A Comparative Study of Traditional and Decentralized Vehicle Ad-Hoc Networks (VANETs): Challenges and Opportunities

Sowmya K S[1] , Shivani A[2*], Shree Charan M L[3] ,Swetha Swaminathan[4]
[1]Assistant Professor, Department of Information Science and Engineering, B.M.S College of Engineering Bengaluru, Karnataka, India
[2, 3, 4]UG Scholars, Department of Information Science and Engineering, B.M.S College of Engineering Bengaluru, Karnataka, India

[*]Corresponding Author: shivani1812a@gmail.com

Received Date: March 16,2023 *Published Date April 7,2023:*

ABSTRACT

This survey paper presents a comprehensive comparative analysis of traditional and decentralized Vehicle Ad-hoc Networks (VANETs), which are wireless networks established between vehicles to enhance road safety and efficiency. The paper examines the challenges and opportunities present in both types of VANETs by evaluating their respective architectures. Traditional VANETs are characterized by centralized control and communication involving a principal trusted authority, whereas decentralized VANETs are characterized by distributed control and communication between vehicles without the need for a third-party to mediate communication between two vehicles. The paper meticulously highlights the advantages and disadvantages of both approaches, providing a systematic evaluation of the current state of VANETs. It analyzes the key aspects of VANETs, such as security, privacy, scalability, and reliability. The paper offers insightful perspectives on the potential benefits and limitations of traditional and decentralized VANETs, including their impact on traffic safety, communication efficiency, and system complexity. The paper discusses the applications of the existing VANET-based systems, such as collision avoidance, traffic congestion management, and emergency services. It also provides directions for future research and development in the area, identifying the key challenges and open research issues. It also highlights the critical importance of security and privacy in VANETs, emphasizing the need to prevent malicious attacks and unauthorized access to sensitive data. Overall, the paper provides a valuable resource for researchers and practitioners interested in VANETs, offering a comprehensive and up-to-date survey of the field, highlighting the advantages and limitations of traditional and decentralized VANETs, their applications, and future research directions.

Keywords- Communication, Dedicated short-range communications (DSRC), Digital signatures, Traditional, Vehicle ad-hoc networks (VANETs)

INTRODUCTION

Intelligent Transport Systems (ITS) have been gaining significant attention in recent years due to the integration of advanced technologies into the transportation sector. The main objective of ITS is to improve the efficiency, safety, and sustainability of the transportation system. The growing demand for a safe and reliable road transport system, combined with the advancements in communication technologies and the increasing popularity of connected and autonomous vehicles, has resulted in the development of Vehicular Ad Hoc Networks (VANETs).

Vehicular Ad Hoc Networks (VANETs) are a type of mobile ad hoc network (MANET) that allows vehicles to communicate with each other and with roadside units. These networks are designed to support various applications and services for the road transport sector, such as road safety, traffic efficiency, entertainment, and infotainment. VANETs enable vehicles to exchange information about their speed, location, and road conditions, and use this information to improve the overall safety and efficiency of the road transport system.

VANETs are considered an important component of Intelligent Transport Systems (ITS) and have received significant attention from researchers and practitioners in recent years. This is due to the growing demand for safe and reliable road transport systems and the

increasing need for connected and autonomous vehicles. Additionally, advancements in communication technologies have enabled the development of VANETs, making it possible to offer a wide range of services and applications to support the road transport sector.

VANETs can be implemented as either centralized or decentralized systems. Centralized VANETs rely on a central server to manage communication and information exchange between vehicles. In this type of system, vehicles send their data to a central server, which processes and distributes the information to other vehicles. This approach offers more centralized control and management of the network but also requires a large amount of infrastructure and resources to support it. Due to VANET characteristics, such as high-speed vehicles, real-time distribution and analysis of information, there have been performance bottlenecks in the traditional architecture of VANET that relies on centralized trusted authority to ensure the authenticity and reliability of the message.

