An Edge Enabled Region-oriented DAG-based Distributed Ledger System for Secure V2X Communication

S. Thangam[1] and S. Sibi Chakkaravarthy[2*]
[1]Center of Excellence, Cyber Security and School of Computer Science and Engineering, VIT-AP University, Amaravati, 522237, Andhra Pradesh, India.
[e-mail : thangam.21phd7031@vitap.ac.in]
[2]Center of Excellence, Artificial Intelligence Robotics (AIR) and School of Computer Science and Engineering, VIT-AP University, Amaravati, 522237, Andhra Pradesh, India.
[e-mail: chakkaravarthy.sibi@vitap.ac.in]
[*]Corresponding author: S. Sibi Chakkaravarthy

Received February 7, 2024; revised May 24, 2024; revised July 3, 2024; accepted July 31, 2024; published August 31, 2024

Abstract

In the upcoming era of transportation, a groundbreaking technology, known as vehicle-to-everything (V2X) communication, is poised to redefine our driving experience and revolutionize traffic management. Real-time and secure communication plays a pivotal role in V2X networks, with the decision-making process being a key factor in establishing communication and determining malicious nodes. The proposed framework utilizes a directed acyclic graph (DAG) to facilitate real-time processing and expedite decision-making. This innovative approach ensures seamless connectivity among vehicles, the surrounding infrastructure, and various entities. To enhance communication efficiency, the entire roadside unit (RSU) region can be subdivided into various sub-regions, allowing RSUs to monitor and govern each sub-region. This strategic approach significantly reduces transaction approval time, thereby improving real-time communication. The framework incorporates a consensus mechanism to ensure robust security, even in the presence of malicious nodes. Recognizing the dynamic nature of V2X networks, the addition and removal of nodes are aligned. Communication latency is minimized through the deployment of computational resources near the data source and leveraging edge computing. This feature provides invaluable recommendations during critical situations that demand swift decision-making. The proposed architecture is further validated using the "veins" simulation tool. Simulation results demonstrate a remarkable success rate exceeding 95%, coupled with a significantly reduced consensus time compared to prevailing methodologies. This comprehensive approach not only addresses the evolving requirements of secure V2X communication but also substantiates practical success through simulation, laying the foundation for a transformative era in transportation.

Keywords: Consensus mechanism, DAG, V2X, V2X security threats, and Edge computing.

1. Introduction

V2X is a technological system facilitating communication between vehicles and several entities inside their environment. The integration of this technology into intelligent transportation systems (ITS) [1] plays a critical role in enhancing road safety, optimizing traffic flow, and enhancing the overall driving experience. V2X facilitates the establishment of connections and interactions between vehicles (V2V) [2], infrastructure (V2I) [3], pedestrians (V2P) [4], and network services (V2N) [5]. This extensive connectivity facilitates a diverse array of applications and services that augment the functionality and capabilities of vehicles. V2X plays a crucial role in accident prevention, driver hazard awareness, and collision avoidance systems by facilitating the exchange of information among vehicles regarding their position, speed, and other essential factors [6]. An instance, a vehicle equipped with V2X technology can receive notifications regarding the surrounding vehicles, pedestrians, or road barriers. This enables the driver to undertake suitable measures to prevent accidents. Additionally, it aids in the optimization of traffic flow and the mitigation of congestion on road networks [7]. Through the exchange of information with various infrastructure components such as traffic lights, road signs, and traffic management systems, vehicles obtain real-time traffic updates, receive ideas for the most ideal routes, and receive guidance regarding traffic signal timings [8]. This data provides drivers with the knowledge necessary to make well-informed choices and select the most optimal routes. V2X communication has the potential to enhance the entire user experience by facilitating tailored in-vehicle services, entertainment systems, remote diagnostics, and over-the-air upgrades. It employs wireless communication technologies, such as dedicated short-range communication (DSRC) [9] and cellular vehicle-to-everything (C-V2X) [10], to establish communication connections between vehicles and their immediate surroundings. These technologies provide the transmission of information, encompassing the current state of vehicles, velocity, rate of change in velocity, and other pertinent data.

1.1 Addressing the Security Risks and Challenges in V2X Networks

Security and privacy are major concerns for vehicle networks due to their distributed nature. This is primarily because the data they transmit is vulnerable in an open-access environment. To effectively achieve the primary objectives of V2X, particularly in road safety applications, robust security procedures must be established to ensure the seamless operation of the V2X network. Without optimum security standards, there is a high risk of exploiting the V2X network to compromise security and disrupt traffic management [11]. Therefore, protecting the privacy and security of these networks from potential threats is an immediate necessity, with a focus on safeguarding the message transmission, and personal information of drivers and passengers.

1.1.1 Unleashing the Potential of Mobility

Due to the high mobility of nodes, vehicle networks are in a constant state of evolution, presenting unique challenges for communication systems. A significant issue arises from the difficulty in accurately distinguishing neighboring nodes, leaving them vulnerable to exploitation by attackers for disseminating false topology information. This misinformation can disrupt the network's topology, leading to misleading pathways, and potentially resulting in traffic accidents [12]. Therefore, it is imperative to implement robust security protocols, authentication systems for topology data, and anomaly detection mechanisms to effectively

mitigate these threats. Collaboration among technology providers, vehicle manufacturers, and regulatory authorities is essential for establishing and enforcing stringent security standards.

1.1.2 Shared Communication Medium Utilization

Wireless airborne radio transmission in automotive networks enables passive eavesdropping. In promiscuous mode, attackers can intercept all transmitted data using sniffer software, rather than just their own. Passive surveillance enables attackers to obtain data without actively participating in the network, rendering detection more challenging. Subsequently, upon capturing data, attackers may attempt to decode it to access sensitive information such as location or personal data. To safeguard vehicle networks from these threats, robust encryption, authentication, and intrusion detection solutions are imperative [13][14].

1.1.3 Diverse Communication Methods

Long-range wireless communication in V2X networks necessitates multi-hop protocols. These protocols facilitate routing data packets through multiple vehicles when direct communication is not feasible. While this collaborative approach enhances connectivity, it also introduces security vulnerabilities. Malicious nodes may exploit this mechanism to interfere with or disrupt data transmission, potentially leading to the dissemination of misinformation and compromising network security. Robust security measures such as encryption, node authentication, and intrusion detection are essential to mitigate these risks. Furthermore, implementing algorithms designed to detect and isolate malicious nodes enhances the reliability and safety of V2X communication networks [15].

1.1.4 Efficient Information Distribution Strategies

Vehicular network protocols necessitate that nodes to transmit beacon messages to maintain network operation and deliver services. These messages contain node positions and other pertinent network data. However, this practice also poses security risks. Malicious nodes can

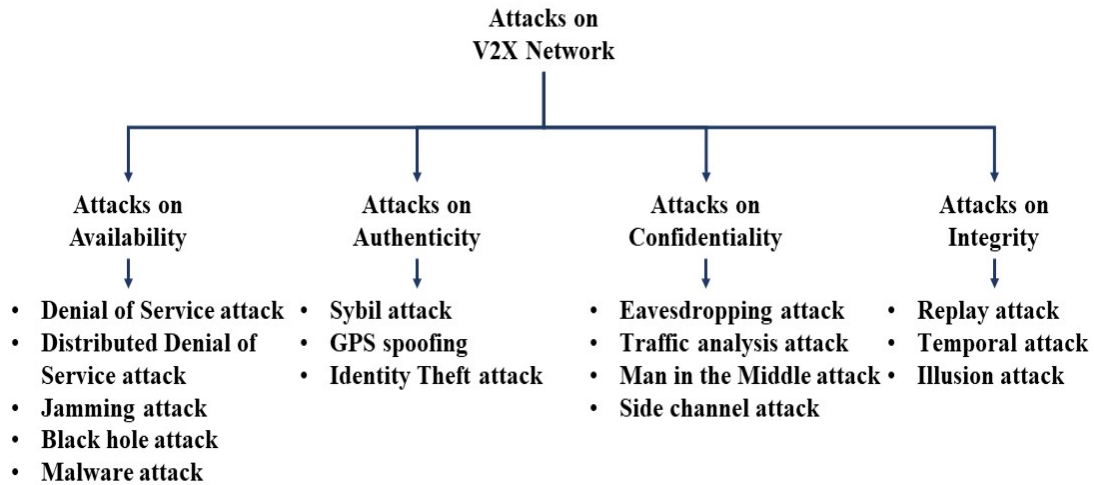

Fig. 1. Classifications of V2X threats

exploit beacon messages to track vehicles' movements and behaviors, potentially leading to stalking, targeted attacks, and unauthorized observation. To mitigate these risks, vehicular network protocols must incorporate robust security measures. This could involve anonymizing beacon messages, restricting data transmission, or implementing encryption. Furthermore, the detection and prevention of illegal data gathering and processing can further thwart exploitation by malicious nodes. Ensuring user privacy and security is paramount for the resilience and reliability of vehicle communication systems [16].

1.2 Categorizing V2X Network Threats

It is imperative to recognize that significant obstacles exist in the concept of expanding vehicle connectivity to encompass every aspect. Among these obstacles, ensuring the safety of the diverse stakeholders within V2X networks is paramount. Due to the increased degree of interconnectivity, these systems are vulnerable to malevolent attacks. Furthermore, the transmission of sensitive information complicates the task of preserving privacy. To safeguard this network from such risks, it is critical to classify them [17]. A comprehensive overview of several attack types vital to the security of V2X communication systems is provided in **Fig. 1**. Attacks against availability [18], authenticity [19], confidentiality [20], and integrity [21] constitute the four primary categories. Each of these categories targets different aspects of V2X security. Attacks on availability are particularly crucial, as they undermine the core purpose of V2X systems: ensuring continuous network service availability and instantaneous information accessibility for user safety. This category encompasses popular attacks such as denial of service, jamming, blackhole, and malware, which seek to disrupt networks. operations and services. Authenticity attacks, the second type, are essential for ensuring proper authentication of all network stations before gaining access to services. This category includes identity theft, Sybil attacks, and GPS spoofing, which can lead to misinformation and network diversion. The importance of preserving data privacy and confidentiality in V2X communications is underscored by attacks on confidentiality. These include man-in-the-middle attacks, traffic analysis, and eavesdropping, aiming to gain unauthorized access to data flows between nodes. Lastly, integrity attacks ensure data reliability and unmodified transmission. This category encompasses temporal attacks and illusion attacks, which pose risks such as message latency and deceptive data distribution, respectively.

1.3 Exploring Breakthroughs and Challenges in V2X Network Evolution

V2X communication in urban environments with dense vehicle populations presents several significant challenges that must be effectively addressed for its deployment to be successful. Scalability is a crucial consideration. The increasing number of automobiles and infrastructure components presents numerous scaling issues with different protocols. The capacity to effectively manage a significant number of participants and substantial message traffic is imperative to facilitate the dynamic and complex nature of urban V2X networks [22]. Latency is an additional crucial element [23]. The timely exchange of information holds significant significance, particularly in the context of safety-related communications. However, certain protocols may introduce latency due to factors such as routing overhead, network congestion, or dependence on external network infrastructures. Protocols should be resistant to network disruptions, interference, and adverse environmental conditions to ensure consistent and reliable transmission of sensitive information. Ensuring the preservation of privacy, integrity, and authenticity in V2X communication holds significant importance.

