IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 5, Ser. I (Sep - Oct 2019), PP 80-86
www.iosrjournals.org

Comparative Analysis and Performance with Emphasis on Security of MANET, WLAN, and LAN

Mr. Sachin Y. Zade[1,] Dr. Aruna J. Chamatkar[2] and Dr. Pradeep K .Butey[3]
[1]*Research Scholar, Kamla Nehru Mahavidyalaya, Nagpur*
[2]*Associate Prof., MCA Department, Kamla Nehru Mahavidyalaya, Nagpur*
[3]*HOD, Department of Computer Science, Kamla Nehru Mahavidyalaya, Nagpur*

Abstract: *Wireless networks, including Mobile Ad Hoc Networks (MANETs), Wireless Local Area Networks (WLANs), and Local Area Networks (LANs), play pivotal roles in contemporary communication ecosystems. This paper conducts a comprehensive comparative analysis of these networks, focusing on three critical dimensions: performance, security, and applications, with a specialized emphasis on security challenges. In this paper we provide a concise overview of the study.*

This study concludes by synthesizing the findings, offering a nuanced understanding of the strengths, weaknesses, and potential advancements in MANETs, WLANs, and LANs. This comparative analysis contributes valuable insights for practitioners, researchers, and policymakers involved in the optimization and fortification of wireless networks.

Keyword: *MANET,WLAN,LANs, ATM and WPA2/WPA3*

I. Introduction

In the rapidly evolving landscape of wireless communication, Mobile Ad Hoc Networks (MANETs), Wireless Local Area Networks (WLANs), and Local Area Networks (LANs) play pivotal roles in facilitating seamless connectivity and information exchange. These diverse network architectures cater to distinct requirements, spanning from mobile and flexible communication in MANETs to localized, high-speed data transfer in WLANs and LANs.

The significance of these networks is underscored by their pervasive adoption in various domains, ranging from everyday communication to critical applications in healthcare, military operations, and the Internet of Things (IoT). As these networks become integral to our daily lives and professional activities, the necessity to address performance, security, and application-specific considerations becomes paramount.

Performance AnalysisAssess the throughput, reliability, and scalability of MANETs, WLANs, and LANs, considering factors such as data transfer rates, connection stability, and the impact of network size on performance. By comprehensively addressing these objectives, this research aims to contribute valuable insights into the comparative analysis of MANETs, WLANs, and LANs, offering a foundation for informed decision-making, network optimization, and the advancement of wireless communication technologies.

This research embarks on a comprehensive comparative analysis of MANETs, WLANs, and LANs, with a particular emphasis on evaluating their performance, security features, and diverse applications. Understanding the intricacies of these networks and their respective strengths and weaknesses is crucial for network architects, policymakers, and researchers striving to optimize and secure wireless communication.

II. Literature Review

This literature review provides a comprehensive overview of key papers in the realm of networking and wireless communication, covering a broad spectrum of topics. Haas (1997) [1] investigates "High-Speed Networking over ATM-Based MANETs," focusing on challenges and advancements in mobile ad hoc networks (MANETs) utilizing Asynchronous Transfer Mode (ATM). Corson and Macker (1999) [2] delve into "Mobile Ad Hoc Networking (MANET)," addressing routing protocol performance issues and evaluation considerations. Perkins and Bhagwat (1994) [3] contribute "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," emphasizing the adaptability of routing for mobile devices. Bharghavan et al. (1994) [4] discuss "The IEEE 802.11 Protocol for Wireless LANs," providing foundational insights into wireless LAN standards. Tanenbaum and Wetherall (2003) [5] present a comprehensive overview of "Computer Networks," covering fundamental principles of network architecture. Hu, Perrig, and Johnson (2003) [6] propose "Packet Leashes" as a defense against wormhole attacks in wireless networks. Raya et al. (2004) [7] focus on "Securing Vehicular Ad Hoc Networks," addressing security concerns in dynamic vehicular environments. Clausen and Jacquet (2003) [8] introduce the "Optimized Link State Routing Protocol (OLSR)" for efficient routing in mobile ad hoc networks. Raychaudhuri et al. (2005) [9] provide an "Overview of the

