International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *09 October 2023* ***Accepted:*** *18 October 2023*

Simulating MIMT Attackers' Strategies in VANET to Secure ITS in Smart Cities via Multiverse Optimization-based Hybrid Routing Approach

Sumit[1], Rajender Singh Chhillar[2], Sandeep Dalal[3]
[1]Department of Computer Science & Applications, Maharshi Dayanand University, Rohtak, Haryana, India
e-mail: sumit.rs.dcsa@mdurohtak.ac.in
[2]Department of Computer Science & Applications, Maharshi Dayanand University, Rohtak, Haryana, India
e-mail: rajender.dcsa@mdurohtak.ac.in
[3]Department of Computer Science & Applications, Maharshi Dayanand University, Rohtak, Haryana, India
e-mail: sandeepdalal@mdurohtak.ac.in

Abstract—The connection between moving vehicles and stationary Road Side Units is made possible by VANET technology, which is an essential component of Intelligent Transportation Systems. Vanet based intelligent transportation system (ITS) security is major issue in present days. MIMT Attackers' Strategies are taken into account to test the security of VANET based ITS system in present research paper. The major objective of research paper is to evaluate the potential of security model in case of different type of message dropping and delay attack. It is observed that there is probability of message delay, message drop, and message tampering attack in VANET based ITS system. Due to such attacks there is huge impact on content delivery ratio, packet delay and dropping. Thus proposed hybrid routing approach that is considering Multi-verse optimization has been used to simulate the Quantifying MIMT attacks. In present research, Vanet security in case of intelligent transportation system in smart cities has been considered.

Keywords- VANET, MVO, Routing, Intelligent Transportation Systems (ITS), MITM.

I. INTRODUCTION

VANET technology is an integral aspect of ITS since it acts as a transmission between mobile vehicles (cars) and stationary infrastructure. Some examples include alerts before dangerous curves, warnings of approaching crashes, and even in-car entertainment. It's possible that both traffic flow and safety may benefit from cars being able to exchange critical information with one another. One approach is to lessen the number of mishaps brought on by motor vehicle crashes [1]. Attacks on the communication between nodes, such as MITM attacks [2], are a key cause for worry when it comes to VANET network security [3]. Such attacks happen when a malicious computer in the network modifies or intercepts data meant for two other, legal computers. We investigated the potential impact of several MITM attack vectors on VANET throughput [4]. Examples of such methods include the use of a fleet and the adoption of a random strategy. Delay in communication, dumping of messages, and interference with transmission are the three primary goals of this investigation into MITM assaults [5]. The results of the simulations show the catastrophic effect that these attacks have on the individual nodes that make up a VANET. This leads to widespread packet loss, high latency, and communication interception [6]

A. Intelligent transport systems (ITS)

ITS are cutting-edge applications with the overarching goal of improving the way people utilise transport networks by making them more accessible, user-friendly, and effective [7]. Information can be sent in a wide variety of ways, including over wired or wireless connections, via Fibre optics, for ETC, CYO, parking management, signal preemption, in-vehicle signage, in-vehicle traveler information, and beacon-based route guiding systems [8]. Using technology for sensing, analysing, controlling, and communicating within the context of ground transportation to improve security, accessibility [9], and productivity is what is meant by the phrase ITS. This setup makes use of a VANET network. ECUs and other parts within a car need to communicate with one another so that they can carry out the many dispersed control tasks that need to be performed [10]. CAN, or Controller Area Network, is a serial bus used in many modern electronic devices, and FlexRay are just a few examples of in-vehicle networks that provide this kind of communication inside a given vehicle. Security assaults, in which an adversary takes entire control of the car from a distance, oblivious to the driver's actions, have previously been shown to be a weakness of in-vehicle networks. Figure 1 shows an example of safe and intelligent transportation. In order to maximize efficiency, Fig.1 shows how connected cars might form "convoys" via the use of V2V

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *09 October 2023* ***Accepted:*** *18 October 2023*

(vehicle-to-vehicle) communication. The study of VANETs has made it feasible for cars to share information and form clusters [11]. To improve the security and efficacy of transportation networks, cars may form a network using wireless communication devices to share information about hazards, travel times, and more

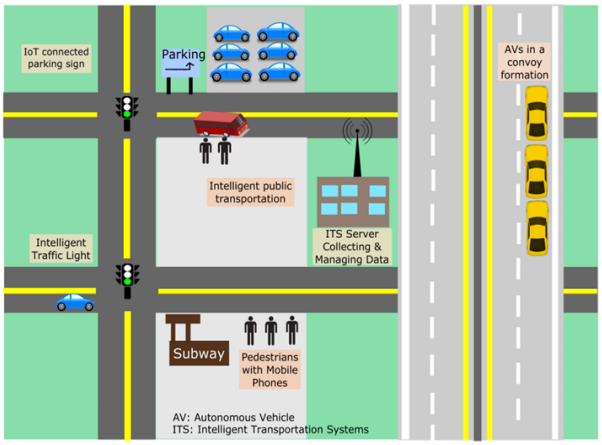

Figure 1. Smart and secure intelligent transportation [26]

However, there is still a safety concern. As a result, the smart intelligent transportation system must include safety measures. Security eliminates the risk of assault from the outside [12]. The VANET system enabling clever intelligent transportation consists of various levels, including the application layer and the perception layer. The data is protected and shared across levels via the privacy and security layer [13].

B. Attacks on VANET

The propagation of messages over the network must occur in an environment that is secure, trustworthy, and free from attack because of the sensitive nature of VANET [15]. Information shared on VANET, such as advisories concerning black ice, is of the highest significance; as such, it must be authentic and sourced from legitimate channels. Availability and data integrity are two more standard security features that the network must provide [16]. A VANET network poses a significant danger to its users, however defending the network is difficult due to the network's exposure to a broad range of threats [17]. MITM attack occurs when a malicious node intercepts or modifies communications between two legitimate vehicles [18]. Important data may be included in the transmission, such as cautions regarding dangerously steep slopes. This compromises the network's availability, confidentiality, and integrity since compromised and incorrect information is propagated across the system [19]. The distribution of compromised information through malicious MITM nodes has the potential for significant ramifications on the network because of the direct involvement of human life in VANET. Rogue nodes, for instance, may cause car

accidents by interfering with steep-curve warning systems [20].

