Journal of Theoretical and Applied Information Technology
15th July 2024. Vol.102. No. 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENHANCING SECURE V2V AND V2I COMMUNICATION: DESIGNING AN EFFICIENT VEHICLE-AUTHORIZED SHORTEST ROUTE SELECTION ALGORITHM FOR MINIMIZING DATA LOSS

SPANDANA MANDE MANDE [1] AND NANDHA KUMAR RAMACHANDRAN [2*]

School of Computer Science and Engineering, VIT-AP University, Vijayawada 522237, Andhra Pradesh, India;
Email 1: spandana.mande@gmail.com, nandhakumarr03@gmail.com,
Correspondence:nandhakumarr03@vitap.ac.in

ABSTRACT

Ensuring the security and efficiency of information exchange between vehicles (V2V) and infrastructure (V2I) is of utmost importance in the realm of vehicular communication systems. The main objective of this study is to enhance the security and efficiency of these systems. To achieve this, we will create a vehicle-authorized algorithm for selecting the shortest route, to minimize data loss. This algorithm employs cryptographic authentication mechanisms to prioritize secure routes based on vehicle authorization, effectively mitigating potential security risks during information exchange. Implementing optimized routing protocols, such as the A* algorithm, allows the system to determine the most efficient routes for vehicles, taking into account factors like traffic conditions and network congestion. It specifically focuses on the critical issues of choosing the best route and ensuring data security in communications between vehicles. This algorithmic solution enhances both route selection and network security while also establishing a robust framework for secure and efficient vehicular communication systems. It guarantees the accurate and secure reception of information between vehicles or infrastructure.

Keywords: *Vehicle to Vehicle, Vehicle to Infrastructure, A *, Shortest Route Selection, Vehicular Communications, Data Loss.*

1. INTRODUCTION

Autonomous vehicles, a revolutionary advancement in transportation systems, are progressing rapidly. Nevertheless, the incorporation of these technologies creates major difficulties, particularly in the areas of security and effectiveness. V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) communications can improve the safety and functionality of autonomous systems. However, these networks are currently vulnerable to security risks, including data breaches, unauthorized access, and cyberattacks. These vulnerabilities have the potential to result in severe consequences, such as accidents, inefficiencies in traffic, and compromised personal information.

Moreover, increasing urban traffic and limited network capacities exacerbate the inefficiencies of the existing vehicular communication systems. These inefficiencies lead to substantial delays, heightened pollution, and increased energy consumption. To address these critical issues, we propose implementing a new algorithm that chooses the shortest authorized route for vehicles. This algorithm has two main objectives: to optimize routing decisions by taking into account real-time traffic conditions and to ensure the secure exchange of information between vehicles and infrastructure by using advanced cryptographic authentication mechanisms. The growing intricacy of vehicular networks and the rising demand for more resilient and dependable transportation systems underscore the need for this innovation. It contributes to improving the safety and reliability of autonomous and connected vehicles by enhancing the security and efficiency of V2V and V2I communications. This data would encompass the velocity of the vehicle, the size of the vehicle, the location of the vehicle, and the decrease in stability [1]. V2V innovation employs dedicated short-range communications (DSRC). Occasionally, it has been likened to Wi-Fi. However, automated vehicles are currently not ready for large-scale commercial deployment. Human-operated vehicles require the assistance of traffic signals. As intersections become more

complex, automation is necessary to ensure safety. That is why it is highly important to study the theoretical maximum capacity of a network of intersections controlled by traffic lights. One of the possible frequencies is 5.9 GHz. Given the limited availability of wireless bandwidth networks, it is necessary to efficiently utilize resources to facilitate high throughput and excellent communication in multi-hop wireless systems The Secure V2V and V2I Communication model is shown in Figure 1.