In recent years, there have been notable developments in V2X communication protocols aimed at addressing current limits and enhancing attributes such as reliability, scalability,

security, and efficiency [24]. Prominent research endeavors encompass the utilization of hybrid communication methodologies that integrate infrastructure-based and ad-hoc networking to enhance coverage and reduce latency. Edge [25][26] and fog [27] computing utilize network edge resources in order to minimize latency and improve the processing of real-time data. In edge computing, processing data closer to the source is crucial for real-time V2X applications. Deploying edge computing infrastructure comes with its fair share of costs that need to be taken into account. To evaluate the cost-effectiveness of deploying edge computing, various factors must be considered. Edge computing offers a major advantage by greatly reducing latency, a crucial factor for real-time V2X communication. Processing data at the edge improves system performance and safety by reducing message travel time between vehicles and central servers. The utilization of machine learning and artificial intelligence methodologies effectively enhances network performance and optimizes resource allocation in V2X communication [28]. Although modern processes have strong security measures, they remain susceptible to attacks. Blockchain-based protocols provide a decentralized and tamper-resistant mechanism for exchanging data, thereby ensuring the integrity of data and fostering trust among participants through the utilization of smart contracts.

1.3.1 Addressing Challenges and Harnessing of Blockchain in V2X Networks

Numerous scholarly articles and reports have examined the implementation of blockchain technology across various industries, including transportation, cybersecurity, and healthcare. Blockchain is increasingly being integrated into vehicle networks, notably enhancing security, especially in V2X dataset exchange. Importantly, Blockchain-based solutions have bolstered privacy protections in sectors such as data protection, cybersecurity, healthcare, electronic voting, and government database management. Identity and healthcare records can be securely accessed via private keys, ensuring accountability and protection. Researchers are leveraging Blockchain to develop secure, autonomous, and decentralized intelligent transportation solutions, thereby strengthening vehicular network security. However, adopting blockchain in V2X networks present certain limitations that need addressing to ensure the efficiency and security of these systems [29].

Considering vehicles' dynamic and resource-constrained nature, updating the blockchain in a vehicular environment can be quite challenging regarding computing demands. Dealing with the constant generation of V2X messages and the need to validate and add them to the blockchain can be quite demanding in terms of computational resources [30]. In addition, vehicles often have limited computational and storage capabilities compared to traditional blockchain nodes, which can pose challenges when it comes to handling intensive processing requirements. Network latency and bandwidth limitations in vehicular networks can also affect the timely spread and synchronization of blockchain data, making the computational load worse.

In order to tackle these challenges, we suggest implementing several optimizations. Integrating edge computing can be a game-changer when it comes to offloading computational tasks related to blockchain updates. By leveraging RSUs with higher processing capabilities, the burden on individual vehicles is reduced, resulting in faster transaction processing. Additionally, implementing a region-oriented architecture allows for the network to be divided into smaller, more manageable regions. Each region is overseen by an RSU, which helps distribute the workload and reduces the overall computational demand. Furthermore, incorporating lightweight and efficient consensus mechanisms can significantly reduce the computational burden involved in reaching consensus on blockchain updates. By implementing incremental block updates, the system can transmit only the necessary changes

instead of updating the entire blockchain for each transaction. This approach effectively reduces the amount of data that needs to be processed and transmitted, resulting in a decreased computational load. The intrinsic parallelism and decentralized nature of designs based on DAGs contribute to enhanced security, hence increasing the difficulty for attackers to undermine the network [31][32]. DAG-based systems diverge from typical blockchain [33] architectures by not depending on miners or validators for consensus attainment. Any node that is part of the network can contribute to the consensus mechanism, thus preventing the necessity for resource-intensive mining activities and mitigating the potential for centralization. There is no sequential block creation, hence transactions can be rapidly confirmed, making the system more responsive to real-time V2X communication requirements. Furthermore, the DAG [31] structure's intrinsic parallelism and decentralization contribute to its robustness in mitigating single points of failures and malicious attacks. Consequently, the decentralized architecture of DAG-based systems offers better resilience to system failures and a higher capacity to endure the failure of individual parts.

Motivation: The conventional V2X communication protocols, including centralized and semi-centralized systems, have difficulties managing the increasing number of vehicles, establishing user trust, and defending against intrusions. This encourages the exploration of alternative methods that could overcome these constraints and provide a more resilient and effective communication framework. Due to their inherent decentralization, transparency, and secure data storage, the use of distributed ledger technologies (DLTs) [34] in V2X communication has generated considerable enthusiasm. In a variety of industries, including finance and supply chain management, blockchain technology has demonstrated promise for bolstering trust and preserving data integrity. However, scalability and latency issues make these systems less effective for V2X networks due to their dynamic and time-sensitive nature. The adoption of the DAG approach stems from its distinct advantages as compared to conventional blockchain designs. DAG topologies facilitate concurrent processing, hence obviating the necessity for mining and leading to substantial enhancements in throughput and transaction confirmation time. DAG-based systems exhibit tremendous scalability and efficiency, enabling them to effectively manage the substantial volume of data created inside V2X networks.

The primary objective of this study is to devise and execute a novel methodology that effectively overcomes the limitations associated with conventional V2X communication. This work will ultimately address the following research questions (RQ):

RQ1: How does the DAG-based distributed ledger system effectively manage the growing an influx of interconnected nodes in the V2X environment?
RQ2: Does the edge-enabled region-oriented system significantly enhance performance in terms of latency, thereby mitigating transaction delays?
RQ3: How does the proposed consensus mechanism effectively mitigate the security threats and privacy issues in V2X environments?

Contribution:
This research article introduces a V2X communication system that utilizes DAG technology. The primary contributions of the proposed study are outlined below:

- This research presents a pioneering Region-Based Directed Acyclic Graph technology augmented by edge computing, specifically tailored for V2X communications. By partitioning the network into discrete regions managed by edge nodes, we enable the

joining and leaving of nodes dynamically, while significantly reducing latency, thereby revolutionizing the efficiency and responsiveness of V2X communication networks.
- This study introduces a novel algorithm tailored to partition the roadside unit region into finely tuned subregions, effectively enhancing system performance and alleviating scalability concerns.
- To further strengthen the reliability, security, and privacy of V2X communication, a novel consensus mechanism has been devised. This guarantees the integrity and confidentiality of data in V2X contexts and lays a solid foundation for private and secure information sharing.
- In-depth analysis of the suggested system's performance in terms of scalability, latency, security, and privacy is provided by this research. In addition to highlighting the system's potential influence on improving the security and dependability of V2X communication networks, the thorough examination offers invaluable insights into its capabilities.

2. Related Work

Existing research in V2X communication has primarily focused on various communication protocols, including DSRC [35], Cellular V2X (C-V2X) [36], and IEEE 802.11p [37][38]. These protocols make use of different wireless technologies, frequency ranges, and communication modes to enable V2X communication. Each protocol has distinct advantages and limitations concerning its coverage, communication range, data rate, and interoperability. In recent years, there has been a growing interest in employing distributed ledger technologies, particularly blockchain and DAG, to enhance the security and reliability of V2X communication. The evolving research in secure V2X communication emphasizes the architecture of a distributed ledger system based on DAGs, aiming to leverage the benefits provided by DAG structures. The authors [39] have put up a recommendation centered around the utilization of edge computing techniques to augment trust and reliability. The blockchain and federated learning methodology utilized by the researchers effectively mitigates the end-to-end delay associated with updating the blockchain on the edge device, resulting in a notable improvement in the throughput of vehicle communication.

The DAG-based scheduling strategy was introduced by [40]. The researchers incorporated a lightweight vehicle charging schedule mechanism into the DAG-based blockchain approach. They employed sophisticated cryptographic algorithms to guarantee the security and safety of vehicles. The use of blockchain technology presents a decentralized methodology that serves to augment the security measures of contemporary autonomous vehicles. Nevertheless, the substantial computing demands of the blockchain, in conjunction with the ever-changing characteristics of vehicles, provide notable obstacles during the process of updating the blockchain. [41] proposed a lightweight DAG structure to mitigate the constraints associated with current blockchain methodologies. They exploited the DAG lattice in practical byzantine fault tolerance (PBFT) to boost the efficiency of their proposed consensus technique. [42] proposed an approach for information sharing that utilizes a DAG structure. Unlike conventional methods that employ blocks for storing shared information, this method involves the utilization of sites. The mutual supervisor method was created by [32] and was designed to enhance the privacy of the social internet of vehicles. A technique under consideration is founded upon the DAG and has been specifically devised to mitigate latency issues. Reputation updates are of utmost importance in distributed ledger technology based on DAGs, as reputation is established through consensus transactions. The technique developed by [43] augmented the reputation mechanism inside dynamic vehicular networks by promoting the

active involvement of all nodes. [31] presented a tip selection algorithm to enhance authentication and security measures for the internet of vehicles. The current solutions implemented in-vehicle networks incorporate new technologies such as Artificial Intelligence and Blockchain for preventing and detecting attacks. Nevertheless, their efforts are inadequate when it comes to confirming the reliability of nodes and addressing security concerns within the V2X domain. Moreover, it has been observed that these frameworks exhibit increased delay as the number of transactions increases. Hence, our work suggests a methodology to successfully combine DAG and trust mechanisms that address these constraints, thereby guaranteeing a secure and efficient V2X environment.

3. System Model

The architecture (**Fig. 2**) uses a DAG structure to ensure the parallelism required for rapid data processing. The V2X environment is organized into regions, administered by RSUs.

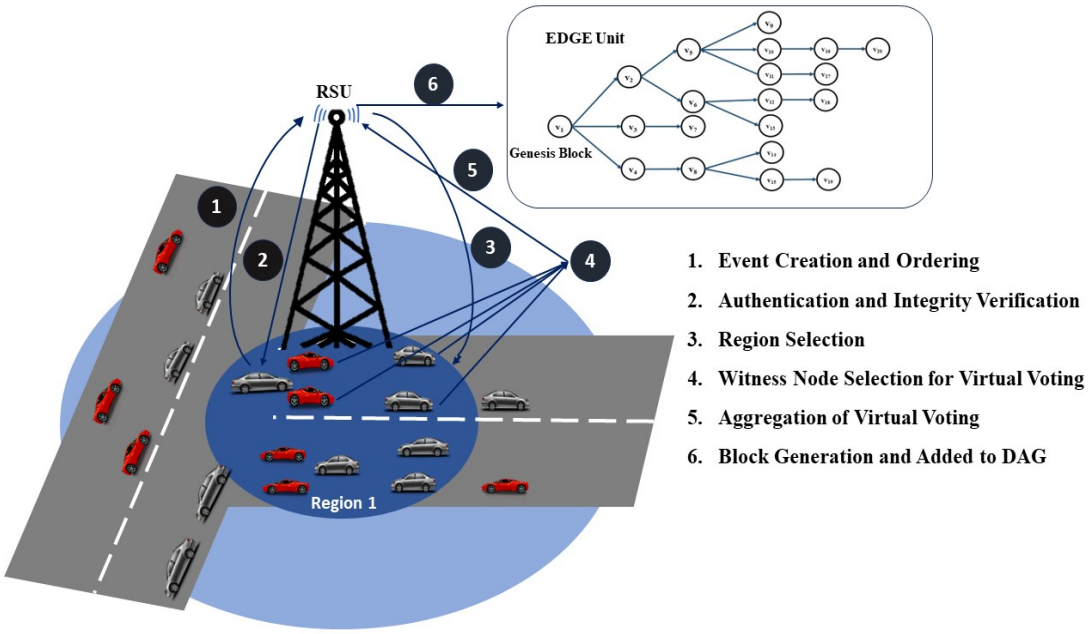

Fig. 2. The architecture of an edge enabled region-oriented DAG-based distributed ledger system.