MITM attacks occur when malicious nodes in a VANET forge, drop, or delay critical network information. An adversary may use either a passive or an aggressive MITM assault. MITM assault might be launched against a police car [21], which might result in the sale of sensitive information. If an attacker is present in the network, data that is actively received may be distorted, garbled, or lost altogether [22].What if your attacker finds out anything vital, like the fact that you got a crash alert? If the MITM attacker modifies the content of the message, delays or drops the message, or does both, this might have a major impact on the network. Not only that, but the attack patterns and methods themselves may have a major impact on network speed and stability [23]. To give you an example, the effects of the assailants' individual assaults are different from those of their collective attacks. Therefore, the network's efficiency varies from case to case. However, present studies do not account for MITM attacks that use a wide range of attack techniques. As a result, it has been suggested to do research on the means by which man in the middle might be avoided [24, 25], filling the resulting knowledge gap.

C. Research Motivation

A new computing paradigm, IoT enables the networked gathering, analysis, and dissemination of data from a broad range of sensor- and processor-enabled devices. WiFi, LTE, and 5G are just some of the communication technologies that allow these devices to connect to the internet and power a wide range of smart building and home applications. With the help of VANET, millions of automobiles throughout the globe may be connected to improve traffic flow.Using V2V or V2I communication, the smart automobiles in a VANET network, each with its own individual set of sensors, may intelligently share information and provide a broad variety of services. Uses for this technology range from traffic management to warning drivers of potential dangers and assisting them in avoiding congestion and accidents.

II. LITERATURE REVIEW

The EHTAR routing system for VANET was developed by Lo et al. (2015) [1] and it has the potential to be beneficial for the infrastructure of the city. Active nodes of the network were positioned in such a manner as to monitor all of the roads in real time. These nodes were carefully placed at junctions. A Junction-Tracker was the name of this piece of machinery in the past. The nodes in the network would be motivated to open up to one another and share information in order to enhance the coordination.

The study that was carried out by Sandeep Arora and colleagues (2016) [2] did research on the algorithms that move data across moving cars' networks. They offered a thorough categorization of routing systems, one that accounted for the many advantages of each approach and the various uses to

which it was best suited. The Intelligent Transportation System was developed as a result of extensive consideration given to all of the available choices in terms of transportation.

Some position-based routing algorithms were presented in Neha Goel et al.'s (2016) [3] research. This survey is designed to be filled out by anybody who has an interest in successful position-based routing systems and how they operate.

Brenda et al. (2017) [4] proposed the novel VANET to decrease traffic accidents and improve road safety. The difficulty of deciding on a routing scheme was compounded by the nodes' mobility. This has serious ramifications for the network's architecture when considering maximum throughput that data packets might achieve. This made it even more difficult to decide on a routing strategy. The present ways that are often employed to overcome routing difficulties were analyzed in this article, and it was shown how such approaches had all failed up to this point.

Qin et al. [5] used a network-dependent technique to explore how VANET routing methods impact traffic signal timing and vehicle density. Based on their results, they developed a new routing protocol to put their findings into practise. If just unicast packets are monitored, it may be possible to achieve the highest possible level of performance.

MITM attacks on automobile ad hoc networks were the topic of F. Ahmad et al.'s (2018) [6] research, as well as how the effects of these attacks might be assessed. Two-way communication between moving vehicles and stationary RSU, which is made possible by VANET, a crucial component of ITS technology, is required in order for some services, like as collision avoidance warnings and in-car entertainment, to function properly. The findings of the simulations indicate that the genuine nodes that make up a VANET suffer a great deal as a consequence of these assaults, including high rates of messages that have been corrupted.

In 2018, N. B. Gayathri and colleagues [7] developed the first technique that is successful in dealing with VANETS. The development of a pair-free platform, which speeds up both the transport of data and the processing of data, was the primary impetus for the breakthrough. This method not only reduces the complexity of the processing tasks in VANETs but also makes it simpler and more efficient to analyze batches of data.

Quick and effective unicast routing techniques were introduced by A.U. Khan [8]. Specifically, Vehicular Ad Hoc Network has made use of this technology. This study's survey and suggestions were made to boost productivity.

Gazori et al. (2019) [9] examined a unique plan to use traffic lights as bridges to reroute traffic that is actively moving rather than traffic that is stopped at a stop sign. This would ensure that the network was stable during the whole process of route selection. The transmission of data packets across bridge nodes was intended to be made less complicated as a direct result of the development of this protocol's main goal. After taking into consideration the total throughput as well as the total number of intermediate stops, the most time- and cost-effective route was selected.

By optimizing the cluster's lifespan while minimizing its overhead, Joshua et al. (2019) [10] addressed a multi-objective issue utilizing RWCP settings as input. The best configuration settings for the RWCP variables (MOFA) were determined using a version of the Multi-Objective Firefly Algorithm still under development. The analysis is carried out using the same evolutionary optimization approaches. In addition to this, they contrasted the results of their experiments with those obtained by MOPSO and CL-PSO, which are two further multi-objective optimization algorithms. For this purpose, they used real maps obtained from Open Street Maps.

For use in applications for mobile ad hoc networks (also known as VANETs), Cardenas et al. [11] developed an entirely new protocol that they named ProMRP. They should have done the following, since the ProMRP makes use of specific procedures, if they want for their neighbour to pick up their package and effectively send it on their behalf.

Selective broadcast routing, which was based on cosine similarity, was merged in Nahar et al.'s (2020) [12] research. Clustering was used to achieve optimisation of the data delivery channels in this technique. Using the strategy that was advised resulted in a decrease in latency of up to 25% while simultaneously leading to an increase in PDF of between 5% and 10%.

Research conducted by Nazib et al. (2020) [13] looked at the role that routing protocols play in VANETs. They might be assigned to one of seven different categories dependant on the practicality of their code as well as the originality of their ideas.

Debnath et al. (2021) [14] outlined two primary factors that should be taken into account while developing a transport mechanism. They had succeeded in developing the very first metric, and they decided to call it the CQF. In the current technique, in addition to CQF, the "Communication expiry time" option was used in order to identify the vehicle that was to be utilized for forwarding. The simulation results showed that our suggested technique outperformed the existing systems across a wide range of traffic and population concentrations.

In order to improve the quality of service provided by VANET, Nazib et al. [15] developed RL-based routing techniques. Bandwidth and packet delivery ratio are two examples of QoS and Quantity properties. The new approach was far more successful than the previous one by a wide margin.

Singh et al. (2022) [18] offered a recommendation to increase the speeds at which VANET users may communicate with one another. To optimize routes in both sparse & dense VANETs, they employed a combination of GA characteristics and the Firefly algorithm. The innovative HGFA algorithm provided superior outcomes than those attained by the Firefly

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 12 August 2023 **Revised:** 09 October 2023 **Accepted:** 18 October 2023*

and PSO approaches, by a margin of 0.77 and 0.55 percentage points, respectively, in both the packed and sparse network conditions.