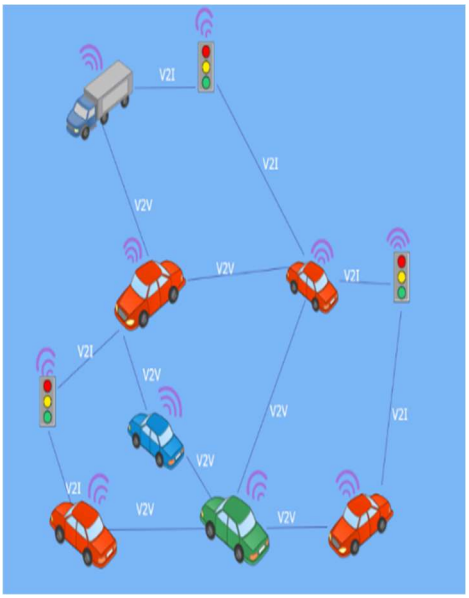

Figure 1. Secure V2V and V2I Communication

The backpressure algorithm is an efficient approach for routing traffic in a multi-hop network by utilizing congestion indications. The technique can be connected to remote communication systems, such as sensor systems, mobile ad hoc networks (MANETs), and heterogeneous systems that have both remote and wired components [2]. Tassiulas and Ephremides [3] initially conducted the computation of backpressure. Their computation entailed utilizing a maximum-weight interface assurance sorting technique and a differential development coordinating platform. Throughout their progression, they did not label it as back pressure. In the context of data frameworks, the phrase "backpressure" refers to a specific type of stream control system that is based on congestion. Vehicular ad hoc networks (VANETs) have received growing interest and research efforts from the medical, industrial, and academic sectors in recent years. Vehicular Ad Hoc Networks (VANETs) are a distinct form of wireless communication network that facilitates cars to exchange information among themselves and with infrastructure. The selection of the optimal path in vehicular ad hoc networks (VANETs) is determined by the quality of service (QoS), which focuses on the dependability and availability of the network. The QoS routing algorithm is crucial for determining the most optimal routes based on specific QoS criteria, including end-to-end delay, hop count, energy, and mobility. The presence of several Quality of Service (QoS) constraints leads to the emergence of the Multi-Constrained (Optimal) Path issue, which is acknowledged as NP-hard. Swarm intelligence techniques can effectively solve the MC(O)P problem by making use of their self-organizing characteristics. Ant colony optimization techniques represent the most precise embodiment of swarm intelligence. ACO is enhancing the process of routing and mitigating risks associated with routing security.

The main purpose of this routing message is to protect the network from prospective enemies. Instances of security attacks encompass route diversion, route disruption, and inaccurate routing status information. This research introduces a robust routing algorithm for Vehicular Ad-hoc networks (VANETs) that utilizes ant colony optimization. The objective of SACO is to ascertain feasible paths between two vehicles, considering the constraints of quality of service (QoS), to provide routing services that are both efficient and reliable. An analysis is conducted on the SACO routing algorithm within the framework of a highway scenario, and its performance is assessed. The network topology must adhere to the requirements for dependable communication links and effectively manage link failures between vehicles, which are essential characteristics of VANETs. The paper primarily focuses on the following topics: Firstly, ascertain the viable pathways within the network, and subsequently enhance its security. Security overhead might occur while routing. The result of a simulation depends on the restrictions of Quality of Service (QoS) and the routing mechanism that includes security measures. The main goal is to guarantee the stability of the transportation network. Vehicular ad hoc networks (VANETs) have received growing interest and research efforts from the medical, industrial, and academic sectors in recent years. Vehicular Ad Hoc Networks (VANETs) are a distinct form of wireless communication network that facilitates communication between automobiles and infrastructure. In Vehicular Ad Hoc Networks (VANETs), the selection of an optimal route is determined by the Quality of Service (QoS), with

a primary emphasis on the network's stability and availability [4]. The QoS routing algorithm plays a critical role in selecting optimal routes depending on specific QoS criteria, such as end-to-end delay, hop count, energy, and mobility. The application of various Quality of Service (QoS) constraints results in the emergence of the Multi-Constrained (Optimal) Path problem, which is recognized as NP-hard. Swarm intelligence techniques are suitable for solving the MC(O)P problem because they exhibit efficient self-organization. Ant colony optimization techniques are the most efficient manifestation of swarm intelligence. ACO is improving the routing process and reducing security risks associated with routing. The main purpose of this routing message is to protect the network from prospective enemies [5]. Examples of security assaults encompass route diversion, route disruption, and inaccurate routing state information. This research introduces a robust routing algorithm for Vehicular Ad-Hoc Networks (VANETs) that utilizes ant colony optimization. The objective of SACO is to ascertain feasible paths between two vehicles, considering the restrictions of quality of service (QoS), to provide routing services that are both efficient and reliable. An analysis is conducted on the SACO routing algorithm within the framework of a highway scenario, and its performance is assessed. The network structure must satisfy the criteria for reliable communication links and handle link failures between vehicles, which are fundamental attributes of VANETs [6]. The paper mostly concentrates on the subsequent concerns: First, determine the feasible routes within the network and then improve the security of the network. The routing procedure may have security costs. The result of a simulation depends on the restrictions of Quality of Service (QoS) and the routing mechanism that includes security measures [7]. The main goal is to guarantee the stability of the transportation network. As a result of increasing urbanization, there has been a substantial rise in the number of motor vehicles. The primary objective of the Intelligent Transportation System (ITS) is to enhance the communication and coordination between infrastructure, vehicles, and persons [8]. The Vehicle Ad-hoc Network (VANET) is a fundamental element of the Intelligent Transportation System (ITS). Vehicular ad hoc networks (VANETs) provide instantaneous communication among vehicles and a range of entities, including other vehicles, individuals, road systems, infrastructure, clouds, and so on. This is made possible by the incorporation of advanced wireless communication technology. Vehicular ad hoc networks (VANETs) possess the potential to intelligently oversee, coordinate, and administer infrastructure, cars, and roads. Consequently, users can experience a driving environment that is secure, pleasant, and intelligent, while also having the ability to utilize efficient traffic services [9].

