IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

A Review on Ad Hoc Network and Security Issues

Amar B M, Anagha Udupa Y N, Anirudh Kamath K, Ananya
Department of Information Science and Engineering
Alvas Institute of Engineering and Technology, Mijar, Karnataka, India

Abstract: *The term 'ad hoc' refers to self- configuring wireless networks made of mobile devices or nodes that form temporary connections dynamically without the need for any pre-existing infrastructure or centralized control. Because of their potential applications in a variety of fields, such as military operations, disaster response, and sensor networks, these networks have received so much attention. Ad hoc networks' decentralized nature and dynamic topology alternatively , present significant security challenges which is analyzed in this survey paper.*

With numerous sponsored studies and trials of "packet radio" systems in the 1970s, the idea of an ad hoc network emerged. In 1972, the Packet Radio Network was established, followed by the Survivable Radio Network (SURAN) and Low-cost Packet Radio (LPR) efforts in the 1980s. Ad hoc networks emerged in the commercial sector in the 1990s due to the entry of inexpensive radiofrequency wireless interfaces into the commodity computing market.[1]

In contrast to a wired network, an ad hoc network is typically thought of as having nodes that are more mobile. As a result, unlike the Internet, which is a wired network, the network architecture is far more dynamic and the changes are frequently unpredictable.[2] An ad hoc network is a group of nodes that may maintain connectivity without relying on a predetermined infrastructure. The utilization of open-source technologies that are common in the civilian world is a current trend in military ad hoc networking.[11]

This abstract provides an overview of ad hoc networks and the security systems designed to address the their unique security requirements . This paper highlights the key security challenges faced in ad hoc networks and presents an overview of the existing security mechanism, including secure routing protocols, authentication schemes and instruction detecting systems. In this article, the current issues and security vulnerabilities of Ad Hoc networks are surveyed.

Keywords: Ad hoc Network

I. INTRODUCTION

Ad hoc networks are a sort of wireless network that develop spontaneously and dynamically without the requirement for a centralized control or pre-existing infrastructure. In an ad hoc network, gadgets like computers, smartphones, and other wirelessly equipped devices communicate with one another directly to form temporary connections and exchange data. Alternate names for this type of network include "self-configuring network" and "spontaneous network."

Future smart environments will rely heavily on ad hoc sensor networks to sense, gather, and transmit data on environmental events. Security concerns rise to the forefront as the use of sensor networks expands.[4] The absence of cables enables deployment in dangerous areas or mobile scenarios, overcoming the majority of limitations of conventional wired networks. Wireless ad-hoc networks are the name given to wireless networks when nodes are independent of any established infrastructure. Communication in this scenario is dependent on the nodes' capacity to create a multi-hop radio network.[7]

With a focus on the most recent research and development in the quickly expanding field of ad hoc networks, Mobile Ad Hoc Networking thoroughly examines all aspects of the technology, including protocols and models.[5]

The term "mobile ad-hoc network" (MANET) refers to a system of wireless mobile devices, which are typically referred to as "nodes," that are capable of spontaneously and dynamically self-organizing1 into arbitrary and temporary network topologies. This makes it possible for individuals and devices to seamlessly collaborate in locations where there is no existing communication infrastructure.[6]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

Ad hoc networks, in general, offer a flexible and adaptable solution for circumstances when conventional infrastructure-based communication is not viable or feasible. However, because of their dynamic and decentralized nature, they also present difficulties in terms of network management, security, and dependable communication.
Ad hoc networking and security need a delicate balancing act between the need for dependable, secure communication and the dynamic nature of the network. Ad hoc network networking and security concerns are still being addressed through research and development in this field.

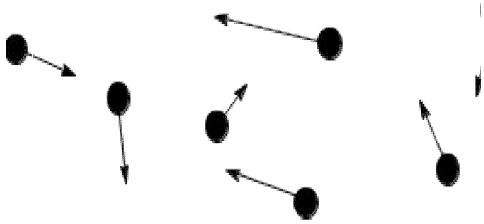

Figure 1: An ad hoc network with nodes moving in different directions and speeds.

