Volume 9, Issue 6, June – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN980

Intrusion Detection and Prevention Systems for Ad-Hoc Networks

Lakshin Pathak
Department of Computer Science and Engineering
Nirma University
Ahmedabad, India

Kiran Kher
Department of Computer Science and Engineering
Nirma University
Ahmedabad, India

Hetvi Kotak
Department of Computer Science and Engineering
Nirma University
Ahmedabad, India

Priyal Shah
Department of Computer Science and Engineering
Nirma University
Ahmedabad, India

Abstract:- Ad-hoc networks are vulnerable to various types of attacks due to their decentralized and dynamic nature. Intrusion detection and prevention systems (IDPSs) have been proposed to secure these networks by detecting and preventing attacks. This paper presents a comprehensive survey of IDPSs for ad-hoc networks. The survey covers the recent advancements in IDPSs for ad-hoc networks, including the detection techniques, prevention methods, and deployment strategies. The paper also discusses the challenges and open issues in developing effective IDPSs for ad-hoc networks. The survey concludes with a discussion on the future research directions for IDPSs in ad-hoc networks. The survey provides a valuable reference for researchers and practitioners working on securing ad-hoc networks.

I. INTRODUCTION

Imagine a world without networks - no internet, no social media, no online shopping. It's hard to fathom, right? Networks have become the beating heart of our digital lives, connecting us to people, information, and entertainment from all around the globe. From the humble home network to the vast and complex systems that power our most essential services, networks are everywhere. A network is a group of interconnected devices that are able to communicate and exchange information with each other. From simple home networks that allow us to access the internet from different devices to large-scale corporate networks that connect entire organizations, networks have become an integral part of our daily lives. The development of networks has revolutionized the way we communicate and share information. They have enabled us to connect with people all around the world, share data instantly, and collaborate in real-time, regardless of our physical location. With the advent of the Internet, networks have become even more pervasive, connecting people and devices on a global scale. As with any technology, networks come with their own set of challenges, particularly when it comes to security. The rise of cybercrime means that protecting networks is more critical than ever before. And the growth of networks has also given rise to new security threats, as cybercriminals seek to exploit vulnerabilities and gain unauthorized access to sensitive data. This has made network security an essential concern for individuals and organizations alike.

In today's digital age, the threat of cyber attacks looms large, and organizations must remain vigilant in protecting their networks from malicious intruders. That's where Intrusion Detection and Prevention Systems (IDPS) come in.

These powerful security tools act as the watchful guardians of computer networks, tirelessly scanning for suspicious activity and preventing cyber attacks in their tracks. From traditional signature-based detection to cutting-edge machine learning algorithms, IDPS have evolved to stay one step ahead of even the most sophisticated attackers. In this paper, we will explore the world of IDPS and uncover the secrets behind their success in the ongoing battle against cybercrime. So, buckle up and get ready to discover how IDPS are changing the game in network security.

II. THE NETWORK IN NEED: AD-HOC NETWORKS

When it comes to networks, we often think of the stable and structured systems that connect our devices to the internet. But, what happens when you need to communicate with other devices in a more dynamic and unpredictable environment, where traditional networks may not be feasible? That's where ad-hoc networks come in. Ad-hoc networks are a type of decentralized network that can be formed on-the-fly, without the need for a pre-existing infrastructure. They allow devices to connect and communicate with each other, even in remote or hostile environments, making them a critical technology in

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN980

disaster relief efforts, military operations, and emergency response situations. Ad-hoc networks can take many forms, from simple peer-to-peer networks between two devices, to more complex networks involving multiple devices and nodes. They are particularly useful in environments where traditional networks may not be feasible, such as disaster zones, remote locations, or military operations. Ad-hoc networks use a variety of communication technologies, such as Wi-Fi, Bluetooth, or cellular networks, to establish connections between devices. They rely on complex routing algorithms to ensure that data is transmitted efficiently and reliably, and may also use encryption and other security measures to protect communication from eavesdropping and other security threats. While ad-hoc networks have many advantages, such as flexibility and ease of deployment, they also come with their own set of challenges. Maintaining communication in a constantly changing environment can be difficult, and ensuring the security and reliability of communication is a constant concern. However, with the development of new technologies and techniques, ad-hoc networks continue to evolve and play a critical role in connecting devices and people in dynamic and unpredictable environments.