Each RSU is responsible for maintaining the integrity of the DAG within its region and serves as a gossip node to efficiently distribute information among nodes in a network. The gossip protocol is used for preserving data synchronization, and information consistency in V2X communication. One of the distinguishing characteristics of the architecture is its ability to enable independent block creation within various regions. To ensure secure transaction validation even in the presence of malicious nodes, the system implements a new consensus mechanism.

3.1 DAG

DAG is a structure composed of nodes (or vertices) and directed edges that connect these nodes. DAG is distinguished by the absence of cycles, which implies that a path cannot be

traversed to finally return to the starting node by following edges. In this network, every edge possesses a unidirectional connection from one node to another. This directional attribute of the edges symbolizes a relationship or reliance that exists between the respective nodes. The system is devoid of cycles, thereby guaranteeing unidirectional flow. The system model incorporates DAG inside specific areas of the V2X network, thereby improving the efficiency of data processing while ensuring strong security measures and adaptability.

Consider the DAG denoted as G = (V, E), where: V = v_1, v_2, v_3, ..., v_n denotes the collection of nodes that symbolize events or transactions within the V2X network. E is the collection of directed edges (v_i, v_j) where v_i and v_j are elements of V. These edges describe the causal linkage that exists between nodes. Every node vi belonging to V represents a distinct event or transaction within the V2X communication system. Each directed edge (v_i, v_j) signifies that event v_i occurs before event v_j in the chronological sequence of V2X communication events. In order to incorporate a new event into DAG, it is a straightforward process of generating a new node, v_{n+1} and establishing directed edges to the appropriate preexisting nodes. The aforementioned structure exhibits a branching pattern, hence facilitating the simultaneous execution of several transactions. The interdependencies among the blocks in the DAG-based system are depicted using a hierarchical structure in **Fig. 3**.

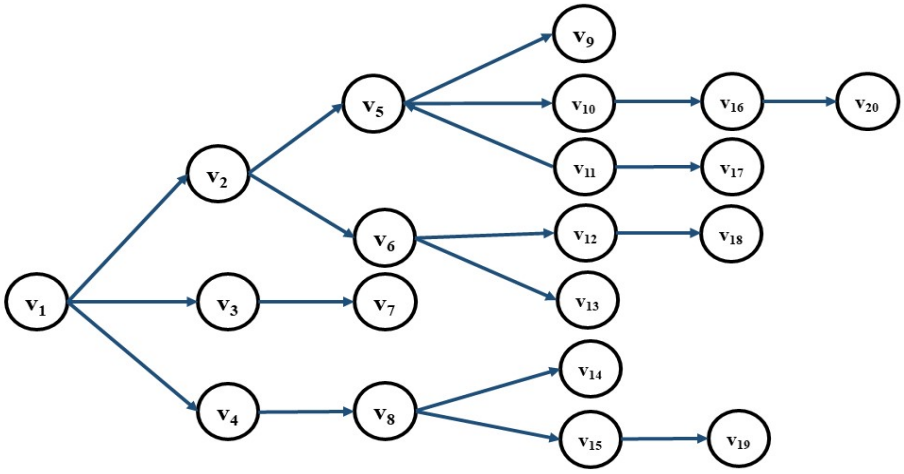

Fig. 3. DAG structure, G(V, E).

A DAG system with 20 blocks, designated as v_1 through v_{20}, is depicted in the figure. The system commences with the genesis block, denoted as v_1, which functions as the starting entity. Following the first emergence of v_1, further entities v_2, v_3, and B4 manifest, thereby building tangible connections to v_1. These connections generate direct dependencies from v_2 to v_1, v_3 to v_1, and v_4 to v_1. Block v_5 emerges after v_2, wherein the presence of a direct edge from v_2 to v_5 denotes the dependence of v_5 on v_2. Similarly, the creation of v_6 follows the creation of v_2, resulting in the establishment of a tangible connection from v_2 to v_6. This connection signifies the direct reliance of v_6 on v_2. Subsequently, v_7 arises after v_3, with a direct edge linking v_3 to v_7. Blocks v_8, v_9, v_{10}, v_{11}, v_{12}, v_{13}, v_{14}, and v_{15} exhibit a consistent pattern wherein each block is derived from its corresponding parent block and establishes direct connections to establish their interdependencies. Block v_5 emerges after v_{11}, Block v_16 is reliant on Block v_{10}, whereas Block v_{17} is reliant on Block v_{11}. v_{18} has a direct dependency on v_{12}, and v_{19} is reliant on v_{15}. Subsequently, the creation of v_{20} ensued after the formation of $v16$, building a direct edge connecting v_{16} to v_{20} and consequently establishing v_{20}'s direct reliance on v_{16}.

Advantages of DAG for real-time processing in V2X environments: DAG facilitates parallel processing, enabling the simultaneous confirmation of multiple transactions. This significantly reduces latency and enhances the speed of information dissemination, essential for efficient and secure V2X operations. Additionally, DAG is designed to support high scalability, managing increased loads without substantial delays and accommodating the dynamic and rapidly increasing number of connected devices. It also minimizes confirmation times by directly linking transactions rather than grouping them into blocks, ensuring rapid responsiveness for critical applications such as emergency brake signals. Finally, the DAG structure improves security through decentralized consensus mechanisms, which verify the validity of each transaction by examining the data of multiple antecedent transactions, thereby ensuring the authenticity and integrity of V2X communication.

3.2 Block Generation in DAG

The suggested architectural design facilitates the autonomous generation of transaction blocks by entities connected with RSU situated in different geographical areas. This feature leads to a notable reduction in delay while confirming transactions. The decentralized block creation mechanism in the DAG-based system allows for the concurrent formation of several blocks. The overall methodology for generating a new block is depicted in **Algorithm 1**.

1. **Input**
   - Set D represents the data generated in V2X Networks.
   - Set B represents the blocks.
2. **Initialization**
   - Let B = {Block_1, Block_2, ..., Block_n} be the set of blocks to be created.
   - Each Block_i contains a set of transactions T_i ⊆ D, a timestamp Timestamp_i, a hash value Hash(Block_i), and a reference to the previous block Previous_Block_i.
3. **Genesis block**
   - Let Block_0 be the genesis block with no previous block.
   - Block_0: {Transactions_0}, Timestamp_0, Hash(Block_0) = Hash(Block_0), Previous_Block_0 = NULL.
4. **Block i creation**
   - For each subsequent block Block_i (i > 0), do the following:
     - Select a set of transactions T_i ⊆ D for inclusion in Block_i.
     - Assign a timestamp Timestamp_i to Block_i representing its creation time.
     - Calculate the hash value Hash(Block_i) using a cryptographic hash function with input as {Transactions_i, Timestamp_i, Previous_Block_i}.
     - Set Previous_Block_i as the hash value of the previous block, i.e., Previous_Block_i = Hash(Block_{i-1}).
5. **Output**
   - The set of blocks B = {Block_0, Block_1, ..., Block_n} with each block containing its data, timestamp, hash value, and reference to the previous block.
   -

Algorithm 1. Algorithm for block generation

3.3 Region Partitioning by RSU

The scalability and efficiency of the proposed system architecture for secure V2X communication are significantly influenced by the implementation of region-based partitioning by RSU. **Algorithm 2** illustrates the process by which regions are divided by RSU. The algorithm for region partitioning by RSU is a crucial element of the proposed system. By utilizing optimization methods, the V2X network is intelligently divided into regions, taking into account traffic patterns, vehicular density, and other relevant criteria. This approach aims to improve the system's efficiency and scalability. However, it is important to handle the additional complexity with caution. The region partitioning algorithm utilizes various optimization techniques, such as clustering algorithms like K-means and dynamic load balancing strategies, to ensure that each RSU can efficiently handle its assigned region. These methods are designed to seamlessly adjust to variations in network conditions, guaranteeing efficient partitioning even when traffic patterns and vehicular densities change. A systematic tuning process has been employed to address the complexity associated with these optimization methods. In this process, we need to carefully choose the important factors that impact the effectiveness of the partitioning algorithm. These factors include the number of clusters, threshold values for vehicular density, and criteria for load balancing. Conducting sensitivity analysis allows for a deeper understanding of how changes in these parameters can affect the performance of the system. This analysis helps in determining the most optimal parameter settings that strike the right balance between efficiency and complexity. The specific functions f(), g(), h(), i(), and j() are the optimization methods used to find the traffic load, density, network connectivity, workload, and resource usage respectively.

The goal of the algorithm is to find the best partitioning plan that distributes work evenly, improves network connectivity, and changes based on new information. When an entity wants to send a message notifies its target nodes when it starts a conversation. Upon receiving this information, the RSU, a key element in the network, determines the location of the sender and destination devices. Messages are checked for validity using cryptography and digital signatures that have already been set before the messages are put forward for voting, this part of verification makes sure that they are honest and correct. With regard to scalability, the implementation of partitioning guarantees that the architectural framework can effectively and smoothly handle the increasing quantity of interconnected vehicles and devices inside the V2X environment. The architecture enhances transaction processing capacity while mitigating network congestion by granting RSUs the ability to independently generate blocks in various locations. Transactions and data are confined to certain locations, hence reducing the necessity for broad consensus on each transaction. The implementation of localization in processing results in a reduction of communication overhead and latency. In addition, the elasticity of the design enables nodes to dynamically join or depart from the network, hence enhancing operational efficiency and optimizing the consumption of resources.