On the other hand, decentralized VANETs use a peer-to-peer communication model, where vehicles communicate directly with each other without the need for a central server. With this approach, vehicles can share information and collaborate in real-time, which offers more robustness and scalability. However, decentralized systems are also more challenging to implement, as they require vehicles to be equipped with advanced communication and processing capabilities, and to make use of complex routing and coordination algorithms.

The objective of this survey paper is to provide a comprehensive analysis of various implementation approaches for VANETs. Firstly, we will provide an overview of traditional centralized VANETs and examine their architecture, advantages, and limitations. Secondly, we will examine the most popular decentralized implementation approach for VANETs, and analyze its advantages and limitations in terms of security, efficiency, and scalability.

In addition to the analysis of the various implementation methods of VANET systems, this paper will also explore the various applications of VANETs in the field of transportation. We will delve into the potential benefits that these systems can bring to the transportation industry and highlight their key advantages. Additionally, the paper will also discuss the challenges that VANETs currently face and their future scope of development.

TRADITIONAL VANET
Architecture

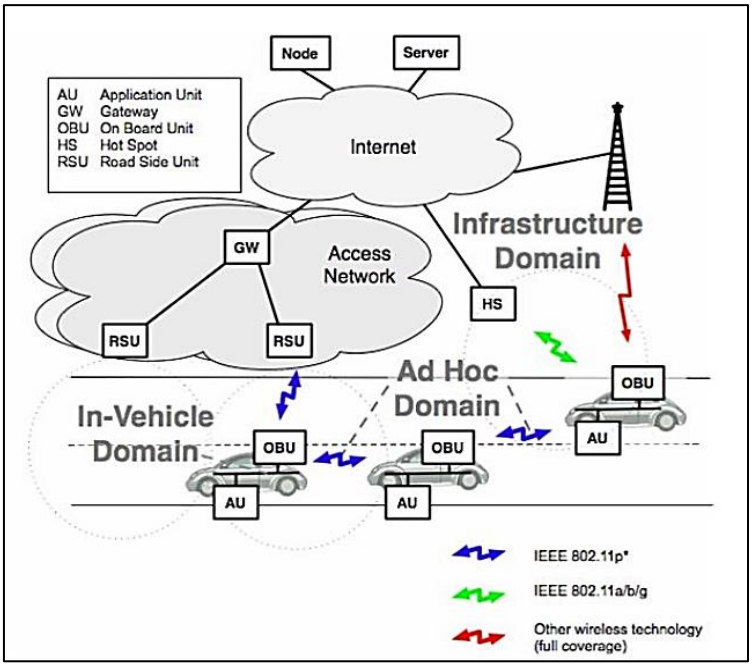

Figure 1: *Traditional VANET.*

Fig. 1 [1] is a schematic representation of the Traditional VANET architecture. According to the European architecture standard for VANETs [1], the entire system can be partitioned into 3 major domains:

- ***In-Vehicle Domain:*** This consists of all moving vehicles composed of application units (AU) and an On-Board Unit (OBU). The OBU, comprising electronic components such as sensors, user interfaces, and command processor [2] is a GPU-tracking device responsible for collecting critical information from vehicles such as vehicle speed, location etc. and communicating it to the RSUs or other OBUs [3].
- ***Ad-Hoc Domain:*** The Ad-Hoc domain consists of the interactions between the OBUs present in the moving vehicles and the Road Side Units (RSU) placed in fixed positions along the roads. The RSU is responsible for performing computations with the information received from these vehicles, providing local connectivity to other vehicles present within its range and also communicating with the other components present in the infrastructure domain.
- ***Infrastructure Domain:*** This mainly deals with exchanges between the RSUs and the internet, which consists of a Trusted Authority (TA) that is responsible for registering RSUs, OBUs and users before adding them to a network. Other functionalities of the TA include identifying and authenticating registered users and weeding out potential attackers.
- The types of communication that take place in a vehicular ad-hoc network majorly include in-vehicle communication between OBUs and their AUs, Vehicle-to-vehicle (V2V) communications between vehicles through OBUs, Vehicle-to-infrastructure (V2I) bidirectional wireless communications between vehicles and RSUs and finally Infrastructure-to-Infrastructure (I2I) communications between RSUs [4].