A. General Architecture of Ad-Hoc Networks

Ad hoc networks are decentralised networks that emerge spontaneously, with no infrastructure or pre-existing network architecture. These networks, also known as mobile ad hoc networks (MANETs), are established when mobile devices such as smartphones, laptops, or tablets connect with one another over wireless links. Ad hoc network design is built on distributed computing concepts, with no central controller or defined topology. Instead, each node in the network serves as both a host and a router, with the nodes jointly making routing decisions. The network's nodes are self-organizing, which means they may discover and connect to other nodes without requiring centralised management or configuration. Each node has a routing table with information about the nodes in its immediate neighbourhood, and it utilises this information to forward packets to their destinations.

Ad hoc networks can be classified into two types based on their architecture:

➢ *Infrastructure-Based Ad Hoc Networks*

In this type of network, there is a central node or a set of nodes that act as a coordinator or a controller. The coordinator node is responsible for managing the network topology, maintaining the routing tables, and ensuring the reliability of the network. The other nodes in the network communicate with the coordinator node to exchange information and to participate in the network operations.

➢ *Infrastructure Less Ad Hoc Networks*

In this type of network, there is no central coordinator or controller. Each node in the network is equal and has the same capabilities as the other nodes. The nodes communicate with each other directly, and the routing decisions are made collectively by the nodes themselves.

Ad hoc networks are used in a variety of applications, including military, disaster response, healthcare, and transportation. They offer a flexible and resilient communication infrastructure that can be quickly deployed in situations where the traditional infrastructure is unavailable or unreliable.

B. Advantages of Ad-Hoc Networks

Ad-hoc networks offer several advantages over traditional networks that make them an attractive option for a variety of applications. One of the most significant advantages of ad-hoc networks is their flexibility. As they can be set up quickly and easily in a variety of environments without the need for pre-existing infrastructure, they are highly adaptable and can be used in situations where traditional networks are not feasible. Additionally, ad-hoc networks are highly mobile,

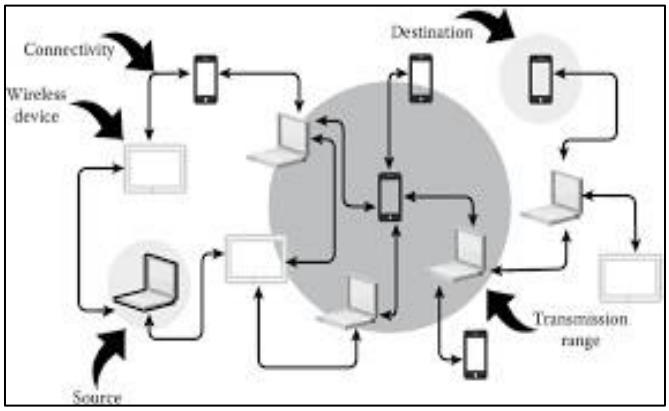

Fig 1: Architecture of Ad-Hoc Network

Allowing devices to communicate with each other regardless of their location or proximity to a central server or router. This mobility also makes ad-hoc networks more resilient than traditional networks, as they can adapt to changes in the environment and continue to function even if some devices fail. Ad-hoc networks are also cost-effective, as they do not require expensive infrastructure or ongoing maintenance. Finally, ad-hoc networks can offer a higher degree of privacy and security than traditional networks, as data is transmitted directly between devices without the need for a central server or router. Overall, these advantages make ad-hoc networks an attractive option for a wide range of applications, from military operations to disaster relief efforts and beyond.

- Flexibility: Ad-hoc networks are highly flexible, as they can be set up quickly and easily in a variety of environments, without the need for pre-existing infrastructure.
- Mobility: Ad-hoc networks allow devices to move freely and communicate with each other, regardless of their location or proximity to a central server or router.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN980

- Cost-effectiveness: Ad-hoc networks are often more cost-effective than traditional networks, as they don't require expensive infrastructure or ongoing maintenance.
- Resilience: Ad-hoc networks are designed to be resilient, as they can adapt to changes in the environment and continue to function even if some devices fail.
- Privacy: Ad-hoc networks can offer a higher degree of privacy and security than traditional networks, as data is transmitted directly between devices without the need for a central server or router.
- Accessibility: Ad-hoc networks can provide connectivity in areas where traditional networks are unavailable or unreliable, such as disaster zones or remote locations.
- Ease of use: Ad-hoc networks are often easier to use than traditional networks, as they don't require complex configurations or technical expertise.

