






## Enhancing Data Dissemination Security and Quality Through the Authenticated Relay Selection and Scheduling Framework (ARSSF) in VANET

Abdulkareem Dawah Abbas<sup>1</sup>, Abidulkarim K.I. Yasari<sup>2</sup>, Mustafa Maad Hamdi<sup>3\*</sup>

<sup>1</sup> Department of Computer Engineering Techniques, College of Engineering, University of Al-Maarif, Al-Anbar 31001, Iraq

<sup>2</sup> Department of Electronics & Telecommunication, College of Engineering, Al-Muthanna University, Al-Muthanna 66001, Iraq

<sup>3</sup> Department of Computer Science, College of Computer Science and IT, University of Anbar, Al-Anbar 31001, Iraq

Corresponding Author Email: [mustafa.maad.hamdi@uoanbar.edu.iq](mailto:mustafa.maad.hamdi@uoanbar.edu.iq)

Copyright: ©2024 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/mmep.110906>

### ABSTRACT

**Received:** 25 August 2023

**Revised:** 10 November 2023

**Accepted:** 20 November 2023

**Available online:** 29 September 2024

#### Keywords:

*VANET, MANET, quality of service (QoS), data dissemination, authentication relay*

A Vehicular Ad Hoc Network (VANET) is an emergent wireless technology that enables high-speed communication. It became attractive to automobile manufacturers because of the secure information transmission without fatal accidents. It has several unique features, such as data dissemination, frequently disconnected networks during transmission, dynamic network density, and dynamic topology, that differentiate VANETs. Data dissemination is vital because it ensures the safety and performance of the vehicle. Conversely, VANET has limitations in providing effective communication between the vehicles due to delays and frequent disruptions. Thus, data dissemination needs an effective routing and scheduling process to avoid collisions of vehicles. Based on this fact, we proposed a novel Authenticate Relay Selection and Scheduling Framework (ARSSF) for secure and quality data transmission in VANET. ARSSF is a novel VANET communication method that prioritizes trustworthy relay nodes and dynamic scheduling to increase network performance and safety as data dissemination needs rise. It used the SNR, utility, and relay selection schemes for choosing the relay nodes that can cover the capacity of the network, thus minimizing the data dissemination delay. Additionally, an authentication method was utilized during the relay transmission phase to ensure both data security and authorization. The proposed framework performance was assessed by NS2 simulation. The results demonstrate that ARSSF is beneficial. ARSSF's minimum delay of 47 ms, throughput of 98.17%, and security measures of 98.38% show its value in VANETs. It enhances VANET safety, efficiency, and data distribution and could serve as a high-end vehicular network research platform.

## 1. INTRODUCTION

A VANET was created in accordance with the principles of a Mobile Ad Hoc Network (MANET) [1]. It automatically generates mobile devices within the vehicle's domain, where network communication is established, thus generating renewed interest in mobile communication applications. A VANET for vehicle-to-vehicle communication was introduced in 2001. Later, it was demonstrated for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), and vehicle to vehicle-to-the roadside unit (V2R) to ensure secured roadside services [2]. Subsequently, VANET has assumed a pivotal role in the development of the intelligent transport system (ITS) owing to its ability to facilitate a clear understanding of the boundaries of the Internet of Vehicle (IoV) and support the deployment of autonomous vehicles [3]. VANET communication leverages a variety of wireless networking technologies, including short-range radio technologies like ZigBee and Wi-Fi (WLAN), as well as cellular technologies such as LTE and visible light

communication (VLC) [4]. Owing to its efficient communication technologies, VANET serves a wide range of purposes, encompassing applications such as electronic brake lights, traffic information systems, platooning, on-road services, and emergency services in the domain of road transportation [5]. Concerning this matter, data distribution plays a critical role in delivering security and safety services to vehicles. Every vehicle situated within a designated Area of Interest (AoI) receives diverse information pertaining to congestion status [6], Information like local weather updates, traffic conditions, business advertisements, and more is received from the road side unit (RSU) [7]. The RSU's main purpose is to oversee the environment of the intelligent transportation system (ITS), traffic conditions, and weather status, thus transmitting the collision notices to the vehicles for safety. In short, such effective dissemination of traffic data enables to avoid accidents [8].

Modern transportation systems depend on VANETs for vehicle-to-vehicle and vehicle-to-infrastructure interaction. However, the full potential of VANETs in modern

transportation systems hinges on addressing the fundamental challenges that accompany their implementation. Among these challenges, data dissemination stands as a prominent concern. Ensuring that information reaches its intended recipients in a timely and accurate manner, particularly in dynamically changing environments, poses a significant hurdle. Reliability is also paramount, especially in the context of safety-related applications, as it necessitates robust communication even in the presence of network disruptions and interference. The integrity of safety-critical messages and the privacy of sensitive data must be protected, and the network must be secure to prevent attacks. Furthermore, technical factors like voltage and frequency regulation are important in VANETs. Effective data transfer and network performance need constant and precise monitoring and management of voltage and frequency levels within devices connected to a VANET. For reliable communication within VANETs robust and dependable, these parameters must always remain within prescribed ranges. The main issue addressed in this section is the challenge of data dissemination within Vehicular Ad Hoc Networks (VANETs). It is stressed how difficult it is to guarantee the timely and accurate dissemination of information, especially in contexts that are always evolving. In addition, the difficulties of ensuring data integrity in safety-critical applications are discussed, as are the requirements for precise control of voltage and frequency levels within VANETs to ensure efficient data transfer and network performance. Issues with maintaining network stability, random interactions that enhance collision likelihood, and high-time-variant mobile channels are additionally covered. Because of these issues, an Authenticate Relay Selection and Scheduling Framework (ARSSF) is required to fix the data distribution and network performance issues. The primary objective of VANET is to swiftly convey information with minimal delay and achieve the highest data transmission rate possible [9]. Typically, the propagation delay is calculated based on the duration it. Despite the assurance of minimum latency and uncertainty in the data dissemination process, the V2V channel modeling related to high-time variant mobile channels remains challenging [10]. Moreover, VANET faces constraints when it comes to initiating transmission requests during random interactions, consequently elevating the likelihood of collisions [11]. Hence, when a collision impacts the network, there is a risk of data loss, and this could potentially expose sensitive information to intermediate users, leading to security and privacy concerns [12]. Recent years have seen a surge in in-depth research aimed at analyzing diverse features and network structures within VANET, enhancing comprehension of data transmission strategies that can address the highly time-varying challenges involves developing random-channel protocols. However, these protocols have proven inadequate in sustaining network stability over extended periods, thus giving rise to security issues [13].