Motivation

The importance of vehicular communication systems is apparent in contemporary transportation networks; as technological advancements have resulted in their growing prevalence. These systems allow vehicles to establish communication with one another and with infrastructure components, making it easier to implement different applications like traffic control, accident prevention, and entertainment services. Nonetheless, the progress in these developments brings about an increased focus on the security aspect of vehicle communication. The transmission of sensitive data between vehicles and infrastructure presents substantial security obstacles, as it is susceptible to threats such as data interception, tampering, and unauthorized access, which can compromise the integrity and confidentiality of communication. It is essential to address these security concerns to guarantee the reliability of vehicular communication systems. Moreover, there is an urgent requirement for routing algorithms that are both efficient and secure. These algorithms should not only optimize route selection based on factors such as distance and traffic conditions but also prioritize secure communication channels to reduce security risks. This research aims to enhance the security and efficiency of communication systems in vehicles. This has the potential to improve transportation safety and efficiency. Enabling the timely exchange of critical information, such as traffic updates and hazard warnings, achieves this. This reduces the risk of accidents and traffic congestion. This study aims to develop a novel algorithm that combines cryptographic authentication mechanisms and efficient routing protocols to prioritize secure routes and minimize data loss during transmission, using recent advancements in cryptographic techniques and routing protocols.

Contribution

The main contribution of this work is the development of a novel algorithm that selects the shortest route in a way that is authorized for vehicles. This algorithm combines cryptographic authentication mechanisms and efficient routing protocols to prioritize secure routes based on

vehicle authorization. This algorithm improves vehicle communication systems' security and efficiency by significantly reducing potential security vulnerabilities in the exchange of information between vehicles (V2V) and infrastructure (V2I). In addition, by taking into account variables such as traffic conditions and network congestion, it enhances the effectiveness of vehicular communication systems while guaranteeing an accurate and secure exchange of information. The algorithm creates a strong and reliable framework for secure and efficient communication systems between vehicles and infrastructure. It reduces data loss during transmission and enhances network security. This establishes a solid basis for secure communication channels in vehicular networks. Moreover, the proposed strategy seeks to reduce security vulnerabilities in communication between vehicles by giving preference to secure routes and taking into account traffic conditions. This helps guarantee the safe transmission of information in vehicular networks. Incorporating the A* algorithm is critical in determining efficient routes for transmitting data between vehicles (V2V) and infrastructure (V2I) while adhering to strict security protocols. It systematically determines the best routes, minimizes data loss, and prioritizes security protocols for secure information exchange.

Research Gap

Several studies do not recognize the importance of vehicle-authorized routing in vehicular communication systems. They only concentrate on route selection algorithms, disregarding the need for vehicle authorization when selecting secure routes. This study aims to fill this void by creating an algorithm that integrates vehicle authorization status to improve the security and effectiveness of vehicle communication systems. In addition, current routing algorithms frequently lack strong cryptographic authentication mechanisms, resulting in the insecure transmission of data. This work guarantees secure communication by incorporating cryptographic authentication mechanisms into the routing algorithm. Moreover, existing routing algorithms face difficulties in adjusting to real-time traffic conditions, leading to less-than-optimal route selections and heightened data loss during transmission. This paper enhances the efficiency of vehicular communication systems by integrating real-time traffic conditions and network congestion into route selection, surpassing existing approaches. Furthermore, although certain studies suggest specific security measures, there is a lack of a comprehensive framework that incorporates various security mechanisms. The objective of this study is to address this issue by proposing an all-encompassing structure that considers vehicle authorization, encryption, and authentication to establish secure transmission routes and reduce data loss. Furthermore, the prospective benefits of integrating vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication modes are overlooked in a considerable number of studies. The objective of this research is to address this gap by creating an algorithm that facilitates smooth communication between vehicles and infrastructure, consequently enhancing the overall efficiency and security of vehicular communication systems.

2. RELATED WORK

Wang et al. [10] suggest many current studies overlook the significance of vehicle-authorized routing in vehicular communication systems. In contrast to the routing protocols presently employed in VANETs, geographic routing that relies on location is widely acknowledged as the most efficient approach for managing the continuously evolving network topologies. Liu et al. [11] suggest that the Vehicles ascertain their precise locations using GPS technology and subsequently disseminate their status updates nearby. The routing paths are selected based on the geographic coordinates of the next hop and the final destination. IEEE 1609.2 [12] employs Public Key Infrastructure (PKI) to manage security services for wireless access in vehicular environments and facilitate communication between entities. This framework is well-suited for VANETs. Cui et al. [13] suggest utilizing PKI-based systems as a dependable approach to ensure secure information sharing in VANETs. These systems offer identity authentication for entities and ensure the integrity of messages. Xie et al. [14] propose a public key infrastructure (PKI)--based authentication protocol for broadcasting vehicle messages in vehicular ad-hoc networks (VANETs). Furthermore, Joshi et al. [15] suggest a highly efficient system that employs an event trigger mechanism for VANETs. This system utilizes PKI-based signatures to verify the authenticity of broadcast beacons and ensure their validity. Foll et al. [16] suggest traffic causes latency, which is the loss of data due to the accumulation of packets in queues, resulting in increased delays. Common backpressure designs take into account all possible routes, regardless of the amount of work, which can make routing more complex and lead

to substantial delays. The inefficiency in thoroughly examining all potential routes restricts the rapid transmission of data packets, resulting in a reduction in throughput. Warr et al. [17] suggest to address these constraints, we propose the implementation of an algorithm that prioritizes minimizing the latency of data transmission from the source to the destination while simultaneously maximizing the throughput capacity for data transfer. This algorithm facilitates the rapid and effective transmission of data packets. Aman et al. [18] suggest to implement backpressure on a specific group of routes, which may restrict the capacity range but can enhance the organized transmission of packets and reduce latency.

