Security Problems in Vehicle Ad-Hoc Networks: Comprehensive Review

K.S. Hosan, W.A.H.V. Perera, W.A.D.T Jayawardhana, H.V.V. Priyadarshana, R.J.M.D.D.P. Wijesekara, S.V.A.A Indupama, A. Kelum, H.D.C.N. Gunawardana, K.R. Koswattage

Abstract Vehicle Ad-Hoc Networks (VANETs) are a widely used network type in transportation, and these network systems are rapidly updating and upgrading in the current world of vehicle communication. This paper comprehensively reviews the security issues, solutions, and vulnerabilities. This review paper fills the current research gaps in the research and review papers related to this topic and deeply discusses the future research opportunities by reviewing the VANETs security-related papers comparatively. Furthermore, this review paper not only reviews the security problems but also explains the real-time connectivity problems and other structure-oriented problems. According to the analysis of the VANETs, security issues are not the only problem because VANETs have some operational limitations. In the future, these VANETs will do a huge revolution in inter-vehicle communication. In addition to that, these Vehicle Ad-Hoc Networks (VANETs) are widely used in modern aircraft communications by integrating artificial intelligence and machine learning-based technologies. Current Vehicle Ad-Hoc Networks (VANETs) can communicate with 5G Mobile Ad-Hoc Networks (MANETs). Some special-purpose vehicles use Bluetooth and Wi-Fi-based VANETs to communicate with each other for security reasons. In the industrial world, these VANETs are known as Vehicular Ad-Hoc Networks.

***Index Terms*— VANETs, MANETs, ECU, CAV, AI, ML**

I. Introduction

IN the current automobile and transportation industries, Vehicle Ad-Hoc Networks (VANETs) are widely used for communicating between vehicles and other vehicle infrastructure-based devices. As well as these, VANETs are used to control drones. The following sections describe and discuss the VANETs [1] based security problems and prevention methods. As well as discussing the structure of these VANETs and protocols. In the background, focus on the overview of VANETs, and in section three, describe the VANET-based security threats. In the fourth section, discuss the security solutions for the security threats, and in section five, explains about the comprehensive discussion about the VANETs and future research directions of the VANETs. Figure 1 shows the simplest structure of VANET.

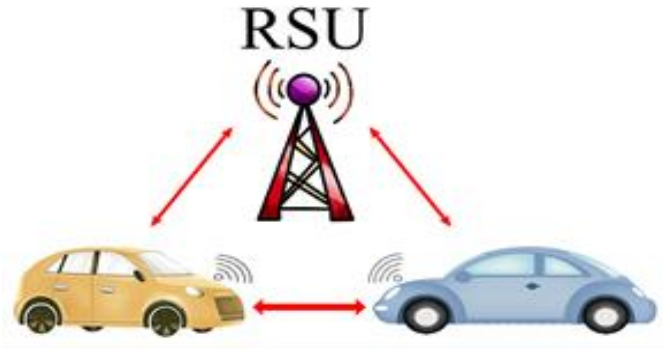

Fig. 1: Structure of VANET

II. Background

When discussing the literature background of this topic [2], the research paper provides more structural analysis than the above [1] review paper discussed in the above section. The structural analysis and review are below.

K.S. Hosan is with the Department of Engineering Technology, Faculty of Technology, Sabaragamuwa University of Sri Lanka, Sri Lanka. (Emails: shenhosan@gmail.com)

W.A.H.V. Perera is with the Department of Biosystems Technology, Faculty of Technology, Sabaragamuwa University of Sri Lanka, Sri Lanka. (Emails: hasithvihangaperera725@gmail.com)

W.A.D.T Jayawardhana is an undergraduate student associated with Faculty of Technology, Sabaragamuwa University of Sri Lanka, Sri Lanka.