To overcome the shortcomings of VANET, an authentication framework is established in tandem with a central server to mitigate collision issues in the process of data dissemination [14]. In this study, the Authenticate Relay Selection and Scheduling Framework (ARSSF) is introduced, which utilizes relay node selection and dynamic scheduling to address issues related to data dissemination in VANETs. ARSSF is a novel VANET communication method that prioritizes trustworthy relay nodes and dynamic scheduling to increase network performance and safety as data

dissemination needs rise. The study aims to investigate its effects on VANET security and performance, including voltage and frequency variations, end-to-end delay, and network throughput. In real-world VANET scenarios, the research attempts to show its practical consequences. In this framework, the scheduling process used the feedback stage, relay nodes selection, and transmission that allowed maintaining the network coverage and latency. Furthermore, every message transmitted by the vehicles was subject to verification through the generation of a secret key and trust authority, ensuring the proper management of vehicle authorization [15]. The AoI region underwent thorough examination, with the vehicle's position and velocity being leveraged to monitor changes in the network. Consequently, the network gained the capability to anticipate potential relay nodes, thus reducing packet loss in VANET. This research yielded the following significant contributions:

- The issue of collisions in VANET was circumvented through the selection and transmission of relay nodes based on a central server, ensuring a more reliable network.
- The introduction of the novel Authenticate Relay Selection and Scheduling Framework (ARSSF) effectively minimized delays and reduced data transmission failures by incorporating relay nodes.
- Enhanced system reliability and quality were achieved by implementing authentication procedures for vehicles and transmitting packet details through a secret key generated by a trusted authority.
- The ARSSF played a crucial role in efficiently managing data security and vehicle authorization, as evidenced by the simulation results.

The organization of this paper is as follows: In Section 2, we provide an overview of related works, encompassing essential concepts, frameworks, and theoretical analyses of data dissemination within VANET. Section 3 delves into the proposed ARSSF, elaborating on its details. In Section 4, we evaluate the performance of the ARSSF. The paper conclusion in the final section.

## 2. RELATED WORK

Some researchers are handling the security issue. Al-Shareeda et al. [16] implemented a privacy-preserving communication scheme known as VPPCS in VANET was described. This scheme employed identity encryption and elliptic curve cryptography (ECC) techniques to secure the communication within VANET. The security of the VPPCS system was assessed using the Burrows-Abadi Needham (BAN) logic. The findings indicated that the devised scheme could resist different types of attacks, including man-in-the-middle, impersonation, and replay attacks. An intelligent V2V communication scheme, centered around Electric Vehicle (EV) pair matching and utilizing the Q-learning algorithm, was introduced by Li et al. [17]. This approach effectively minimized the computational burden associated with V2V service decision-making, streamlined the handling of charging-related concerns among EVs, and harnessed a charging coordination process to guarantee dependable communication. Furthermore, it leveraged a learning process to enhance the identification of EV locations, effectively addressing charging issues. The system introduced demonstrated a remarkable balance of flexibility and

reliability.

In work conducted by Singh et al. [18], the p-RSA scheduling (p-RSAS) algorithm was introduced to manage data quality in VANET within a dynamic cloud storage environment. It achieved comprehensive management of vehicle information using central control units. In emergency situations, it promptly notified the nearby police control room to facilitate user assistance. The p-RSA scheduling procedure incurred a bandwidth usage of 12.0 and an energy consumption of 5.56% during data allocation within the VANET environment. Shrivastava et al. [19] demonstrated the Multicast Energy-Efficient Data Scheduling (MEEEDS) algorithm was presented to handle data allocation within the VANET environment. The primary objective was to enhance throughput and reduce energy consumption during communication. The process began by analyzing the number of users and identifying the optimal data rates based on channel state information. Subsequently, similar users were grouped together for multicast transmission. The outcomes demonstrated a significant reduction in both energy consumption and computational complexity. In this study reported by Oliveira et al. [20], VANET traffic applications were analyzed for implementing a reliable data dissemination protocol for effective communication. The message was disseminated using the adaptive data dissemination protocol (ADDP) via the beacon periodicity. This process was discerned to minimize many message involvements, thus making the protocol flexible and reliable during data transmission in VANET. Liu et al. [21] implemented a VANET strategy that integrated cluster formation and probabilistic broadcasting to enhance data distribution efficiency. The process commenced by employing clustering techniques to assess vehicle information and driving data. Subsequently, multiple connected vehicles were grouped into clusters, and the probabilistic forwarding method was employed for information dissemination. Probability calculations were utilized to designate cluster heads and their corresponding members. Experimental results revealed that this approach effectively covered nearly the entire area of interest during transactions. Furthermore, the system exhibited minimal latency and maximized packet delivery ratios thanks to the probabilistic forwarding attributes.

Liu et al. [22] explored the concept of software-defined heterogeneous data distribution within the VANET setting, with the objective of addressing issues related to fog-assisted cooperative services. This was accomplished through the utilization of the Clique Searching Scheduling Algorithm (CSSA), which incorporated data encoding techniques for data transmission in foggy and cloudy conditions. The encoding process contributed to the overall feasibility and reliability of the system while reducing computational complexity. Various studies have indicated that data distribution challenges in VANET can be effectively tackled by implementing scheduling procedures. Despite the promising results of the proposed methods, challenges persist in terms of complexity, reliability, and security. The overall performance of VANET is impacted by these factors. To resolve these issues, we proposed a novel ARSSF that can improve the overall reliability and security of data dissemination in VANET. Finally, Hamdi et al. [23] presented the enhanced form of the multi-objective optimization technique came to be known as the adaptive jumping multi-objective firefly algorithm (AJ-MOFA). Following this, AJ-MOFA was fused with a clustering and forwarding approach (CFM). This approach

comprises three key elements. Initially, there is the clustering aspect, which employs cluster head score-based arbitration. The subsequent element involves a forwarding strategy utilizing probabilistic forwarding, and ultimately, the incorporation of AJ-MOFA. The configuration of the solution space within CFM is based on two variables: the first involves the forwarding probability, while the second concerns the upper limit for the number of nodes within a single cluster.

Vehicular Ad Hoc Networks are the focus of this investigation examining the literature on this field from data dissemination, security, and network performance perspectives. It points out where the current body of knowledge is lacking, such as a unified theory of data sharing, safety, and performance in VANETs. The choice of a particular study is contingent upon the precise priorities and objectives inherent to the VANET project in question. notwithstanding the merits of each study, and the study [23] emerges as particularly comprehensive, given its endeavor to confront an extensive spectrum of VANET challenges, encompassing intricacy, dependability, and security. Nevertheless, a more exhaustive assessment is requisite to ascertain its pragmatic efficacy. This research presents the Authenticate Relay Selection and Scheduling Framework (ARSSF), a safe, effective, and trustworthy option for Vehicular Ad Hoc Networks (VANETs). It utilizes relay node selection and dynamic scheduling to increase network speed and decrease latency without compromising security. The purpose of this research is to boost VANET efficiency.

### 3. ARSSF PROPOSED

As aforementioned, the information in the VANET environment is transmitted from V2V, V2I, and V2R. Particularly, vehicle-based communication in VANET requires extreme security and safety. Hence, ITS is required to deliver message transmissions of the highest quality, ensuring both complete security and trust in the information dissemination process. In this context, the primary goal of the recently introduced ARSSF is to enhance the security and safety of the transmitted vehicle data, as illustrated in Figure 1. Furthermore, the system's design must uphold the resilience and reliability of the messages being conveyed.