C. Disadvantages of Ad-Hoc Networks

Ad-hoc networks offer several advantages, but they also come with some disadvantages, including:

- Security: Because ad-hoc networks are often formed without a centralized authority, they can be vulnerable to security threats such as eavesdropping, data interception, and denial-of-service attacks. This means that ad-hoc networks require robust security protocols to ensure the safety and privacy of communication.
- Complexity: Ad-hoc networks can be more complex than traditional networks, as they require advanced routing algorithms to ensure efficient communication between devices. This complexity can make ad-hoc networks more challenging to set up and maintain.
- Bandwidth Limitations: As ad-hoc networks rely on wireless communication technologies such as Wi-Fi or Bluetooth, they are subject to bandwidth limitations. This can result in slower data transfer rates, and reduced network capacity.
- Interference: Ad-hoc networks can be susceptible to interference from other wireless devices, such as microwave ovens or cordless phones, which can disrupt communication and reduce network performance.
- Power Consumption: Ad-hoc networks can consume more power than traditional networks, as devices need to maintain continuous wireless communication to remain connected. This can be a concern in battery-operated devices, such as smartphones or tablets.
- Limited Range: Ad-hoc networks typically have a limited range compared to traditional networks. This means that devices need to be in close proximity to each other for communication to take place. The range can be extended through the use of relaying, but this can add complexity and decrease performance.
- Lack of Quality of Service (QoS): Ad-hoc networks may lack QoS, which is the ability to prioritize certain types of traffic over others. This can result in lower performance for applications that require high bandwidth or low latency, such as video streaming or online gaming.
- Scalability: Ad-hoc networks may be limited in scalability, meaning that they may not be able to accommodate a large number of devices. As the number of devices in the network increases, the complexity of the routing algorithm and the likelihood of interference and contention also increase.
- Maintenance: Ad-hoc networks may require more maintenance than traditional networks, as devices need to be configured to join the network and to maintain connectivity. In addition, devices in the network may need to be replaced or repaired more frequently due to their mobile nature and exposure to environmental factors.

III. LITERATURE REVIEW

The paper by Hande Alemdar and Cem Ersoy titled "Wireless sensor networks for healthcare [1]: A survey" provides a comprehensive review of the use of wireless sensor networks (WSNs) in healthcare applications. The authors survey the existing literature on WSNs and healthcare, discussing the key applications of WSNs in healthcare, including patient monitoring, remote diagnosis, and emergency response. They also examine the various technologies and protocols used in WSNs and the challenges associated with their deployment and implementation in healthcare settings. One of the key contributions of the article is the identification of the different types of healthcare applications that can benefit from the use of WSNs. These include monitoring of physiological parameters, such as heart rate, blood pressure, and body temperature, as well as monitoring of environmental factors, such as temperature, humidity, and air quality. The authors also discuss the use of WSNs for tracking and monitoring patients with chronic conditions, such as diabetes and asthma. The article also highlights the importance of data quality and security in healthcare applications of WSNs. The authors discuss the need for reliable and accurate data collection and transmission, as well as the need for secure storage and transmission of sensitive patient data. They also examine the various security and privacy issues associated with the use of WSNs in healthcare settings, such as unauthorized access, data tampering, and privacy violations. Overall, the article provides a valuable survey of the use of WSNs in healthcare applications. It highlights the potential benefits of WSNs for improving patient care and reducing healthcare costs, as well as the challenges associated with their deployment and implementation in healthcare settings. The article is a useful resource for researchers, healthcare practitioners, and policymakers who are interested in the application of WSNs in healthcare.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN980

The article "Hybrid Cryptographic Scheme for Secure Communication in Mobile Ad Hoc Network-Based E-Healthcare System" by Sirajuddin et al. explores the use of mobile ad hoc networks (MANETs) in healthcare systems and proposes a hybrid cryptographic algorithm for secure medical information exchange among mobile healthcare nodes. The authors highlight the significance of MANETs in healthcare systems, especially during pandemic situations like COVID-19, and discuss the challenges associated with ensuring secure communication in such systems. The authors propose a hybrid cryptographic scheme that uses the logistic map for key generation. The proposed scheme is compared with existing cryptographic schemes, and simulation results show that the proposed hybrid cryptographic scheme exhibits better security against various attacks in MANET-based healthcare systems. The article contributes to the literature by highlighting the importance of secure communication in MANET-based healthcare systems and proposing a hybrid cryptographic scheme for the same. The proposed scheme could be useful for healthcare practitioners and policymakers who are interested in developing secure and efficient MANET-based healthcare systems. However, the article does not provide a detailed discussion of the limitations and potential drawbacks of the proposed scheme, which could be a topic for future research. [2]