H.V.V. Priyadarshana is with the Department of Engineering Technology, Faculty of Technology, Sabaragamuwa University of Sri Lanka, Sri Lanka. (Emails: vimukkthi@tech.sab.ac.lk)

R.J.M.D.D.P. Wijesekara is with the Department of Biosystems Technology, Faculty of Technology, Sabaragamuwa University of Sri Lanka, Sri Lanka. (Emails: dasith@tech.sab.ac.lk)

S.V.A.A Indupama is with the Department of Engineering Technology, Faculty of Technology, Sabaragamuwa University of Sri Lanka, Sri Lanka. (Emails: amalka@tech.sab.ac.lk)

A. Kelum with the Kingston University, United Kingdom, London and Esoft Metro Campus, Sri Lanka. (Emails: anjula.kelum@esoft.lk)

H.D.C.N. Gunawardana is with the Department of Engineering Technology, Faculty of Technology, Sabaragamuwa University of Sri Lanka, Sri Lanka. (Emails: niroshan@tech.sab.ac.lk)

K.R. Koswattage is with the Department of Engineering Technology, Faculty of Technology, Sabaragamuwa University of Sri Lanka, Sri Lanka. (Emails: koswattagekr@appsc.sab.ac.lk)

ISSN: 2961-5992

A. Overview of VANETs: Architecture, Communication Protocols

According to the Vehicle Ad-Hoc Networks (VANETs), the transformative approach to vehicle communication diverging from traditional cellular networks that depend on fixed base stations, through establishing a decentralized network, VANETs provide direct communication between vehicles as vehicle-to-vehicle (V2V) and between vehicles and infrastructure [2] of roadside units(V2I). This architecture provides a real-time information exchange capability, which is very important for improving road safety, traffic management, and the overall driving experience. The dynamic behaviour of VANETs allows for a more responsive and adaptive system, capable of managing the rapidly changing situations typical of road traffic conditions. Therefore, VANETs are becoming an integral part of intelligent transportation systems, and these decentralized VANETs contribute to smarter, safer, and more efficient roadways.

a) Key Components of a VANET Architecture:

• On-Board Units (OBUs):

OBUs [3] are the devices installed in the vehicle that enable communication with vehicles and roadside units. OBUs include processing units, transceivers for the Dedicated Short-Range Communication (DSRC) protocol, and interfaces for connecting to sensors such as GPS, cameras, and other necessary devices.

• Roadside Units (RSUs):

Modern transportation systems use road fixed infrastructure units installed with cameras, traffic guiding systems, lane assisting systems, and more. RSUs [3] behave as gateways between vehicles and the broader internet, depending on traffic information and safety alerts.

• Management Center:

These management centers [3] need to manage the network operations and include authentication, key management, and security policy enforcement. In some situations, vehicle internal Electronic Control Units (ECUs) can work as a management center.

b) Communication Protocols:

• Dedicated Short-Range Communication (DSRC):

This standardized protocol supports short-range wireless communication between vehicles and roadside units at a frequency of 5.9 GHz. DSRC [4] provides the exchange of safety messages and alerts such as collision warnings, traffic congestion updates, and weather alerts.

• Cellular Network Integration:

VANETs can develop with cellular networks and Mobile Ad-Hoc Networks (MANETs) [5] for broader internet access and communication with remote areas.

B. Security Requirements for VANETs (CIA triad: Confidentiality, Integrity, Availability)

However, compared to the review paper [1], security is important for VANETs as compromised information can lead to safety risks and privacy violations. The CIA triad works as a fundamental framework [1] for security requirements in VANETs.

• Confidentiality:

Unauthorized users should not be able to access or capture sensitive information transmitted through the network. This contains vehicle location data, driver identity, and the content of safety messages and alerts. Cryptographic methodologies such as encryption ensure only authorized persons can decrypt and interpret transmitted data.

• Integrity:

These transmitted data should remain unaltered or unchanged during communication. This means that ensuring messages have not been tampered with, potentially leading to misleading false information or fake alerts. Digital signatures and message authentication codes are used to verify and validate data integrity and the content of the transmitted information.

• Availability:

In the VANET communication process, authorized users must be able to access valuable information and network resources reliably without facing any issues. However, more than the [1] review paper covered part. Denial-of-Service (DoS) attacks that flood and create the network with fake messages can interrupt communication and prevent legitimate safety messages and alerts from reaching vehicles. Therefore, robust network protocols and intrusion detection systems are important for maintaining availability in VANETs.