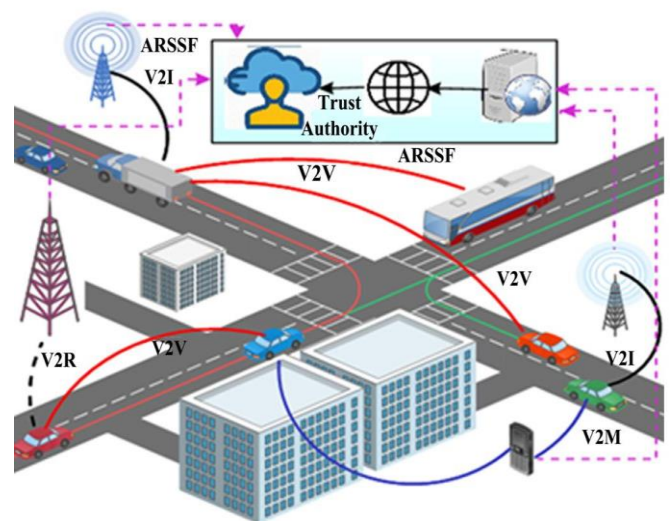
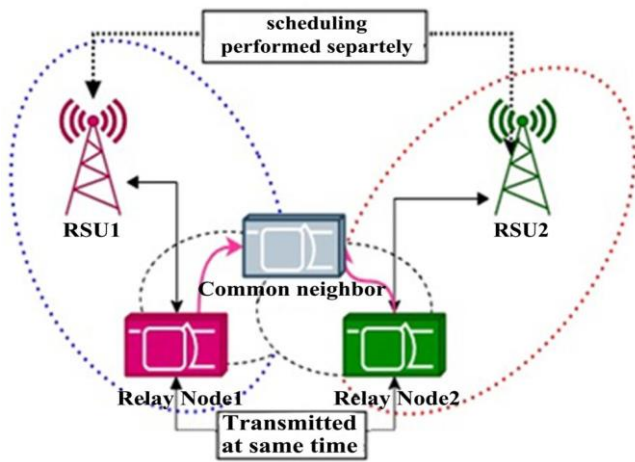


Figure 1. Overview of ARSSF architecture

The ARSSF is an infrastructure overhaul for VANETs that prioritizes data safety and quality. It implements registration and request methods and employs authentication and trust authorities to authenticate vehicle identities and decode data using secret keys. Collisions and delays are managed using a combination of signal-to-noise ratio (SNR) utility, relay node utility, and a relay selection technique. Reduced wait times and better adaptation to shifting vehicle locations result from constant feedback monitoring. The ARSSF emphasizes authentication of vehicles and selection of relay nodes, guaranteeing that only authorized vehicles can participate and considering the network's capacity and dependability.

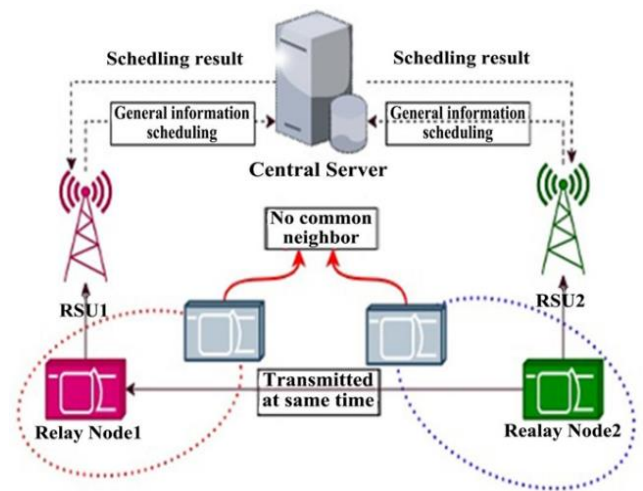
Figure 1 provides an overview of the ARSSF architecture in VANET, emphasizing security, authentication, and message robustness in both V2V and V2I communication facilitated by the RSU. The RSU plays a pivotal role in delivering information to end-users in the Area of Interest (AoI). Internet connectivity is established with the RSU, allowing the distribution of information to vehicles within its coverage (V2I) and to nearby vehicles requesting messages (V2V). Within the AoI, there are  $p$  RSUs denoted as  $R_1, R_2, \dots, R_p$ , and an ITS system with  $k$  vehicles denoted as  $U_1, U_2, \dots, U_k$ . Each vehicle ( $V_k$ ) within the RSU is equipped with a GPS system, enabling synchronized position data acquisition during data transmission. Notably, control channels and service channels are integrated into the data dissemination process to ensure system reliability.



**Figure 2.** RSU-guided relay node selection and collision resolution process

The process of data dissemination necessitated the involvement of control nodes in selecting relay nodes, as this allowed for the effective management of node capacity and coverage. In this network, each vehicle registered its information with the RSU. This approach offers a holistic view of the vehicle topology and scheduling process, facilitating a thorough understanding. A central node or server was consistently maintained to ensure collision-free operation during the communication process. However, in scenarios where two vehicles were adjacent but selected by different RSUs (e.g., RSU1 and RSU2), this situation could lead to contention and unintended scheduling conflicts among neighboring vehicles. Consequently, it was imperative to prevent collisions during data dissemination. This was achieved through a relay node selection process that also addressed collision avoidance, managed by the RSU as illustrated in Figure 2.

In Figure 3, we observe the collision-free selection of RSU nodes. Prior to the selection of RSU's relay nodes, a central server (CS) was established and linked to the RSU to oversee the scheduling process, as previously depicted. As mentioned earlier, the RSU had access to vehicle details, encompassing position, velocity, and vehicle decoding information, which it shared with the CS to assist in making scheduling decisions within the Area of Interest (AoI). The scheduling process involved three distinct phases: relay node selection, transmission, and feedback. These three phases were strategically utilized to establish a robust data dissemination approach within VANET. Additionally, the CS played a pivotal role in scheduling the vehicles, and the time interval between the two scheduling events represented the data dissemination cycle. This cycle included all three phases of the scheduling process.



**Figure 3.** Relay node selection process by RSU using a central server

### 3.1 Relay selection stage

During the initial phase, known as the relay selection stage, the decision-making process was overseen by the CS, and the selected nodes were subsequently passed on to the relay transmission stage. Inside the RSU, the number of transmission frames was denoted as  $(R=t_1, t_2, \dots, t_n)$ . For each transaction, the CS determined the relay selected node ( $\Omega_r$ ) with the goal of maximizing dissemination efficiency. Once the RSU had chosen the relay node for each transaction ( $r=1, 2, 3, \dots, R$ ), the vehicle's status transitioned from failure to success. Throughout the relay selection process, specific vehicle position and velocity information was required after the completion of the  $(t_{he\ r-1})$  frame. Let  $R_x$  represent the relay node involved in the ITS-RSU  $\{R_x \in RSU \cup U\}$ . In each transaction ( $r=1, 2, 3, \dots, R$ ),  $R_x$  had to be chosen. The Signal-to-Noise Ratio (SNR) of the node value was initially calculated to estimate the relay node. SNR played a crucial role in determining the node utility measure, as it considered both network coverage and energy levels. The relay value of  $R_x$  was determined from the vehicle  $U_k$ . The decoded packet was then calculated using the following process:

$$\gamma_{kn}^{t_r, R_x} = \sum_{i=1}^{r-1} \frac{P_k^i L_k^i \|h_k^i\|^2}{N_0 \epsilon_n} \hat{\beta}_{ikn}^{t_{i-1}} + \frac{P_{R_x} L_{R_x k}^{t_r} \|h_{R_x k}^t\|^2}{N_0 \epsilon_n} \hat{\beta}_{xn}^{t_{r-1}} \quad (1)$$

The calculation of the node utility value ( $\gamma_{kn}^{t_r, R_x}$ ) was based



on factors including the power transmission by the RSU ( $R_x$ ) denoted as ( $P_{R_x}$ ) and the path loss ( $L_{R_x k}^{t_r}$ ) in the transmission frame ( $t_r$ ) between vehicle  $U_k$  and  $R_x$ . The path loss ( $L_{R_x k}^{t_r}$ ) was influenced by the specific attributes of  $U_k$  and  $R_x$ , and can be represented as  $L_{R_x k}^{t_r} = f_L(d_{R_x k}^{t_r})$ . The value of  $R_x k$  was estimated using the distance between the vehicles  $U_k$  and  $R_x$  in the transaction frame ( $t_r$ ).