ORBIT Radio Grid Testbed," offering a platform for evaluating next-generation wireless network protocols. Jahanian and Syverson (1997) [11] revisit "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV)" for mobile computers. Perkins and Royer (1999) [12] present "Ad-hoc On-Demand Distance Vector Routing," a dynamic routing approach for ad hoc networks. The IEEE 802.11 Working Group (1997) [13] contributes to the literature with "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," setting standards for wireless LANs. Boukerche et al. (2002) [14] conduct a "Performance Evaluation of the IEEE 802.11 MAC for Quality of Service in Mobile Ad Hoc Networks," addressing quality of service aspects. Wu and Chen (1999) [15] provide a "Performance Comparison of Ad Hoc Wireless Network Routing Protocols," offering insights into the comparative analysis of various routing protocols in ad hoc networks. Deng, Han, and Mishra (2006) [20] present "Countermeasures against Routing Attacks in Ad Hoc Networks," addressing security concerns and proposing solutions to mitigate routing attacks. Saha and Johnson (2010) [21] focus on "Secure and Resilient Time Synchronization for Wireless Sensor Networks," discussing the importance of secure time synchronization in sensor networks. Zeadally et al. (2009) [22] explore "Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, and Future Directions," providing a comprehensive overview of challenges and potential directions for VANETs. Meier and Tarkoma (2011) [23] conduct "A Survey of Mobile Ad Hoc Network Routing Protocols" (2011), offering a contemporary review of routing protocols in mobile ad hoc networks. Zouridaki and Karapistoli (2016) [24] contribute a "Performance Evaluation of Wireless Ad Hoc Routing Protocols under Different Mobility Models" (2016), examining the performance of routing protocols under varying mobility scenarios. Ali and Wang (2012) [25] present a "Survey on Wireless Mesh Networks" (2012), providing insights into the architecture and challenges of wireless mesh networks. Yadav and Chana (2016) [26] conduct "A Survey on Secure and Efficient Data Aggregation Techniques in Wireless Sensor Networks" (2016), summarizing techniques to enhance data aggregation security in sensor networks. Singh, Tripathi, and Singh (2018) [27] explore "Secure and Efficient Data Aggregation in Wireless Sensor Networks: A Survey" (2018), providing an updated overview of secure data aggregation techniques. Alaba, Othman, and Hashem (2018) [30] explore "Big IoT data analytics: Architecture, opportunities, and open research challenges" (2018), discussing the architecture and challenges in analytics for large-scale IoT data. Mishra, Naik, Pattanaik, and Mohapatra (2014) [31] conduct "A survey of data dissemination protocols in vehicular ad hoc networks" (2014), summarizing protocols for efficient data dissemination in vehicular networks. Jain and Somani (2015) [32] present "A comprehensive survey of security issues in vehicular ad-hoc networks" (2015), providing an extensive overview of security challenges in vehicular ad hoc networks. Kaur, Kaur, and Malhi (2016) [33] offer "A survey on mobile ad-hoc network" (2016), summarizing the challenges and advancements in mobile ad-hoc networks. Cheng, Sun, and Cao (2016) [34] conduct a "Survey of wireless network architectures and technologies" (2016), providing an overview of various wireless network architectures and technologies. This literature review serves as a valuable resource for researchers and practitioners interested in understanding the evolution and current state of networking technologies, encompassing issues ranging from routing protocols and security to performance evaluations and network architectures.

III. Performance Analysis

In the realm of wireless communication, the performance of networks is a critical factor that directly influences user experience and the efficiency of data transfer. The analysis encompasses key metrics such as throughput, reliability, and scalability to provide a comprehensive understanding of how these networks operate under various conditions.

A detailed examination of the performance characteristics of Mobile Ad Hoc Networks (MANETs), Wireless Local Area Networks (WLANs), and Local Area Networks (LANs) involves considering various factors related to their design, operation, and performance. Let's explore each network type individually:

A. Mobile Ad Hoc Networks (MANETs):

Mobile Ad Hoc Networks (MANETs) represent a class of wireless networks where nodes communicate with each other dynamically, forming an infrastructure-less and decentralized network. In MANETs, each node is capable of acting as a router, forwarding data for other nodes.

1.Topology and Structure:

MANETs are decentralized networks where nodes communicate with each other without a fixed infrastructure. Dynamic topology changes due to node mobility and the absence of a fixed infrastructure pose unique challenges.