Require: (Input)

1. Geographic area to be partitioned (A)
2. Traffic load (TL) and density (TD)
3. Network connectivity (NC)
4. Number of Partitions (N)
5. Workload (W)
6. Resource utilization (U)

Output: Set of optimized partitions (Sub Region (P))

Procedure

1. **Initialize**
   - P = { }
2. **Particular region into initial partitions**
   - $P_0 = \{p_1,p_2,...,p_n\} \forall p_i \in P_0, p_i \subseteq A$
   - Assign RSUs to partitions, $RSU(p_i) = \{r_1,r_2,...,r_m\} foreach\ p_i \in P_0$
3. **Evaluate the load and density of each partition**

   Calculate the traffic load and density
   - $TL(p_i) = f(p_i,TL)$ *for each* $p_i \in P_0$
   - $TD(p_i) = g(p_i,TD)$ *for each* $p_i \in P_0$
4. **Analyze network connectivity between RSU regions**
   - $NC(p_i,p_j) = h(p_i,p_j,NC)$ *for each* $p_i,p_j \in P_0$
5. **Calculate load balancing for each partition**
   - $W(p_i) = i(p_i)$ *for each* $p_i \in P_0$
   - $U(p_i) = j(p_i)$ *for each* $p_i \in P_0$
6. **Partition optimization**

   While $|P| < N$
   - Identify the partition pair (pi, pj) such that NC(pi, pj) is minimized
   - Join p_i and p_j into a new partition p_k: $p_k = p_i \cup p_j$.
   - *ModifyRSUassignment* : $RSU(p_k) = RSU(p_i) \cup RSU(p_j)$.
   - $ModifyW(p_k) = W(p_i) + W(p_j), U(p_k) = U(p_i) + U(p_j)$.
   - $Remove p_i and p_j from P_0 and add p_k to P_0$.
7. **Adjust partition boundaries:**
   - While partitions' workload and resource utilization are imbalanced
   - Identify the partition pair (p_i, p_j) with the highest W and U ratio.
   - Adjust the partition boundaries (p_i,p_j) to redistribute W.
   - Calculate new p_i and p_j
   - Update the RSU assignment and W and U accordingly.
8. **Consider dynamic partitioning**

   Monitor traffic patterns, road conditions, and network dynamics continuously

   If changes occur
   - Perform dynamic partitioning based on real-time data.
   - Update partition boundaries, RSU assignment, workload, and resource utilization.

Algorithm 2. Algorithm for region participation

3.4 Consensus Mechanism

Assumption: To ensure correct implementation, we assumed that all vehicles are present in the same region (R1) and maintain and transmit node information within this area only. To maximize the efficiency of the consensus processes, the percentage of malicious nodes in a region is kept at no more than one-third of all entities in that specific region. If the number of malicious nodes exceeds this limit, the risk of predicting incorrect trust values increases.

Integration of DAG and trust mechanisms: Integrating DAG and trust mechanisms into the proposed system involves several critical stages. Initially, RSUs initialize their local DAG ledger and establish contact with neighboring vehicles. These vehicles register and disclose their identity and public key as part of the node registration and initialization process. RSUs then verify the authenticity of the vehicles and record this information in the DAG ledger. When a vehicle generates a transaction, the nearest RSU is notified and uses its parallel processing capabilities to incorporate the transaction into the local DAG. Transaction validation is influenced by trust scores, prioritizing transactions from high-trust nodes for quicker processing. The consensus mechanism employs virtual voting within the DAG, where trust scores influence voting power, ensuring a tamper-proof and reliable ledger agreement.

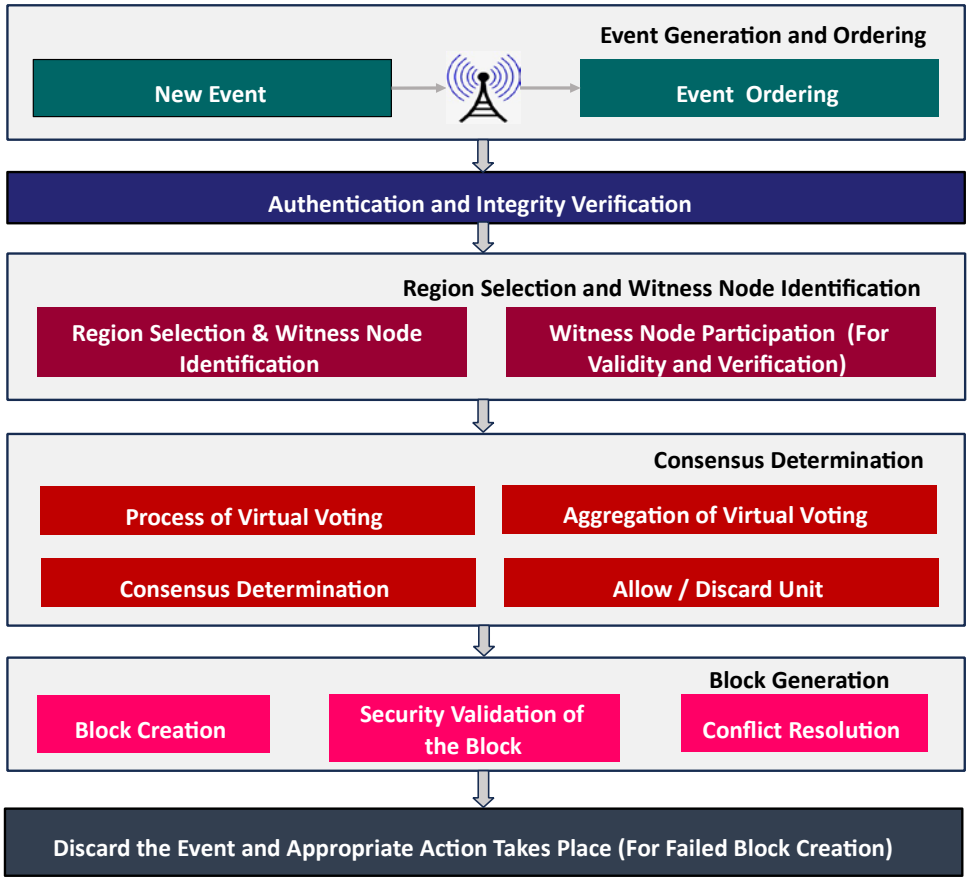

Fig. 4. Proposed consensus mechanism.

Design: The consensus process comprises a sequence of pivotal steps, as depicted in **Fig. 4**. When a device located within the coverage region (R1) desires to send a message, it initiates an event (e_1) that encompasses transactional data and destination information. The RSU, acting as the intermediary node for gossip dissemination, receives the event and employs cryptographic methods to validate its genuineness and integrity. Once the verification processes have been completed, the RSU tentatively adds the event to G = (V, E) and moves to further stages of the communication process. RSU commences a virtual voting procedure to reach a consensus regarding the authenticity and accuracy of the event. For this, RSU selects a specific group of witness nodes from R1. Witness nodes autonomously evaluate the

authenticity of the event using digital signatures, and predetermined regulations that are mutually agreed upon by the RSU. During the virtual voting process, witness nodes signify their judgment on the validity or invalidity of the event.

The RSU collects the collective input from the witness nodes and computes the count of votes for both validity and invalidity separately. Consequently, valid events are added to the RSU's DAG ledgers associated with R1. The order of the consensus decision is determined by the chronological order of the occurrences that receive the highest level of agreement from the witness nodes. Each event contains transactions and timestamps along with the previous event's details. To maintain a coherent ledger in cases when competing blocks arise, the consensus process is employed to resolve the disagreement by giving priority to the chain that has gained the highest amount of agreement. In cases where the majority of witness nodes' representations indicate that the message is invalid, the RSU disregards the occurrences and proceeds to take the necessary measures.

3.5 Dynamic Block Insertion and Deletion

Ensuring the smooth integration of a new block into the network or the orderly departure of an existing block is crucial for preserving the system's integrity and resilience. In order to become part of the network, the newly added block must initiate the process of discovering already established blocks. This can be accomplished by employing techniques that rely on a centralized service to acquire the addresses of currently active blocks. After successful authentication, the newly added block gains the ability to engage in the consensus mechanism. This includes the block's capability to propose its transactions, as well as actively contribute to virtual voting and the ordering of events inside the ecosystem. In addition, the newly added block must engage in ledger synchronization with the existing blocks to obtain the most up-to-date status of the distributed ledger. This involves retrieving any missing blocks to ensure a complete and accurate ledger.

Conversely, in the event that a block elects to withdraw, it is imperative that it transmits a farewell message to duly notify the centralized block about its departure. In the event of the departure of a leader block, it is necessary to initiate a leader election process to designate a successor who would assume the responsibilities formerly held by the departing leader. The departing block should also cease its involvement in the consensus process, rendering its votes and contributions to virtual voting. In addition, it is necessary to eliminate the data associated with the block from the ledger, and thereafter update the distributed ledger to accurately represent the deletion of the block.

3.6 Event Validation and Security

With a DAG, events or transactions can be recorded in a parallel structure, resulting in improved scalability and reduced confirmation times when compared to linear blockchain structures. With the ability to process multiple transactions simultaneously, the system becomes more adept at handling higher transaction loads more efficiently. By dividing the V2X network into smaller regions, transaction processing can be optimized by localizing it within specific areas. This approach helps reduce network congestion and latency, resulting in more efficient operations. Every event that is delivered is accompanied by a digital signature, which is generated using the principles of asymmetric cryptography. This involves the employment of a private key possessed by the event generator/ sender and a corresponding public key that is accessible to all participants. The act of appending a digital signature to an event is performed by the sender utilizing their private key, while the recipients can ascertain

the event's genuineness using the sender's public key. The digital signature's validity serves as confirmation that the message has not undergone any modifications along its transit.

3.7 Result Analysis and Discussion

In order to assess the efficiency of the proposed system, the traffic flow analysis was conducted using SUMO, a simulation tool for traffic analysis. The network simulation is designed using OMNETPP (event analysis simulation tool), and the experiment is carried out on the Veins (V2X simulation tool), with a road length of 2500m. The intelligent driver model (IDM) and the lane changing model (LCM) were employed for modeling traffic flow. A two-way lane is designated to facilitate vehicular movement. The prescribed speed limits on this lane are set at 30 km/s and 60 km/s, representing the minimum and maximum speeds, respectively. Additionally, a safety distance of 100 meters is ensured for the well-being of road users.

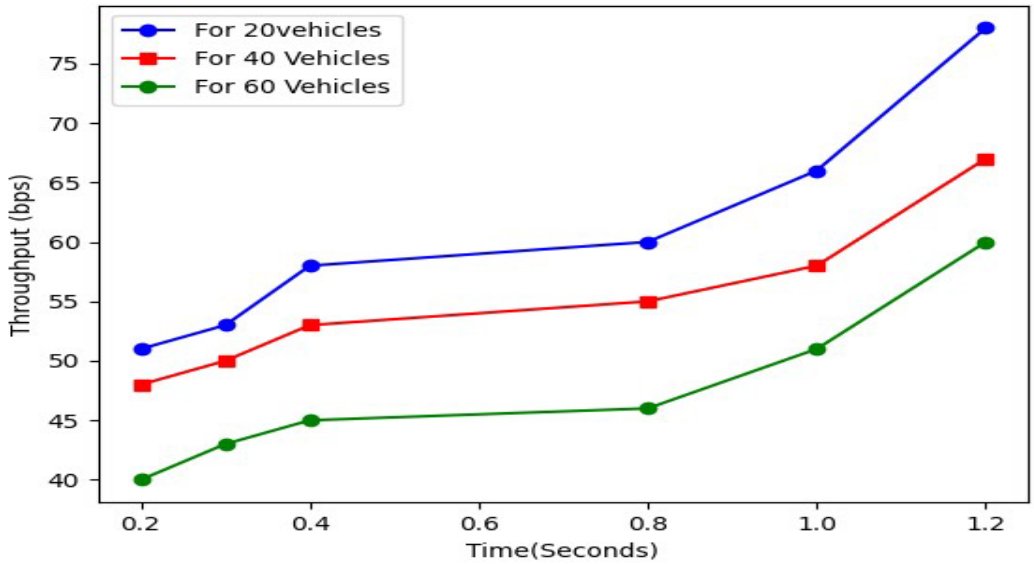

Fig. 5. Comparison of throughput for the number of vehicles.