III. Review Methodology

Throughout this entire paper, followed the compare and contrast-based review approach and through the subtopics mainly narrow downed the specific selected areas deeply. In chapter four discuss the security issues based on the classifications. As well as, through chapter five, discuss the comparative review for existing solutions.

IV. Security Issues in VANETs: Classifications

This section deeply discusses the VANETs security issues more than the above-discussed [5] review paper. These Vehicle Ad-Hoc Networks (VANETs) hold enormous potential for improving traffic safety, traffic management [6], and efficiency. Anyhow, compared to the [6] research paper, their reliance on open wireless communication makes them susceptible to various security threats and problems. This can be divided into two common classifications of security issues and problems in VANETs.

A. Layer-based Classification

This classification categorizes security problems based on the specific layer of the Open Systems Interconnection (OSI) [7] structure they impact. This OSI model gives a standardized framework for network communication. Each layers have specific functions and specifications. VANETs use a bit different layer structure than the general structure. Therefore, using [7] review paper discussed and unfilled important knowledge gap in below layers filled from this review paper.

• Physical Layer:

This layer directly works with the hardware level of the network infrastructure, which means this layer directly works with the binary transmission of data bits over the physical communication medium (such as radio waves in VANETs). In this layer, security concerns contain jamming attacks where

ISSN: 2961-5992

malicious actors or programs intentionally transmit signals to interrupt communication or signal transmission.

• MAC (Media Access Control) Layer:

This layer is responsible for controlling how devices access and share wireless channels. Therefore, attacks at this layer could involve gaining unauthorized access to the network, crashing, or manipulating channel access mechanisms.

• Network Layer:

This layer controls the routing and addressing of data packets. In addition to the [7] research paper, these potential problems include spoofing attacks where a malicious node impersonates another permissible node to interrupt routing or fake information injection.

• Transport Layer:

This layer verifies the trustworthy and properly ordered delivery of data between applications. However, after analyzing the [1] [7] review and research papers. Denial-of-Services (DoS) or Distributed Denial-of-Services (DDoS) types of attacks that flood the network with traffic and prevent permissible communication are a main concern in this layer.

• Application Layer:

This layer gives services to user applications. Security issues in this layer involve unauthorized access to or manipulation and change of application data. Such as emergency alerts and warnings or traffic information.

B. Attack Categories

When considering the nature of attack categories, [8] can be classified according to security threats based on the type of attack they represent:

• Sybil Attacks:

In this type of attack, a malicious node pretends to be multiple identities, interrupting the consensus mechanism inside the network.

• Message Tempering:

In this message tempering attacker changes the original content of a message during transmission, which can potentially lead to misleading or harmful information being disseminated and can make massive impact on communication.

• Denial-of-Service (DoS) Attacks:

The attacker targets to flood the network with artificial traffic and makes its unavailable to permissible users. These attacks involve jamming or flooding the network with fake messages.

• Masquerading Attacks:

In this type of attack, an attacker impersonates the permissible node to take unauthorized access to the network and change or manipulate data.

• Replay Attacks:

In replay attacks, the attacker captures the network and retransmits a permissible message later. These attacks potentially confuse or interrupt operations in the network.

• Privacy Attacks:

In this type of attack, the attacker tries to track or monitor vehicle location, movement details, and violate the user's privacy by accessing the internal components of the vehicle.

V. Comparative Review of Existing Security Solutions

Under this section overview of the currently available security solutions is provided, including more than [5] [6] [7] review and research papers, by comparing different security solutions used in various structures. It analyzes and studies their effectiveness, identifies strengths and weaknesses, and highlights probable areas for improvement. These problems have a landscape view of the security solutions that currently exist.

A. Cryptographic Techniques for Secure Communication (Encryption, Digital Signatures)

In this subsection divide into the world of cryptography [8] and focus on the methods that secure communication channels. Encryption secures data using a secret key, making it unreadable to others without the key. These digital signatures electronically verify and validate the authenticity and integrity of a transmitted message. Breakdown as follows:

1) Encryption Algorithms:

However, when compared to the [8] research paper more descriptively describes this solution in [9] research paper. Different algorithms currently exist, each one with varying security strengths, computational demands, and security key management complexity. General examples include the following:

• Symmetric Encryption (AES):

In this [9] type, the same key is used for both parties' encryption and decryption. This process is fast but need security key exchange during the communication process.