2. Routing Protocols:

MANETs use dynamic and adaptive routing protocols to cope with changing network topologies. Common protocols include AODV (Ad Hoc OnDemand Distance Vector), DSR (Dynamic Source Routing), and OLSR (Optimized Link State Routing).

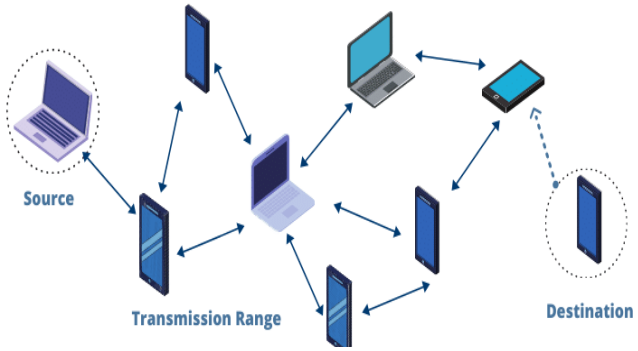

Figure 1: Mobile Ad Hoc Networks (MANETs)

3. Node Mobility:
Performance is influenced by the speed and unpredictability of node movements.Higher mobility may lead to frequent topology changes and route updates.
4. Security Challenges:
Lack of a centralized authority and dynamic topology make MANETs susceptible to security threats like routing attacks and eavesdropping.

B. Wireless Local Area Networks (WLANs):
Wireless Local Area Networks (WLANs) represent a fundamental component of modern wireless communication, providing flexible and convenient connectivity in various settings. A Wireless Local Area Network (WLAN) is a type of computer network that enables devices to communicate and exchange data wirelessly within a limited geographic area, typically within the range of a few hundred feet. Unlike traditional wired networks, WLANs use radio frequency signals or infrared signals for communication, allowing for greater mobility and flexibility of device placement.

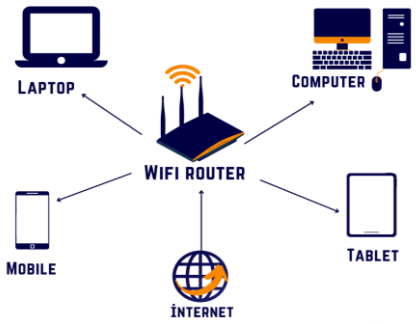

Figure 2: Wireless Local Area Networks (WLANs)

1. Infrastructure vs. Ad Hoc Mode:
WLANs can operate in infrastructure mode (using access points) or ad hoc mode (peertopeer communication).Infrastructure mode provides centralized control and easier management.
2. Interference and Channel Management:
WLANs operate in shared frequency bands, leading to potential interference.Efficient channel management and coexistence mechanisms are essential for optimal performance.
3. Throughput and Data Rates:
WLANs support various data rates, and throughput is influenced by modulation schemes, channel conditions, and interference.
4. Security Mechanisms:
WLANs implement security measures such as WEP, WPA, and WPA2 to secure wireless communications.Encryption and authentication are critical for protecting data integrity and privacy.
C. Local Area Networks (LANs):
A **Local Area Network (LAN)** is a network of interconnected computers, devices, and resources within a limited geographic area, such as a single building, office, or campus. LANs facilitate the sharing of resources, information, and services among connected devices, allowing for efficient communication and collaboration. Unlike wide area networks (WANs) that span larger geographical distances, LANs are characterized by their localized scope.

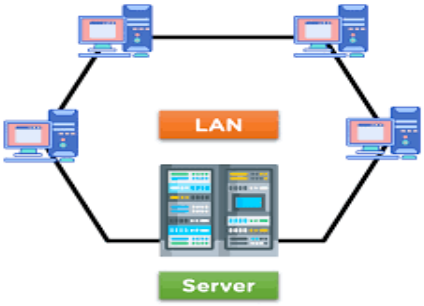

Figure 3 : Local Area Network (LAN)

1. Wired Infrastructure: LANs typically have a wired infrastructure with Ethernet being a common technology. High data rates and low latency characterize wired LANs.
2. Switching and Routing: LANs use switches for efficient packet forwarding within the network. Routing within LANs is minimal, as devices are usually connected directly through switches.
3. Reliability and Stability: Wired LANs provide a high level of reliability and stability compared to wireless networks.Performance is less affected by environmental factors and interference.
4. Security: Security in LANs often involves access controls, firewalls, and intrusion detection systems.Physical security is also a consideration as LAN devices are physically connected.
Common Considerations:
1. Latency and Delay: All three types of networks experience latency, but the sources and impact may differ.
2. Scalability: Scalability challenges arise in all networks but manifest differently. MANETs deal with dynamic scalability due to node mobility, WLANs with interference concerns, and LANs with the growth of connected devices.
3. Reliability: Reliability is influenced by factors such as node mobility in MANETs, interference in WLANs, and physical connections in LANs.
The performance characteristics of MANETs, WLANs, and LANs vary significantly due to their distinct features and applications. The choice of network type depends on the specificrequirements of the intended use case.