The experimentation in observed for a duration of 1200 seconds. The baseline configuration assumes that there are 20 vehicles. Subsequently, the number of vehicles is incrementally augmented to 40, 60, 80, 100, and 140. The following parameters are taken into account while analyzing performance. The consensus time ($T_{consensus}$) details how long it takes to receive valid confirmation while adding an event to the DAG. It can be determined by subtracting the time at which consensus is confirmed ($T_{include}$) from the time at which the proposal ($T_{proposed}$) for consensus is made.

$$T_{consensus} = T_{include} - T_{proposed} \quad (1)$$

.

T_{ps} refers to the number of blocks that are encompassed throughout the DAG and are utilized to depict the transactions per second. Csuccess is defined as the proportion of transactions that have been successfully incorporated (T_{st}) in relation to the total number of transactions (T_{tr}).

$$C_{success}\ (\%) = ((T_{st} / T_{tr}) * 100) \quad (2)$$

The following section provides a comprehensive analysis of the performance of the proposed system, which is evaluated and validated using several parameters.

3.7.1 Throughput and Load Analysis

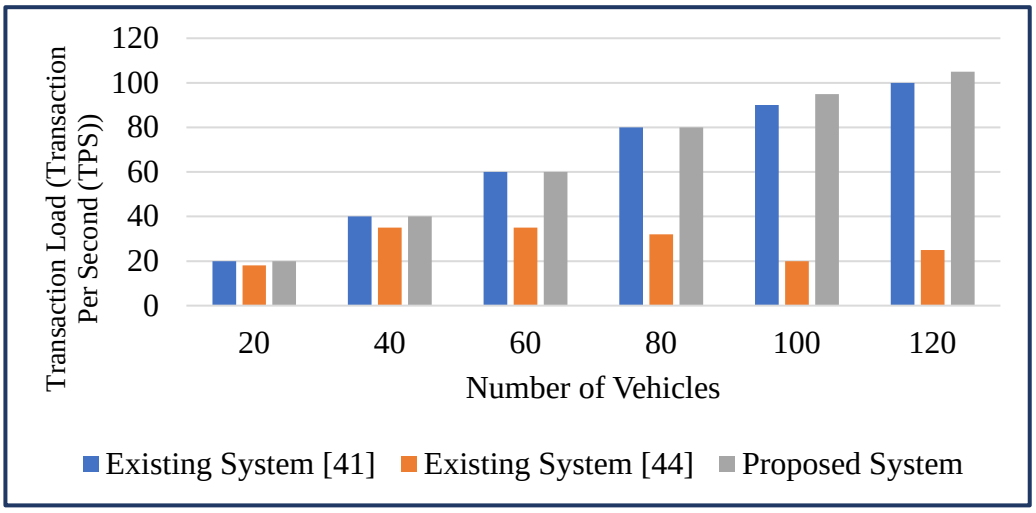

Fig. 6. Comparison of transaction load with the number of vehicles.

The graph (**Fig. 5**) illustrates a gradual increase in throughput as the increase in duration of time for three different scenarios - 20, 40, and 60 vehicles. This can be exacerbated by an increase in the number of vehicles on the road, which can have a negative impact on the system's real-time capabilities. The observed pattern indicates a gradual increase in network saturation when the number of vehicles is increased, which can be attributed to the growing amount of data being transmitted between vehicles and infrastructure.

Fig. 6 demonstrates the load test of our proposed system compared to existing systems. The number of transactions is compared across varying numbers of vehicles, with quantities increasing from 20 to 120. The observed pattern suggests that a modest level of transaction load positively impacts the system's efficiency in processing and confirming transactions compared to existing systems.

3.7.2 Scalability Analysis

Transaction load represents the number of transactions a system is able to process within a given timeframe, whereas confirmation time refers to the amount of time it takes for an event to be validated and added to the DAG ledger. **Fig. 7** demonstrates the system's scalability by demonstrating that, while confirmation times only slightly increase, the transaction load rises together with the number of vehicles. This indicates that the system effectively manages increased transaction load within a particular region, enabling localized scalability. In other words, each subregion is capable of handling increased transaction loads without substantially increasing confirmation times

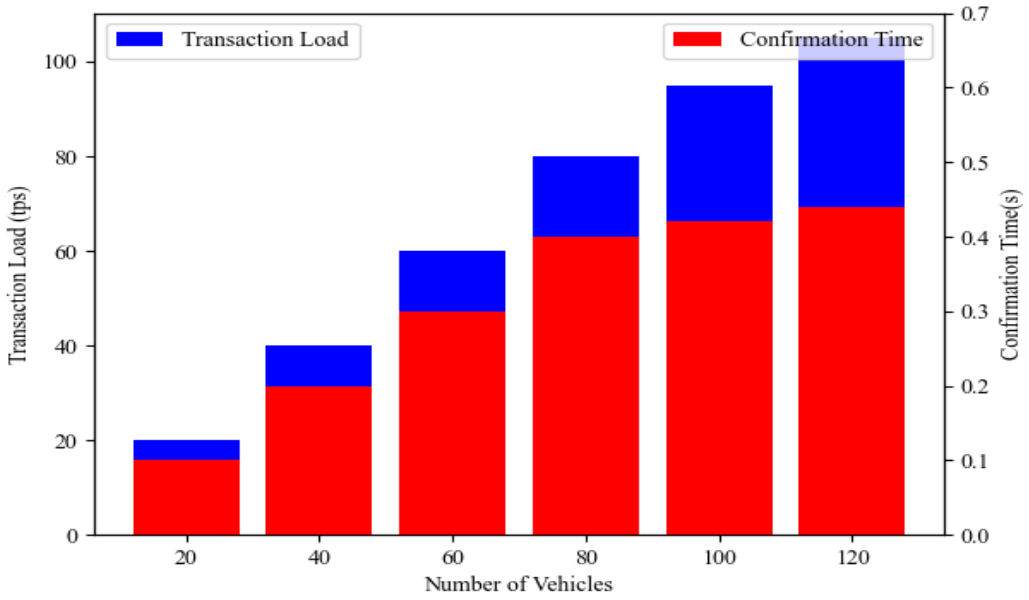

Fig. 7. Scalability analysis.

The observed discrepancy arises due to the current arrangement where consensus nodes are distributed around the network. As these nodes relocate, they may have challenges in establishing communication with other consensus nodes, leading to a decrease in the likelihood of successful consensus. The model under consideration successfully addresses this issue. Furthermore, it offers a highly effective method for detecting and recognizing malevolent communications. Success is attained just by messages that are deemed valid and reliable, as surrounding nodes tend to reject other events on account of doubts over their trustworthiness. The proposed system localizes communication and significantly reduces the computational overhead on any single node by dividing the V2X network into regions and sub-regions. This localized approach ensures that each region can autonomously maintain a high success rate without being overwhelmed by the total network load. The success rate in the proposed system remains consistently high, with approximately 96% for 20 vehicles and 94.1% for 120 vehicles compared with the existing systems [41][44], as illustrated in **Fig. 8**. This indicates that the system can efficiently manage communication, regardless of the network's size. Conversely, the current system shows a lower initial success rate, which gradually increases as the number of nodes rises. This demonstrates its efficacy and scalability in managing a large number of nodes. Furthermore, **Fig. 9** compares our proposed system to the existing one in terms of consensus time. This comparison shows that our system has a higher success rate, implying it requires less consensus time under various network traffic conditions.

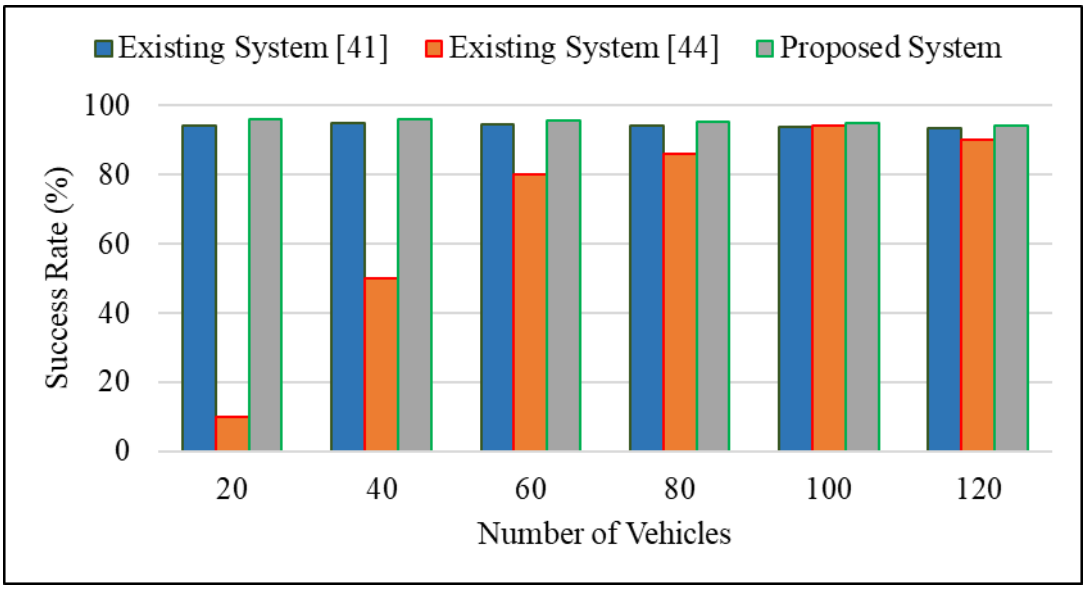

Fig. 8. Comparison of success rate with an existing system based on the number of nodes.

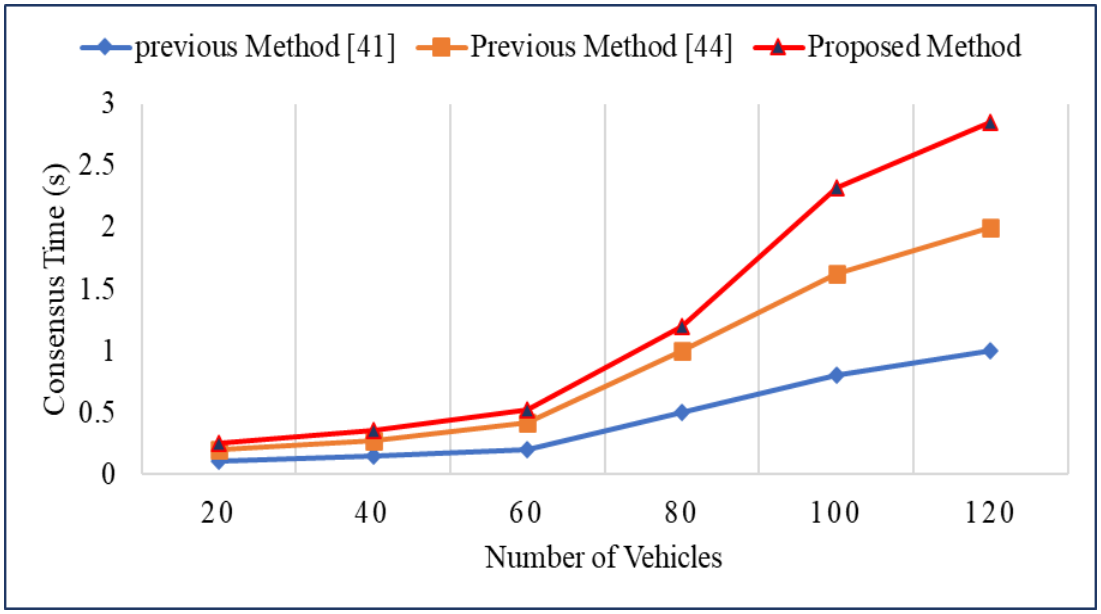

Fig. 9. Comparison of success rate with an existing system based on the latency.