The research article "CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care" [3]. discusses the development and implementation of a wireless sensor network infrastructure, called CodeBlue, for emergency medical care. The authors highlight the importance of real-time monitoring of patients in emergency situations and discuss the challenges associated with achieving this goal using existing medical technologies. CodeBlue is designed to provide real-time monitoring of patients using wireless sensors that can transmit data to a central server. The authors describe the architecture of CodeBlue, including the hardware and software components, and discuss the challenges associated with developing a reliable and efficient wireless sensor network infrastructure. The authors also present the results of a pilot study that was conducted to evaluate the effectiveness of CodeBlue in a real-world emergency medical setting. The pilot study involved the deployment of CodeBlue in an emergency department and the evaluation of its performance in a simulated emergency scenario. The authors report that CodeBlue performed well in the pilot study and demonstrated the potential to improve the quality of care in emergency medical situations.

The paper "A Cost-Effective Solution for Telemedicine in Rural Health Care Using Mobile Ad Hoc Networks" by Srivastava and Sahu [4] discusses the use of mobile ad hoc networks (MANETs) as a means of providing cost-effective telemedicine services in rural areas. The authors highlight the challenges associated with providing healthcare services in rural areas, including the lack of healthcare infrastructure and limited resources. The article presents a solution that uses MANETs to enable real-time communication between healthcare providers and patients in rural areas. The authors describe the design and implementation of the MANET-based telemedicine system, which includes mobile devices equipped with sensors and cameras, as well as a central server for data processing and storage. The authors report on the results of a pilot study that was conducted to evaluate the effectiveness of the MANET-based telemedicine system in a rural healthcare setting. The study involved the deployment of the system in a remote village in India and the evaluation of its performance in providing telemedicine services to patients in the village. The authors report that the system performed well in the pilot study and demonstrated the potential to improve access to healthcare services in rural areas. The article contributes to the literature by presenting a novel approach to providing telemedicine services in rural areas using MANETs. The authors provide a detailed description of the design and implementation of the system, as well as the results of a pilot study that demonstrates its effectiveness in a real-world setting. The authors of paper titled "A framework for enabling patient monitoring via mobile ad hoc network" [5] proposes a framework to enable patient monitoring through the use of mobile ad hoc networks (MANETs). The authors address the need for continuous monitoring of patients with chronic diseases, elderly patients, and those in critical condition, who may require constant monitoring while being mobile. The proposed framework utilizes the concept of MANETs to provide a low-cost solution for patient monitoring, where nodes in the network are mobile and can communicate with each other wirelessly without requiring any infrastructure. The authors describe the architecture of the framework and highlight the importance of data security in such a system. They propose a three-layer security model that includes authentication, confidentiality, and integrity to ensure the security of patient data transmitted over the network. The paper also discusses the implementation of the framework and presents simulation results that demonstrate the effectiveness of the proposed framework in enabling patient monitoring through a MANET-based system. Overall, the paper provides valuable insights into the use of MANETs for patient monitoring and highlights the potential of such systems in addressing the challenges of providing continuous healthcare services in remote or low-resource settings.

The paper "Bignurse: A wireless ad hoc network for patient monitoring" by Roland Bader et al. proposes a patient monitoring system using wireless ad hoc networks. The authors highlight the importance of patient monitoring in healthcare, especially in critical care environments. They argue that the traditional wired patient monitoring systems are cumbersome, expensive, and limit patient mobility. The authors propose Bignurse, a wireless ad hoc network consisting of small wireless sensors attached to patients, which transmit real-time data to a central monitoring station. The Bignurse system is designed to be low-cost, scalable, and easy

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN980

to deploy. The authors describe the architecture of the Bignurse system and the sensor nodes used in the network. They also discuss the network protocols and algorithms used for data transmission and routing. The authors evaluate the performance of the Bignurse system through simulations and experiments. They conclude that the Bignurse system is a promising solution for patient monitoring, offering low-cost, high mobility, and scalability. However, the authors also acknowledge that the Bignurse system still faces some challenges, such as energy consumption and security, which need to be addressed in future research. Overall, the Bignurse system proposed in this paper presents a promising solution for wireless patient monitoring in healthcare. [6]