Ad-Hoc networks includes the following features:
1) Decentralization: Ad hoc networks function without a central point of control, which allows every device connected to the network to function as a node capable of direct communication with other nodes.
2) Dynamic Formation: Ad hoc networks can be created dynamically, on the spot, without preparation or forethought. Because they mayenter or exit the network as needed, devices are very versatile and adaptable.
3) Limited Range: Due to the limited range of wireless communication technologies like Wi-Fi or Bluetooth, devices in an ad hoc network often need to be close to one another.
4) Temporary Nature: Ad hoc networks are frequently created for particular purposes and for a brief period of time. The network could disintegrate after the communication requirements are met

II. CLASSIFICATION OF AD HOC NETWORK

1) Wireless Mesh Network

A wireless mesh network (WMN) is a communications network comprised of radio nodes coordinated in a cross-section geography. Mesh clients, mesh routers, and mesh gateways are frequently found in wireless mesh networks. The cross-section clients are in many cases PCs, PDAs and other remote gadgets while the lattice switches forward traffic to and from the passages which may however require not associate with the Web.

2) Wireless Sensor Networks (WSN)

A wireless sensor network (WSN) is comprised of spatially dispersed autonomous sensors that work together to cooperatively transmit their data over the network to a central location while monitoring physical or environmental factors including pressure, humidity, temperature, sound, vibration, mobility, or pollution. Their creation was motivated by military applications of wireless sensor networks, such as battlefield surveillance. Machine health monitoring, process control, and industrial process monitoring are just a few of the many commercial and consumer uses for these networks today.[14]

3) Mobile Ad Hoc Network (MANET)

Mobile devices connected by wireless networks form a self-configuring network known as a mobile ad hoc network. Latin's ad hoc means "for this purpose" in English. As each device in a MANET can move independently in any direction, it frequently switches ties with other devices. Each should go about as a switch by sending traffic irrelevant to its own utilization. A gateway node that participates in both networks for traffic relay allows MANET to work alone or in conjunction with a wired infrastructure.[15]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

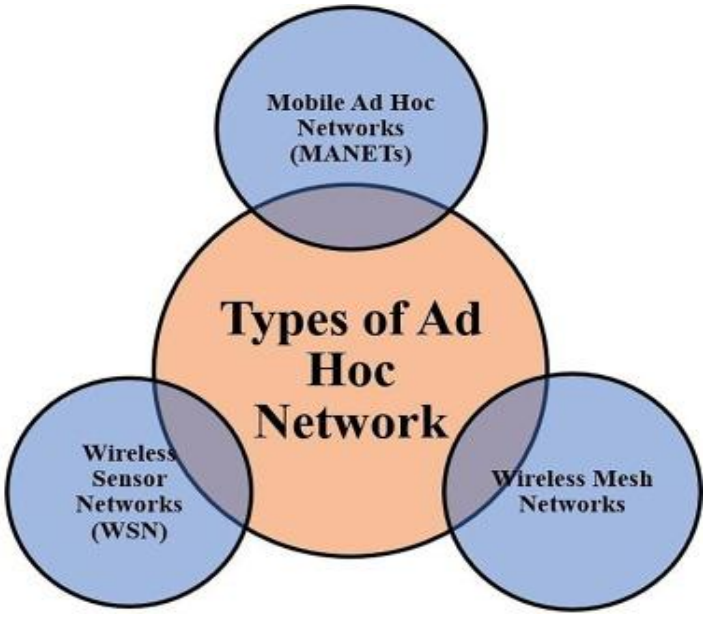

Figure 2: Classification of ad hoc networks[19]

III. LITERATURE REVIEW

This paper concentrate on the study of Ad Hoc network, its conventions and various kinds of organizations exhaustively, as we probably are aware this is an arising field which spots part of commitment in systems administration. Due to the fact that nodes move from one location to the next, the Ad Hoc network also introduces the concept of dynamic mobility. Any node in this network can join or leave at any time. Examples of systems or devices that fall under the category of nodes include personal computers, MP3 players, laptops, personal digital assistants, and mobile phones. These nodes can simultaneously serve as both a host and a router. A remote impromptu organization is a decentralized sort of remote organization. The network is ad hoc because it doesn't depend on a pre-existing infrastructure, like access points in managed (infrastructure) wireless networks or routers in wired networks. Instead, routing involves each node sending data to other nodes, and the network connectivity determines which nodes are used to forward data on a dynamic basis. Ad hoc networks give the choice of using flooding in addition to traditional routing to forward data. Any group of networks that are free to connect to any other ad hoc network devices within link range are often referred to as ad hoc networks. All devices in an this network have equal status on the network. In a mobile ad hoc network, nodes choose how to route packets between computing devices under the guidance of an ad-hoc routing protocol. Nodes in ad hoc networks are not familiar with their networks' topologies. Instead, they have to discover it.[14]

