitive data from insider threats and unauthorized access.
- **Intrusion Detection System (IDS):** IDS helps to detect and prevent cyberattacks by identifying and alerting system administrators of potential security breaches.
- **Patch Management:** Patch management is a process of updating and fixing software

vulnerabilities to protect against cyberattacks. Software vulnerabilities can be exploited by hackers to gain unauthorized access to a system or steal sensitive data.

- **Security Information and Event Management (SIEM):** SIEM helps to detect and prevent security breaches by analyzing data from firewalls, intrusion detection systems, and other security systems.

Data Security in Wireless Network

Data security in wireless networks is critical since wireless transmissions can be intercepted by unauthorized parties, leading to potential data breaches, identity theft, and other cybercrimes. To ensure data security in wireless networks, several measures can be taken:

- **Use Encryption:** Encryption is the process of converting plain text into a coded form to make it unreadable to anyone who does not have the decryption key. Therefore, it is essential to use strong encryption protocols such as WPA2 (Wi-Fi Protected Access 2) or WPA3 to protect wireless networks' data.
- **Use Strong Passwords:** Strong passwords that are difficult to guess can help to prevent unauthorized access to the wireless network.
- **Disable Unnecessary Services:** It is crucial to disable any unnecessary services, such as remote administration or file sharing, to reduce the attack surface of the wireless network.
- **Implement Access Control:** Access control mechanisms, such as MAC filtering, can be used to restrict access to the wireless network. MAC filtering allows only specific devices to connect to the network by filtering out unauthorized devices' MAC addresses.
- **Use Virtual Private Networks (VPNs):** VPNs can provide secure communication over the internet, protecting sensitive data from eavesdropping and other cyber-attacks.
- **Conduct Regular Security Audits:** Regular security audits can help to identify any vulnerabilities or weaknesses in the wireless network's security and take appropriate measures to mitigate them.

Fraud Detection in Wireless Network

Fraud detection in wireless networks is an important area of research as wireless networks are increasingly being used for critical applications such as financial transactions, healthcare, and government services. Fraud in wireless networks can take many forms, including identity theft, data manipulation, and unauthorized access.

Here are some techniques that can be used for fraud detection in wireless networks:

- Anomaly detection: This technique involves detecting deviations from normal behavior patterns in the wireless network. For example, if an unauthorized user is accessing the network or a user is transmitting a large amount of data at an unusual time, it could be a sign of fraud.
- Signature-based detection: This technique involves using known patterns or signatures of fraudulent behavior to identify potential fraud. For example, if a specific type of attack has been previously observed in the network, its signature can be used to detect it in the future.
- Machine learning-based detection: This technique involves training a machine learning model on a dataset of known fraudulent and non-fraudulent behavior. The model can then be used to detect fraudulent behavior in the future.
- Protocol analysis: This technique involves analyzing the communication protocols used in the wireless network to identify any anomalies or deviations from expected behavior.
- Reputation-based detection: This technique involves tracking the reputation of users and devices in the wireless network. If a user or device has a history of fraudulent behavior, it can be flagged as a potential threat.

Additionally, it is important to continually monitor and update fraud detection techniques as new threats emerge.

II. Literature Review

Parwez et al. (2017), The authors begin by highlighting the challenges associated with processing and analyzing large amounts of data generated by mobile wireless networks, and how traditional methods are no longer sufficient for dealing with such vast amounts of data. They then propose a framework for big data analytics that is specifically designed for user-activity analysis and user-anomaly detection in mobile wireless networks.

Ahmed et al. (2016), The paper starts with an introduction to network anomaly detection, where the authors explain the need for detecting anomalies in network traffic and the challenges associated with it. They then proceed to describe different types of network anomalies, such as denial-of-service attacks, port scanning, and botnets, among others. The authors then review the various anomaly detection techniques, including statistical-based, machine learning-based, and rule-based approaches. For each approach, they describe the underlying principles, advantages, and limitations. They also provide a comparison of the different techniques, highlighting their strengths and weaknesses.