The article by Insom et al. [7] presents the implementation of a human vital monitoring system using ad hoc wireless networks for smart healthcare. The authors designed a wearable sensor device to measure vital signs such as heart rate, blood pressure, and body temperature, and used a ZigBee ad hoc wireless network to transmit the data to a base station. The base station then transmitted the data to a central server for storage and analysis. The authors also developed a web-based user interface for patients and medical staff to access the data remotely. The system was tested in a hospital environment, and the results showed that the system was able to accurately monitor and transmit vital signs in real-time. The authors concluded that the system has great potential in improving the quality of healthcare and reducing medical costs by enabling remote patient monitoring and reducing the need for hospital visits. However, the authors noted that the system's reliability and security need to be improved to ensure its widespread adoption in the healthcare industry. Overall, the article provides valuable insights into the design and implementation of ad hoc wireless networks for healthcare applications, highlighting the potential of such networks in improving healthcare delivery.

In the paper [8] "Implementing role based access in healthcare ad hoc networks", the author addresses the security challenges in healthcare ad hoc networks (HANETs) and proposes a role-based access control (RBAC) mechanism to enhance the security of patient data. The author highlights the importance of secure data transmission and access control in HANETs due to their highly sensitive and confidential nature. The proposed RBAC mechanism is designed to ensure that only authorized personnel have access to patient data based on their roles in the healthcare system. The article provides an overview of the RBAC model and its implementation in HANETs. The RBAC mechanism is shown to be effective in improving the security of patient data by limiting access to authorized users, reducing the risk of data breaches, and improving overall system efficiency. The article concludes that RBAC should be considered as an important security measure in HANETs to protect patient privacy and ensure secure communication among healthcare providers. Overall, the article provides valuable insights into the security challenges faced by HANETs and offers a practical solution to enhance their security through RBAC.

The paper [9] provides an overview of intrusion detection mechanisms in ad-hoc networks and ambient intelligence frameworks. The paper highlights the need for effective intrusion detection mechanisms to protect such systems against various attacks. The author proposes a new approach based on the clustering technique to detect intrusions in ad-hoc networks. The clustering technique reduces the communication overhead and enhances the detection rate. The paper also discusses the use of various machine learning algorithms for intrusion detection in ambient intelligence systems. The author emphasizes the importance of considering the dynamic nature of ambient intelligence systems while designing intrusion detection mechanisms. The paper provides a comprehensive overview of the current state-of-the-art in intrusion detection mechanisms in ad-hoc networks and ambient intelligence frameworks. Overall, the paper highlights the challenges and opportunities in developing effective intrusion detection mechanisms in such systems.

The paper "Patient Monitoring Using Ad Hoc Wireless Networks: Reliability and Power Management" [10] discusses the use of ad hoc wireless networks for patient monitoring and focuses on issues of reliability and power management. The authors suggest that ad hoc wireless networks are particularly suited for patient monitoring because they can be quickly deployed in emergency situations, are cost-effective, and provide reliable communication. The paper presents a framework for patient monitoring using ad hoc wireless networks, which involves sensors attached to the patient's body, a mobile ad hoc network, and a remote monitoring station. The authors also discuss the challenges in achieving reliability in ad hoc networks, such as node failures, packet losses, and network congestion. To address these challenges, they propose a number of techniques, including redundancy, multipath routing, and error control coding. The authors also discuss power management issues in ad hoc wireless networks, which are particularly relevant for patient monitoring applications, where the sensors are typically battery-powered. They propose a power management scheme that involves dynamically adjusting the transmission power of the sensors based on the network conditions, such as the distance between nodes and the level of interference. The authors conclude that ad hoc wireless networks can provide reliable and cost-effective patient monitoring solutions, provided that appropriate reliability and power management techniques are used.

In their paper titled "Reliable multimedia transmission in wireless ad-hoc networks for telehealth systems", [11] Hohmann, Debbah, and Kropfl proposed a novel approach for ensuring reliable multimedia transmission over wireless ad-

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN980

hoc networks for telehealth systems. The authors highlighted the importance of telehealth systems in providing medical services remotely and the potential of wireless ad-hoc networks in enabling such systems. The paper presented a cross-layer approach that incorporates a prioritization scheme at the application layer, an adaptive modulation and coding scheme at the physical layer, and a dynamic route selection scheme at the network layer. The proposed approach aims to ensure reliable and efficient transmission of multimedia data in wireless ad-hoc networks, which is critical for telehealth systems. The authors evaluated the performance of the proposed approach through simulations and compared it with traditional approaches. The results showed that the proposed approach significantly outperforms traditional approaches in terms of packet loss rate, delay, and throughput. Overall, the paper presented a valuable contribution to the field of telehealth systems by proposing a reliable and efficient approach for multimedia transmission over wireless ad-hoc networks. The proposed approach has the potential to improve the quality of medical services delivered remotely and overcome the challenges posed by unreliable wireless ad-hoc networks.