The DORA for automotive AHN was introduced by Satyanarayana Raju and colleagues in 2022 [20]. The primary goals of the research were to reduce the number of traffic accidents and to improve road safety. The network's mobile nodes, its dynamic topology, and the absence of a centralised controller all add to the complexity of routing while at the same time allowing for little overhead and delay in the delivery of messages.

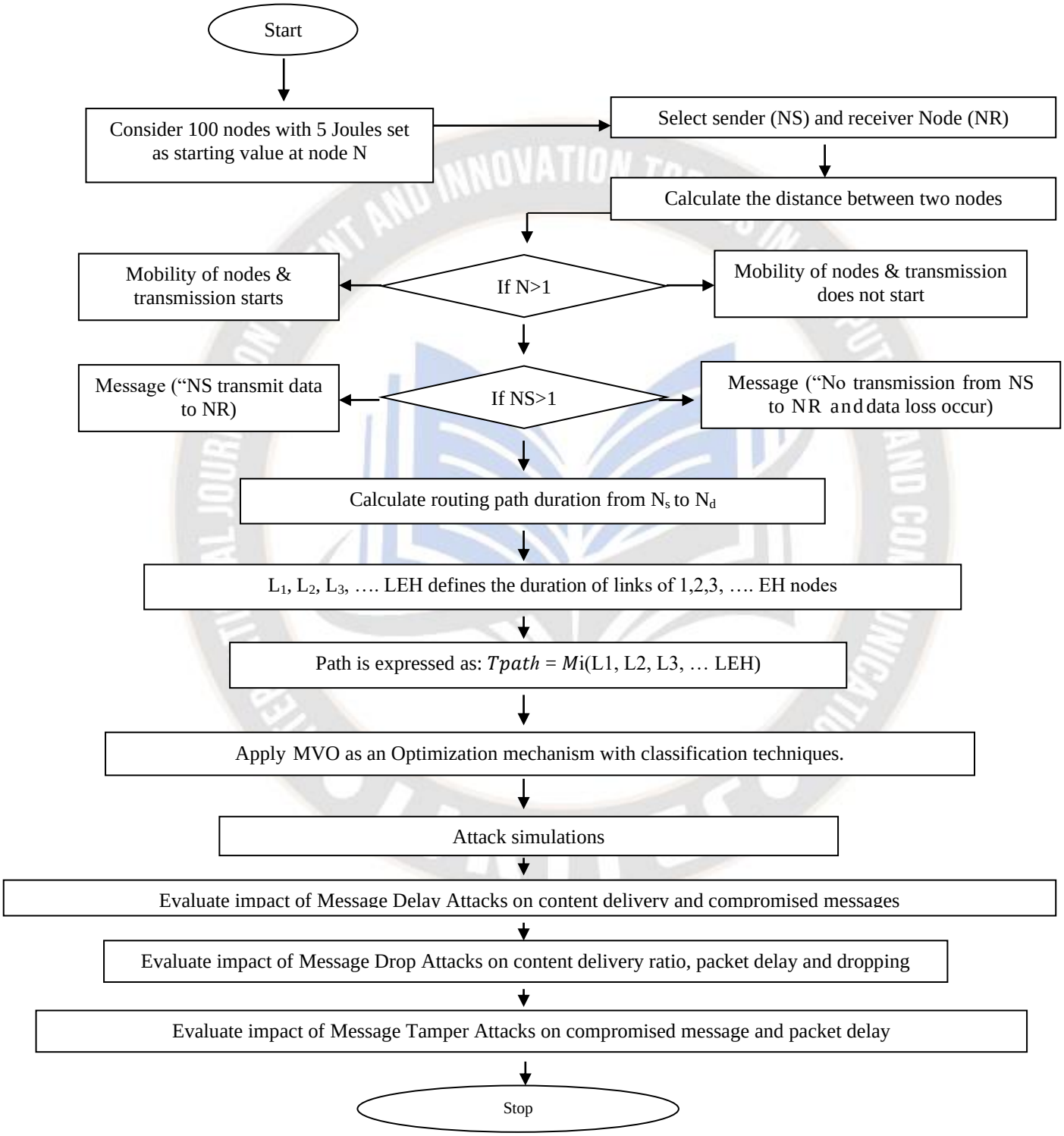

Figure 2. Process flow of proposed Hybrid model to simulate Attackers' Strategies

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *09 October 2023* ***Accepted:*** *18 October 2023*

III. PROPOSED WORK

Present work is focusing on Multiverse optimization as a potential solution to the issues of end-to-end latency and content delivery ratio. Advanced sorting and routing algorithms are required for smart city transit systems. This model is crucial for smart city transportation since it incorporates route classification and optimization methods. The precision of Vanets is the subject of contemporary research. The safety of a node may be evaluated using these techniques. The aim is to integrate MVO optimization into existing initiatives. The MVO algorithm has theoretical ties to black holes, white holes, and wormholes. Mathematical models are constructed using these three principles in order to assess exploitation and local search. It is believed that white holes are the primary cause of the Big Bang and subsequent cosmic expansion. Black holes have so strong gravity that they devour anything in their vicinity. In the same way as time and space tunnels facilitate speedy interplanetary transit, so do wormholes. Mvo-based hybrid dynamic and optimized routing approach (MHDORA)

The MHDORA technology allows geographical routing to be determined on the fly. It's likely that choosing safe routes throughout the network might benefit from taking into account the traffic density and number of automobiles at intersections. Using maps, we may find specific intersections. The junction is chosen as the next stop based on a score that considers the average transit time between metric curves and the amount of traffic travelling through each. Popular websites now load much faster than before. When deciding which route to follow next, a packet's past travels are taken into account. A network node will transmit data to the server (gateway) whenever it is in range to do so. Every vertice is linked to the hub in its own unique way. The software considers a broad range of criteria, such as supplying continuous energy to all vehicles, determining the most efficient routes, recovering previously used routes, performing dynamic rerouting, and recovering previously used routes. The optimal path is determined by the MHDORA based on data collected from the base stations. The BS will use the messages as a means of responding to the route inquiry. Figure 3 is presenting process flow of proposed Hybrid model.