Therefore,  $R_x k = \sqrt{(X_{R_x}^{t_r} - X_k^{t_r})^2 + (Y_{R_x}^{t_r} - Y_k^{t_r})^2}$  was calculated from the position of  $R_x$  ( $X_{R_x}^{t_r}, Y_{R_x}^{t_r}$ ) and vehicle  $U_k$  ( $X_k^{t_r}, Y_k^{t_r}$ ) in  $t_r$ . The nodes ( $U$ ) positions were determined based on the  $t_f$  node feedback positions ( $X_U^{t_f}, Y_U^{t_f}$ ) of  $U$ . Thus, the obtained node position was  $X_U^{t_r} = X_U^{t_f} + v_U^X \cdot T_{rf}$  and  $Y_U^{t_r} = Y_U^{t_f} + v_U^Y \cdot T_{rf}$ . The  $U$  velocity ( $v_U^X, v_U^Y$ ) and frame as well as feedback time  $t_r$  and  $t_f$  were used to obtain the time distance and then for calculating the SNR value of the node in  $R_x$ . The average Signal-to-Noise Ratio (SNR) value was computed using the following equation to assess the node's average utility within the Area of Interest (AoI):

$$\hat{\beta}_{kn}^{t_r} = \begin{cases} 1, & \gamma_{kn}^{t_r, R_x} \geq \gamma_{th} \\ 0, & \gamma_{kn}^{t_r, R_x} < \gamma_{th} \end{cases} \quad (2)$$

The decoding status of packets by vehicles was assessed using Eq. (2) with the decoding threshold value ( $\gamma_{th}$ ). Similarly, the utility of  $R_x$  was computed based on the relay node's transmission frame ( $t_r$ ) as follows:

$$\Phi^{t_r, R_x} = \sum_{k=1, U_k \in N^r_{R_x}}^K \sum_{n=1}^N \varphi_{kn}^{t_r, R_x} \quad (3)$$

Subsequently, the utility ( $\Phi^{t_r, R_x}$ ) of the relay node was computed based on the utility of the vehicle ( $U_k$ ) in the context of packet  $X_n$  being decoded in time slot  $t_r$  ( $\varphi_{kn}^{t_r, R_x}$ ). These values, ( $\varphi_{kn}^{t_r, R_x}$ ), were calculated as the difference between  $\hat{\beta}_{ikn}^{t_{i-1}} - \hat{\beta}_{xn}^{t_{r-1}}$ . The set of neighboring nodes in  $R_x$  at time slot  $t_r$  was denoted as  $N^r_{R_x}$ . Following the calculation of the Signal-to-Noise Ratio (SNR) value ( $\gamma_{kn}^{t_r, R_x}$ ), the utility of the vehicle node for decoding packet  $X_n$  ( $\hat{\beta}_{kn}^{t_r}$ ) and the utility of the relay node in  $R_x$  for vehicle  $U_k$  ( $\Phi^{t_r, R_x}$ ) were determined. A relay selection scheme was then formulated to facilitate data dissemination. The relay node selection was determined based on the utility factor of nodes and  $R_x$  during time slot  $t_r$ . The chosen optimal nodes were denoted as  $\Omega_r = \{R_1^*, R_2^*, R_3^*, \dots, R_{L_r}^*\}$ . The relay node selection approach was derived from:

$$\max_{L_r, \Omega_r} \sum_{i=1}^{L_r} \Phi^{t_r, R_i^*} \quad (4)$$

$$N^r_{R_i^*} \cap N^r_{R_j^*} = \emptyset \quad i \neq j \quad \forall i, j = 1, 2, 3, \dots, L_r \quad (5)$$

$$\Phi^{t_r, R_i^*} > 0, \quad \forall i = 1, 2, 3, \dots, L_r \quad (6)$$

As data distribution commenced, the RSU at  $R_x$  initially possessed the utility value for the dissemination cycle. Leveraging this utility value, the system selected the first relay node, denoted as  $\Omega_1$ . However, with the increase in the number of vehicles and transmissions, the system encountered challenges associated with computational complexity. To

address this issue, a utility rate was calculated for the  $R_x$  packet decoding status, and a suboptimal relay selection scheme was implemented. As a result, the initial choice of the relay node was made in accordance with the maximum utility rate from  $R_{L_r}^*$ . When the relay node  $R_{L_r}^*$  shared common neighboring nodes with other nodes, the remaining nodes were removed. The candidate relay node included a set of  $R_x$  and  $U_k$ , represented as  $\{RSU(R_x) \cup U_k\}$ . Initially, the chosen relay node ( $L_r$ ) was set to 0, and the set of chosen relay nodes was not empty, denoted as  $\Omega_r \neq \emptyset$ . Consequently, for the subsequent relay node selection,  $L_r$  was incremented ( $L_r = L_r + 1$ ), and the node was chosen from set A based on the maximum utility of  $R_{L_r}^*$  (as described in Eq. (4)). The selected node was then added to the  $\Omega_r$  set, which can be defined as  $\Omega_r \leftarrow \Omega_r \cup \{R_{L_r}^*\}$ . Collisions were prevented by removing common neighboring nodes from set A with respect to  $R_{L_r}^*$ .

Following that, the set A was modified as  $\mathcal{A} \leftarrow \mathcal{A} - \{\hat{R} | N^r_{\hat{R}} \cap N^r_{R_{L_r}^*} \neq \emptyset\} (R_{L_r}^* \neq \emptyset)$ . Finally, the selected relay nodes were updated within  $\Omega_r$ . Once the relay node selection was completed, the packet decoding status of vehicle  $U_k$  was refreshed with each transmission  $t_r$  using the following equation:

$$\hat{\beta}_{kn}^{t_r} = \begin{cases} \hat{\beta}_{kn}^{t_r, R_k^*}, & \text{if } U_k \in N^r_{R_k^*} \in \Omega_r \\ \hat{\beta}_{kn}^{t_{r-1}}, & \text{otherwise} \end{cases} \quad (7)$$

The subsequent relay node selection for transmission ( $t_{r+1}$ ) was determined based on  $\hat{\beta}_{kn}^{t_r}$ . This approach effectively reduced collisions and effectively managed network capacity.