The main goal of introducing VANETs is to improve the driving experience by enhancing road safety, convenience, and transportation efficiency, while also reducing traffic accidents. However, VANETs encounter a multitude of security vulnerabilities and privacy issues inside the framework of Intelligent Transportation Systems (ITS). Qiu et al. [19] propose that vehicles should engage in a substantial interchange of information with each other and with traffic infrastructure using wireless channels. However, this approach makes them vulnerable to both passive and active attacks. Furthermore, the security of VANETs is compromised by both prospective malicious users and malicious nodes. Creating a safe and efficient authentication and session key agreement mechanism for Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communication techniques in Vehicular Ad-Hoc Networks (VANETs) is a difficult undertaking. Cooperative intelligent transport systems (C-ITS) have gained considerable attention from both academia and industry as a practical implementation of artificial intelligence (AI) in transport systems in recent years. The vehicular communication network is a fundamental basis of C-ITS. Furthermore, it holds the position of being the second-largest market in terms of spending on the Internet of Things (IoT). The automobile industry allocated $78 billion towards Internet of Things (IoT) investments in 2017 and is expected to sustain substantial expansion in the future. The present installation of C-ITS-enabled transport and driving systems has had a substantial influence on persons' everyday schedules. Currently, there is a wide range of intelligence-driven applications, including intelligent navigation systems, intelligent traffic flow control systems, and intelligent speed monitoring systems, among others. The further advancement of C-ITS relies on the exploration of edge intelligence technologies, which enable vehicles to not only gather data but also analyze it using onboard intelligent computation engines. For instance, vehicles that are equipped with cameras and on-board computers can navigate intricate algorithms by utilizing a real-time visual feed. This enables them to transmit and analyze data on C-ITS servers. Furthermore, the establishment of communication channels among neighboring vehicles, which are regarded as intelligent endpoints, can facilitate a streamlined exchange of data for critical objectives such as collision prevention. Thus, C-ITS depends on data transmission techniques and Significant technologies, edge-intelligent algorithms have the potential to facilitate autonomous driving on roadways shortly. Haid et al. [20] propose that the advancement of C-ITS technology holds great potential and has resulted in several advantages. However, there are still specific limitations that hinder the practical implementation of V2X communication. Petit et al. [21] suggest an emerging concern in V2X communication systems is the inadequate provision of security measures, which poses a significant problem. An individual with malicious intent can disrupt the system by disseminating false messages or uncovering private information about another person, such as their true identity or professional address. In contrast to alternative network architectures, V2X networks exhibit exceptional latency responsiveness, specifically when it comes to safety-related applications. An increase in latency may give rise to erroneous judgments concerning the trajectory of the vehicle or potentially cause transportation accidents. Table 1 presents a comparison of proposed solutions for vehicular communication systems.

Table 1: Comparison of Proposed Solutions for Vehicular Communication Systems

Main Focus	Proposed Solution	Challenges
Vehicle-authorized routing in vehicular communication systems	Geographic routing based on location	Overlooked significance of vehicle-authorized routing
Utilization of GPS for precise location determination	Dissemination of status updates, routing based on coordinates	None Specified
PKI for managing security services in vehicular environments	Identity authentication, message integrity verification	Security risks, privacy concerns
PKI-based systems for secure information sharing	Identity verification	None Specified
Efficient system with PKI-based signatures for beacon verification	Beacon authenticity verification	None Specified
Minimizing transmission latency and maximizing throughput	Algorithm for minimizing latency, maximizing throughput	Traffic-induced latency, reduced throughput
Prioritizing minimizing transmission latency	Algorithm for minimizing latency, maximizing throughput	Traffic-induced latency, reduced throughput
Implementing backpressure on specific route groups	Enhancing packet transmission organization, reducing latency	None Specified
Security risks and privacy concerns in VANETs	Secure communication protocols, attack mitigation	Security risks, privacy concerns
Benefits and limitations of C-ITS technology	None Specified	Practical usage limitations, system restrictions
Inadequate security measures in V2X communication systems	Enhanced security protocols, attack prevention	Vulnerability to attacks, privacy breaches

3. PROPOSED WORK

The proposed research aims to develop a novel algorithm for selecting the most efficient route in a vehicle-authorised manner, to improve the security and efficiency of communication systems in vehicles. This algorithm will utilize cryptographic authentication mechanisms to prioritize secure routes based on vehicle authorization, thereby reducing potential security risks in the exchange of information between vehicles (V2V) and infrastructure (V2I). The proposed approach will employ the A* algorithm and efficient routing protocols to determine the shortest routes, considering variables such as traffic conditions and network congestion. The primary objective is to minimize data loss during transmission and guarantee accurate and secure information exchange. In addition, the algorithm will enhance the network's route selection while bolstering its security, establishing a robust framework for secure and efficient communication systems between vehicles and infrastructure.