It is possible to compare the journey times and costs of two vehicles to find the optimal route. Our use of Euclidean distance as the basis for determining the appropriate spacing between automobiles is an illustration of the importance of distance. It is also taken into account that the algorithm may dynamically reroute automobiles without disrupting the supply of electricity to anybody. Using information gathered from base stations, the MHDORA chooses a path. The BS will use the messages as a means of responding to the route inquiry. It is possible to compare the journey times and costs of two vehicles to find the optimal route. Our use of Euclidean distance as the basis for determining the appropriate spacing between automobiles is an illustration of the importance of distance. Algorithm of Proposed model is shown below:

Algorithm

Step 1. Data Collection:

- Collect relevant data needed for routing
- Network topology
- Traffic demand
- dynamic data sources

Step 2. Network Representation:

- Represent the network as a graph, where nodes represent locations or intersections
- Edges represent road segments or links.

Step 3. Multi-Objective Optimization (MVO):

- Define multiple objectives you want to optimize, which could include minimizing travel time
- Minimizing fuel consumption
- Maximizing traffic flow efficiency
- Set up a multi-objective optimization framework that takes into account these objectives.

Step 4. Dynamic Updates:

- Implement a mechanism for dynamically updating the routing based on real-time data
- Traffic congestion
- Accidents
- Weather conditions.

Step 5. Hybrid Routing Strategy:

- Develop a hybrid routing strategy that combines static and dynamic routing.

$$Route(x,y) = \begin{cases} Static\ Route\ (x,y) & if\ condition\ (x,y)\ is\ met \\ Dynamic\ Route\ (x,y,t) & otherwise \end{cases}$$

Where

Route(x,y) represents the selected route from node x to node y.

Static Route(x,y) computes the route using the static routing algorithm.

Dynamic Route(x,y,t) computes the route using the dynamic routing algorithm at the current time t.

Condition(x,y) is a condition or set of conditions that determine whether to use the static or dynamic routing.

- Define rules or heuristics for switching between static and dynamic routing based on the current traffic conditions or other relevant factors.

Step 6. Path Selection:

- Implement an algorithm for selecting the optimal paths for each objective.

Let $G = (V, E)$ be a weighted graph representing the network, where

V is the set of nodes (vertices) in the network

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *09 October 2023* ***Accepted:*** *18 October 2023*

E is the set of edges (links) between nodes, with associated weights or costs.

- This could involve various techniques such as Dijkstra's algorithm, A* search, or genetic algorithms, depending on the complexity of the problem.

Step 7. Pareto Front Analysis:

- Calculate and analyze the Pareto front, which represents the trade-offs between the different objectives.

Consider a multi-objective optimization problem with m objectives and a set of solutions *S*, where each solution x_i is associated with a vector of objective values $F(x_i) = (f_1(x_i), f_2(x_i), \dots, f_m(x_i))$.

The goal of Pareto Front Analysis is to find the Pareto front, which consists of solutions that are not dominated by any other solutions. A solution x_i is said to dominate another solution x_j if:

$$\forall k \epsilon \{1,2,\dots,m\}: f_k(x_i) \leq f_k(x_j) \text{ and}$$
$$\exists k \epsilon \{1,2,\dots,m\}: f_k(x_i) < f_k(x_j)$$

In other words, x_i dominates x_j if it is at least as good as x_j in all objectives and strictly better in at least one objective.

The Pareto front consists of all non-dominated solutions in the solution set *S*. Here are the general steps for Pareto Front Analysis:

1. **Initialization:** Start with an empty set PF to store the Pareto front.
2. **Non-Domination Check:** For each solution x_i in the set *S*, check whether it is dominated by any other solution in *S*. If x_i is not dominated, add it to PF.
3. **Remove Dominated Solutions:** Remove any solutions from *S* that are dominated by x_i. This step ensures that we are left with only the undominated solutions for the next iteration.
4. **Repeat:** Repeat steps 2 and 3 until no new solutions are added to PF.
5. **Pareto Front:** PF now contains the Pareto front solutions, which represent the trade-offs between the multiple objectives.

- Select a suitable solution from the Pareto front based on user preferences or policies.

Step 8. Real-time Updates and Feedback:

- Monitor the network for changes and update the routing accordingly.
- Collect feedback data to improve the performance of the routing algorithm over time.

Step 9. User Interface:

- Develop a user-friendly interface that allows users to input their preferences
- view route suggestions
- receive real-time updates

Step 10. Testing and Validation:

- Test the algorithm using historical data
- Simulations to ensure that it meets the defined objectives
- find performance metrics.

Step 11. Deployment:

- Deploy the routing system in a real-world environment, if applicable, and monitor its performance in practice.

Step 12. Maintenance and Updates:

- Regularly update the algorithm and data sources to adapt to changing conditions and improve performance.

Step 13. Attack simulations

Step 14. Evaluate impact of Message Delay Attacks on content delivery and compromised messages

Step 15. Evaluate impact of Message Drop Attacks on content delivery ratio, packet delay and dropping

Step 16. Evaluate impact of Message Tamper Attacks on compromised message and packet delay

MITM attacks in VANET have been evaluated using the location map. The network's current complement of 200 cars is more than enough to handle most urban emergencies. An incident (a car crash) involving many vehicles is triggered at a location picked at random from the network. The cars disseminate this information throughout the neighbourhood for mutual use. The cars in the picture wait a little time, then decide to take another route to escape the congestion after hearing this. To learn more about the impact of these adversaries, we measured delays, dropouts, and modifications to the transmitted data after inserting 10%, 20%, 30%, 40%, & 50% hostile nodes into the network. Table 1 displays the simulation results.

TABLE I. SIMULATION DETAILS

Simulation	Parameters
Framework	Network simulator Traffic simulator V2X simulator
Description	No. of Vehicles No. of RSUs No. of Malicious Nodes Simulation Area Simulation Time
Protocols	MAC Protocol Network Protocol Radio Propagation Model

IV. RESULT AND DISCUSSION

The results of man-in-the-middle assaults on a VANET are described. Based on the aforementioned two scenarios, we simulated MITM attacks and evaluated the network's resilience

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *09 October 2023* ***Accepted:*** *18 October 2023*

using the aforementioned metrics. Twenty-five simulations are conducted for each scenario, with a new random seed value used to distribute automobiles around the network in the first place. It follows is an average of 25 separate simulations for each scenario.

A. Message Delay Attacks

E2E delay that occurs when MITMs cause packet delays of 2 seconds is seen in the following figure. Malicious nodes that induce delays to otherwise lawful connections raise the E2E latency. However, MITM attackers with message-delaying capability slow down the delivery of these legitimate communications to the authorized nodes. Furthermore, the image demonstrates that E2E latency grows when attackers are scattered throughout the network. The total end-to-end (E2E) latency of the network increases when it is disrupted on a large scale by geographically dispersed attackers. But the fleet's attackers are just slowing down traffic in some regions. Therefore, there are only little delays in the network from end to end, even when an assault fleet is present. In Table 2, Delay in case of message delay attack has been simulated. It is observed that as number of malicious nodes increases, the delay also increases. But proposed work is showing less delay as compared to conventional work.