### 3.2 Relay transmission stage

The output of the relay selection phase was employed to facilitate the transmission of both vehicle and RSU data according to a predetermined schedule. This transmission process was characterized by time slots  $t_1, t_2, t_3, \dots, t_r, t$ , which denoted the selection of relay nodes from  $\Omega_r$ , where  $\Omega_1$  represented the first relay node, and  $\Omega_r$  was the final relay in the data transmission chain. The duration of each time slot  $t_r$  was denoted as  $t_r$ . A relay node was selected for each time slot  $t_r$  and subsequently decoded using the space-time network coding technique. This packet decoding process significantly enhanced the efficiency of data dissemination. Prior approaches entailed sending packets from the roadside unit to vehicles without utilizing acknowledgment procedures. Nevertheless, the systems security and reliability were ensured through the application of an authentication procedure. Consider a packet  $X = \{X_n | n=1, 2, \dots, N\}$  disseminated within the Area of Interest (AoI) using a relay node-based scheduling process. This packet contained several pieces of confidential information and symbols that needed protection from external interference. As a result, each node involved in the transmission phase underwent authentication by the Trust Authorities (TA) by possessing a unique node ID and generating a private key ( $\theta_{TA}$ ) using the hash function  $h(\cdot)$ , as indicated by the following equation:

$$\theta_{TA} = h(\text{ID}_{TA} || \mathfrak{R}_{TA}) \quad (8)$$

The private key  $\theta_{TA}$  was derived from the TAs ID and the random number,  $\mathfrak{R}_{TA}$ , generated by the TA. It necessitated either an input packet  $X_n \in X$  or a message length, and the

resultant output was converted into 128 bits. Security measures were implemented by utilizing the MD5 hash function, which divided the data block into 16 sub-blocks, each containing 32 bits. The result was obtained by concatenating the 32-bit segments from four groups. This methodology was applied within the framework of VANET communication, users were required to register their vehicles  $U_k$  with their ID ( $ID_{U_k}$ ) and security key ( $S_{U_k}$ ). This registration process was designed to reduce computational overhead when the respective vehicles entered the communication environment. Vehicle registration with specific parameters was accomplished as follows:

$$U_k = h(ID_{U_k} || S_{U_k}) \quad (9)$$

Vehicle-related attributes, including position and velocity, were computed, and the vehicle information was consolidated as  $\mu_{U_k} = A_{U_k} + B_{U_k}$ , which was then relayed to the Trust Authority (TA). Upon receiving  $\mu_{U_k}$ , the TA generated a random number for executing the hash function. This hash function played a critical role in authenticating the vehicles during data dissemination in VANET. Subsequently, the TA computed the trust factor using.

$$\rho_{TA} = h(\mu_{U_k} || U_k) \oplus \theta_{TA} \quad (10)$$

The resulting hash value of the trust authority,  $h_{TA}$ , and  $\theta_{TA}$  were communicated to the vehicle. This procedure played a crucial role in authenticating the user vehicle and enhancing security during data transmission within the VANET environment. The computed Trust Authority (TA) factors were verified by comparing the transmitted information with the registered details. When a match was confirmed, the user gained authorization to share data. Additionally, the data transmission process for the connection was validated through a request and reply message verification process, thereby ensuring the security of data dissemination.

#### A. Request message

When vehicle  $U_1$  intended to transmit a message to  $U_2$ , it initiated the process by sending a request to  $U_2$  while monitoring the request time. Meanwhile,  $U_1$  generated the trust authority factors  $\mu_{U_k}$  and the hash value associated with  $U_2$ . Subsequently, with the assistance of the Roadside Unit (RSU), the vehicle segregated these factors and computed the secret key for the trust authority (TA) as follows:

$$\sigma_{TA} = h(\mu_{U_k} || \omega_{U_k}) \oplus \theta_{TA}; \omega_{U_k} = I(D_{U_k} || h_{TA}) \quad (11)$$

The definition of the transmission request was as follows:

$$T_{U_k} = h(\theta_{TA} || S_{tx}) \oplus \mu_{U_k} \quad (12)$$

$$S_{U_k} = T_{U_k} \oplus \mu_{U_k} \oplus \theta_{TA} \quad (13)$$

Ultimately, the message transmission request was created, incorporating a timestamp ( $S_{tx}$ ) determined by the following relationship.

$$\eta_{U_k} = Req \oplus T_{U_k} \oplus \theta_{TA} \oplus S_{tx} \quad (14)$$

The derived  $\theta_{TA}$  and hash  $h_{TA}$  value were transmitted to vehicle  $U_k$ . Upon receiving the request message, the generated

factors ( $\mu_{U_k}$ ,  $\omega_{U_k}$ ,  $h_{TA}$ , and  $\sigma_{TA}$ ),  $h_{TA}$ , and  $\sigma_{TA}$ , were retained in the database for subsequent verification.

#### B. Relay transmission stage

Vehicle  $U_2$  received the request message  $\eta_{U_k}$ . In the preceding step, the factors ( $T_{U_k}, \eta_{U_k} \wedge S_{tx}$ ) were designated as  $S_{rx}$ . The request timestamps were compared with the system factor  $\alpha S1$ , and if there was a delay in transmission, it was determined by  $S_{rx} - S_{tx} \geq \alpha S1$ . When this condition was met, the received factors ( $T_{U_k}, \eta_{U_k} \wedge S_{tx}$ ) were considered expired, thereby ensuring the security of data transmission. Subsequently,  $U_2$  recalculated the secret key as  $S_{U_k}$  and the hash factor  $h_{U_2} = T_{U_k} \oplus h$  via:

$$\widehat{S_{U_k}} = T_{U_k} \oplus h_{U_2} \oplus \theta_{TA} \quad (15)$$

The request message was scrutinized as  $Req = \eta_{U_k} \oplus T_{U_k} \oplus \theta_{TA} \oplus S_{tx}$ , and it was validated by vehicle  $U_1$  through the computation of two factors using the provided parameters.

$$F_{U_2} = h(h_{U_1} || \widehat{\alpha S1} || \theta_{TA}) \quad (16)$$

$$L_{U_2} = F_{U_2} \oplus \theta_{TA} \oplus \widehat{\alpha S1} \oplus h_{U_2} \quad (17)$$

Upon the computation of these parameters, the confirmation was established, and the response was provided in a decrypted format.  $EN_{reply}$  was defined as  $ECD_{F_{U_2}}$ . Subsequently, the response was forwarded to the original request as  $\{EN_{reply}, L_{U_2}\}$ . The successive generation of these factors played a crucial role in maintaining data confidentiality and consequently reducing computational time.

#### C. Communications units

After receiving a response from  $U_2$ , vehicle  $U_1$  accepted and stored the trust authority's incoming factors. Following this,  $S_{rx}$  examined the reply message  $\{EN_{reply}, L_{U_2}\}$  to determine the response delay. Subsequently, the delay was calculated as  $S_{rx} - S_{tx} \geq \alpha S2$ . If this condition was met, the vehicle engaged with another vehicle; otherwise, the communication was terminated. Finally, the reply messages were decrypted to retrieve the original dissemination message as per:

$$Reply = DCP_{F_{U_2}}(EN_{reply}) \quad (18)$$

$$\widehat{F_{U_2}} = L_{U_2} \oplus \theta_{TA} \oplus S_{U_k} \oplus h_{U_1} \quad (19)$$

In summary, in a VANET environment, the exchange of information among vehicles was carried out with a primary emphasis on ensuring system authentication, security, and reliability, all of which hinged on the decryption process.