IV. POTENTIAL BENEFITS

Energy efficiency, i.e., how much battery energy consumed to send bits across a remote connection, is a basic plan boundary for remote impromptu organizations. When many nodes serve as sources, we investigate the issue of broadcasting information to every node in an ad hoc network.[8]

Flexibility and Mobility: Ad hoc networks allow devices to form a temporary network without depending on a centralized infrastructure. In circumstances like emergency response scenarios or rural places, when standard networks are unavailable or unfeasible, this flexibility enables speedy deployment and facilitates communication. Mobility makes it suited for dynamic situations like mobile computing or vehicle networks by allowing devices to join or exit the network on demand.

Scalability: Ad hoc networks are simple to scale since new devices can join or leave the network without changing the structure of the entire network. This scalability is especially helpful when networks need to be quickly established and modified to meet changing requirements, or when the number of network participants may expensive.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

Vehicular Ad hoc Networks (VANET) is emerging as a promising technology of the Intelligent Transportation systems (ITS) due to its potential advantages for travel planning, warning of road hazards, averting emergency situations, reducing traffic, providing parking facilities, and addressing environmental issues.[10]

Secure Communication: Ad hoc network security systems aim to provide secure communication channels among participating devices. By employing encryption, authentication, and integrity mechanisms, they can protect data from unauthorized access or tampering, ensuring confidentiality and integrity of transmitted information.

Privacy Protection: Ad hoc network security systems can safeguard the privacy of users' data by protecting against interception by unwanted parties or eavesdropping on communications. Encryption techniques can be employed to ensure that only authorized recipients can access the information.

Defense against Attacks: Ad hoc network security systems can detect and mitigate various types of attacks, including network intrusion, Denial of Service (DoS) attacks, or malicious code injection. Intrusion detection systems, firewalls, and other security measures can be implemented to identify and prevent such attacks, enhancing the overall network security.

Use of Artificial Intelligence

Artificial intelligence (AI) can play a significant role in enhancing the capabilities and performance of ad hoc networks. Without need for any pre-existing infrastructure , ad hoc networks are decentralized wireless networks that can dynamically form and reconfigure.

Optimization of the network and Routing: Ad hoc networks' routing decisions can be improvised using AI algorithms. To create intelligent routing choices which consider several parameters such as link quality, energy efficiency, and congestion, machine learning techniques can learn from historical data and network conditions. Optimization of network factors such as transmission power, channel allocation, and bandwidth allocation may also be assisted byAI

Resource distribution in ad hoc networks ,AI can be used to optimize resource allocation. Ai algorithms are able to efficiently dynamically allocate network resource like bandwidth , transmission power and spectrum by analyzing patterns of traffic and user demands ,the network's effectiveness as a whole user experience both benefit from this .

Management of Quality of Service (QoS): Ad hoc networks can be managed with AI techniques. AI algorithms are able to dynamically adjust the network settings to satisfy the desired QoS requirements by accounting for factors such as delay, throughput, packet loss, and jitter. In order to guarantee the best performance for a variety of applications and services, this includes dynamic bandwidth allocation, traffic prioritization, and load balancing.

Self-Configuration and Network Administration: In ad hoc networks, AI can automate network management tasks. AI algorithms can make it possible for network parameters to self-configure and self-optimize in response to changing conditions by making use of techniques like reinforcement learning. This makes it possible for the network to dynamically adapt to a variety of environments and reduces the need for manual intervention.

The study of VANET (Vehicular Ad-hoc Network) has been going strong for more than ten years. Similar to how recent advancements in computing technologies have accelerated the adoption of AI techniques in many fields (medical, transportation, engineering, manufacturing, healthcare, and several others), vehicular networks aim to enhance the security and efficiency of transportation systems by exchanging information among vehicles, pedestrians, and roadside infrastructures.[16]

A hybrid of static and dynamic topologies is known as a hybrid ad-hoc network (HANET). This network's nodes are each made up of low-capacity battery. The nature of the network parameters is imprecise due to the heterogeneous characteristics of the topology. As a result, the network's performance and lifespan suffer. An optimized energy efficient routing (OE2R) approach is put forward in this paper as a means of resolving these issues. This strategy is roused by man-made reasoning methods, for example, multi-objective enhancement, mathematical programming, desire level, and resistance limit. An efficient instrument for simultaneously optimizing multiple conflict objectives and estimating imprecise network parameters is created by combining these stated artificial intelligence techniques.[17]

The transmission of video data over dynamically connected ad-hoc networks is challenging. Real-time video transmission must adhere to strict minimum latency standards and have a low bit error rate. Path selection seeks to strike the ideal mix between real-time video demand and efficient use of network resources.[18]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

Ad hoc security systems, which are intended to provide security in environments that are subject to rapid change and are prone to unpredictability, may benefit greatly from the adoption of artificial intelligence.