The paper by Olufemi Fasunlade, Shikun Zhou, and David Sanders titled "Security Threats and Possible Countermeasure in Digital Healthcare"[12] provides an overview of the security threats faced by the digital healthcare industry and suggests possible countermeasures to mitigate these risks. The paper highlights the vulnerabilities of digital healthcare systems, which include data breaches, identity theft, malware attacks, and denial of service attacks. The authors also discuss the potential impact of these threats on the healthcare industry, such as compromised patient data, legal and financial liabilities, and damage to reputation. To address these security concerns, the paper proposes several countermeasures, including the use of encryption, authentication, access controls, intrusion detection and prevention systems, and security awareness training for healthcare professionals. The authors also emphasize the importance of regulatory compliance and adherence to industry standards for data security and privacy. Overall, the paper provides a comprehensive overview of the security challenges faced by the digital healthcare industry and offers practical recommendations for healthcare organizations to protect patient data and maintain the trust of their stakeholders.

The paper [13] proposes the use of XML-based role-based access control in healthcare ad hoc networks. The authors discuss the importance of secure information exchange in healthcare networks and how RBAC can provide a flexible and scalable approach to access control. The paper provides an overview of the RBAC model and how it can be implemented using XML. The authors also discuss the benefits and limitations of using XML for RBAC in ad hoc networks. The paper presents a case study of the proposed RBAC implementation in a healthcare ad hoc network. The authors demonstrate the effectiveness of the RBAC model in controlling access to patient data and the flexibility of the XML-based implementation. The study also shows the performance impact of using XML for RBAC in ad hoc networks. Overall, the paper provides a useful contribution to the field of secure healthcare networks and highlights the potential of RBAC and XML in providing flexible and scalable access control. However, the study is limited by its focus on a single case study and its evaluation of performance impact using a small network. Further research is needed to validate the effectiveness of the proposed approach in larger and more complex healthcare networks.

The paper [14] "An architecture for resilient intrusion detection in ad-hoc networks" proposes an architecture for intrusion detection in ad-hoc networks that aims to improve their resilience against attacks. The architecture is based on a hybrid intrusion detection system that combines signature-based and anomaly-based detection techniques, and it is designed to be adaptive and dynamic in order to address the challenges of ad-hoc networks such as limited resources, high mobility, and frequent topology changes. The authors also propose a clustering algorithm that enables the efficient distribution of the intrusion detection tasks among the nodes in the network. The proposed architecture is evaluated using a simulation approach, and the results show that it is effective in detecting various types of attacks with a low false positive rate and a reasonable overhead. The authors conclude that their architecture can enhance the security of ad-hoc networks, especially in healthcare systems where the confidentiality and integrity of medical data are critical.

IV. APPLICABLE MACHINE LEARNING ALGORITHMS FOR IDS IN AD-HOC NETWORKS

Machine learning algorithms are often used in intrusion detection systems (IDS) to identify abnormal network behavior and potential intrusions. Machine learning algorithms can analyze large amounts of data and identify patterns and anomalies that may indicate an attack. Machine learning algorithms are used in various stages of an IDS, including pre-processing of data, feature selection, training of models, and detection of anomalies. However, there are challenges in using machine learning in IDS, such as the need for large amounts of data for training, the need for feature engineering, and the risk of false positives and false negatives.

A. Autoencoders

Auto-encoders are the neural networks that aims to copy their input to output. It works by compressing the input into latent representation (x) and from there it reconstructs the output. The output is generated from the latent representation by learning salient features. The auto-encoder consists of encoder followed by latent representation and the decoder.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN980

Encoder - This area of the network compresses the input into a representation of latent space. h=f(x) can be used to represent it.