TABLE II. DELAY IN CASE OF MESSAGE DELAY ATTACKS

Malicious Node	Conventional Work	Proposed work
10	232.032172	241.15399
20	400.947792	417.67957
30	427.738957	439.86706
40	486.929111	526.35321
50	532.26034	573.132

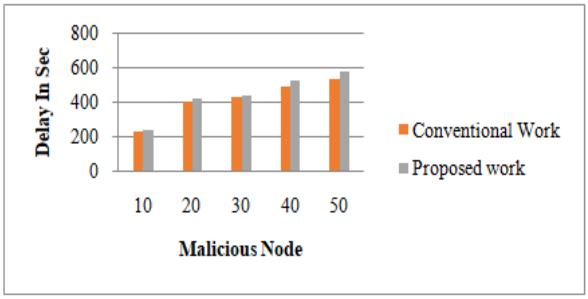

Figure 3. Delay in Case of Message Delay Attacks

Table 3 is presenting content delivery ratio in case of message delay attacks. It is concluded that as number of malicious nodes increases, the content decreases. But proposed work is showing less decrement in content delivery as compared to conventional work.

TABLE III. CONTENT DELIVERY RATIO IN CASE OF MESSAGE DELAY ATTACKS

Malicious Node	Conventional Work	Proposed work
10	96.6	97.9
20	91.1	96.2
30	84.1	94.1
40	79.6	91.2
50	67.6	79.1

By considering table 3, figure 5 is showing graph of delivery ratio in case of message delay attacks. Figure is presenting that content delivery ratio of proposed work is more than that of conventional work.

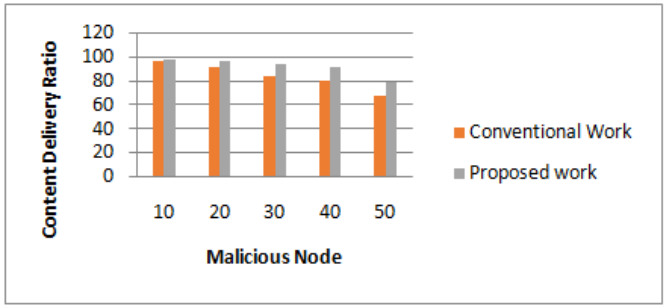

Figure 4. Content Delivery Ratio in Case of Message Delay Attacks

Table 4 is presenting compromised Message in Case of Message Delay Attacks. It is observed that as number of malicious nodes increases, the compromised messages also increase. But proposed work is showing less increment in compromised message as compared to conventional work.

TABLE IV. COMPROMISED MESSAGES IN CASE OF MESSAGE DELAY ATTACKS

Malicious Node	Conventional Work	Proposed work
10	10.4	8.0
20	20.3	18.4
30	27.0	24.0
40	40.5	37.5
50	51.2	46.6

Considering table 4, fig 6 is presenting comparison of compromised message in case of conventional and proposed work.

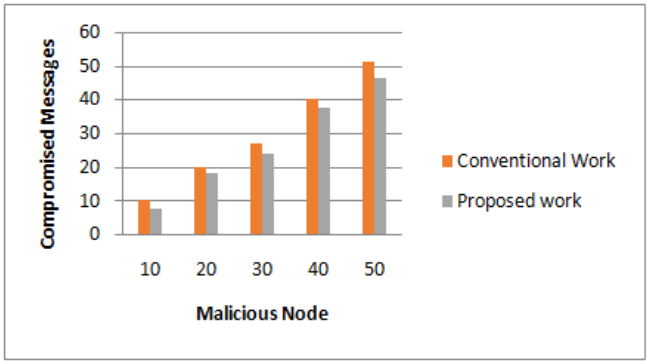

Figure 5. Compromised Messages in Case of Message Delay Attacks

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *09 October 2023* ***Accepted:*** *18 October 2023*

Table 5 is presenting packet delay ratio in case of message delay attacks. It is concluded that as number of malicious nodes increases, the packet delay decreases. But proposed work is showing less decrement in packet delay as compared to conventional work.

TABLE V. PACKET DELAY RATIO IN CASE OF MESSAGE DELAY ATTACKS

Malicious Node	Conventional Work	Proposed work
10	10.1	8.4
20	18.1	15.2
30	31.3	28.4
40	51.4	48.3
50	60.1	56.2

By considering table 5, figure 7 is showing graph of delay ratio in case of message delay attacks. Figure is presenting that packet delay ratio of proposed work is more than that of conventional work.

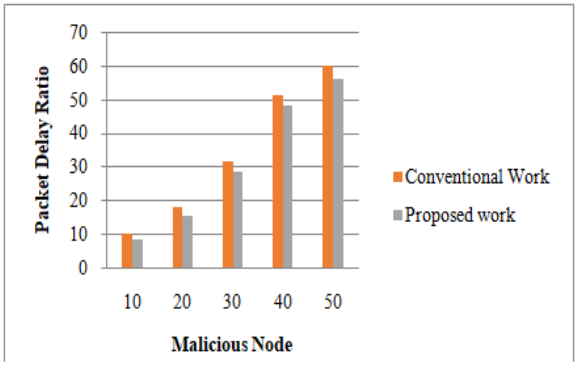

Figure 6. Packet Delay Ratio in Case of Message Delay Attacks

B. Message Drop Attacks

It shows how the CDR drops when malicious nodes are added to a network and cause messages to be dropped. The network also ensures a large amount of material remains accessible, even if it has been compromised by an army of hostile attackers. Since the attacker's reach is limited, any compromised data will only affect that specific location. The local nodes may be able to listen in on conversations from legitimate nodes. To be more specific, when there are malicious nodes dispersed over the network, they might trash genuine packets, which can lead to a low CDR. Assuming 10% of nodes are malicious, the CDR of the network with fleet harmful nodes will be about 12.44 percentage points greater than the CDR of the network with malicious nodes scattered apart. Even with 50% more malicious nodes, the CDR is lower (44.89%) in networks experiencing a fleet attack. This is due to the fact that when potentially hazardous vehicles are scattered at random across the system, valuable information is lost. That's why whenever there are cybercriminals around, data is at danger. In the case of fleet attackers, however, information is only deleted at certain network nodes, while other nodes in the network may continue to exchange data with one another. As the number of malicious nodes in a simulated network grows, the percentage of communications lost rises sharply. Almost as many messages are lost while using scattered as when using FAP, yet both have a significant impact on the network. Packet loss generated by fleet attackers is, for instance, 4.60 percentage points more than that caused by scattered attackers in a network where 50% of nodes are under attack. Table 6 is showing delay in case of message drop attacks.