Analysis and Detection of Threats: For identifying potential threats or anomalies, AI algorithms are able to analyze real-time data from a variety of sensors, including cameras, motion detectors, and thermal imaging devices. AI can identify suspicious behavior, unauthorized access attempts, or irregular patterns that might be a sign of a security breach by learning patterns and comparing them to known security threats.

Prevention and detection of intrusions: Man-made intelligence can be utilized to foster interruption identification frameworks that continually screen network traffic and recognize any unapproved or malevolent exercises. The system can proactively respond to potential threats and prevent security breaches by learning from historical data and recognizing patterns associated with known attacks.

Analytics for Predictive Security: AI algorithms are able to identify patterns and trends in large amounts of historical and current security data, allowing the system to predict potential security threats. AI is able to anticipate attacks, prioritize security measures, and provide security personnel with early warnings by utilizing techniques like anomaly detection and predictive analytics.

Information Sharing and Threat Intelligence: AI can help gather and analyze threat intelligence from a variety of sources, such as industry reports, public databases, and security forums. AI can extract relevant information, classify threats, and disseminate actionable intelligence to security teams by utilizing techniques from natural language processing and machine learning. This enables security teams to make informed decisions and effectively respond to new threats.

V. CHALLENGES

It's important to note that while ad hoc networks and security systems offer these potential benefits, they also have challenges and considerations that need to be addressed, such as network stability, power management, key distribution, and the overhead associated with security mechanisms. A major challenge when evaluating ad hoc routing protocol proposals is to choose a metric by which a protocol's performance will be evaluated. Finding the essential properties and developing methods to measure them is crucial because the majority of proposed ad hoc protocols have different objectives.[3]Ad hoc networks have difficulties such node mobility (devices entering and leaving the network), bandwidth restrictions, interference, security issues, and routing issues.

Due to severe resource constraints like a dynamic and varying topology, lack of centralized control, unsecure medium, and limited battery power, among others, a MANET faces numerous obstacles. [9]

Dynamic Topology: The self-configuring and dynamic nature of ad hoc networks makes them unique. Since nodes in the network can join or leave at any time, the network's topology frequently shifts. It is difficult to establish and maintain stable network connections, efficiently route packets, and effectively manage network resources with this dynamic topology.

Limited Resources: Smartphones or sensor nodes, for example, are typical components of ad hoc networks. The processing power, memory, battery life, and bandwidth of these devices are frequently limited. It is difficult to manage network operations while keeping in mind these restrictions. It is necessary to create security mechanisms that use as few resources as possible while still providing adequate protection against attacks.

In the context of vehicular ad hoc networks, the development of a secure and reliable communication architecture has faced numerous obstacles. Security challenges within these vehicular ad hoc networks may prove to be a devastating and would thus inhibit the effective working of this technology. The security challenges within the vehicular ad hoc networks can thus, be summarized as follows [23]:

Dynamic nature and high mobility of vehicles: Since the vehicles of the network are in constant motion with average speed being about 100 km/hour, it becomes extremely difficult to respond to an urgent situation and if the incoming communications are not validated in certain circumstances within a specified length of time, serious mishaps may occur. Therefore, the VANETs' security configuration should include provisions for these issues. [20].

Large number of peers in the VANET: The problem of network congestion may arise in densely populated locations where millions of vehicles would make up the network due to information overload, making it challenging to identify

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

the peers to be connected with. Because of this, the network configuration must include clever provisions for the easy identification of the necessary information to react appropriately and so avoid hazardous circumstances. [20].

Decentralized: Because the VANET network is an open system without a centralized infrastructure, participant automobiles are free to enter and exit the network as they see fit. Such a system makes it impossible to rely on processes with centralized systems or social networks and makes it unpredictable as to whether peers are trustworthy because it does not ensure that the same vehicle will interact in the near future. [21].