• Asymmetric Encryption (RSA):

In this [9] encryption use a public key is used for encryption, and a specific private key is used for decryption. This process is slower but uses a wider key distribution.

2) Digital Signatures:

Methods such as DSA (Digital Signature Algorithm) [10] and ECDSA (Elliptic Curve Digital Signature Algorithm) allow verification and validation of the sender and ensure the message has not been tampered with, such as a digital stamp with the sender's unique stamp mark or identification.

B. Privacy-Preserving Mechanisms (Pseudonymization, Group Signatures)

This section describes the mechanisms and methods that provide secure communication while protecting user identities and data. The following describes how those mechanisms work.

• Pseudonymization:

In this mechanism [11], the real identities are changed to temporary aliases, and this protects individual identities while still communicating.

• Group Signatures:

This technique [12] verifies and validates membership in a group without exposing individual identities. As an example, in the situation of a group email where only the group affiliation is shown and does not reveal the individual senders.

ISSN: 2961-5992

C. Intrusion Detection and Prevention Systems (IDPS) for VANETs

This section explains the securing of Vehicle Ad-Hoc Networks (VANETs) used for communication between vehicles. VANETs, such as temporary and self-forming networks on the road. As well as IDPS [13], play a significant role in:

• Intrusion Detection:

This detection identifies the malicious activities and behaviors in the network. As an example, a fake message or an attempt to interrupt the communication. When compared to the real world, a security guard spots suspicious behavior on the road or in a place.

• Intrusion Prevention:

This method of taking actions to stop these malicious activities and behaviors is mostly achieved by blocking suspicious messages or alerting the authorities and responsible parties. When compared to the real-world practical scenario, a security guard stops the suspicious vehicle.

Currently, various IDPS approaches are available, some approaches focusing on analyzing network traffic, while other approaches involve cooperation between vehicles to find and monitor threats.

D. Trust and Reputation Management Systems

This part explains mechanisms [14] for assessing the trustworthiness of operational entities in the network. According to a real-world example online marketplace where customers rely on seller ratings before making a buying decision:

• Establishing Trust:

Under these systems may analyze earlier interactions, ratings, user reviews, or other data points to validate and assign the trust scores.

• Reputation Management:

This technique is used for users to make ratings or leave feedback and influence the complete and overall reputation scores.

E. Comparative Analysis of Reviewed Solutions (Strengths, Weaknesses, Open Issues)

Under this topic, discuss the general overview of the provided security solutions side by side and compare:

• Strengths:

These security solutions improve the VANET's stability and security and provide a proficient level of trust standard.

• Weaknesses:

Sometimes VANETs have connectivity issues, and that timing issue can be used as a security vulnerability to make an impact on the network.

• Open Issues:

Under the current challenges if can improve the stability of the VANETs connectivity, and is currently working on this [15].

VI. Discussion and Future Research Directions

When compared to the above [15] research paper, this section widely discusses the future research directions in this paper. VANETs started the huge revolution in the automobile and transportation industry and are still in development, as well as these networks are currently trying to overcome the problems and practical issues.

A. Challenges and Limitations of Existing VANET Solutions

Under the current limitations, the main challenges [16] and main limitations [17] are as follows:

• Scalability and network density:

When VANETs spread widely, some problems crucially occur because this type of network components needs to connect a higher number of devices within a limited time, and currently VANETs do not have this capability.

• Standardization and interoperability:

In the transportation industry, various kinds of manufacturers create different Vehicle Ad-Hoc Network components, which makes difficulties for developing the standardization and common protocols for VANETs. In some cases, this part problem causes some issues in VANETs inter operatable capabilities.

• Limited communication range:

Environmental conditions and connectivity issues create communication issues and impose limitations on the VANETs' range. Therefore, by developing multi-hop relaying or extending the range of the network transmitters and receivers.

• Constraints of resources:

VANETs-based network components have limited computational power and widely use the dedicated ECUs in the vehicle. Therefore, in operational vehicles, some data processing problems can occur while communicating the data.