TABLE VI. DELAY IN CASE OF MESSAGE DROP ATTACKS

Malicious Node	Conventional Work	Proposed work
10	244.975441	278.71431
20	417.975763	456.81152
30	425.170595	469.44442
40	477.760615	501.388
50	502.77177	511.434

By considering table 6, figure 8 is showing graph of delay in case of message drop attacks. Figure is presenting that delay of proposed work is more than that of conventional work.

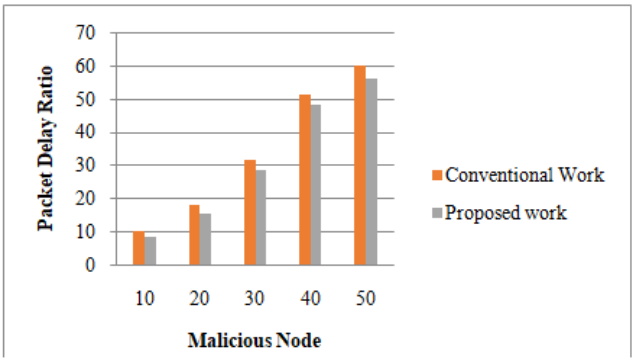

Figure 7. Delay in Case of Message Drop Attacks

Table 7 is presenting Content Delivery Ratio in the Case of Message Drop Attacks.

TABLE VII. CONTENT DELIVERY RATIO IN CASE OF MESSAGE DROP ATTACKS

Malicious Node	Conventional Work	Proposed work
10	98.9	100.1
20	93.5	97.0
30	86.3	94.6
40	80.0	93.0
50	69.7	80.9

By considering table 7, figure 9 is showing graph of content delivery ratio in case of message drop attacks. Figure is presenting that content delivery ratio of proposed work is more than that of conventional work.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *09 October 2023* ***Accepted:*** *18 October 2023*

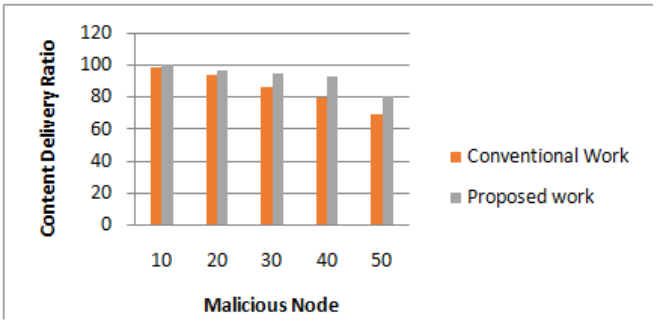

Figure 8. Content Delivery Ratio in Case of Message Drop Attacks

Table 8 is presenting the compromised message in case of message drop attacks.

TABLE VIII. COMPROMISED MESSAGES IN CASE OF MESSAGE DROP ATTACKS

Malicious Node	Conventional Work	Proposed work
10	9.2	8.8
20	21.3	18.3
30	28.7	25.5
40	40.6	36.8
50	51.7	44.0

Considering table 8, figure 10 is presenting that Compromised Messages in Case of Message Drop Attacks of proposed work is more than that of conventional work.

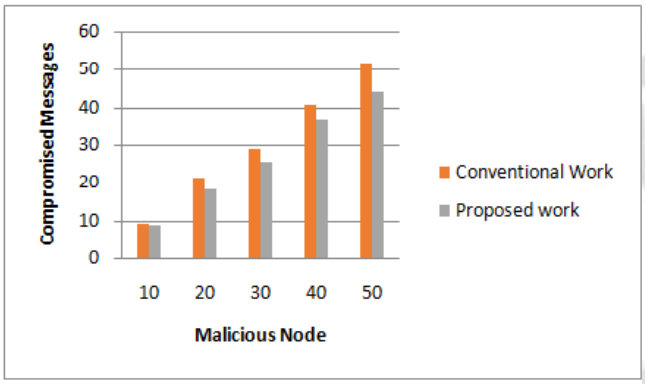

Figure 9. Compromised Messages in Case of Message Drop Attacks

Table 9 is showing packet delay ratio in case of message drop attacks

TABLE IX. PACKET DELAY RATIO IN CASE OF MESSAGE DROP ATTACKS

Malicious Node	Conventional Work	Proposed work
10	11.2	8.1
20	19.9	17.4
30	31.5	25.5
40	52.5	37.0
50	60.4	44.2

Considering table 9, figure 11 is presenting that packet delay ratio in Case of Message Drop Attacks of proposed work is more than that of conventional work.

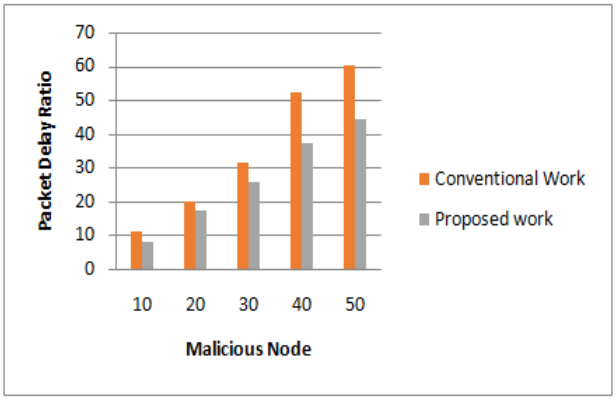

Figure 10. Packet Delay Ratio in Case of Message Drop Attack

C. Message Tamper Attacks

As was just discussed, the rogue node can tamper with the genuine message by changing its time, data, or location. In particular assault, we zeroed in on the message's content. As a result, anytime a rogue node receives a message, it alters the content into junk data and broadcasts it to the surrounding vehicles. End-to-end network latency caused by rogue nodes altering message content is seen in figure a below. To begin, it is clear that as the number of mobility of nodes grows, so does the network's E2E delay. Second, because of the wide range of attacks launched by scattered malicious nodes, the network has a large E2E delay in their presence. Conversely, a group of malicious nodes is initiating localized attacks, therefore low E2E delay is possible since legal messages are sent throughout a wide portion of a network. A network with 50% bad nodes, for instance, will have 69.91% higher E2E latency if scattered attackers are used instead of fleet attackers.