Decoder - With the representation of latent space, this section seeks to recreate the input. The decoding algorithm is r=g(h)

By considering both encoder and decoder the whole function is z=g(f(x)) where we want z to be as close as the original x

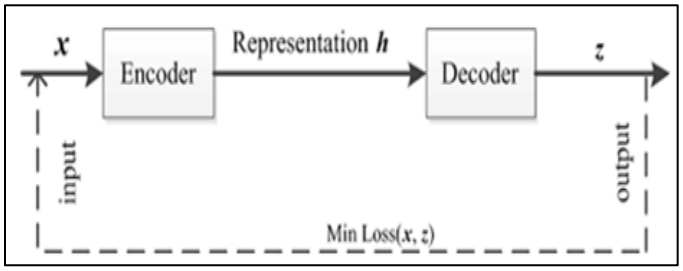

Fig 2: Autoencoder Architecture

B. Types of Autoencoders

Basically there are 4 types of autoencoders

- Vanilla Autoencoders: It is the simplest form of autoencoder having 3 layers including one input layer, one hidden layer and one output layer. We can have the total command over the architecture and make it powerful by increasing the number of layers. It is advised to keep a sandwich architecture by which the model can perform well.
- Multi-layer Autoencoders: Essentially, a multi layer autoencoder reconstructs the input with more hidden layers in its network. It has more than one hidden layer and follows the same sandwich architecture. The hidden layers learns the salient features and reconstructs the output by passing through the hidden layers.
- Convolutional Autoencoder: When the hidden layers in the autoencoder comprises of convolution network it is a convolutional autoencoder. The encoder and decoder both have convolution networks. Encoder is a down-sampling layer while decoder is an up-sampling layer. This type of autoencoder can be useful on image processing tasks.
- Regularized Autoencoder: There are additional techniques to limit an autoencoder's reconstruction besides imposing a hidden layer with smaller dimensions than the output. In addition to being able to copy its input to output, regularised autoencoders use a loss function that promotes the model to have other characteristics.

C. Applications of Autoencoders

- Data compression: Autoencoders can be used to compress large datasets by encoding them into a smaller representation that can be used for storage or transmission. The compressed representation can be later decoded back to the original data format.
- Anomaly detection: Autoencoders can be used to detect anomalies or outliers in data that don't fit the normal patterns. The autoencoder is trained on normal data and when presented with anomalous data, it will not be able to reconstruct it accurately, indicating an anomaly.
- Image and video processing: Autoencoders can be used for image and video processing tasks such as image denoising, image and video super-resolution, and video frame prediction.
- Feature learning: Autoencoders can be used to learn a low-dimensional representation of the input data that captures the most important features of the data. This can be useful for tasks such as image and speech recognition, where the high-dimensional input data can be reduced to a lower-dimensional feature space.
- Generative modeling: Autoencoders can be used as generative models that can generate new data that is similar to the training data. Variation autoencoders (VAEs) and generative adversarial networks (GANs) are two popular types of generative models that use autoencoders as their building blocks.

D. How Autoencoders are useful in IDS

Autoencoders are useful in intrusion detection systems (IDS) as they can learn the normal behavior of a system or network and detect any anomalies or deviations from this normal behavior. Autoencoders are a type of neural network that learns to encode input data into a low-dimensional representation and then decode it back to its original form. In the context of IDS, an autoencoder can be trained on normal network traffic to learn the patterns of normal behavior. Once trained, the autoencoder can be used to detect any anomalies in the network traffic by comparing the decoded output with the original input. One advantage of using autoencoders for IDS is that they can detect both known and unknown attacks. Known attacks are detected by comparing the network traffic to a database of known attack patterns, while unknown attacks are detected as anomalies in the network traffic. Autoencoders can also be combined with other machine learning techniques, such as clustering or classification, to improve the accuracy of intrusion detection. For example, autoencoders can be used to reduce the dimensionality of the data, and then a clustering algorithm can be applied to group the data points into normal and anomalous clusters.

V. CHALLENGES IN AD-HOC NETWORKS

Ad-hoc networks pose several challenges for intrusion detection, including:

- Dynamic Topology: Ad-hoc networks have a dynamic topology, where the network structure is continuously changing due to node mobility and failure. This makes it challenging to maintain accurate information about network connectivity and detect intrusions.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN980

- Limited Resources: Nodes in ad-hoc networks typically have limited resources such as processing power, memory, and battery life. This limitation makes it difficult to deploy resource-intensive intrusion detection techniques.
- Lack of Central Authority: Ad-hoc networks are often decentralized, with no central authority or trusted entity, which makes it difficult to manage and coordinate intrusion detection activities.
- Limited Bandwidth: Ad-hoc networks often operate on limited bandwidth, which can make it challenging to detect and respond to intrusions in real-time.
- Security Threats: Ad-hoc networks are vulnerable to various security threats such as eavesdropping, packet sniffing, and denial-of-service attacks, which can compromise the integrity and confidentiality of the network.
- Lack of Security Infrastructure: Ad-hoc networks often lack security infrastructure such as firewalls and intrusion detection systems, making them more susceptible to attacks.