Bandwidth Limitation: When the network is overloaded with wireless nodes, this issue arises, which results in interference, weak signals, message delivery delays, etc. [22]. This increases complexity in the functioning of the VANET environment.

Malicious Attackers: This is one of the most challenging security issues in VANET networks. This is carried out by the attackers by disrupting the network functionality by gaining control over the network and thus manipulating, suppressing altering the message or by dropping the packet from network and later using these packets to draw personal benefits out of these. This may include Sybil attack, ID disclosure etc.[21]

Wireless Links: The wireless links inside VANETs are susceptible to some passive attackers who may use the network to gather evidence or manipulate the messages that are sent. [21].

VI. APPLICATIONS OF AD HOC NETWORKS

A few of the numerous applications of ad hoc networks are discussed in the following section:

1) Military: With an emphasis on data rate, real-time needs, rapid rerouting during mobility, data security, radio range, and integration with current systems, armed forces deploy military or tactical MANETs(Toh, 2002). Military ad hoc networks allow quick operation, rapid deployment, infrastructure-free operation, and no communication with fixed radio towers. Using a mobile, Air Force UAV, Navy ship, or robot, tactical networks may be formed during an operation and then evaporate after it is finished.

2) Community and Wireless Mesh Networks: By sending data to other nodes in the network, each node creates a non-hierarchical network. This type of network topology is called mesh networking. As nodes are added, the network becomes more resilient, which lessens reliance on any one link. For internet connectivity, some cities have built locally owned wireless mesh networks, such as NYC mesh, Toronto mesh etc. Since any node in the network has the ability to send data to any other node in the network, everyone can access the internet with just one node connected to it. Mesh networks are dynamic, meaning they automatically rearrange to ensure connectivity when users join or leave. These networks may alter in definition to become local area networks when hardware and network connections become more fixed than dynamic. These networks are classified as "ad hoc" insofar as users can join and leave the network.[24]

3)Blockchain-based Ad Hoc networks: For the purpose of social coordination, blockchains and cryptocurrencies are employed as ad hoc information networks. These economic infrastructures enable "peer-to-peer" value transfers between individuals without the need for a third-party service or central middleman, like a bank (Nakamoto, 2008, 1). According to some academics, transient blockchain networks resemble a "pop up economy" (Rennie, 2019). Ad hoc, blockchain-based coordination is also shown in the organizational structure of "Decentralized Autonomous Organizations" (DAOs). The non-profit organization Oxfam used the cryptocurrency stable-coin Dai for emergency financial transfers in Vanuatu, which is one example of a "pop-up economy" (Rust, 2019). During catastrophe relief efforts, Oxfam wanted to test out cash-based help that could boost local economies. Local sellers were assisted by Oxfam and its technology partners in accepting payments using "Near Field Communication" (NFC) cards that had been given out to locals. Decentralized Autonomous Organizations (DAO) are another type of grouping of people who can come together around a shared goal using network technology to create an ad hoc network. DAOs have made it possible to quickly and ad hoc mobilize and direct resources in a decentralized manner without depending on a central authority for coordination of response.[24]

VII. ISSUES CURRENTLY ASSOCIATED WITH AD HOC NETWORK AND SECURITY:

The concept of ad hoc networking raises a number of concerns or problems. This includes certainissues, such as network upkeep, digital inclusion, and the interdependencies between hardware, software, policy, and standard frameworks. Some issues include:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

1) Security Concerns: Ad hoc networks are frequently decentralized, making them vulnerable to security risks such data manipulation, eavesdropping, and denial-of-service attacks. It is still difficult to create reliable security systems that can manage the dynamic nature of ad hoc networks.

2) Routing and Scalability: Ad hoc networks need effective routing protocols in order to create communication pathways between nodes. The dynamic topology and the constrained resources of individual nodes make it difficult to create scalable and dependable routing algorithms.