Table 10 is presenting delay in case of message tamper attacks

TABLE X. DELAY IN CASE OF MESSAGE TAMPER ATTACKS

Malicious Node	Conventional Work	Proposed work
10	193.95	254.03
20	381.83	453.04
30	400.07	435.00
40	418.34	458.39
50	448.34	509.91

Considering table 10, figure 12 is presenting that delay in Case of Message tamper Attacks of proposed work is more than that of conventional work.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *12 August 2023* ***Revised:*** *09 October 2023* ***Accepted:*** *18 October 2023*

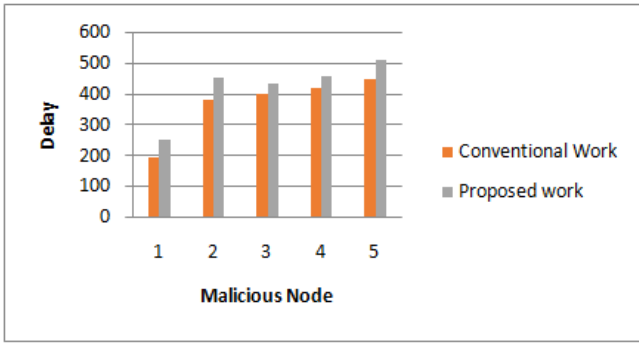

Figure 11. Delay in Case of Message Tamper Attacks

Table 11 is showing content delivery ratio in case of message tamper attacks

TABLE XI. CONTENT DELIVERY RATIO IN CASE OF MESSAGE TAMPER ATTACKS

Malicious Node	Conventional Work	Proposed work
10	96.4	99.6
20	90.7	94.4
30	82.5	92.8
40	76.9	91.1
50	66.1	80.9

Considering table 11, figure 13 is presenting that content delivery ratio in Case of Message tamper Attacks of proposed work is more than that of conventional work.

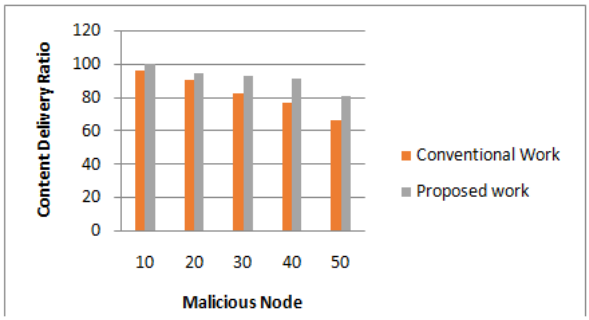

Figure 12. Content Delivery Ratio in Case of Message Tamper Attacks

Table 12 is presenting the compromised message in case of message tamper attacks

TABLE XII. COMPROMISED MESSAGES IN CASE OF MESSAGE TAMPER ATTACKS

Malicious Node	Conventional Work	Proposed work
10	9.9	6.5
20	22.1	16.2
30	29.2	18.5
40	41.1	35.8
50	52.5	40.1

Considering table 12, figure 14 is presenting that compromised message in Case of Message tamper Attacks of proposed work is more than that of conventional work.

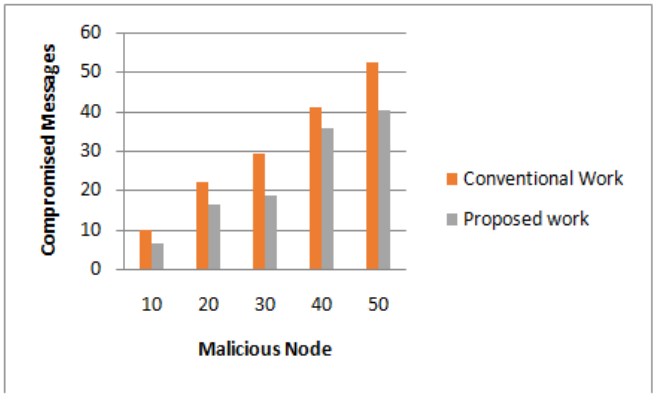

Figure 13. Compromised Messages in Case of Message Tamper Attacks

Table 13 is presenting the packet delay ratio in case of message tamper attacks

TABLE XIII. PACKET DELAY RATIO IN CASE OF MESSAGE TAMPER ATTACKS

Malicious Node	Conventional Work	Proposed work
10	11.5	5.1
20	19.8	14.1
30	31.6	25.6
40	52.3	34.6
50	59.7	40.8

Considering table 13, figure 15 is presenting that Packet delay ratio in Case of Message tamper Attacks of proposed work is more than that of conventional work.

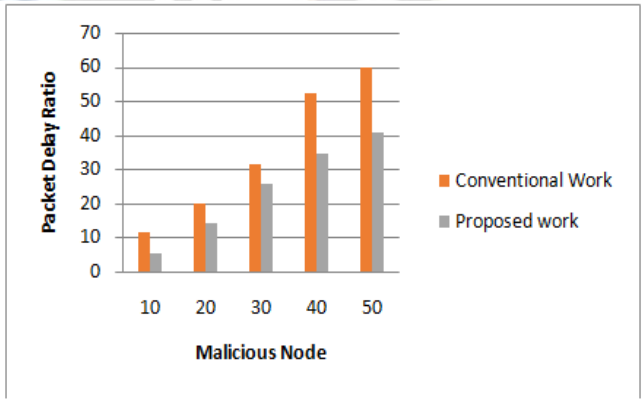

Figure 14. Packet Delay Ratio in Case of Message Tamper Attacks

The proposed improvement has been acknowledged to reduce latency while increasing the percentage of material delivered. In the case of the proposed work, the proportion of successfully sent packets has risen, and the number of compromised messages has dropped.

V. CONCLUSION AND SCOPE OF RESEARCH

Transportation in smart cities requires innovative approaches to classification and routing. The optimum route finding techniques included into this model classification and optimisation are crucial to smart city transportation. Our research presents a strategy for dealing with VANET networks'

various problems by combining dynamic routing with optimal routing. The proposed method determines the minimal travel time between two points. The little packet loss is also compensated for by this strategy. HDORA was designed with VANET data connections and inter-node communication in mind. Improvements in efficiency may be made with MHDORA's help. The simulation group has considered several different measures, including E2E latency, CDR, CM, and PLR. The suggested technique was shown to have higher security than ACO, DORA, and HDORA. There are a lot of issues with dynamic routing, and we'll need better simulation techniques to figure them out. The suggested system's security has been improved with the use of a machine learning technique. It has been determined that the suggested work lessens the possibilities of a MITM attack or a denial of service. There is a proposal for increased performance and security. Managing delays, content delivery, compromised messages, and packet delay ratios in the face of diverse attacks requires further research in this field. There will be less delay and more content will be supplied thanks to the suggested change. The suggested effort has resulted in a rise in the percentage of successfully sent packets and a fall in the percentage of compromised messages. Perhaps in the future we'll learn about a method that takes into account even more factors.