B. Emerging Security Threats and Countermeasures

As discussed in the above sections, VANETs are mainly exposed to the threats of Denial-of-Services attacks, message tampering and injection vulnerabilities, therefore need to develop fast threat detection and prevention software programs specially for VANETs. As well as need to develop some programs for improving the privacy information communicated through the VANETs, such as location, real-time moving patterns, remote vehicle access details, and privacy-based sensitive information.

C. Open Research Opportunities and Future Directions

•Integration and develop with Cellular Vehicle-to-Everything (C-V2X):

VANETs should have capabilities to work with all other networks and components, not only vehicles and road infrastructure components; therefore need improvements in wider network [18] coverage and improved information dissemination.

• Integration with Cloud Computing:

Currently, cloud computing [18] is used for storing, processing, and analyze real time data; therefore, in the future, cloud-connected VANETs can be used for traffic management and monitoring the driving patterns of vehicles.

• Artificial Intelligence (AI) and Machine Learning (ML) Applications:

Using this AI and ML [19] can make predictions of traffic patterns and watch the real-time vehicle behavior through analyzing the VANETs. Therefore, if VANETs can manage

ISSN: 2961-5992

through AI, this will be a terrific opportunity for the future transportation industry.

• VANETs for Cooperative Autonomous Vehicles (CAVs):

VANETs method can be applied to driver-based vehicles. If VANETs cooperate with the CAVs [20], they can improve the autonomous driving experience and capability of driverless vehicles, and as an ultimate goal, can apply this network structure to interconnected future hypersonic fighting aircraft and drones [21].

VII. CONCLUSION

When considering the above facts, identified security problems and connectivity can be marked as the main issues in VANETs. Therefore, need to focus on the innovations to solve these problems. As well as these, VANET-based information can be used for improving the Intelligent Transportation Systems (ITS) [22]. Furthermore, merging these VANETs with Artificial Intelligence and Machine Learning can create road traffic prediction methodologies. In the case of security issues, need for specified security software systems to solve these problems, and existing solutions are not enough to solve these problems. In the future, VANETs will be the turning point of fast, close, and near area communication.

REFERENCES

[1] A Mahmood, Jabar & Duan, Zongtao & Yang, Yun & Wang, Qinglong & Jamel, Nebhen & Bhutta, Muhammad Nasir Mumtaz. (2021). Security in Vehicular Ad Hoc Networks: Challenges and Countermeasures. Security and Communication Networks. 2021. 1-20. 10.1155/2021/9997771.

[2] Hua Qin, Xiang Xiao, Weihong Chen, Ni Li, Min Zeng, Buwen Cao, Yang Peng,Utilizing VANETs as supplementary communication infrastructure for delay-tolerant bulky data transportation,Ad Hoc Networks,Volume 112,2021,102394,ISSN 1570-8705,https://doi.org/10.1016/j.adhoc.2020.102394.

[3] S. Kanithan, S. V, L. K. V, S. Pragathi and S. K, "Inter Vehicle Communication using Vehicular Ad-hoc Network (VANET)," 2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), Bangalore, India, 2021, pp. 191-196, doi: 10.1109/ICDI3C53598.2021.00046.

[4] S. R. Govindarajulu, R. Hokayem and E. A. Alwan, "Dual-Band Antenna Array for 5.9 GHz DSRC and 28 GHz 5G Vehicle to Vehicle communication," 2020 IEEE International Symposium on Antennas and Propagation and North American Radio Science Meeting, Montreal, QC, Canada, 2020, pp. 1583-1584, doi: 10.1109/IEEECONF35879.2020.9330220.

[5] M. Sharma, M. Singh, K. Walia and K. Kaur, "A Comprehensive Study of Performance Parameters for MANET, VANET and FANET," 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2019, pp. 0643-0646, doi: 10.1109/IEMCON.2019.8936159.

[6] S. Shirabur, S. Hunagund and S. Murgd, "VANET Based Embedded Traffic Control System," 2020 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), Bangalore, India, 2020, pp. 189-192, doi: 10.1109/RTEICT49044.2020.9315602.

[7] G. Amponis et al., "Efficient Peer-to-Peer Unicasting for VANET Architectures via Enhanced Monolithic Protocols," 2022 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Ioannina, Greece, 2022, pp. 1-8, doi: 10.1109/SEEDA-CECNSM57760.2022.9932897.