The proposed work aims to improve the efficiency of vehicular communication, reduce security risks, and ensure the secure exchange of information in vehicular

networks by giving priority to secure routes and taking into account traffic conditions. The A* algorithm is essential in the "Enhancing Secure V2V and V2I Communication: Designing an Efficient Vehicle-Authorised Shortest Route Selection Algorithm for Minimising Data Loss project. The algorithm rates nodes based on their cost, taking into account their location, traffic, and how busy the network is. This is done to find the best ways for vehicles (V2V) and infrastructure (V2I) to send data while following strict security protocols. By implementing cryptographic authentication mechanisms, the system can establish secure routes by verifying vehicles' authorizations. This ensures the protection of data integrity and confidentiality. Dynamic adaptation allows for the modification of routes based on up-to-date information, ensuring that there is minimal loss of data and giving priority to secure communication channels.

In general, the integration of the A* algorithm enhances communication efficiency by methodically identifying the most efficient routes, reducing data loss, and giving priority to security protocols for the exchange of secure information. Figure 2 illustrates the proposed model architecture.

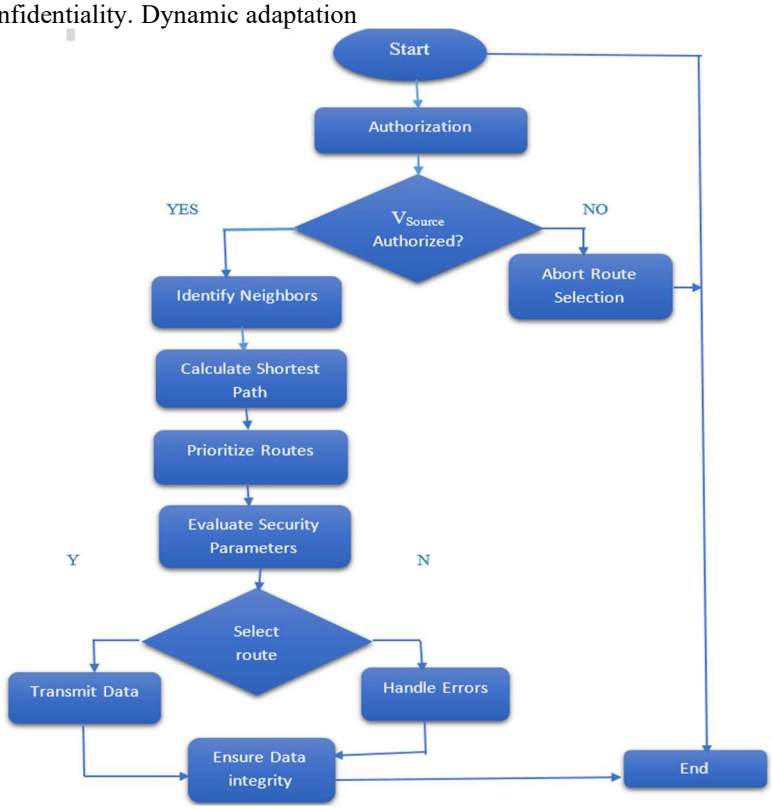

Figure 2. Proposed Model Architecture

.

It presents a systematic procedure for achieving both efficient and secure transmission of data in vehicular communication systems. The process starts by verifying the authorization status of the source vehicle and terminates the selection of the route if it is found to be unauthorized. Next, a routing algorithm computes the most efficient routes to the destination by identifying nearby vehicles and infrastructure nodes that the starting vehicle can reach.

The authorization status determines the order of priority of routes, and it assesses security parameters like encryption and authentication requirements for each route. The algorithm chooses the most optimal route to minimize data loss while also guaranteeing security and efficiency. It then transmits the data using this chosen route and continuously monitors the transmission for any errors or security breaches. Upon detection, error detection and correction

mechanisms are utilized, and data transmission may be redirected. Only after ensuring end-to-end data integrity and security can we conclude the process. This methodical approach seeks to improve the dependability, effectiveness, and safety of data transfer in automotive communication systems. The Efficient Vehicle-Authorized Shortest Route Selection Algorithm for Minimizing Data Loss is shown in Algorithm 1.

Algorithm: Efficient vehicle-authorized Shortest Route Selection Algorithm for Minimizing Data Loss

Input:

V_s: Source vehicle ID

V_d: Destination vehicle/infrastructure ID

Auth (V_s): Authorization status of V_s

N: Neighbouring vehicles and infrastructure nodes accessible from V_s (function notation $f_N(V_s)$

R(V_s, V_d): Shortest Paths from V_s to V_d

Calculated using a routing algorithm

P(SP): Prioritized routes based on the authorization status of vehicles and infrastructure nodes along the paths

ES(PR): Security parameters evaluated for data transmission along each route

CR(PR): Route selected that minimizes data loss while prioritizing security and efficiency

Data: Data to be transmitted

Output:

SR: Secure the shortest route for data transmission

1. **Verif**y the authorization status of V_s. If unauthorized, abort route selection.

if Auth(V_s.)

return True

else:

return False

2. **Determin**e neighboring vehicles and infrastructure nodes accessible from V_s.

$N = f_N(V_s)$

return N

3. Calculate the shortest paths from V_s to V_d using a suitable routing algorithm (A* algorithm).

$SP = R (V_s, V_d)$

return SP

4. Prioritize routes based on the authorization status of vehicles and infrastructure nodes along the paths.

PR= P(SP)

return PR

5. **Evalua**te security parameters such as encryption and authentication requirements for data transmission along each route.