REFERENCES

[1] C. Lo and Y. Kuo, "Enhanced Hybrid Traffic-Aware Routing Protocol for Vehicular Ad hoc Networks," 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), 2015, pp. 1-6, doi: 10.1109/VTCFall.2015.7390924.

[2] Arora, Sandeep & Monga, Himanshu. (2016). A comprehensive review on routing in VANET. International Journal of Grid and Distributed Computing. 9. 375-384. 10.14257/ijgdc.2016.9.10.33.

[3] Goel, Neha & Sharma, Gaurav & Dhyani, Isha. (2016). A study of position-based VANET routing protocols. 655-660. 10.1109/CCAA.2016.7813803.

[4] R. Brendha and V. S. J. Prakash, "A survey on routing protocols for vehicular Ad Hoc networks," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), 2017, pp. 1-7, doi: 10.1109/ICACCS.2017.8014615.

[5] H. Qin and C. Yu, "A road network connectivity aware routing protocol for Vehicular Ad Hoc Networks," 2017 IEEE International Conference on Vehicular Electronics and Safety (ICVES), 2017, pp. 57-62, doi: 10.1109/ICVES.2017.7991901.

[6] F. Ahmad, A. Adnane, V. N. L. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," Sensors (Switzerland), vol. 18, no. 11, pp. 1–19, 2018, doi 10.3390/s18114040.

[7] N. B. Gayathri, G. Thumbur, P. V. Reddy and M. Z. Ur Rahman, "Efficient Pairing-Free Certificateless Authentication Scheme With Batch Verification for Vehicular Ad-Hoc Networks," in IEEE Access, vol. 6, pp. 31808-31819, 2018, doi: 10.1109/ACCESS.2018.2845464

[8] A.U. Khan, "Real-time and Efficient Unicast Routing Protocols for Vehicular Ad Hoc Network: A Survey and Recommendations for efficiency enhancement," 2018 15th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT (HONET-ICT), 2018, pp. 117-121, doi: 10.1109/HONET.2018.8551330.

[9] R. Gazori and G. Mirjalily, "SBGRP as an Improved Stable CDS-Based Routing Protocol in Vehicular Ad Hoc Networks," 2019 27th Iranian Conference on Electrical Engineering (ICEE), 2019, pp. 1979-1983, doi: 10.1109/IranianCEE.2019.8786705.

[10] L. L. Cardenas, A. M. Mezher, P. A. B. Bautista and M. A. Igartua, "A Probability-Based Multimetric Routing Protocol for Vehicular Ad Hoc Networks in Urban Scenarios," in IEEE Access, vol. 7, pp. 178020- 178032, 2019, doi 10.1109/ACCESS.2019.2958743.

[11] A. Nahar, H. Sikarwar and D. Das, "CSBR: A Cosine Similarity Based Selective Broadcast Routing Protocol for Vehicular Ad-Hoc Networks," 2020 IFIP Networking Conference (Networking), 2020, pp. 404-412.

[12] R. A. Nazib and S. Moh, "Routing Protocols for Unmanned Aerial Vehicle-Aided Vehicular Ad Hoc Networks: A Survey," in IEEE Access, vol. 8, pp. 77535-77560, 2020, doi: 10.1109/ACCESS.2020.2989790.

[13] Debnath, A.; Basumatary, H.; Dhar, M.; Debbarma, M.K.; Bhattacharyya, B.K. Fuzzy logic-based VANET routing method to increase the QoS by considering the dynamic nature of vehicles. Computing 2021, 103, 1391–1415.

[14] R. A. Nazib and S. Moh, "Reinforcement Learning-Based Routing Protocols for Vehicular Ad Hoc Networks: A Comparative Survey," in IEEE Access, vol. 9, pp. 27552-27587, 2021, doi: 10.1109/ACCESS.2021.3058388.

[15] Qoradi, M. D., Al-Harbi, M. S., and Aina, Y. A. (2021). Using GIS-based intelligent transportation systems in the enhancement of university campus commuting in a smart city context. Arabian Journal of Geosciences, 14(9). https://doi.org/10.1007/s12517-021-07098-z

[16] Belhadi, A., Djenouri, Y., Srivastava, G., and Lin, J. C. W. (2021). SS-ITS: secure scalable intelligent transportation systems. Journal of Supercomputing, 77(7), 7253–7269. https://doi.org/10.1007/s11227-020-03582-7

[17] Singh, G.D.; Prateek, M.; Kumar, S.; Verma, M.; Singh, D.; Lee, H.N. Hybrid genetic firefly algorithm-based routing protocol for VANETs. IEEE Access 2022, 10, 9142–9151.

[18] Sindhwani, M.; Sachdeva, S.; Arora, K.; Yoon, T.; Yoo, D.; Joshi, G.P.; Cho, W. Soft Computing Techniques Aware Clustering-Based Routing Protocols in Vehicular Ad Hoc Networks: A Review. Appl. Sci. 2022, 12, 7922. https://doi.org/ 10.3390/app12157922

[19] K. S. Raju and K. Selvakumar, “Dynamic and Optimized Routing Approach (DORA) in Vehicular Ad hoc Networks (VANETs),” Int. J. Adv. Comput. Sci. Appl., vol. 13, no. 3, pp. 151–156, 2022, doi: 10.14569/IJACSA.2022.0130320.

[20] Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., and Santos, O. (2022). Digital twins: artificial intelligence and

the IoT cyber-physical systems in Industry 4.0. International Journal of Intelligent Robotics and Applications, 6(1), 171–185. https://doi.org/10.1007/s41315-021-00180-5

[21] Dai, D., and Boroomand, S. (2022). A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges. Archives of Computational Methods in Engineering, 29(2), 1291–1309. https://doi.org/10.1007/s11831-021-09628-0

[22] Bento, M. E. C. (2022). Monitoring of the power system load margin based on a machine learning technique. Electrical Engineering, 104(1), 249–258. https://doi.org/10.1007/s00202-021-01274-

[24] Sumit and R. S. Chhillar, "A Review of Intelligent Transportation Systems in Existing Framework using IoT," *Int. J. Eng. Trends Technol.*, vol. 70, no. 6, pp. 137–143, 2022, doi: 10.14445/22315381/IJETT-V70I6P217.

[25] R. S. Chhillar and S. Dalal, "INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING Secure Multiverse Optimization based Dynamic Routing Approach for Intelligent Transportation System in Smart Cities," vol. 11, no. 2, pp. 252–261, 2023.