[8] F. Azam, S. Kumar, K. P. Yadav, N. Priyadarshi and S. Padmanaban, "An Outline of the Security Challenges in VANET," 2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Prayagraj, India, 2020, pp. 1-6, doi: 10.1109/UPCON50219.2020.9376518.

[9] S. Srivastava, A. Tiwari and P. K. Srivastava, "Review on quantum safe algorithms based on Symmetric Key and Asymmetric Key Encryption methods," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 905-908, doi: 10.1109/ICACITE53722.2022.9823437.

[10] H. A. A. Al–Sewadi, R. A. Al-Shnawa and M. M. Rifaat, "Signature Verification Time Reduction for GOST Digital Signature Algorithm," 2021 International Conference on Communication & Information Technology (ICICT), Basrah, Iraq, 2021, pp. 279-283, doi: 10.1109/ICICT52195.2021.9568409.

[11] A. Westerbaan and L. Hendriks, "Polymorphic Encryption and Pseudonymisation of IP Network Flows," 2020 IFIP Networking Conference (Networking), Paris, France, 2020, pp. 494-498.

[12] J. Lu, R. Qi and J. Shen, "A Novel Dynamic Group Signature with Membership Privacy," 2021 IEEE Conference on Dependable and Secure Computing (DSC), Aizuwakamatsu, Fukushima, Japan, 2021, pp. 1-5, doi: 10.1109/DSC49826.2021.9346238.

[13] I. Naqvi, A. Chaudhary and A. Rana, "Intrusion Detection in VANETs," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2021, pp. 1-5, doi: 10.1109/ICRITO51393.2021.9596141.

[14] J. Zhao, J. Huang and N. Xiong, "An Effective Exponential-Based Trust and Reputation Evaluation System in Wireless Sensor Networks," in IEEE Access, vol. 7, pp. 33859-33869, 2019, doi: 10.1109/ACCESS.2019.2904544.

[15] E. Agarwal and D. Kakkar, "Connectivity Improvement in Cluster-Based VANET," 2022 2nd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2022, pp. 1-5, doi: 10.1109/CONIT55038.2022.9848190.

[16] A. Pullanatt and A. Anitha, "Large Data Block Transmission In VANET," 2023 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA), Ernakulam, India, 2023, pp. 1-8, doi: 10.1109/ACCTHPA57160.2023.10083381.

[17] H. M. Moyeenudin, S. H. Kumar, M. Narender, J. A. A. and J. Amutharaj, "Comparative Analysis of Video Transmission in Vehicular Networks using IEEE 802.11g and IEEE 802.11p Standards," 2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI), Tiruchengode, India, 2023, pp. 1-7, doi: 10.1109/ICAEECI58247.2023.10370925.

[18] R. Krishnan P. and A. R. Kumar P., "Security and Privacy in VANET : Concepts, Solutions and Challenges," 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2020, pp. 789-794, doi: 10.1109/ICICT48043.2020.9112535.

[19] S. Singh, N. Sood, S. Dutt, S. N. Sai and N. S. Sathvik, "AI and ML in Vehicular Communication: A Cybersecurity Perspective," 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2022, pp. 750-755, doi: 10.1109/ICCES54183.2022.9835791.

[20] M. S. Alam, J. Oluoch and J. Kim, "A Mechanism to Localize, Detect, and Prevent Jamming in Connected and Autonomous Vehicles (CAVs)," in IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 2, pp. 1215-1224, Feb. 2024, doi: 10.1109/TITS.2023.3314737.

ISSN: 2961-5992

[21] M. W. Akram et al., "A Secure and Lightweight Drones-Access Protocol for Smart City Surveillance," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 10, pp. 19634-19643, Oct. 2022, Doi: 10.1109/TITS.2021.3129913.

[22] P. Ramkumar, R. Uma, S. Usha and R. Valarmathi, "Real Time Path Planning using Intelligent Transportation System for Hybrid VANET," 2020 International Conference on Power, Energy, Control and Transmission Systems (ICPECTS), Chennai, India, 2020, pp. 1-7, Doi: 10.1109/ICPECTS49113.2020.9337057.

ISSN: 2961-5992