Hussain et al. (2018), The article provides a thorough review of related work in the field of anomaly detection in mobile wireless networks, highlighting the challenges of using traditional supervised learning approaches in this context. The authors then describe their semi-supervised learning approach, which combines a clustering algorithm and a support vector machine (SVM) to identify anomalies**.**

Thing (2017), The paper first introduces the background of the IEEE 802.11 network and wireless network attacks. Then, the authors explain the design of their proposed deep learning-based system for anomaly detection and attack classification. They use a stacked autoencoder (SAE) to learn the underlying patterns of normal network traffic and use the learned features to classify network traffic as either normal or anomalous. Furthermore, they use a deep neural network (DNN) to classify the anomalous traffic into different attack categories**.**

Fernández Maimó et al. (2019), The authors provide a comprehensive overview of the current state-of-the-art techniques used for anomaly detection in network systems and highlight the importance of developing effective and efficient anomaly detection mechanisms for 5G networks. The article presents a detailed analysis of the proposed deep learning model for anomaly detection and outlines its key components, including the pre-processing of network data, the feature extraction process, and the neural network architecture used for classification.

Sun et al. (2006), present a paper titled "Enhancing Security Using Mobility-Based Anomaly Detection in Cellular Mobile Networks," published in the IEEE Transactions on Vehicular Technology. The authors propose a new approach to detecting anomalous behavior in cellular mobile networks by analyzing mobility patterns.

Shiu (2011), Discussed several key physical layer security techniques, including secrecy capacity, artificial noise, and cooperative jamming. The authors provide a detailed explanation of each technique, including its underlying principles, advantages, and limitations. They also highlight some of the key challenges in implementing these techniques in practical wireless networks, such as the need for accurate channel state information and the impact of noise and interference.

Frunza&Scripcariu (2007), proposes modifications to the standard RSA encryption algorithm to enhance the security of wireless networks. The authors argue that the traditional RSA algorithm is susceptible to various attacks, such as the man-in-the-middle attack, and propose a solution to overcome these vulnerabilities. The authors propose two modifications to the RSA algorithm. The first modification involves the randomization of the encryption process, which enhances the security of the algorithm. The second modification involves the use of a secret key generated from a user's biometric data, which makes the encryption process more secure.

Sari &Karay (2015), The paper provides a detailed analysis of the two protocols and their respective strengths and weaknesses. The authors explain the vulnerabilities in WEP that make it susceptible to attacks such as passive attacks, active attacks, and attacks that exploit weaknesses in the key scheduling algorithm. The paper also discusses the improvements made in WPA to address the weaknesses of WEP. WPA utilizes a stronger encryption algorithm, Temporal Key Integrity Protocol (TKIP), and provides better security through the use of the Advanced Encryption Standard (AES) algorithm.

Nazir et al. (2021), The authors begin by defining wireless networks and their vulnerabilities, including the potential for attacks such as eavesdropping, man-in-the-middle attacks, and denial-of-service attacks. The authors then review a variety of security protocols, including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and the more recent WPA3. They also discuss the limitations of these protocols and highlight the need for new, more robust security measures. The article goes on to examine a range of wireless network security threats, including rogue access points, social engineering attacks, and attacks on Internet of Things (IoT) devices. The authors also provide an overview of various security tools and technologies that can be used to protect wireless networks, such as intrusion detection systems, firewalls, and virtual private networks (VPNs).

III. Methodology In Wireless Network

Methodology In Wireless Network

Wireless networks are a type of computer network that allows devices to communicate and exchange data using radio waves or other wireless communication technologies. Developing a methodology for designing, implementing, and maintaining wireless networks is essential to ensure their reliability, security, and performance. Here are some key steps to follow when developing a wireless network methodology:

1. Define the network requirements: Before designing a wireless network, it is essential to define the requirements, such as the number of devices to be connected, the range and coverage area, the required bandwidth, and the level of security needed.
2. Plan the network topology: Based on the requirements, plan the network topology, including the placement of access points, routers, and switches, and the wireless channel assignment.
3. Choose the wireless technology: Depending on the network requirements, choose the appropriate wireless technology, such as Wi-Fi, Bluetooth, or Zigbee.
4. Choose the equipment: Select the appropriate equipment, including access points, routers, switches, and wireless adapters, based on the network requirements.
5. Configure the network: Configure the network, including the network security, wireless encryption, and Quality of Service (QoS) settings.
6. Test the network: Test the network to ensure that it meets the requirements, including coverage, throughput, and security.
7. Monitor and maintain the network: Monitor the network performance and troubleshoot any issues that arise. Regularly update the network equipment and software to ensure optimal performance and security.