3) Node Mobility: Ad hoc networks usually contain moving nodes, which frequently results in changes to the network's topology. Effective management is required for the route disruption, packet losses, and reconfigurations that can be brought on by this dynamic mobility.[26]

Ad hoc networks are increasingly frequently used to tether devices. In terms of knowledge and resources, as well as the expectations and constraints of ad hoc networks as a technical or socio-political solution, they can be difficult to develop and sustain. To build and sustain these networks, a large quantity of labor and expertise are needed, resources that are more prevalent in rich communities. Additionally, certain ad hoc networks might not be appropriate for the applications that people use them for. For instance, impromptu ad hoc networks were unable to maintain uninterrupted service during the Occupy Wall Street protests (Baccelli, 2012). Ad hoc networks may in some cases present chances for digital inclusion. For instance, depending on the devices and the network's location, ad hoc networks can enable several users to share a single internet connection in remote or rural areas, offer free or less expensive access, or extend connectivity to previously unreachable areas. Ad hoc networks, on the other hand, also feature aspects of digital isolation. To set up and run a network, for example, an existing infrastructure, such as a mobile network, satellite, or router, may be required.[24]

A wireless network called a vehicular ad hoc network (VANET) links a number of stationery or moving cars together. A collection of connected vehicles is referred to as a VANET, which is a subset of mobile ad hoc networks (MANETs).However, as technology advances and VANETs gain popularity, security flaws multiply quickly, which ultimately prevents the broad use of the VANETs. The open wireless channel the VANET employs makes it vulnerable to a wide range of attacks. There is therefore a significant chance of an assault. Services are inaccessible because the attackers want to inconvenience legitimate users. The assaults include some of the following attacks like Eavesdropping attack, Denial of Service attack (DOS), Illusion attack, Message tampering attack etc.[25]

VIII. METHODOLOGY

The most fundamental and crucial function of every ad hoc network is routing. Any ad hoc network operation must succeed through optimization and conservation. The bandwidth utilization ratio and load index, two new metrics for ad hoc networks, are discussed in this research. Both the network's usability and its efficiency can be improved by employing these metrics to effectively distribute load. They can be used to predict how much additional stress will be added which the network can support without experiencing congestion or overflows. Additionally, a new load balancing routing strategy for ad hoc networks and an effective load balancing mechanism are presented. This method seeks to balance the load on multiple pathways or channels using the load index as a statistic. The load index of a node, which is a measurement of how much it contributes to message routing, determines the load of that node. In order to achieve maximum efficiency, we only employ a small number of efficient pathways. The degree of distribution is determined by how many other routes were used out of all those that were accessible..[9]

IX. CONCLUSION

In conclusion, ad hoc networks present unique challenges with regard to network management and security. The dynamic topology, limited resources, scalability issues, open medium, lack of centralized authority, mobility, trust and authentication, and vulnerability to denial-of-service attacks all pose significant hurdles for ensuring secure and reliable communication within ad hoc networks.

To overcome these challenges, robust security systems need to be designed specifically for ad hoc networks. These systems must take into consideration the network's dynamic nature, resource constraints of the devices, and the need for decentralized decision-making. Secure routing protocols, cryptographic mechanisms, intrusion detection systems, and a complete ad hoc network security system must include effective resource management strategies.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

MANETs: Current situation and prospects identifies and examines the most pressing research problems in Mobile Ad hoc Networks (MANETs).[12]

It is probable that the number of wireless devices will expand quickly in the near future. Ad hoc network functionality which includes self-configurability and independence from existing infrastructures are important concerns in this setting.[13]

Addressing the challenges requires a mixture of secure routing protocols, cryptographic mechanisms, intrusion detection systems, and efficient resource management techniques are designed for the specific characteristics of ad hoc networks. These techniques are tailored to optimize the utilization of resources in these networks.

There is huge scope of improvement in case of authentication schemes as there are manynumber of attacking ways. This review paper will allow you to understand the various area and the various scope of improvement in various techniques and schemes

ACKNOWLEDGMENT

I extend my gratitude to Mr. JAYANTH RATHOD for their invaluable guidance.

REFERENCES

[1]. Kopp, Carlo. "Ad Hoc Networking." *Systems Journal* (1999): 33-40.

[2]. Lundberg, David. *Ad hoc protocol evaluation and experiences of real world ad hoc networking*. Diss. Master's thesis, Department of Information Technology, Uppsala University, Sweden, 2002.

[3]. Conti, Marco, and Silvia Giordano. "Mobile ad hoc networking: milestones, challenges, and new research directions." *IEEE Communications Magazine* 52.1 (2014): 85-96.

[4]. Hu, Fei, and Neeraj K. Sharma. "Security considerations in ad hoc sensor networks." *Ad Hoc Networks* 3.1 (2005): 69-89.