Advantages and Disadvantages of Centralized VANET

Vehicular Ad-Hoc networks support a wide range of applications from safety purposes to improving traffic flow efficiency. It can be used to detect and prevent rear-end collisions [1], usually caused by sudden braking of vehicles, by quickly sharing the information between the braked vehicle and the vehicles in the vicinity of it. It is also used to disseminate information about road conditions and potential accident sites or dangerous locations that could be used by vehicles to decide on alternate routes and increase traffic flow efficiency. Other examples of traffic efficiency applications include Enhanced Route Guidance and Navigation [1], which collects traffic data of a large region to predict traffic congestion on roadways and transmits it to vehicles, and Green Light Optimal Speed Advisory [1], which provides information related to the signalized intersection and signal timing to vehicles approaching the intersection to avoid stopping and increase traffic flow. Moreover, the clear chain of command in the centralized VANET architecture proves to be useful in troubleshooting networks and detecting potential vulnerabilities.

Some of the major disadvantages of the centralized approach for vehicular communication is the single point of failure i.e. the failure of a trusted authority or an RSU will result in the entire network in a particular region going down. Real-life networks require quick message dissemination and interpretation and security procedures such as source identification and authentication, ensuring message integrity can delay these quick transmissions [5]. Moreover, scalability becomes a big problem as the number of vehicles in a certain region increases, whereas the traffic handling capacity of the system remains the same. Finally, VANET systems are highly heterogeneous, with different types of vehicles, communication technologies, and applications. Therefore, interoperability and standardization are critical issues that need to be addressed to ensure seamless communication among the vehicles.

DECENTRALIZED VANET

Decentralized VANET systems are a network in which the vehicles communicate with one another directly without relying on a centralized server or infrastructure. Decentralized VANET systems differ from traditional ones in that they transform each vehicle in the network into a node that communicates directly with neighbouring vehicles. These nodes exchange important information such as their location, speed, and direction of travel, without sending this data to a centralized server or structure. Since

decentralized networks do not rely on a centralized server, they are more robust and resilient to failures.

Decentralised VANETs can be implemented in several ways. This paper discusses the most popular implementation, which is the blockchain-based network.

Blockchain-Based Network

Vehicular Ad-Hoc Networks (VANETs) are complex distributed systems that depend on multiple entities to maintain and share information. In traditional VANETs, centralization is typically utilized to accomplish this task. However, the integration of blockchain technology into a VANET network presents the opportunity to establish a fully decentralized system, eliminating the need for a central authority. Blockchains are known to integrate seamlessly with distributed systems; therefore, this architecture has immense potential to significantly improve the performance of VANET systems.

Architecture

As seen in Fig. 2. [6] A blockchain-based decentralized VANET system will contain the following components [5]:

Groups: Vehicles in the network will be organized into different groups based on their location, function, or other criteria. Each group will have a leader or coordinator responsible for managing communication and data sharing within the group.

Roadside Units (RSUs): RSUs will be installed along roadways to provide connectivity between vehicles and the core network. They would act as gateways between the VANET and the core network, and would also be responsible for relaying information between vehicles that are out of direct communication range.

Core Network: The core network would consist of servers and other infrastructure that provide connectivity and support services for the VANET. It will be responsible for managing the blockchain network and maintaining the distributed ledger of all transactions.

Blockchain: The blockchain network will be used to securely and immutably record all transactions within the VANET. It would consist of a distributed network of nodes that validate and propagate transactions and would use consensus algorithms to ensure that all nodes have a consistent view of the state of the network.

Blockchain Network: The blockchain network would be composed of several different blockchain platforms such as Ethereum, Hyper ledger, EOS etc. which will be used depending on the use case. Each platform will have its consensus algorithm and smart contract functionality.