SP = ES(PR)

return SP

6. **Selec**t the route that minimizes data loss while prioritizing security and efficiency.

SR=CR(PR)

return SR

7. **Transm**it data from V_s to V_d using the selected route.

transmit (SR, Data)

8. **Monito**r data transmission.

9. **Handle** Errors/Breaches

if ErrorDetected ()

handleError

elif breach detected

handle breach()

10. **Ensure** Data Integrity
VerifyDataIntegrity()
End

The below Figure 3 gives a visual representation of the fundamental distinctions between Dijkstra's algorithm and the A* algorithm. Dijkstra's algorithm utilizes a priority queue based on the distance from the source node, while the A* algorithm selects a priority queue based on the total costs incurred thus far and an estimated cost to the goal node (heuristic). Dijkstra's algorithm and the A* algorithm may produce different Shortest Path Trees due to the distinct priorities assigned to nodes in the priority queue.

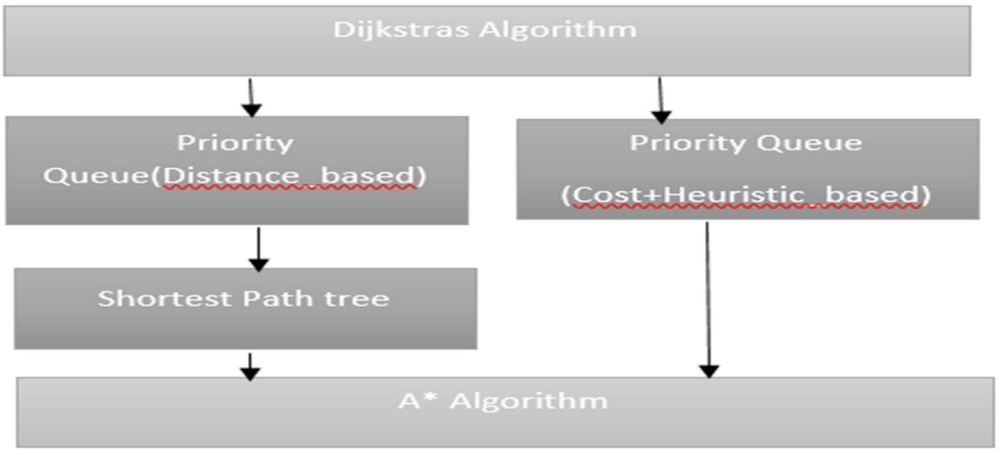

Figure 3. Proposed Model Architecture

.

4. SIMULATION RESULTS

The examination of both algorithms encompassed multiple key variables to ensure an extensive comparison. To assure fair analyses of scalability and performance over time, the network size was maintained at 100 vehicles, and the simulation time was set to 1000 seconds. The simulation utilized authentic traffic and mobility models, specifically the Random Waypoint and Manhattan Grid models, which accurately represented common patterns of vehicular movement and traffic situations. The routing protocols and security mechanisms differed among the algorithms. Dijkstra's algorithm employed DSR routing and basic encryption, whereas the A* algorithm utilized AODV routing and advanced encryption. The transmission parameters, including range, packet size, and communication range, were standardized to ensure consistency throughout the simulations. In addition, the evaluation included testing the algorithm's performance under different conditions, such as varying traffic loads and data transmission rates. Five simulation runs were conducted for each algorithm, and performance metrics such as throughput, delay, and packet loss were analyzed using mean and standard deviation values to gain insights into the average performance and stability. In summary, this thorough approach allowed for a strong evaluation of the algorithm's effectiveness and dependability across various situations. All the simulation factors are listed in Table 2.

Table 2: Simulation Factors

Parameters	Dijkstra's Algorithm	A* Algorithm
Network Size	100 vehicles	100 vehicles
Simulation Time	1000 seconds	1000 seconds
Traffic Model	Random Waypoint	Random Waypoint
Routing Protocol	DSR (Dynamic Source Routing)	AODV (Ad hoc On-Demand Distance Vector)
Security Mechanism	Basic Encryption	Advanced Encryption
Mobility Model	Manhattan Grid	Manhattan Grid
Transmission Range	250 meters	250 meters

Journal of Theoretical and Applied Information Technology
15th July 2024. Vol.102. No. 13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Packet Size	1000 bytes	1000 bytes
Traffic Load	Moderate	Heavy
Data Transmission Rate	10 Mbps	10 Mbps
Communication Range	500 meters	500 meters

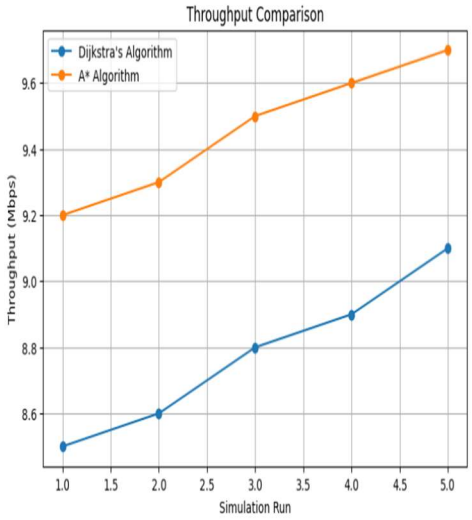

Figure 4. Comparison of Throughput

The above graph as shown in Figure 4, illustrates the comparative throughput achieved by Dijkstra's algorithm versus the A* algorithm in different simulation runs. The x-axis corresponds to the simulation runs, while the y-axis represents the measured throughput in Mbps.