### 3.3 Feedback stage

$TAS_{U_k}$  in the communication process between vehicles  $U_k$ , collisions were prevented by verifying that there were no neighboring vehicles with which they were already acquainted. Moreover, the issue of collisions was resolved by coordinating vehicle allocation through the control channel during the feedback phase. With each transaction  $t_r$ , the feedback system maintained the currency of vehicle information, encompassing  $TA$ ,  $S_{U_k}$ , and hash factors. All information, block transformations, and control channel details within the

feedback phase were consistently renewed and applied in subsequent transactions. As vehicles transitioned from one Central Server (CS) range to another within a single dissemination cycle, a new CS was established based on the feedback section. Consequently, the old CS was removed from the list of registered vehicles, which effectively prevented collisions during communication. These three phases were carried out periodically, ensuring the execution of data dissemination. In summary, the system was engineered to provide dependability, security, authentication, and efficient data distribution while minimizing computational complexity and time constraints.

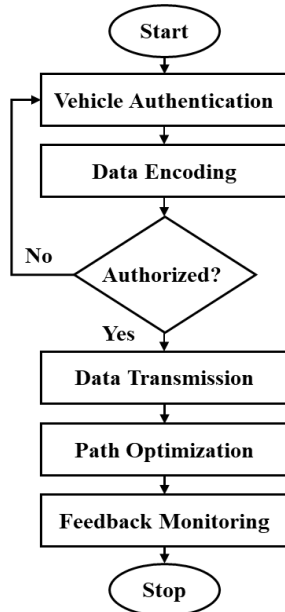


Figure 4. Flowchart of ARSSF algorithm

The flowchart in Figure 4 illustrates the logic behind the ARSSF algorithm, which aims to improve data sharing on VANETs without compromising security. It verifies that only approved vehicles are participating, encodes the data for security, optimizes the communication line, and constantly monitors and changes the process to ensure dependable data transmission. Improving VANET safety and efficiency relies heavily on this algorithm.

#### 4. RESULT AND DISCUSSION

The effectiveness of the ARSSF proposal was assessed concerning its ability to ensure secure data dissemination in VANET. This system integrated authentication methods with a relay node selection-driven scheduling process, effectively resolving concerns related to energy consumption and node capacity. Furthermore, the algorithm facilitated vehicle authorization and improved security. The system under discussion was put into practice using the NS2 simulator, and a range of parameters were detailed in Table 1.

The developed system's performance was assessed by comparing it with four established benchmarks. These algorithms proved effective in the VANET environment, managing both scheduling and data dissemination processes. The primary objective of this system was to minimize collisions and reduce delays during the transmission of information from the vehicle to the roadside unit and RSU.

Table 1. Simulations parameter

| Parameters                          | Setting   |
|-------------------------------------|---|
| Relay selection phase time duration | 10 ms   |
| Feedback phase time duration        | 10 ms   |
| Transmission duration               | 1 ms  |
| Upper limit relay transmission of R | 100   |
| Original packet size                | 10  |
| Modulation mode                     | BPSLK   |
| RSU transmission power              | 40 dBm  |
| Vehicle transmission power          | 20 dBm  |
| SNR decoding threshold value        | 3 dB  |
| Highway scenario                    | (Sparse-100 vehicle, Dense-300 vehicle)                                 |
| Vehicle velocity                    | (20-30) randomly down m/s and 0.5 m/s <sup>2</sup> maximum acceleration |
| Urban scenario                      | (Sparse-160 vehicle, Dense-400 vehicle)                                 |
| Vehicle speed                       | 5-35 m/s  |
| Simulation run                      | 50 iterations   |
| Broadcast interval                  | 0.05 second   |

#### 4.1 End-to-end delay

Figures 5 and 6 illustrate the analysis of end-to-end delays for different packets and vehicles. The delay time was calculated as the average time required to transmit packets from the vehicle to the RSU units. This delay was determined for each step of the process, including scheduling, relay node selection, relay node scheduling, and packet forwarding. In the context of VANET, packets were transmitted in various scenarios, including V2V and V2I communication.

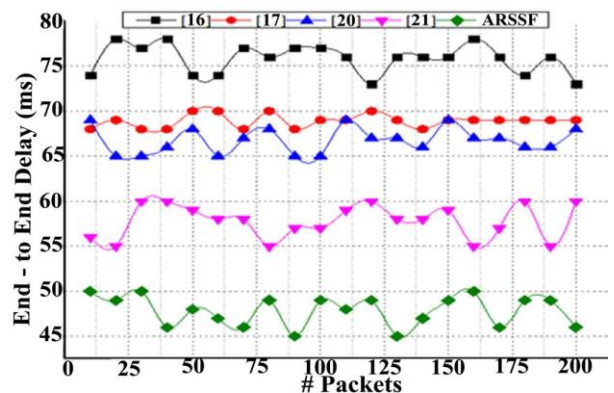


Figure 5. End-to-end delay of various packets compared with benchmarks

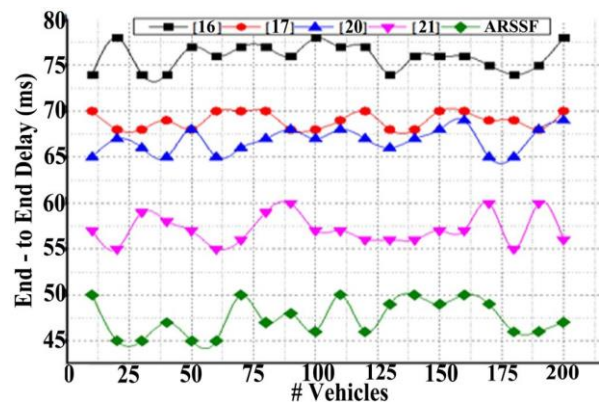


Figure 6. End-to-end delay of various vehicles compared with benchmarks

The ARSSF approach made use of the node utility value  $\gamma_{kn}^{t_r, R_x}$  estimated for each transmission power level  $P_{R_x}$ . The maximum utility value was chosen for subsequent transactions, as a higher value directly indicated faster delivery between V2V and V2I connections. Furthermore, the path loss ( $L_{R_x k}^{t_r}$ ) between the vehicle  $U_k$  and  $R_x$  was calculated to minimize computational delays during packet transmission within the transaction timeframe  $t_r$ . This system exhibited minimal delay, which directly correlated with its high throughput performance.

### 4.2 Throughput analysis

Within VANET, throughput refers to the successful delivery of packets from either V2V or V2I connections at a specific moment when the connection between  $U_k$  and  $R_x$  within the Area of Interest is assessed. The computed connection served to pinpoint the relay node, effectively overseeing network capacity and dependability. The system determined the node utility  $\hat{\beta}_{kn}^{t_r}$  in accordance with the transmission threshold value  $\gamma_{th}$  for each transaction  $t_r$  within the roadside unit  $R_x$ . Furthermore, the utility of  $R_x$  was determined to find the maximum network node utility  $\Phi^{t_r, R_x}$ . Relay nodes were selected from the pool of nodes according to signal-to-noise ratio (SNR) and utility values. The accurate selection of relay nodes greatly facilitated efficient packet transmission. Moreover, utility values were continuously updated throughout the process.

$$\hat{\beta}_{kn}^{t_r} = \begin{cases} \hat{\beta}_{kn}^{t_r, R_k^r}, & \text{if } U_k \in N_{R_k^r} \in \Omega_r \\ \hat{\beta}_{kn}^{t_r-1}, & \end{cases}$$

For each transaction Otherwise, within the Area of Interest (AoI), the system upheld a high throughput value, all the while preserving its security against unauthorized access by intermediaries.