IV. Security Evaluation

Security is a paramount concern in the design and operation of wireless networks, and it becomes increasingly critical as these networks permeate diverse aspects of modern life. A security evaluation will give you a comprehensive security analysis with a specific focus on authentication, encryption, access control, and intrusion detection and prevention mechanisms.

a. Authentication

Authentication is the procedure of confirming the identity of users or devices seeking access to a network. In Mobile Ad Hoc Networks (MANETs), the dynamic nature of nodes and frequent changes in network topology pose distinct challenges for traditional authentication mechanisms. Unlike Wireless Local Area Networks (WLANs) and Local Area Networks (LANs), which benefit from more stable infrastructures and established authentication protocols, MANETs require specialized authentication methods to address their dynamic and ever-changing environment.

b. Encryption

Encryption is a fundamental aspect of network security, ensuring the confidentiality and integrity of data during transmission. In Mobile Ad Hoc Networks (MANETs), encryption faces challenges due to dynamic and decentralized node communication. Common methods include symmetric key and public key encryption, implemented through protocols like IPsec and TLS. Wireless Local Area Networks (WLANs) employ WPA2/WPA3, enhancing security with modern encryption techniques. Local Area Networks (LANs), whether wired or wireless, utilize encryption methods such as MACsec for data link layer security. The choice of encryption depends on network characteristics, security requirements, and resource constraints. Regular updates are vital to address evolving security threats in each network type.

c. Access Control

Access control mechanisms, which regulate network entry to prevent unauthorized access, face distinctive challenges in Mobile Ad Hoc Networks (MANETs) compared to more structured WLANs and LANs. MANETs lack a fixed infrastructure and are decentralized, making traditional access control methods challenging. Challenges include establishing trust among nodes, developing efficient authentication mechanisms, and dynamically adapting policies to the network's changing topology. Access control solutions for MANETs need to be decentralized, adaptive, and consider resource constraints, ensuring they are lightweight, energy-efficient,

and suitable for devices with limited processing power and memory. Researchers are exploring innovative models, such as reputation-based access control and lightweight authentication, to address these unique challenges in MANETs.

d. Intrusion Detection and Prevention System

Intrusion Detection and Prevention Systems (IDPS) are vital for network security, actively monitoring and responding to malicious activities. In Mobile Ad Hoc Networks (MANETs), their effectiveness faces challenges due to the dynamic nature of the network. MANETs lack a fixed infrastructure, making intrusion detection adaptability crucial. Challenges include routing issues, collaborative attacks, and resource constraints. Intrusion detection in MANETs involves anomaly and misbehaviour detection, utilizing machine learning and reputation-based systems. Prevention strategies focus on secure routing protocols and dynamic response mechanisms. Ongoing research explores machine learning applications and behavioral analysis to enhance accuracy. Tailoring IDPS to MANETs' unique characteristics is essential for effective security in these dynamic and resource-constrained networks.

V. Applications

Wireless networks, including Mobile Ad Hoc Networks (MANETs), Wireless Local Area Networks (WLANs), and Local Area Networks (LANs), serve as the backbone for a myriad of applications across diverse domains. This willexplore both common and industry-specific applications, shedding light on how each network type supports and addresses the unique requirements of these applications.

1. Entertainment and Media Streaming:

MANETs: Enable on-the-go media streaming and entertainment in scenarios with dynamic device interactions.

WLANs and LANs: Support high-bandwidth applications such as video streaming, online gaming, and music services.

2. Healthcare:

MANETs: Facilitate communication among healthcare devices and personnel in emergency situations or during patient transfers.

WLANs and LANs: Support electronic health records (EHR), telemedicine, and medical imaging systems in healthcare facilities.