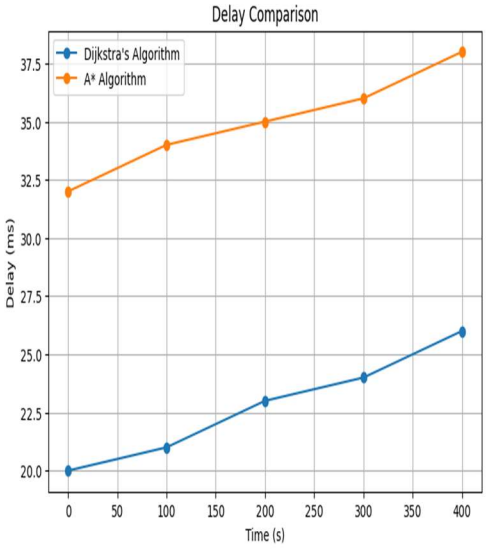

Figure 5. Delay Comparison

The above shown in Figure 5, compares the latency that packets transmitted through Dijkstra's algorithm and the A* algorithm experience. The x-axis represents the temporal dimension, and the y-axis represents the delay in milliseconds.

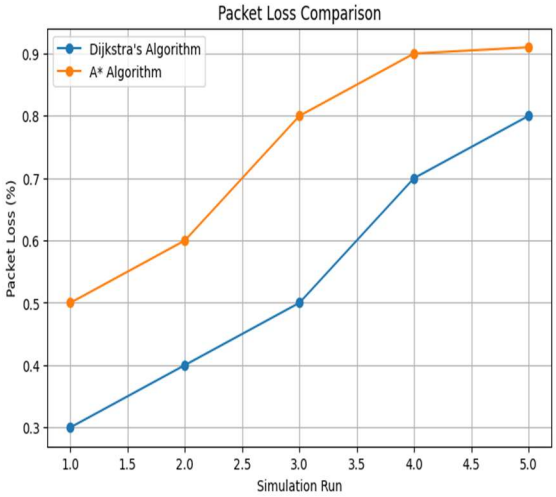

Figure 6. Packet Loss Comparison

The above graph shown in Figure 6, depicts the observed packet loss in both Dijkstra's algorithm and the A* algorithm. The x-axis represents time or simulation runs, while the y-axis indicates packet loss percentage.

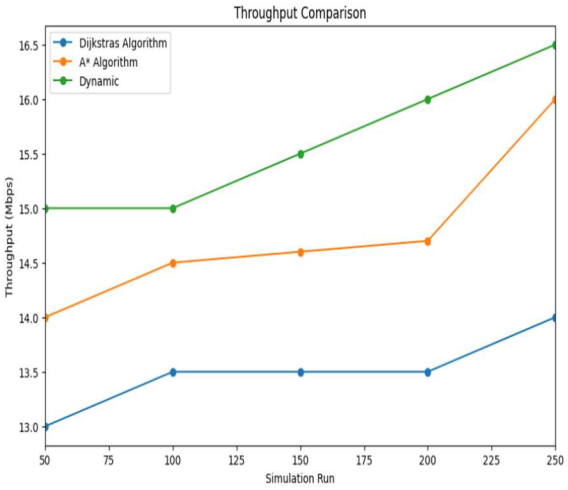

Figure 7. Throughput Comparison using Dynamic routing

The above graph shown in Figure 7, will provide insights into the differences in performance

metrics between the three routing algorithms, enabling a comparison of their effectiveness in vehicular communication systems.

5. CONCLUSION

This paper describes a novel approach to improving the security and efficiency of vehicle communication systems, with a particular emphasis on the exchange of information between vehicles (V2V) and infrastructure (V2I). This study proposes the Vehicle-Authorised Shortest Route Selection Algorithm, which prioritizes secure routes based on vehicle authorization. This approach helps to reduce potential security risks that may arise during data exchange. The algorithm guarantees the integrity and confidentiality of transmitted information by incorporating cryptographic authentication mechanisms. In addition, by integrating optimized routing protocols such as the A* algorithm, it determines the shortest routes, taking into account factors such as traffic conditions and network congestion. The main goal is to minimize the loss of data during transmission, guaranteeing an accurate and secure exchange of information between vehicles and infrastructure. This algorithmic solution enhances both route selection and network security, offering a strong framework for efficient and secure vehicular communication systems.