### 4.3 Security analysis

Figures 7 and 8 illustrate the security assessment involving different packets and vehicles within the VANET data dissemination process. The selection of relay nodes was based on criteria such as Signal-to-Noise Ratio (SNR) utility, node utility, and the relay selection scheme. The maximum utility value  $\max_{L_r, \Omega_r} \sum_{i=1}^{L_r} \Phi^{t_r, R_i^r}$ . The selection of a relay node was made with the aim of reducing the probability of collisions during the scheduling process. Following the relay node selection, relay transactions were initiated through an authentication procedure. Prior to engaging in communication with other vehicles and the surrounding environment, each vehicle underwent registration. The trust authority was responsible for overseeing vehicle information, including details like velocity and position., thus authenticating the user activities in every transaction  $\sigma_{TA} = h(\mu_{U_k} || \omega_{U_k}) \oplus \theta_{TA}$ . During the registration process, the hash function was utilized to  $\rho_{TA} = h(\mu_{U_k} || U_k) \oplus \theta_{TA}$  to calculate the trust authority factors, which are instrumental in facilitating the processing of request messages  $\eta_{U_k} = Req \oplus T_{U_k} \oplus \theta_{TA} \oplus S_{tx}$  was transmitted to the other vehicle with respective timestamps.

The requested information served as an authorization mechanism for the vehicle prior to data sharing. Once a user received authorization through the secret key, the decoding

process was employed to enhance security during data dissemination. Moreover, the network utilized the decoding secret key to ensure a response to the request  $\{EN_{reply}, L_{U_2}\}$  with trust authority factors. Hence the effective utilization of the trust authority factors, registration details and secret keys maintained the data security in VANET. The findings unmistakably demonstrated that the suggested ARSSF significantly decreased authentication delay (47.35 ms) and improved throughput (98.05%) and security (97.94%) in comparison to the benchmarks, as indicated in Table 2.

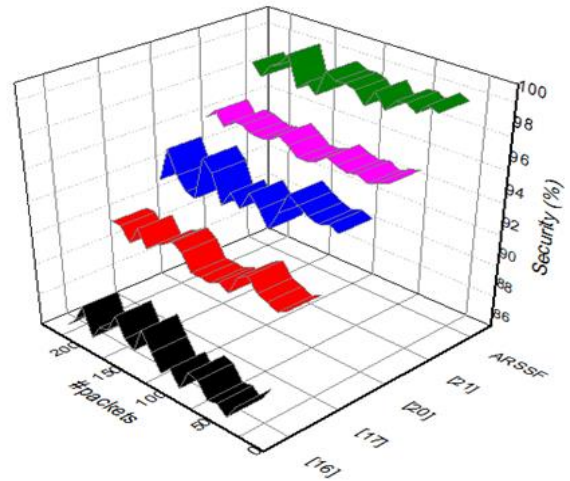


Figure 7. Security analysis of various packets

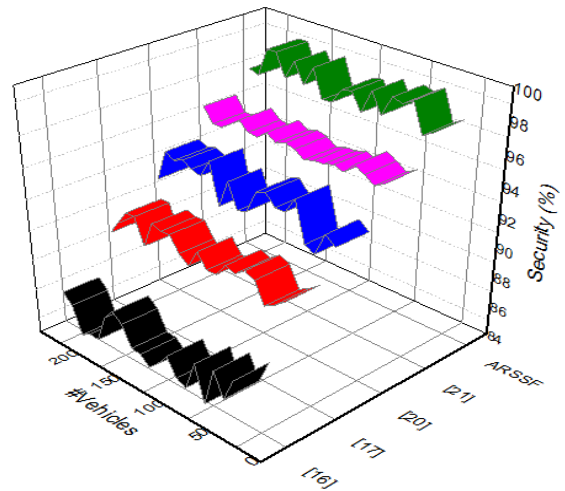


Figure 8. Security evaluation of different vehicles

Table 2. Comparative assessment of multiple packets

| Metrics               | [16]  | [17]   | [20]  | [21]  | ARSSF |
|-----------------------|-------|--------|-------|-------|-------|
| E2E (ms)              | 75.95 | 68.7   | 67    | 57.45 | 47.35 |
| Throughput (%)        | 86.75 | 91.043 | 93.23 | 95.7  | 98.05 |
| Security Analysis (%) | 86.34 | 90.68  | 93.69 | 95.40 | 97.94 |

Table 3. Packet count comparative analysis

| Metrics               | [16]  | [17]  | [20]  | [21]  | ARSSF |
|-----------------------|-------|-------|-------|-------|-------|
| E2E (ms)              | 75.12 | 69.23 | 67.1  | 57.15 | 47    |
| Throughput (%)        | 86.28 | 91.63 | 93.54 | 95.46 | 98.17 |
| Security Analysis (%) | 86.78 | 91.34 | 94.67 | 96.28 | 98.38 |



It was affirmed that the ARSSF algorithm, as currently implemented, effectively achieves data dissemination in VANET with the highest levels of security, reliability, robustness, and minimized delay, as demonstrated in Table 3. The research shows that the proposed ARSSF can significantly boost VANET performance and security over the state-of-the-art. The ARSSF model reduced latency in data transmission to a minimum of 47.35 milliseconds. With a throughput increase of 98.05%, it additionally ensures timely data transmission. Additionally, the model received a score of 97.94% on a security test, making it highly resistant to external threats and internal breaches. The results can direct VANET innovations in the future, facilitating better data sharing, better safety applications, tighter security, and more efficient scheduling. The overall efficiency and safety of VANETs stand to gain a great deal from using ARSSF.

## 5. CONCLUSIONS

This paper introduces the ARSSF, a robust and innovative system designed to ensure secure and high-quality data dissemination within VANETs. The system encompasses multiple stages, including the dissemination cycle, relay node selection, transmission, and feedback mechanisms. A unique characteristic lies in the meticulous choice of relay nodes, determined by factors such as Signal-to-Noise Ratio (SNR) utility, node utility calculations, and a relay node selection scheme., all designed to minimize the risk of collisions. Importantly, these selected relay nodes do not share common neighbors, a result of RSUs sharing AoI vehicle information prior to scheduling. This deliberate strategy ensures collision-free transactions with minimal delays, facilitating the transmission of authenticated vehicles and data. Furthermore, trust authority mechanisms play a pivotal role in guaranteeing security by authenticating vehicle factors through the exchange of request and response messages. Continuous feedback monitoring reduces delays, expanding the scope for data transactions. Although the NS2 simulator was employed for system implementation, it is acknowledged that it has limitations in accurately representing real-world complexities. While the results attest to the system's ability to ensure high security across varying packet loads and vehicle counts, the implications of these findings for the future of data dissemination in VANETs require further exploration. Additionally, the study suggests that the efficiency of the proposed system can be further enhanced by the application of optimized scheduling strategies, though the specific strategies are left for future research to elucidate. The ARSSF paradigm demonstrates the potential to significantly reduce cyber-attacks and unauthorized data access in Vehicle-to-Vehicle (VANET) networks. With an impressive latency of less than 47.35 milliseconds, the system stands as a promising solution, particularly suitable for mission-critical applications like real-time traffic control. The research focus on mitigating the risk of insider attacks and addressing the collision problem makes it a valuable contribution to the field of VANET data dissemination. In future work, it is imperative to address the limitations of the ARSSF system and further enhance its capabilities. One key area of focus should be the development of advanced scheduling strategies, such as machine learning-based relay node selection algorithms, dynamic route planning, and advanced data authentication methods. These strategies can significantly improve the system's efficiency, security, and

overall performance in VANETs, making it more resilient to emerging cyber threats and real-world complexities.