Addressing these challenges requires the development of intrusion detection techniques that are lightweight, efficient, and specifically designed for ad-hoc networks.

VI. CONCLUSION

In conclusion, intrusion detection systems (IDS) can play a vital role in securing ad-hoc networks, especially for healthcare applications. IDS can detect and respond to potential security breaches, unauthorized access, and abnormal activities in real-time. The unique challenges of ad-hoc networks for IDS include limited resources, high mobility, and a dynamic network topology. However, with the advancements in machine learning algorithms and techniques, such as deep learning and autoencoders, IDS can be optimized for ad-hoc networks. By developing efficient and reliable IDS, we can ensure the privacy and security of healthcare data transmitted over ad-hoc networks, making them a feasible and viable option for remote patient monitoring and telemedicine. Additionally, there are challenges related to the unique characteristics of ad-hoc networks, such as limited resources, high mobility, and dynamic topology. These challenges make it difficult to apply traditional IDS techniques to ad-hoc networks. Despite these challenges, researchers have proposed various approaches to IDS for ad-hoc networks, including machine learning algorithms and autoencoders. These approaches have shown promising results in detecting and mitigating security threats in ad-hoc networks. Overall, IDS can be a valuable tool for enhancing the security of ad-hoc networks, but it requires further research and development to address the challenges specific to these networks.

REFERENCES

[1]. Hande Alemdar and Cem Ersoy. Wireless sensor networks for healthcare: A survey. Computer Networks, 54(15):2688–2710, 2010.
[2]. Mohammad Sirajuddin, Ch. Rupa, Surbhi Bhatia, R. N. Thakur, Arwa Mashat, and Kuruva Lakshmanna. Hybrid cryptographic scheme for secure communication in mobile ad hoc network-based e-healthcare system. Wirel. Commun. Mob. Comput., 2022, jan 2022.
[3]. David J Malan, Thaddeus Fulford-Jones, Matt Welsh, and Steve Moulton. Codeblue: An ad hoc sensor network infrastructure for emergency medical care. 2004.
[4]. P.K. Srivastava and S. Sahu. A cost-effective solution for telemedicine in rural health care using mobile ad hoc networks. pages 109–113, 2004.
[5]. Sweta Sneha and Upkar Varshney. A framework for enabling patient monitoring via mobile ad hoc network. Decision Support Systems, 55(1):218–234, 2013.
[6]. Roland Bader, Michele Pinto, Felix Spenrath, Philipp Wollmann, and Frank Kargl. Bignurse: A wireless ad hoc network for patient monitoring. pages 1–4, 2006.
[7]. Poramin Insom, Pakorn Wongpanitlert, Jakree Tipsupa, Kritsakorn Rakjang, Kamol Kaemarungsi, and Pakorn Watanachaturaporn. Implementation of a human vital monitoring system using ad hoc wireless network for smart healthcare. pages 76–81, 2012.
[8]. Qurban A Memon. Implementing role based access in healthcare ad hoc networks. J. Networks, 4(3):192–199, 2009.
[9]. Rituparna Chaki. Intrusion detection: Ad-hoc networks to ambient intelligence framework. pages 7–12, 2010.
[10]. U. Varshney and S. Sneha. Patient monitoring using ad hoc wireless networks: reliability and power management. IEEE Communications Magazine, 44(4):49–55, 2006.
[11]. Bernhard Hohmann, Merouane Debbah, and Andreas Kropfl. Reliable multimedia transmission in wireless ad-hoc networks for telehealth systems. pages 301–304, 2008.
[12]. Olufemi Fasunlade, Shikun Zhou, and David Sanders. Security threats and possible countermeasure in digital healthcare. pages 1297–1302, 2021.
[13]. Qurban A. Memon and Shakeel Khoja. Xml implementation of role based control in healthcare adhoc networks. pages 1223–1226, 2007.
[14]. An architecture for resilient intrusion detection in ad-hoc networks. Journal of Information Security and Applications, 53:102530, 2020.