Group Management: Each group would have a group management system that would be responsible for managing the membership and communication within the group. The system would use smart contracts to automate decision-making processes and ensure that only authorized vehicles have access.

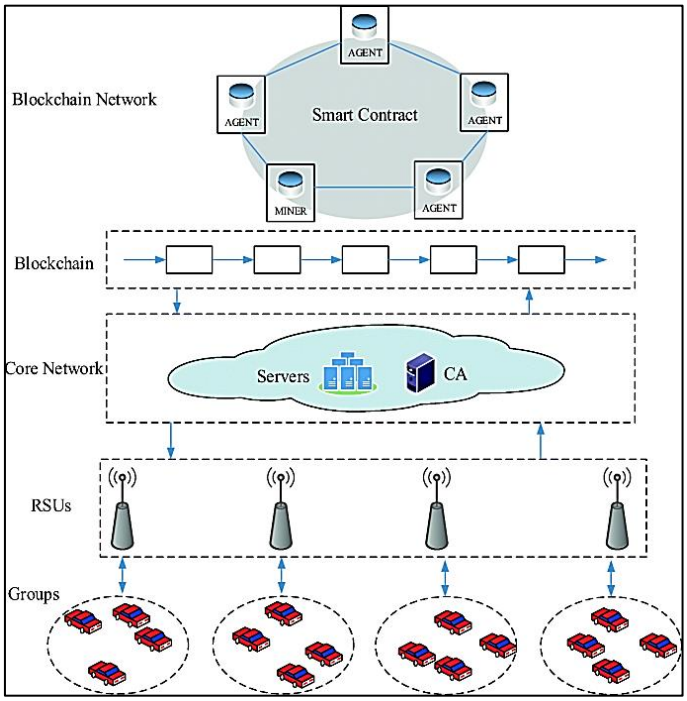

Figure 2: *Layered architecture VANET with Blockchain.*

The blockchain-based network design shown in Fig. 2 [6] can be implemented by taking the actions outlined below. To evaluate the credibility of messages, we will first create a message ranking upload. Specific guidelines will be set, and ratings will be made appropriately. The trustworthiness of the node, its closeness to the scene of the event, and other variables may have an impact on the veracity of messages. Trust value offsets are determined after evaluations are generated. When a Roadside Unit (RSU) receives contradictory evaluations, the offset confidence value is calculated using a weighted aggregation method. Since attackers are unable to take possession of a significant number of cars, the majority of evaluations will be fair, improving the accuracy of confidence value offsets. Decentralized networks do not have a central node that constantly manages the database. A mining server is instead chosen from among RSUs regularly based on proof of work. An RSU receives a nonce from a miner and checks its accuracy before adding a block to its network. A dispersed consensus approach is used to choose one fork and keep adding new blocks after it if an RSU gets multiple blocks at once. The network's distribution agreement is decided by the fork that has garnered the most support from RSUs, with the other branches being disregarded. Each RSU collects the blocks they produced in the abandoned divisions and makes an effort to add them to the blockchain in the future to preserve network stability [7].

Advantages and Disadvantages of Decentralised VANETs

Decentralized VANET systems overcome some of the major limitations of traditional VANET systems. They are more scalable as they don't rely on a single point of control and are hence also resilient to network failures such as the single point of failure. One of the biggest advantages provided by the blockchain mechanism is immutability, i.e. an attacker can't change the hash value of all the blocks as the hash value of each block is linked to the hash value of the previous block. They also preserve the privacy of each user added to the network by providing anonymity to each node. In a decentralized VANET system, there is no need for individual nodes to trust a central authority because the network operates in a distributed manner, thus eliminating the need to have a trusted system. Blockchain-based VANET systems use mechanisms such as consensus and smart contract algorithms [5] to validate each block added to the blockchain and also ensure that only trusted users are added to the network, hence making the system more secure.