## REFERENCES

- [1] Khatri, S., Vachhani, H., Shah, S., Bhatia, J., Chaturvedi, M., Tanwar, S., Kumar, N. (2021). Machine learning models and techniques for VANET based traffic management: Implementation issues and challenges. *Peer-to-Peer Networking and Applications*, 14: 1778-1805. <https://doi.org/10.1007/s12083-020-00993-4>
- [2] Hamdi, M.M., Al-Dosary, O.A.R., Alrawi, O.A.S., Mustafa, A.S., Abood, M.S., Noori, M.S. (2021). An overview of challenges for data dissemination and routing protocols in VANETs. In *2021 3rd International Congress on Human-Computer Interaction, Optimization, and Robotic Applications (HORA)*, Ankara, Turkey, pp. 1-6. <https://doi.org/10.1109/HORA52670.2021.9461396>
- [3] Wang, T.H., Manivasagam, S., Liang, M., Yang, B., Zeng, W., Urtasun, R. (2020). V2vnet: Vehicle-to-vehicle communication for joint perception and prediction. In *Computer Vision-ECCV 2020: 16th European Conference, Glasgow, UK*, pp. 605-621. <https://doi.org/10.1007/978>
- [4] Ali, I., Li, F. (2020). An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs. *Vehicular Communications*, 22: 100228. <https://doi.org/10.1016/j.vehcom.2019.100228>
- [5] Sakiz, F., Sen, S. (2017). A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad Hoc Networks*, 61: 33-50. <https://doi.org/10.1016/j.adhoc.2017.03.006>
- [6] Tahir, M.N., Katz, M., Rashid, U. (2021). Analysis of VANET wireless networking technologies in realistic environments. In *2021 IEEE Radio and Wireless Symposium (RWS)*, San Diego, USA, pp. 123-125. <https://doi.org/10.1109/RWS50353.2021.9360381>
- [7] Lee, M., Atkison, T. (2021). VANET applications: Past, present, and future. *Vehicular Communications*, 28: 100310. <https://doi.org/10.1016/j.vehcom.2020.100310>
- [8] Shaban, A.M., Kurnaz, S., Shantaf, A.M. (2020). Evaluation DSDV, AODV and OLSR routing protocols in real live by using SUMO with NS3 simulation in VANET. In *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Ankara, Turkey, pp. 1-5. <https://doi.org/10.1109/HORA49412.2020.9152903>
- [9] Duc, L., Simonina, O., Buinevich, M., Vladyko, A. (2018). A multi-criteria priority-based V2I communication for information dissemination at RSU in VANET. *JP Journal of Heat and Mass Transfer*, 15(S): 195-203. <https://doi.org/10.17654/HMSI218195>
- [10] Shahwani, H., Shah, S.A., Ashraf, M., Akram, M., Jeong, J.P., Shin, J. (2022). A comprehensive survey on data dissemination in Vehicular Ad Hoc Networks. *Vehicular Communications*, 34: 100420. <https://doi.org/10.1016/j.vehcom.2021.100420>
- [11] Chahal, M., Harit, S. (2019). A stable and reliable data dissemination scheme based on intelligent forwarding in VANETs. *International Journal of Communication Systems*, 32(3): e3869. <https://doi.org/10.1002/dac.3869>

- [12] Haider, S., Abbas, G., Abbas, Z.H., Boudjit, S., Halim, Z. (2020). P-DACCA: A probabilistic direction-aware cooperative collision avoidance scheme for VANETs. *Future Generation Computer Systems*, 103: 1-17. <https://doi.org/10.1016/j.future.2019.09.054>
- [13] Lyu, F., Zhu, H., Zhou, H., Qian, L., Xu, W., Li, M., Shen, X. (2018). MoMAC: Mobility-aware and collision-avoidance MAC for safety applications in VANETs. *IEEE Transactions on Vehicular Technology*, 67(11): 10590-10602. <https://doi.org/10.1109/TVT.2018.2866496>
- [14] Sheikh, M.S., Liang, J. (2019). A comprehensive survey on VANET security services in traffic management system. *Wireless Communications and Mobile Computing*, 2019: 1-23. <https://doi.org/10.1155/2019/2423915>
- [15] Yuan, Y., Tasik, R., Adhatarao, S.S., Yuan, Y., Liu, Z., Fu, X. (2020). RACE: Reinforced cooperative autonomous vehicle collision avoidance. *IEEE Transactions on Vehicular Technology*, 69(9): 9279-9291. <https://doi.org/10.1109/TVT.2020.2974133>
- [16] Al-Shareeda, M.A., Anbar, M., Manickam, S., Yassin, A.A. (2020). VPPCS: VANET-based privacy-preserving communication scheme. *IEEE Access*, 8: 150914-150928. <https://doi.org/10.1109/ACCESS.2020.3017018>
- [17] Li, G., Sun, Q., Boukhatem, L., Wu, J., Yang, J. (2019). Intelligent vehicle-to-vehicle charging navigation for mobile electric vehicles via VANET-based communication. *IEEE Access*, 7: 170888-170906. <https://doi.org/10.1109/ACCESS.2019.2955927>
- [18] Singh, S., Negi, S., Verma, S.K. (2018). VANET based p-RSA scheduling algorithm using dynamic cloud storage. *Wireless Personal Communications*, 98(4): 3527-3547. <https://doi.org/10.1007/s11277-017-5027-0>
- [19] Shrivastava, A., Bansod, P., Gupta, K., Merchant, S.N. (2018). An improved multicast-based energy-efficient opportunistic data scheduling algorithm for VANET. *AEU-International Journal of Electronics and Communications*, 83: 407-415. <https://doi.org/10.1016/j.aeue.2017.10.011>
- [20] Oliveira, R., Montez, C., Boukerche, A., Wangham, M.S. (2017). Reliable data dissemination protocol for VANET traffic safety applications. *Ad Hoc Networks*, 63: 30-44. <https://doi.org/10.1016/j.adhoc.2017.05.002>
- [21] Liu, L., Chen, C., Qiu, T., Zhang, M., Li, S., Zhou, B. (2018). A data dissemination scheme based on clustering and probabilistic broadcasting in VANETs. *Vehicular Communications*, 13: 78-88. <https://doi.org/10.1016/j.vehcom.2018.05.002>
- [22] Liu, K., Xiao, K., Dai, P., Lee, V.C., Guo, S., Cao, J. (2020). Fog computing empowered data dissemination in software-defined heterogeneous VANETs. *IEEE Transactions on Mobile Computing*, 20(11): 3181-3193. <https://doi.org/10.1109/TMC.2020.2997460>
- [23] Hamdi, M.M., Audah, L., Rashid, S.A. (2022). Data dissemination in VANETs using clustering and probabilistic forwarding based on adaptive jumping multi-objective firefly optimization. *IEEE Access*, 10: 14624-14642. <https://doi.org/10.1109/ACCESS.2022.3147498>