The simulation results clearly show the effectiveness of our proposed system in efficiently managing high transaction volumes, resulting in significantly reduced delays compared to current solutions. As the transaction load increases, the delay in current solutions becomes more pronounced due to the sequential process of block creation and validation. On the other hand, our suggested architecture showcases a smoother rise in delay, as a result of the parallel processing capability of the DAG structure and the region-oriented approach that focuses on localizing transaction processing. Furthermore, the network's organization by region and

subdivision into sub-regions allows our system to effectively manage confirmation delays, even during periods of high transaction volume. Every RSU efficiently manages transactions within its assigned region, which helps to minimize the overall computational and communication difficulties.

3.8 Security and Privacy Analysis

In this study, we examine the system's capacity to withstand prevalent security threats [45] with use cases, such as unauthorized access, message tampering, replay attacks, Sybil attacks, and denial-of-service attacks. The primary objective of privacy analysis is to evaluate the safeguarding of confidential data and to ensure that the system's design effectively upholds the privacy of V2X participants. Our proposed system incorporates various privacy-preserving mechanisms to guarantee the privacy of V2X participants. The system utilizes anonymization techniques to safeguard the privacy of vehicles and drivers, with every vehicle using temporary pseudonyms instead of permanent identifiers when communicating with other vehicles or infrastructure. These pseudonyms are regularly updated to avoid any potential tracking or linkage attacks. Data transmitted within the V2X network is securely encrypted using strong cryptographic algorithms, ensuring the security of intercepted data to prevent unauthorized access or tampering. We implement end-to-end encryption for secure communication between vehicles and RSUs, as well as between RSUs and edge nodes. Access to sensitive information is carefully regulated using access control mechanisms, with access to and modification of certain types of data restricted to authorized entities with the required cryptographic credentials. Consider the following example of how the vehicles verify the authenticity of the message during the message transaction. The process begins with the initialization phase, during which Vehicle A registers with RSU1, joins the network, and shares its public key. Vehicle A generates a message that reads, "Obstacle ahead at GPS coordinates," and uses its private key to sign it to notify other vehicles of an obstacle on the road. The message, which includes Vehicle A's digital signature and public key, is then broadcast to nearby vehicles and RSUs. Upon receiving the message, Vehicle B retrieves Vehicle A's public key and verifies the digital signature, confirming the message's authenticity and integrity. RSU1 also receives and verifies the message, recording it in its local DAG ledger.

3.8.1 Use Case: Message Tampering Attack

The architectural design of the proposed system utilizes cryptographic methodologies, such as digital signatures and hash functions, to provide robustness against message manipulation. The sender digitally signs each message, ensuring both integrity and authenticity. Any alteration made to the message will render the signature invalid, thereby notifying the recipient of any attempts to tamper with it. The security of the DAG-based architecture is enhanced due to its distributed nature, which involves the validation and verification of messages by numerous nodes. Additionally, the consensus method serves to guarantee unanimity regarding the sequence and legitimacy of events, thus mitigating the potential for unauthorized manipulation. This use case demonstrates how a malevolent actor would try to alter messages and how the system would respond to mitigate the threat.

Action Scenario:

Actors: Several primary actors fulfill discrete functions within the framework of the V2X network. The attacker known as the Malicious Actor wants to change the messages sent across the V2X network. Vehicles are assigned as authorized V2X-enabled nodes that are actively involved in the communication operations of the network. RSU and Edge units are equipped to facilitate secure communication and manage regional DAG ledgers.

Preconditions: There is active communication between vehicles and RSU on the functioning V2X network. Vehicles are now registered with RSUs, and the DAG ledger is preserving transaction integrity. The proposed consensus technique is used by the network to secure communications, guaranteeing reliable communication and data integrity.

Steps of the Attack:

Preparation: Malicious actors can intercept the communication channel between vehicles and RSUs, either by gaining physical access to network hardware or by utilizing software vulnerabilities.

Message Tampering: It is important to be aware of potential security threats. In this case, the attacker can manipulate intercepted messages, changing important details like traffic updates, collision warnings, and navigational instructions. The intention is to interfere with regular V2X activities by forwarding the altered messages to other network nodes or their intended receivers.

Propagation: Messages that have been tampered with spread across the V2X network via the gossip protocol. The act of vehicles and RSUs receiving these messages could result in potential hazards and disruptions due to the erroneous information they may contain.

Impact: When vehicles receive tampered messages, there is a risk of incorrect decisions being made, which could lead to traffic accidents or inefficient route planning. Furthermore, if tampered messages are recorded as legitimate transactions, it undermines the integrity of the DAG ledger.

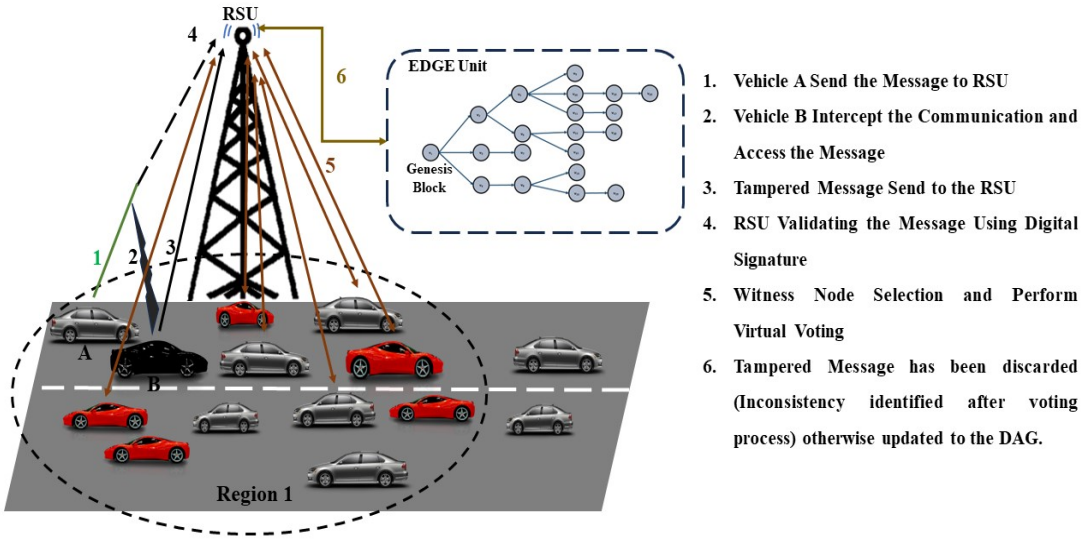

Fig. 10. Handling message tampering attack

Proposed System Response: **Fig. 10** illustrates the system's response to a message tampering attack in the proposed setup. As part of the detection process, the RSUs continuously validate the integrity of received messages using cryptographic hashes and digital signatures. Real-time analysis and comparison with known valid data helps detect anomalies in message contents and patterns. RSU sends the received message to the other nodes present in the selected region for the voting process. When messages are tampered with, they are unable to reach a consensus because the cryptographic verification processes and voting process detect inconsistencies in the integrity of the messages. When the RSU detects tampered messages, it takes immediate action to isolate the compromised communication channels. This is done to

stop the spread of falsified information and prevent any further damage. When nodes are compromised, they are flagged and their credentials are temporarily revoked while we investigate the situation. At the same time, the system implements protocols to remove any tampered entries from the DAG ledger. Messages that have been verified and validated are redistributed to replace any that have been tampered with, thus restoring the network to a state of trust. RSUs keep thorough records of detected tampering attempts and invalidated messages for auditing.

3.8.2 Use Case: Replay Attack

Replay attacks pose a major risk to the credibility and timeliness of V2X messages in the proposed system. In this use case, we will explore a situation where a malicious actor tries to carry out a replay attack. We will also discuss how the system responds to this threat and takes measures to mitigate it. The actors and preconditions for this use case are similar to those for the previous use case that dealt with a message tampering attack. Thus, we take into account the identical actors and preconditions.

Steps of the Attack:

Preparation: Valid V2X communications exchanged between vehicles and RSUs are captured and stored by the malicious actor for later use. This can be accomplished by intercepting the channel of communication.

Replay Attack Execution: When carrying out a replay attack, the attacker resends the intercepted messages into the V2X network at a later point in time. The goal is to deceive vehicles and RSUs into treating these messages as current and legitimate. These repeated messages may contain important information such as traffic alerts, navigation instructions, or safety warnings.

Propagation: The messages are spread throughout the V2X network using the gossip protocol. When vehicles and RSUs receive these messages, they may act on the outdated information, which can result in potential hazards and disruptions.

Impact: Receiving replayed messages can lead to vehicles making incorrect decisions, which could result in traffic accidents or inefficient route planning. Replaying messages as new transactions could potentially compromise the integrity of the DAG ledger.

Proposed System Response

The RSUs and vehicles consistently verify the timestamps and unique identifiers of received messages through cryptographic techniques. Real-time analysis and comparison with the current state of the DAG ledger help detect anomalies in message timing and sequence. When replayed messages are detected, the system takes immediate action to isolate the compromised communication channels. This helps to stop the spread of outdated information and prevent any further issues. When nodes are compromised, they are promptly flagged and their credentials are temporarily revoked while we conduct a thorough investigation. The proposed consensus mechanism guarantees that only messages validated by a majority of honest nodes are accepted into the DAG ledger. Replayed messages struggle to reach a consensus due to discrepancies in message timing and uniqueness detected by the cryptographic verification processes. The system implements protocols to remove duplicated entries from the DAG ledger. Messages that are no longer up-to-date are replaced with accurate ones, ensuring the network is reliable. The RSUs keep thorough records of identified replay attempts and invalidated messages for auditing.

3.8.3 Unauthorized access

The suggested system architecture for V2X communication bolsters resilience against unauthorized attacks by employing various measures such as consensus mechanisms, cryptographic approaches, identity management, network segmentation, and other related strategies. The system ensures that only entities that have been verified and permitted can engage in participation. It also detects and prevents any instances of unauthorized access. Furthermore, it safeguards the integrity and confidentiality of the data involved.

3.8.4 Sybil attacks

Sybil attacks involve a malicious node creating numerous false identities to manipulate the network, often disrupting operations or gaining illegitimate advantages. The proposed method effectively combats such attacks by implementing identity verification through blockchain technology. Each vehicle or node in the V2X network receives a unique cryptographic identity linked to a long-term certificate. This identity is securely stored on the blockchain, ensuring permanence and verifiability. When a vehicle transmits data, RSU verifies its identity by checking blockchain records. If multiple identities claim the same source or display unusual behavior, the system flags them for further scrutiny. This process ensures that only reliable nodes can validate transactions and add new blocks, thwarting attempts by malicious nodes to flood the network with fake identities. The proposed method guarantees that only nodes with verified identities participate in the validation process.