3. Military and Defence:

MANETs: Form resilient and self-organizing communication networks in battlefield scenarios.

WLANs and LANs: Play roles in secure military communication, surveillance, and command and control systems.

4. Internet of Things (IoT):

MANETs: Support dynamic IoT deployments in scenarios with frequent device mobility.

WLANs and LANs: Connect and manage IoT devices in smart homes, industrial automation, and smart cities.

5. Education:

MANETs: Enable collaborative learning and content sharing in dynamic educational settings.

WLANs and LANs: Facilitate e-learning platforms, digital classrooms, and campus-wide connectivity.

WLANs and LANs: Provide the infrastructure for online gaming, virtual reality applications, and augmented reality experiences.

This analysis aims to highlight the versatility of MANETs, WLANs, and LANs in catering to a wide array of applications. Understanding the specific strengths and limitations of each network type in supporting these applications is essential for designing efficient and reliable communication solutions tailored to the unique requirements of different domains.

VI. Future Trends in Wireless Networking

The ever-evolving landscape of wireless networking continues to be shaped by technological advancements and emerging trends. This section explores the future trajectories of Mobile Ad Hoc Networks (MANETs), Wireless Local Area Networks (WLANs), and Local Area Networks (LANs), highlighting key trends that are likely to influence the design, performance, and security of these networks in the coming years.

1. 5G Integration and Beyond:

MANETs: Exploration of seamless integration with 5G networks to enhance connectivity, data rates, and support emerging applications like augmented reality (AR) and virtual reality (VR) in dynamic environments.

WLANs and LANs: Adoption of advanced 5G technologies to deliver enhanced data speeds, low latency, and improved network capacity, fostering a more connected and responsive ecosystem.

2. Hybrid Network Architectures:

MANETs: Development of hybrid architectures combining MANETs with other network types, such as satellite communication or fixed infrastructure, to enhance connectivity and reliability in diverse scenarios.

3. Machine Learning for Network Optimization:
MANETs: Integration of machine learning algorithms to optimize routing, resource allocation, and predict network behavior in dynamically changing topologies.
WLANs and LANs: Deployment of machine learning for intelligent network management, predictive maintenance, and the proactive identification of security threats.

4. Security and Privacy Enhancements:
MANETs: Advancements in secure communication protocols and cryptographic techniques to address the unique challenges posed by the dynamic and decentralized nature of MANETs.
WLANs and LANs: Integration of advanced encryption methods, biometric authentication, and zero-trust security models to bolster the security posture of WLANs and LANs.

5. Internet of Things (IoT) Integration:
MANETs: Customization of MANETs to seamlessly integrate with and support the growing number of IoT devices, fostering efficient and reliable communication in dynamic IoT environments.
WLANs and LANs: Evolution to accommodate the increasing density of IoT devices, emphasizing energy-efficient communication and secure connectivity for a wide range of IoT applications.
WLANs and LANs: Exploration of hybrid approaches that seamlessly integrate WLANs and LANs with emerging technologies, offering flexible and adaptable network solutions.
As wireless networks continue to play a pivotal role in our connected world, these emerging trends signify a shift towards more intelligent, secure, and adaptive network architectures. Understanding and leveraging these trends will be crucial for network planners, researchers, and policymakers to harness the full potential of MANETs, WLANs, and LANs in the dynamic landscape of wireless communication.

VII. Conclusion

The performance characteristics of Mobile Ad Hoc Networks (MANETs), Wireless Local Area Networks (WLANs), and Local Area Networks (LANs) are shaped by their unique design principles, applications, and challenges. MANETs, with their decentralized and dynamic nature, face the complexities of node mobility, energy efficiency, and security in ad hoc communication scenarios. WLANs, operating in both infrastructure and ad hoc modes, grapple with interference, throughput considerations, and the need for robust security mechanisms. On the other hand, LANs, characterized by wired infrastructure, offer high reliability, low latency, and scalability, making them well-suited for stable and high-performance local connectivity. Each network type caters to specific use cases and demands, and the choice among MANETs, WLANs, and LANs depends on factors such as mobility requirements, environmental conditions, and the need for wired or wireless connectivity. Overall, understanding the distinctive features and challenges of each network type is crucial for effectively deploying and managing communication solutions in diverse scenarios.