Mathematical model for a wireless network is the following equation:

$S = P - PL – PN$

where:

- S is the received signal strength at a given location
- P is the transmitted power by the wireless access point or device
- PL is the path loss due to the attenuation of the signal as it propagates through space
- PN is the noise power from other sources in the environment, such as interference from other wireless devices or background noise

This equation describes the fundamental trade-off in wireless communication between transmitted power and received signal strength. As the transmitted power increases, the received signal strength also increases, but so does the noise power and path loss. Therefore, the optimal design of a wireless network involves balancing these factors to achieve the desired coverage and performance while minimizing interference and power consumption.

Methodology in Defence Mechanism for Data Security

Defence mechanisms for data security in wireless networks are essential to protect against unauthorized access, data breaches, and other security threats. A methodology that can be used to implement these defence mechanisms includes the following steps:

1. Risk Assessment: The first step in implementing defence mechanisms for data security in wireless networks is to assess the risks involved. This includes identifying the types of threats that can occur and the potential impact on the network and its users.

2. Security Policies: Once the risks have been identified, security policies should be developed to mitigate these risks. This includes defining access control policies, encryption policies, and other security policies that are necessary to protect the network.

3. Network Design: The network should be designed with security in mind. This includes using secure protocols, such as WPA2 or WPA3, to encrypt wireless communications, and configuring firewalls and intrusion detection systems to protect against attacks.

4. Access Control: Access control mechanisms should be implemented to ensure that only authorized users can access the network. This includes using strong passwords, two-factor authentication, and other access control mechanisms to prevent unauthorized access.

5. Monitoring and Detection: The network should be monitored and audited regularly to detect any unauthorized access or security breaches. This includes using network monitoring tools to identify potential security threats and using intrusion detection systems to detect attacks.

6. Incident Response: Finally, an incident response plan should be developed to respond to security incidents promptly. This includes defining procedures for reporting security incidents, isolating affected systems, and conducting a forensic investigation to determine the cause of the incident and prevent it from happening again.

References

[1] Parwez, M. S., Rawat, D. B., &Garuba, M. (2017). Big data analytics for user-activity analysis and user-anomaly detection in mobile wireless network. *IEEE Transactions on Industrial Informatics*, *13*(4), 2058-2065.

[2] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, *60*, 19-31.

[3] Hussain, B., Du, Q., & Ren, P. (2018). Semi-supervised learning based big data-driven anomaly detection in mobile wireless networks. *China Communications*, *15*(4), 41-57.

[4] Thing, V. L. (2017, March). IEEE 802.11 network anomaly detection and attack classification: A deep learning approach. In *2017 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1-6). IEEE.

[5] Fernández Maimó, L., Huertas Celdrán, A., Gil Pérez, M., García Clemente, F. J., & Martínez Pérez, G. (2019). Dynamic management of a deep learning-based anomaly detection system for 5G networks. *Journal of Ambient Intelligence and Humanized Computing*, *10*, 3083-3097.

[6] Sun, B., Yu, F., Wu, K., Xiao, Y., & Leung, V. C. (2006). Enhancing security using mobility-based anomaly detection in cellular mobile

networks. *IEEE Transactions on Vehicular Technology*, *55*(4), 1385-1396.

[7] Shiu, Y. S., Chang, S. Y., Wu, H. C., Huang, S. C. H., & Chen, H. H. (2011). Physical layer security in wireless networks: A tutorial. *IEEE wireless Communications*, *18*(2), 66-74.

[8] Frunza, M., &Scripcariu, L. (2007, July). Improved RSA encryption algorithm for increased security of wireless networks. In *2007 International symposium on signals, circuits and systems* (Vol. 2, pp. 1-4). IEEE.

[9] Sari, A., &Karay, M. (2015). Comparative analysis of wireless security protocols: WEP vs WPA. *International Journal of Communications, Network and System Sciences*, *8*(12), 483.

[10] Nazir, R., Laghari, A. A., Kumar, K., David, S., & Ali, M. (2021). Survey on wireless network security. *Archives of Computational Methods in Engineering*, 1-20.