[5]. Basagni, Stefano, et al., eds. *Mobile ad hoc networking*. Vol. 461. New York: IEEE press, 2004.

[6]. M. Ilyas, The HandBook of Wireless Ad-Hoc Networks, M. Ilyas, Ed. CRC Press, 2003.

[7]. Di Pietro, Roberto, et al. "Security in wireless ad-hoc networks–a survey." *Computer Communications* 51 (2014): 1-20.

[8]. Widmer, Jörg, Christina Fragouli, and Jean-Yves Le Boudec. "Low-complexity energy-efficient broadcasting in wireless ad-hoc networks using network coding." *Proceedings*. No. CONF. 2005.

[9]. An efficient load balancing method for ad hoc networks-Jaspreet Singh,C.S Rai. 10) N. Malik, D. Puthal and P. Nanda, "An Overview of Security Challenges in Vehicular Ad-Hoc Networks," *2017 International Conference on Information Technology (ICIT)*, Bhubaneswar, India, 2017, pp. 208-213, doi: 10.1109/ICIT.2017.14.

[10]. C. Candolin and H. H. Kari, "A security architecture for wireless ad hoc networks," *MILCOM 2002. Proceedings*, Anaheim, CA, USA, 2002, pp. 1095-1100 vol.2, doi: 10.1109/MILCOM.2002.1179630.

[11]. Loo, Jonathan, Jaime Lloret Mauri, and Jesús Hamilton Ortiz. "Mobile ad hoc networks: current status and future trends." (2011): 538.

[12]. Remondo, David, and Ignas G. Niemegeers. "Ad hoc networking in future wireless communications." *Computer Communications* 26.1 (2003): 36-40.

[13]. Student, V., and Renu Dhir. "A study of ad hoc network: A review." *Int. J* 3.3 (2013): 135-138.

[14]. Goyal, Priyanka, Sahil Batra, and Ajit Singh. "A literature review of security attack in mobile ad-hoc networks." *International Journal of Computer Applications* 9.12 (2010): 11-15.

[15]. M. Chen *et al.* A deep learning based resource allocation scheme in vehicular communication systems.

[16]. Das, Santosh Kumar, and Sachin Tripathi. "Energy efficient routing formation technique for hybrid ad hoc network using fusion of artificial intelligence techniques." *International Journal of Communication Systems* 30.16 (2017): e3340.

[17]. Kwan, Manus, KutluyilDoğançay, and Lakhmi Jain. "Fair multi-path selection for real-time video transmission in ad-hoc networks using artificial intelligence." *Design and application of hybrid intelligent systems*. 2003. 830-841.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, September 2023

[18]. Reeya Agrawal, Neetu Faujdar, Carlos Andres Tavera Romero, Oshin Sharma, Ghadia MuttasharAbdulsahib, Osama Ibrahim Khalaf, Romany F Mansoor, Osama A.

[19]. Reeya Agrawal, Neetu Faujdar, Carlos Andres Tavera Romero, Oshin Sharma, Ghadia MuttasharAbdulsahib, Osama Ibrahim Khalaf, Romany F Mansoor, Osama A. Ghoneim,Classification and comparison of ad hoc networks: A review, Egyptian Informatics Journal

[20]. Jie Zhang, "A survey on Trust Management for VANET," International conference on Advanced Information Networking and Applications, IEEE computer society, pp. 105-112, 2011

[21]. Shrikant S. Tangade, Sunil kumar S. Manvi, "A survey on Attacks security and Trust Management Solutions in VANETs," Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), IEEE computer society, 2013

[22]. Mohamed Salah Bouassida, "Authentication vs. Privacy within vehicular Ad hoc networks," International Journal of Network Security, vol 13, no. 3, pp.121-134, Nov 2011

[23]. Vaibhav, Akash, et al. "Security challenges, authentication, application and trust models for vehicular ad hoc network-a survey." *IJ Wireless and Microwave Technologies* 3 (2017): 36-48.

[24]. Nabben, Kelsie, and Ellie Rennie. "Ad hoc network." *Internet Policy Review* 11.2 (2022).

[25]. Asra, Sahabdeen Aysha. "Security Issues of Vehicular Ad Hoc Networks (VANET): A Systematic Review." *TIERS Information Technology Journal* 3.1 (2022): 17-27.

[26]. Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad Hoc Networks," IEEE Transactions on Dependable and Secure Computing, 2004