Reference

[1]. Haas, Z.J. (1997). "High-Speed Networking over ATM-Based MANETs."
[2]. Corson, M.S., & Macker, J.P. (1999). "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations."
[3]. Perkins, C.E., & Bhagwat, P. (1994). "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers."
[4]. Bharghavan, V., et al. (1994). "The IEEE 802.11 Protocol for Wireless LANs."
[5]. Tanenbaum, A.S., & Wetherall, D.J. (2003). "Computer Networks."
[6]. Hu, Y.C., Perrig, A., & Johnson, D.B. (2003). "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks."
[7]. Raya, M., et al. (2004). "Securing Vehicular Ad Hoc Networks."
[8]. Clausen, T., & Jacquet, P. (2003). "Optimized Link State Routing Protocol (OLSR)."
[9]. Raychaudhuri, D., et al. (2005). "Overview of the ORBIT Radio Grid Testbed for Evaluation of Next-Generation Wireless Network Protocols."
[10]. Hsu, C.H., & Helmy, A. (2007). "Survey of Network Design Problems and Optimizing Techniques in Wireless Ad Hoc Networks."
[11]. Jahanian, F., & Syverson, P. F. (1997). "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers."
[12]. Perkins, C. E., & Royer, E. M. (1999). "Ad-hoc On-Demand Distance Vector Routing."
[13]. IEEE 802.11 Working Group. (1997). "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications."
[14]. Boukerche, A., et al. (2002). "Performance Evaluation of the IEEE 802.11 MAC for Quality of Service in Mobile Ad Hoc Networks."
[15]. Wu, Y., & Chen, H. H. (1999). "Performance Comparison of Ad Hoc Wireless Network Routing Protocols."
[16]. Yang, Y., Liu, L., & Li, X. (2006). "Wireless LAN Security Threats & Vulnerabilities: A Literature Review."
[17]. Marina, M. K., & Das, S. R. (2001). "Ad Hoc On-Demand Multipath Distance Vector Routing."
[18]. Rothenberg, C. E., & Neves, M. A. A. (2007). "An Experimental Evaluation of the Cisco Aironet 350 Wireless NIC."
[19]. Royer, E. M., &Melliar-Smith, P. M. (2000). "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks."
[20]. Deng, J., Han, R., & Mishra, S. (2006). "Countermeasures against Routing Attacks in Ad Hoc Networks."
[21]. Saha, D., & Johnson, D. (2010). "Secure and Resilient Time Synchronization for Wireless Sensor Networks."
[22]. Zeadally, S., et al. (2009). "Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, and Future Directions."

[23]. Meier, A., &Tarkoma, S. (2011). "A Survey of Mobile Ad Hoc Network Routing Protocols." - (2011)
[24]. Zouridaki, C., &Karapistoli, E. (2016). "Performance Evaluation of Wireless Ad Hoc Routing Protocols under Different Mobility Models." - (2016)
[25]. Ali, W. M., & Wang, Z. (2012). "Survey on Wireless Mesh Networks." - (2012)
[26]. Yadav, S., & Chana, I. (2016). "A Survey on Secure and Efficient Data Aggregation Techniques in Wireless Sensor Networks." - (2016)
[27]. Singh, D., Tripathi, R., & Singh, P. (2018). "Secure and Efficient Data Aggregation in Wireless Sensor Networks: A Survey." - (2018)
[28]. Safaei, F., Othman, M., & Abdullah, M. (2015). "A review of routing protocols in vehicular ad hoc networks." - (2015)
[29]. Singh, S., Tyagi, S., & Rodrigues, J. J. P. C. (2018). "Security in wireless sensor networks: Issues and challenges." - (2018)
[30]. Alaba, F. A., Othman, M., & Hashem, I. A. T. (2018). "Big IoT data analytics: Architecture, opportunities, and open research challenges." - (2018)
[31]. Mishra, P., Naik, K., Pattanaik, S., & Mohapatra, S. (2014). "A survey of data dissemination protocols in vehicular ad hoc networks." - (2014)
[32]. Jain, A., & Somani, G. (2015). "A comprehensive survey of security issues in vehicular ad-hoc networks." - (2015)
[33]. Kaur, A., Kaur, A., & Malhi, R. K. (2016). "A survey on mobile ad-hoc network." - (2016)
[34]. Cheng, L., Sun, Z., & Cao, J. (2016). "Survey of wireless network architectures and technologies." - (2016)