Some of the limitations of a decentralized system are its complexity, security,

quality of service (QoS) and interoperability. Decentralized VANETs require more sophisticated routing algorithms and communication protocols, which can make their implementation more challenging. They can also be more vulnerable to security attacks, such as the Sybil attack [8], where the attacker creates multiple identities for nodes and attempts to distribute false messages throughout the decentralized peer-to-peer network using these identities, man-in-the-middle attacks, node impersonation attacks, DoS attacks, packet sniffing etc. Decentralized VANET systems may face challenges related to trust and accountability. Without a central authority to enforce rules and resolve disputes, it can be difficult to establish trust between individual nodes in the network. It can also be more challenging to implement across different types of vehicles and network environments. They may require significant investments in hardware and software to support the distributed nature of the network. This can be a barrier to adoption, particularly in resource-constrained environments.

APPLICATIONS

Blockchain-based VANET systems have several potential applications in the transportation industry, including:

- **Secure Payments:** Blockchain technology can be used to facilitate secure and efficient payments for tolls, parking fees, and other transportation-related expenses. This can help reduce the need for cash and improve the overall efficiency of transportation systems.
- **Traffic Management:** Blockchain-based VANET systems can be used to improve traffic flow and reduce congestion on roads. Using real-time data from sensors and other sources, blockchain technology can help optimize traffic signals and route vehicles more efficiently.
- **Vehicle Tracking:** Blockchain-based VANET systems can be used to track vehicles in real time, which can be helpful for fleet management, logistics, and emergency services. This can also be useful for tracking stolen vehicles or identifying vehicles involved in accidents.
- **Autonomous Vehicles:** Blockchain-based VANET systems can be used to support the development and deployment of autonomous vehicles. By enabling secure and efficient communication between vehicles, blockchain technology can help improve the safety and reliability of autonomous vehicle systems.
- **Car Sharing:** Blockchain-based VANET systems can be used to facilitate car sharing and other shared mobility services. By providing a secure and decentralized platform for transactions, blockchain technology can help reduce the cost and complexity of these services.

CHALLENGES

For a vehicular ad hoc network (VANET) system to function efficiently, it must be continuously available, maintain the confidentiality of user nodes, employ strong authentication mechanisms, ensure data integrity, and practice non-repudiation. However, there are numerous challenges associated with implementing these factors in the network [9]. Threats such as denial-of-service attacks, jamming attacks, malware attacks, and broadcast tampering can hinder the availability of the network, ultimately resulting in reduced system efficiency. Protecting the confidentiality of the network becomes a critical challenge due to the exchange of sensitive information on the network. Various attacks such as eavesdropping, traffic analysis, man-in-the-middle, and social attacks can compromise the confidentiality of the network. Ensuring that malicious nodes are not allowed in the network is another important aspect that must be considered. Malicious nodes can disrupt the network and result in serious consequences. Therefore, strong authentication mechanisms are essential to prevent attacks such as Sybil, tunnelling, GPS spoofing, node impersonation, free-riding, and masquerading attacks. Additionally, managing data integrity is crucial to prevent the dissemination of wrong or malicious information among the nodes. There are several challenges associated with maintaining data integrity, such as preventing replay attacks, message tampering attacks, and illusion attacks.

FUTURE SCOPE

The exponential growth in the scope of Vehicle Ad-Hoc Networks (VANETs) has opened up a multitude of opportunities for future research. With the development of autonomous vehicles, there is a need for a more robust VANET system that can support a high volume of data transfer with good reliability. Researchers continue to focus on the development of more efficient and secure approaches to implement VANETs, addressing critical issues of security and privacy that are prevalent in the current system.

The potential applications of VANETs are vast and include traffic management, emergency response, and other transportation-related services. The use of real-time information on road conditions, congestion, and accidents for traffic optimization is an area that requires continued research and development of algorithms and systems.

The integration of Blockchain technology into VANETs has further enhanced their potential, and future research can focus on exploring the possibilities for enhancing communication and interaction between vehicles. Blockchain-based VANETs can provide improved security, privacy, and transparency, leading to the development of new services and applications.