3.8.5 Denial of Service (DoS)

DoS attacks are designed to impede the regular operation of a network by inundating it with an excessive quantity of malevolent requests. Region-based partitioning is an effective strategy for mitigating the effects of attacks on specific regions and minimizing the overall attack surface. However, there is a potential vulnerability in the form of a distributed denial-of-service (DDoS) attack, when numerous malevolent nodes collaborate to launch simultaneous attacks from diverse locations, therefore overwhelming the system. In order to mitigate the risk of DoS attacks, the system must incorporate rate limitation, traffic filtering, and intrusion detection mechanisms. These tools can detect and alleviate atypical traffic patterns that are linked to DoS attacks. In addition, the decentralized block creation process can serve as a line of defense, as only nodes within particular regions participate in consensus.

3.8.6 Spoofing Attacks

Spoofing attacks encompass the deliberate actions of malevolent individuals who assume the identity or guise of authentic entities or authoritative sources of information. Cryptographic approaches are of paramount importance in guaranteeing the validity and integrity of this architectural framework. Digital signatures are employed to affix signatures to messages, thereby validating their source and deterring any unwanted alterations. The proposed system offers a resilient and secure repository of transactions and communications, rendering it arduous for falsified information to be acknowledged as legitimate. Furthermore, the utilization of consensus techniques guarantees that messages undergo validation from numerous nodes inside the network, hence diminishing the probability of accepting falsified data. The architectural framework can additionally utilize authentication protocols to authenticate the identity of the nodes involved and mitigate illegal access. Through the integration of these security measures, the architecture based on DAG fortifies its ability to

withstand spoofing assaults, hence augmenting the credibility and dependability of V2X communication.

3.9 Discussions

The infrastructure costs of edge computing are substantial, requiring investment in hardware such as edge servers and networking equipment, especially for large-scale implementations. However, the proposed system leverages peripheral computing to improve cost-effectiveness and optimize operations in various ways. Firstly, edge computing enhances system performance by reducing latency, essential for real-time applications like traffic management and collision avoidance, by processing data closer to vehicles. This approach eliminates the need for extensive centralized resources. Secondly, it reduces bandwidth costs by decreasing the amount of data transmitted to centralized servers, which becomes increasingly advantageous as data volumes grow. Thirdly, the system's modular approach allows for incremental scalability, simplifying expansion and spreading costs over time, with local edge nodes managing regions and sub-regions. Finally, local data processing reduces the risk of data intrusions and the associated costs of data protection, thereby improving security and privacy.

Limitations of Simulation Tool Vs Real-world Scenarios: Optimum performance metrics are frequently achieved in our simulation tool (Veins) due to the abundance of computational resources, which can be scaled as necessary. Conversely, the processing speed and overall performance of the system can be impacted by the limited computational capacity and energy resources of real-world RSUs and vehicular onboard units (OBUs). While our simulation tool can replicate packet loss, interference, and signal degradation, it may fail to adequately represent the complexity of real-world scenarios. At the same time, the complexities and interdependencies of large-scale real-world deployments may not be completely captured by our simulation, which tests scalability by artificially increasing the number of vehicles from 20 to 120 and conducting transactions. The latency experienced in the real world may be more variable and higher due to network congestion, physical obstructions, and the varying quality of network infrastructure.

Interoperability Issues: To optimize communication processes and improve compatibility within the V2X network, the proposed system implements a singular protocol format. This design decision simplifies protocol management, reduces overhead, and ensures that all devices within the network communicate seamlessly using the same standards. At the same time, to facilitate interoperability with various V2X communication protocols, a specialized automation tool is implemented in the edge devices. This tool functions as an intermediary, translating and converting messages into a single protocol format. Service providers also play a crucial role in managing and maintaining interoperability within the V2X network. They are responsible for deploying and maintaining specialized automation tools in peripheral devices, monitoring communication channels, and resolving any interoperability issues.

3.10 Open Issues and Challenges in Real-World Implementation

The simulation results provide preliminary validation of the security and efficacy of the proposed architecture. However, transitioning from simulation to real-world implementation presents a series of challenges that may impact the system's reliability and efficacy. These challenges stem from the complexities of real-world vehicular networks and the differences between controlled simulation environments.

The primary advantages of DAG for real-time processing include mitigating network latency and communication delays. Our simulation assumed optimal network conditions with

minimal, repeatable latency. However, in the real world, interference, signal obstruction, and varying distances between nodes can result in substantial variations in network latency.

Real-time processing faces significant challenges due to the variability in-vehicle hardware and infrastructure. It experiences inconsistencies in performance, reliability, and RSU configurations. Weather conditions, physical obstructions, and electromagnetic interference are omitted in our simulation. However, these factors must be accounted for in real-world implementations, as they can adversely affect the network's overall efficacy, including signal strength and communication range. Real-time processing is significantly impeded by the unpredictable and dynamic behavior of vehicles. In simulations, vehicle behavior follows predetermined, predictable patterns and protocols. In reality, vehicle behavior is highly dynamic, influenced by human drivers, varying traffic conditions, and spontaneous events such as accidents or roadblocks. This unpredictability can compromise the consistency and reliability of the V2X communication system.

Blockchain Updates and Their Computing Demands: The incorporation of blockchain into edge-enabled vehicular networks results in a significant volume of data transactions, which encompasses information storage, resource management, and vehicle transactions. Significant resources are consumed by high-density networks that consist of a multitude of heterogeneous and resource-limited devices. It may be difficult to satisfy the resource requirements for blockchain to process large-scale transactions. Furthermore, the consensus mechanism of blockchain necessitates a significant amount of network resources, including transmission power, mining, and bandwidth, resulting in high latency.

Complexities of Tuning RSU Region*:* In the real world, V2X networks face numerous challenges due to their dynamic nature, which involves the continual entry and exit of vehicles, as well as changes in speed and direction. This makes it difficult to maintain optimal region partitioning. Another concern is the complexity of parameter tuning, as each optimization method requires the meticulous adjustment of numerous parameters. This process is time-consuming and may not always yield the best results.

Scalability Challenges**:** In the real world, the V2X system to accommodate a large number of interconnected vehicles presents a scalability challenge. The computational burden increases as each node must manage a larger ledger and process more transactions. The real-time data exchange essential for traffic management and vehicle safety can be affected by increased latency due to the growing number of vehicles. Additionally, the complexity of maintaining a consistent and accurate ledger is heightened by the dynamic network topology, characterized by the constant entry and departure of vehicles.

4. Conclusion and Future Work

V2X communication is becoming increasingly important for transportation safety and efficiency, making every moment on the road safer and more productive. Our edge-enabled region-oriented DAG-based distributed ledger system deviates from traditional blockchain frameworks by incorporating DAG technology to facilitate instantaneous data processing and improved parallelism. The proposed system effectively addresses key challenges such as node mobility, scalability, and security. By dividing the network into regions managed by RSUs, the system ensures efficient handling of dynamic topology and high transaction loads. The fundamental design principle involves the utilization of regions overseen by RSUs to facilitate decentralized block formation, effectively mitigating transaction confirmation delays. The consensus mechanism presented in this work maintains the system’s resilience, even when confronted with malicious nodes. Specifically, the system’s robust security measures,

including PKI, digital certificates, reputation scores, and continuous authentication, effectively detect and mitigate malicious nodes. Our case study also clearly explains how our proposed system reacts when a malicious node is present in the V2X network and attempts to perform malicious attacks within the network. The incorporation of edge computing further reduces latency, thereby improving system responsiveness. The proposed framework provides a robust and instantaneous solution for communication between vehicles and various entities. Our framework has demonstrated its effectiveness through rigorous implementation and evaluation using the "veins" simulation tool. It successfully addresses the intricacies of real-world scenarios and provides strong measures for ensuring secure communication in V2X systems.

Although the proposed system is validated by the simulation results, real-world V2X communication systems may present behaviors and challenges that simulations do not fully capture. Environmental factors, such as varying weather conditions, road surfaces, and physical obstacles, can impact communication reliability and vehicle performance. Additionally, drivers exhibit unpredictable behaviors, such as sudden stops or erratic driving, which are difficult to model accurately in simulations. Furthermore, differences in infrastructure quality, including variations in RSU deployment and maintenance, can affect system performance. Therefore, in the future, we plan to apply our proposed work to real-world vehicular applications to identify performance challenges and discrepancies from the simulated environment.

References

[1] A. Moubayed, A. Shami, P. Heidari, A. Larabi, and R. Brunner, "Edge-Enabled V2X Service Placement for Intelligent Transportation Systems," *IEEE Transactions on Mobile Computing*, vol.20, no.4, pp.1380-1392, 2021. Article (CrossRef Link)

[2] F. Lyu, H. Zhu, N. Cheng, H. Zhou, W. Xu, M. Li, and X. Shen, "Characterizing Urban Vehicle-to-Vehicle Communications for Reliable Safety Applications," *IEEE Transactions on Intelligent Transportation Systems*, vol.21, no 6, pp.2586-2602, 2020. Article (CrossRef Link)

[3] D. Kanthavel, S.K.B. Sangeetha, and K.P. Keerthana, "An empirical study of vehicle to infrastructure communications - an intense learning of smart infrastructure for safety and mobility," *International Journal of Intelligent Networks*, vol.2, pp.77-82, 2021. Article (CrossRef Link)

[4] F. G. Pratticò, F. Lamberti, A. Cannavò, L. Morra, and P. Montuschi, "Comparing State-of-the-Art and Emerging Augmented Reality Interfaces for Autonomous Vehicle-to-Pedestrian Communication," *IEEE Transactions on Vehicular Technology*, vol.70, no.2, pp.1157-1168, 2021. Article (CrossRef Link)

[5] M. A. Naeem, X. Jia, M. A. Saleem, W. Akbar, A. Hussain, S. Nazir, and K. M. Ahmad, "Vehicle to Everything (V2X) Communication Protocol by Using Vehicular AD-HOC Network," in *Proc. of 17th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, pp.384-388, 2020. Article(CrossRefLink)

[6] K. Kiela, V. Barzdenas, M. Jurgo, V. Macaitis, J. Rafanavicius, A. Vasjanov, L. Kladovscikov, and R. Navickas, "Review of V2X–IoT Standards and Frameworks for ITS Applications," *Applied Sciences*, vol.10, no.12, 2020. Article (CrossRef Link)

[7] J. W. Wedel, B. Schünemann, and I. Radusch, "V2X-Based Traffic Congestion Recognition and Avoidance," in *Proc. of 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks*, pp.637-641, 2009. Article(CrossRefLink)

[8] C. R. Storck and F. Duarte-Figueiredo, "A Survey of 5G Technology Evolution, Standards, and Infrastructure Associated With Vehicle-to-Everything Communications by Internet of Vehicles," *IEEE Access*, vol.8, pp.117593-117614, 2020. Article (CrossRef Link)

[9] Y. Sadovaya and S. V. Zavjalov, "Dedicated Short-Range Communications: Performance Evaluation Over mmWave and Potential Adjustments," *IEEE Communications Letters*, vol.24, no.12, pp.2733-2736, 2020. Article (CrossRef Link)