6. FUTURE SCOPE

The future possibilities for this research lie in enhancing the proposed algorithm while incorporating it into real-world vehicular communication systems. An area of future research could involve investigating the scalability of the Vehicle-Authorised Shortest Route Selection Algorithm to handle larger vehicular networks that have a greater amount of data exchange. Furthermore, there is potential for enhancement in optimizing the algorithm's efficiency in managing dynamic changes in network topology and traffic patterns. Moreover, the incorporation of sophisticated machine learning methods could improve the algorithm's capacity to adjust to changing security risks and optimize the selection of routes in real-time. Furthermore, carrying out thorough field trials and performance evaluations in a wide range of urban and rural settings will yield valuable insights into the algorithm's efficacy and practical feasibility. Ultimately, future enhancements to vehicular communication systems could be achieved by investigating the potential connections between emerging technologies like 5G networks, edge computing, and block chain. This exploration could lead to increased security, efficiency, and reliability.

REFERENCES

[1]. Eryilmaz and R. Srikant, “Fair resource allocation in wireless and v2v networks using queue-length-based scheduling and congestion control”, in Proc. IEEE INFOCOM, 2016, vol. 3, pp. 17941803.

[2]. M.Neely,E.Modiano,andC.Li,”Fairness and stochastic optimal control for heterogeneous networks”, in Proc. IEEE INFOCOM,Miami,FL,Mar.2017,vol.3,pp.1 7231734.

[3]. G. B. Folland, “Real Analysis: Simple Techniques and Their Applications, and their uses”, 2nd ed. New York, NY, USA: Wiley, 2018.

[4]. Bhattacharya, Pronaya and Tanwar, Sudeep and Bodkhe, Umesh and Kumar, Ashwani and Kumar, Neeraj, “Evblocks: A blockchain-based secure energy trading scheme for electric vehicles underlying 5g-v2x ecosystems,” Wireless Personal Communications, pp. 1–41, 2021.

[5]. V. Sharma, I. You, and N. Guizani, “Security of 5G-V2X: Technologies, Standardization, and Research Directions,” IEEE Network, vol. 34, no. 5, pp. 306–314, 2020.

[6]. H. M. Furqan, M. S. J. Solaija, J. M. Hamamreh, and H. Arslan, “Intelligent Physical Layer Security Approach for V2X Communication,” 2019.

[7]. J. J. Alcaraz, L. Caballero-Arnaldos, and J. Vales-Alonso, “Rich vehicle routing problem with last-mile outsourcing decisions,” Transportation Research Part E: Logistics and Transportation Review, vol. 129, pp. 263– 286, 2019.

[8]. D. Y. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, “A survey on platoon-based vehicular cyber-physical systems,” IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 263–284, 1st Quart., 2016.

[9]. S. S. Moni and D. Manivannan, “A scalable and distributed architecture for secure and privacy-preserving authentication and message dissemination in VANETs,” Internet Things, vol. 13, Mar. 2021, Art. no. 100350.

[10]. T. Wang, Y. Cao, Y. Zhou, and P. Li, “A survey on geographic routing protocols in delay/disruption tolerant networks,” Int. J. Distrib. Sensor Netw., vol. 12, no. 2, pp. 1–12, 2016.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[11]. J. Liu, J. Wan, Q. Wang, P. Deng, K. Zhou, and Y. Qiao, "A survey on position-based routing for vehicular ad hoc networks," Telecommun. Syst., vol. 62, no. 1, pp. 15–30, May 2016.

[12]. F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[13]. J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks," IEEE Trans. Intell. Transp. Syst., vol. 20, no. 5, pp. 1621–1632, May 2018.

[14]. Q. Xie, P. Zheng, Z. Ding, X. Tan, and B. Hu, "Provable secure and lightweight vehicle message broadcasting authentication protocol with privacy protection for VANETs," Secur. Commun. Netw., vol. 2022, pp. 1–10, May 2022, doi: 10.1155/2022/3372489.

[15]. A. Joshi, P. Gaonkar, and J. Bapat, "A reliable and secure approach for efficient car-to-car communication in intelligent transportation systems,"16in Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET), Mar. 2017, pp. 1617–162.

[16]. G. B. Folland, Real Analysis: Simple Techniques and Their Applications, and their uses 2nd ed. New York, NY, USA: Wiley, 2018.

[17]. Lee, Jaekyu et al. "When Prefetching Works, When It Doesn't, and Why." ACM Trans. Archit. Code Optim. 9 (2012): 2:1-2:29.

[18]. A. Warrier, S. Janakiraman, H. Sangtae, and I. Rhee," DiffQ: Practical differential backlog congestion control for wireless networks", in Proc.IEEE Conf. Comput. Commun., Apr. 2015, pp.262270.

[19]. M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the Internet of Vehicles," IEEE Internet Things J., vol. 8, no. 2, pp. 1123–1139, Jan. 2021.

[20]. H. Qiu et al., "A User-Centric Data Protection Method for Cloud Storage Based on Invertible DWT," IEEE Trans. Cloud Computing, 2019.

[21]. F. Haidar, A. Kaiser, and B. Lonc, "On the Performance Evaluation of Vehicular PKI Protocol for V2X Communications Security," Proc. IEEE 86th Vehicular Technology Conf. (VTCFall), 2017.

[22]. J. Petit and S. Shladover, "Potential Cyberattacks on Automated Vehicles," IEEE Trans. Intelligent Transportation Systems, vol. 16, no. 2, Apr. 2015, pp. 546–56.