CONCLUSION

In recent years, Vehicle Ad-Hoc Networks (VANETs) have emerged as a promising solution for improving traffic management, reducing traffic congestion, and increasing road safety. VANETs can provide real-time communication between vehicles and infrastructure, enabling the development of intelligent transportation systems (ITS) that can improve the efficiency and safety of transportation. Traditional VANETs rely on a centralized infrastructure for communication, which can provide a more reliable communication infrastructure and support a variety of applications. However, decentralized VANETs do not rely on any pre-existing infrastructure and can function in locations without any infrastructure. By utilizing blockchain technology, the risks of message fabrication or modification attacks can be reduced significantly using timestamps and hashing mechanisms. As a result, decentralized VANET provides a secure and tamper-proof method for transmitting information in a trustless environment. This system is more flexible, making it a promising direction for the development of secure, scalable, and efficient vehicular networks that can support a wide range of applications in the transportation industry. The choice of VANET system to be used in a particular network will depend entirely on the requirements at hand, the priorities of the users, and the environment in which it is to be deployed. For instance, in an urban environment with existing infrastructure, traditional VANETs may be more appropriate due to their reliability and support for a variety of applications. On the other hand, in rural areas or areas without existing infrastructure, decentralized VANETs may be more suitable due to their flexibility and ability to function without any pre-existing infrastructure.

REFERENCES

1. T Yeferny and S Hamad (2021). Vehicular ad-hoc networks: Architecture, applications and challenges, *arXiv*, Available at: https://arxiv.org/abs/2101.04539.
2. W Liang, Z Li, H Zhang, et al (2014), Vehicular ad hoc networks: Architectures, research issues, challenges and trends. *International Conference on Wireless Algorithms, Systems, and Applications*, (pp. 102-113). Springer, Cham., Available at: https://link.springer.com/chapter/10.1007/978-3-319-07782-6_10#citeas.
3. Md Sameer Sheikh and J Liang (2019). A comprehensive survey on VANET security services in traffic management system, *Wireless Communications and Mobile Computing*, 2019, Available at: https://doi.org/10.1155/2019/2423915.
4. D Sutariya and S. N. Pradhan (2010). Data dissemination techniques in vehicular ad hoc network, *International Journal of Computer Applications*, 8(10), Available at: https://www.ijcaonline.org/volume8/number10/pxc3871725.pdf#:~:text=Data%20dissemination%20among%20vehicles%20depends%20on%20the%20type,reliability%20as%20selected%20nodes%20participate%20in%20packet%20retransmissions.
5. S Kumar Dwivedi, R Amin, A Kumar Das, et al (2022). Blockchain-based vehicular ad-hoc networks: A comprehensive survey, *Ad Hoc Networks*, 137, Available at:

https://doi.org/10.1016/j.adhoc.2022.102980.

6. H Li, L Pei, D Liao, et al (2019). Blockchain meets VANET: An architecture for identity and location privacy protection in VANET, *Peer-to-Peer Networking and Applications*, 12, 1178-1193, Available at: https://doi.org/10.1007/s12083-019-00786-4.
7. Z Yang, K Yang; L Lei, et al (2019). Blockchain-based decentralized trust management in vehicular networks, *IEEE Internet of Things Journal*, 6(2), 1495-1505, Available at: https://doi.org/10.1109/JIOT.2018.2836144.
8. A Shahid Khan, K Balan, Y Javed, et al (2019). Secure trust-based blockchain architecture to prevent attacks in VANET, *Sensors*, 19(22), Available at: https://doi.org/10.3390/s19224954.
9. A Rasheed, A Qayyum and S Ajmal (2010). Security architecture parameters in VANETs. *2010 International Conference on Information and Emerging Technologies*. IEEE, Available at: https://doi.org/10.1109/ICIET.2010.5625734.

CITE THIS ARTICLE

Sowmya K S et al. (2023). A Comparative Study of Traditional and Decentralized Vehicle Ad-Hoc Networks (VANETs): Challenges and Opportunities, *Advancement of IoT in Blockchain Technology and its Applications*, 2(1), 30-36.