[10] M. H. Bahonar, M. J. Omidi, and H. Yanikomeroglu, "Low-Complexity Resource Allocation for Dense Cellular Vehicle-to-Everything (C-V2X) Communications," *IEEE Open Journal of the Communications Society*, vol.2, pp.2695-2713, 2021. Article (CrossRef Link)
[11] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2X Access Technologies: Regulation, Research, and Remaining Challenges," *IEEE Communications Surveys & Tutorials*, vol.20, no.3, pp.1858-1877, 2018. Article (CrossRef Link)
[12] B. Fong, L. Situ, and A. C. M. Fong, "Smart Technologies and Vehicle-to-X (V2X) Infrastructures for Smart Mobility Cities," *Smart Cities: Foundations, Principles, and Applications*, pp.181-208, 2017. Article (CrossRef Link)
[13] W. Zhou, A. Islam, and K. Chang, "Real-time RL-based 5G Network Slicing Design and Traffic Model Distribution: Implementation for V2X and eMBB Services," *KSII Transactions on Internet and Information Systems*, vol.17, no.9, pp.2573-2589, Sep. 2023. Article (CrossRef Link)
[14] E. Mostajeran, R. M. Noor, M. H. Anisi, I. Ahmedy, and F. A. Khan, "A Realistic Path Loss Model for Real-time Communication in the Urban Grid Environment for Vehicular Ad hoc Networks," *KSII Transactions on Internet and Information Systems*, vol.11, no.10, pp.4698-4716, Oct. 2017. Article (CrossRef Link)
[15] A. Takacs and T. Haidegger, "A Method for Mapping V2X Communication Requirements to Highly Automated and Autonomous Vehicle Functions," *Future Internet*, vol.16, no.4, 2024. Article (CrossRef Link)
[16] Y. Gao, X. Xu, Y. L. Guan, and P. H. J. Chong, "V2X Content Distribution Based on Batched Network Coding With Distributed Scheduling," *IEEE Access*, vol.6, pp.59449-59461, 2018. Article (CrossRef Link)
[17] M. Dibaei, X. Zheng, K. Jiang, S. Maric, R. Abbas, S. Liu, Y. Zhang, Y. Deng, S. Wen, J. Zhang, Y. Xiang, S. Yu, "An Overview of Attacks and Defences on Intelligent Connected Vehicles," *arXiv:1907.07455*, 2019. Article (CrossRefLink)
[18] G. Twardokus and H. Rahbari, "Vehicle-to-Nothing? Securing C-V2X Against Protocol-Aware DoS Attacks," in *Proc. of IEEE INFOCOM 2022 - IEEE Conference on Computer Communications*, pp.1629-1638, 2022. Article(CrossRefLink)
[19] X. Zhang, L. Mu, J. Zhao, and C. Xu, "An Efficient Anonymous Authentication Scheme with Secure Communication in Intelligent Vehicular Ad-hoc Networks," *KSII Transactions on Internet and Information Systems*, vol.13, no.6, pp.3280-3298, Jun. 2019. Article (CrossRef Link)
[20] J. Huang, D. Fang, Y. Qian, and R. Q. Hu, "Recent Advances and Challenges in Security and Privacy for V2X Communications," *IEEE Open Journal of Vehicular Technology*, vol.1, pp.244-266, 2020. Article (CrossRef Link)
[21] M. A. Javed, M. Z. Khan, U. Zafar, M. F. Siddiqui, R. Badar, B. M. Lee, and F. Ahmad, "ODPV: An Efficient Protocol to Mitigate Data Integrity Attacks in Intelligent Transport Systems," *IEEE Access*, vol.8, pp.114733-114740, 2020. Article (CrossRef Link)
[22] Y. Ni, L. Cai, J. He, A. Vinel, Y. Li, H. Mosavat-Jahromi, and J. Pan, "Toward Reliable and Scalable Internet of Vehicles: Performance Analysis and Resource Management," *Proceedings of the IEEE*, vol.108, no.2, pp.324-340, 2020. Article (CrossRef Link)
[23] F. Abbas, P. Fan, and Z. Khan, "A Novel Low-Latency V2V Resource Allocation Scheme Based on Cellular V2X Communications," *IEEE Transactions on Intelligent Transportation Systems*, vol.20, no.6, pp.2185-2197, 2019. Article (CrossRef Link)
[24] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X Communication and Integration of Blockchain for Security Enhancements," *Electronics*, vol.9, no.9, 2020. Article (CrossRef Link)
[25] X. Xu, Y. Xue, X. Li, L. Qi, and S. Wan, "A Computation Offloading Method for Edge Computing With Vehicle-to-Everything," *IEEE Access*, vol.7, pp.131068-131077, 2019. Article (CrossRef Link)
[26] R. Li, Q. Li, J. Zhou, and Y. Jiang, "ADRIoT: An Edge-Assisted Anomaly Detection Framework Against IoT-Based Network Attacks," *IEEE Internet of Things Journal*, vol.9, no.13, pp.10576-10587, 2022. Article (CrossRef Link)

[27] I. Sarrigiannis, L. M. Contreras, K. Ramantas, A. Antonopoulos, and C. Verikoukis, "Fog-Enabled Scalable C-V2X Architecture for Distributed 5G and Beyond Applications," *IEEE Network*, vol.34, no.5, pp.120-126, 2020. Article (CrossRef Link)
[28] M. Rihan, M. Elwekeil, Y. Yang, L. Huang, C. Xu, and M. M. Selim, "Deep-VFog: When Artificial Intelligence Meets Fog Computing in V2X," *IEEE Systems Journal*, vol.15, no.3, pp.3492-3505, 2021. Article (CrossRef Link)
[29] K. Gai, K.-K. R. Choo, and L. Zhu, "Blockchain-Enabled Reengineering of Cloud Datacenters," *IEEE Cloud Computing*, vol.5, no.6, pp.21-25, 2018. Article (CrossRef Link)
[30] H. Zeyu, X. Geming, W. Zhaohang, Y. Sen, "Survey on Edge Computing Security," in *Proc. of 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, pp.96-105, 2020. Article(CrossRefLink)
[31] H. Chai, S. Leng, F. Wu, "Secure Knowledge Sharing in Internet of Vehicles: A DAG-Enabled Blockchain Framework," in *Proc. of ICC 2021 - IEEE International Conference on Communications*, pp.1-6, 2021. Article(CrossRefLink)
[32] Y. Li, X. Tao, X. Zhang, J. Xu, Y. Wang, and W. Xia, "A DAG-Based Reputation Mechanism for Preventing Peer Disclosure in SIoV," *IEEE Internet of Things Journal*, vol.9, no.23, pp.24095-24106, 2022. Article (CrossRef Link)
[33] I. Agudo, M. Montenegro-Gómez, and J. Lopez, "A Blockchain Approach for Decentralized V2X (D-V2X)," *IEEE Transactions on Vehicular Technology*, vol.70, no.5, pp.4001-4010, 2021. Article (CrossRef Link)
[34] M. Zichichi, S. Ferretti, and G. D'angelo, "A Framework Based on Distributed Ledger Technologies for Data Management and Services in Intelligent Transportation Systems," *IEEE Access*, vol.8, pp.100384-100402, 2020. Article (CrossRef Link)
[35] J. Hu, S. Chen, L. Zhao, Y. Li, J. Fang, B. Li, and Y. Shi, "Link level performance comparison between LTE V2X and DSRC," *Journal of Communications and Information Networks*, vol.2, no.2, pp.101-112, 2017. Article (CrossRef Link)
[36] K. Ansari, "Joint use of DSRC and C-V2X for V2X communications in the 5.9 GHz ITS band," *IET Intelligent Transport Systems*, vol.15, no.2, pp.213-224, 2021. Article (CrossRef Link)
[37] V. Vukadinovic, K. Bakowski, P. Marsch, I. D. Garcia, H. Xu, M. Sybis, P. Sroka, K. Wesolowski, D. Lister, and I. Thibault, "3GPP C-V2X and IEEE 802.11p for Vehicle-to-Vehicle communications in highway platooning scenarios," *Ad Hoc Networks*, vol.74, pp.17-29, 2018. Article (CrossRef Link)
[38] Y. H. Kwon, "Improving multi-channel wave-based V2X communication to support advanced driver assistance system (ADAS)," *International Journal of Automotive Technology*, vol.17, pp.1113-1120, 2016. Article (CrossRef Link)
[39] V. A. Patel, P. Bhattacharya, S. Tanwar, N. K. Jadav, R. Gupta, "BFLEdge: Blockchain based federated edge learning scheme in V2X underlying 6G communications," in *Proc. of 2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, pp.146-152, 2022. Article(CrossRefLink)
[40] J. Guo, X. Ding, W. Wu, and D.-Z. Du, "A Double Auction for Charging Scheduling among Vehicles Using DAG-Blockchains," *ACM Transactions on Sensor Networks*, 2024. Article (CrossRef Link)
[41] X. Zhang, R. Li, and H. Zhao, "A Parallel Consensus Mechanism Using PBFT Based on DAG-Lattice Structure in the Internet of Vehicles," *IEEE Internet of Things Journal*, vol.10, no.6, pp.5418-5433, 2023. Article (CrossRef Link)
[42] G. Du, Y. Cao, J. Li, and Y. Zhuang, "Secure Information Sharing Approach for Internet of Vehicles Based on DAG-Enabled Blockchain," *Electronics*, vol.12, no.8, 2023. Article (CrossRef Link)
[43] X. Zhang, R. Li, W. Hou, and H. Zhao, "V-Lattice: A Lightweight Blockchain Architecture Based on DAG-Lattice Structure for Vehicular Ad Hoc Networks," *Security and Communication Networks*, vol.2021, no.1, 2021. Article (CrossRef Link)

[44] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, "Towards secure and practical consensus for blockchain based VANET," *Information Sciences*, vol.545, pp.170-187, 2021. Article (CrossRef Link)

[45] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Computer Networks*, vol.151, pp.52-67, 2019. Article (CrossRef Link)

S. Thangam obtained his B.E. degree in Computer Science and Engineering from M.K University in 2004 and an M.E. degree in Computer and Communication Engineering from Anna University in 2008. Currently, he is a research scholar in the School of Computer Science and Engineering at Vellore Institute of Technology – Andhra Pradesh (VIT-AP) University. His research interests include cyber security, vehicular networks, and cloud computing. He focuses on enhancing the security of vehicle-to-everything communication by identifying and mitigating malicious attacks and ensuring the safety and security of vehicular communication networks.

S. Sibi Chakkaravarthy received the Ph.D. degree from Anna University, in 2018. He is currently working as an Associate Professor with the School of Computer Science and Engineering, Vellore Institute of Technology–Andhra Pradesh (VIT-AP) University. He is the Co-Ordinator of the Artificial Intelligence and Robotics (AIR) Research Center, at VIT-AP University. He is the Lead Engineer for the project VISU, an advanced 3D-printed humanoid robot developed by the VIT-AP. He is an active contributor to the open-source community and a lead writer in top security magazines, such as Pentestmag and eforensics. He is an Active Reviewer of many reputed journals, including IEEE, Springer, IET, IGI Global, and Hindawi. He was a recipient of the DST Fellowship.