International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 06, June 2026)

Security Attack Classification and Mitigation Strategies in VANET-Based Intelligent Transportation Systems

Souvik Dey[1], Swapnanil Mukherjee[2], Sudipta Kumar Dutta[3]

[1]*B. Tech in Computer Science Engineering from B.P. Poddar Institute of Management and Technology*
[2]*B. Tech in Computer Science Engineering from JIS University*
[3]*Department of CSE at B.P. Poddar Institute of Management and Technology*

***Abstract*— Vehicular Ad Hoc Network (VANET) is an advanced wireless communication technology that enables vehicles to communicate with each other and with roadside infrastructure for improving road safety, traffic management, and driving efficiency. Although VANET provides many advantages, it is highly vulnerable to several security attacks due to its open wireless environment and dynamic network topology. This research work discusses different types of attacks in VANET such as Malware Attack, Jamming Attack, DoS Attack, Sybil Attack, Grey Hole Attack, Black Hole Attack, GPS Spoofing, Replay Attack, Message Tampering Attack, Eavesdropping Attack, and many others. These attacks can compromise communication, create false traffic information, cause accidents, and reduce trust among vehicles. The study also highlights the impacts of these attacks and discusses the importance of secure communication mechanisms, encryption, authentication, intrusion detection systems, and trust management techniques to ensure secure and reliable VANET communication.**

***Keywords*— Authentication, Cyberattacks, Intrusion Detection System (IDS), Network Security, Road Safety, Routing Protocols, Trust Management, Vehicular Ad Hoc Network (VANET), Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V)**

❑ *Literature Survey*

Several researchers have studied security issues and attacks in Vehicular Ad Hoc Networks (VANETs). Previous studies show that VANET security is one of the major challenges in Intelligent Transportation Systems due to high mobility, dynamic topology, and wireless communication.

- Researchers identified that Denial of Service (DoS) attacks can overload the network with excessive traffic, resulting in communication failure and delayed safety messages.
- Studies on Sybil attacks explain how malicious vehicles create multiple fake identities to manipulate traffic information and influence routing decisions.
- Research on Black Hole and Grey Hole attacks shows that attackers selectively drop packets or falsely advertise shorter routes to attract traffic and disrupt communication.
- Several works discussed GPS spoofing and replay attacks, where attackers manipulate location data or resend old messages to create confusion among vehicles.
- Security researchers also focused on Man-in-the-Middle (MITM) and Message Tampering attacks, which involve interception and modification of safety-critical messages exchanged between vehicles.
- Many studies suggested solutions such as:
    - Encryption and authentication techniques
    - Intrusion Detection Systems (IDS)
    - Trust management systems
    - Secure routing protocols
    - Digital signatures and blockchain-based security

I. Introduction

Vehicular Ad Hoc Networks (VANETs) have emerged as a critical component of modern Intelligent Transportation Systems, enabling real-time vehicular communication through V2V and V2I paradigms. Extensive research has been conducted to address security vulnerabilities inherent in VANET architectures. Sakiz and Sen **[1]** provided a comprehensive survey of attacks and detection mechanisms on intelligent transportation systems, establishing foundational frameworks for understanding VANET vulnerabilities. Bariah et al. **[2]** documented recent advances in VANET security, while Engoulou et al. **[3]** contributed detailed VANET security analyses. Research on specific attack vectors has been substantial. Le et al. **[4]** investigated behavior-based malware propagation in V2V communications. Mokdad et al. **[5]** developed detection mechanisms for jamming attacks through the DJAVAN framework. Patel and Kumar **[6]** addressed Denial of Service attack detection, while Yu et al. **[7]** examined Sybil attack mitigation strategies.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 06, June 2026)

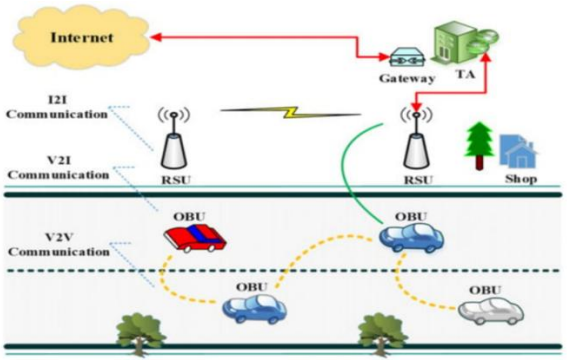
Additional studies by Gowdhami and Nithya **[8]** on Gray Hole attacks, Javeed et al. **[9]** on Man-in-the-Middle attacks, and Malik et al. **[10]** on Black Hole attack prevention have collectively advanced the field. Recent developments include genetic-based frameworks for masquerade and DDoS prevention **[11]**, fuzzy-based approaches for greedy behavior detection **[13]**, and blockchain-integrated security architectures **[21]**. These cumulative efforts demonstrate evolving sophistication in VANET security countermeasures, establishing the foundation for this comprehensive survey's systematic examination of eighteen attack vectors and corresponding mitigation strategies.

Security breaches within VANET infrastructure carry critical real-world consequences, including falsification of safety messages, unauthorized location tracking, packet dropping, and network-wide communication disruption — all of which directly compromise vehicular safety and public infrastructure integrity.

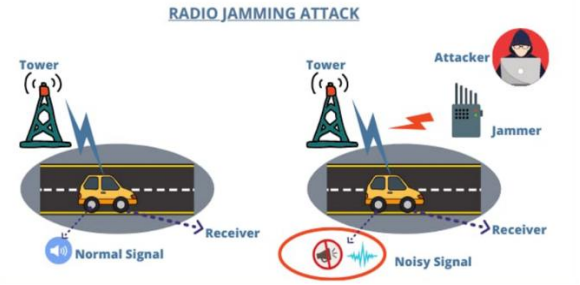
This survey systematically examines eighteen classified security attack vectors targeting VANET, analyzing their exploitation mechanisms, network impact, and applicable mitigation strategies including cryptographic protocols, Intrusion Detection Systems (IDS), trust-based authentication frameworks, and blockchain-integrated security architectures, thereby contributing a structured reference for advancing robust VANET security research.

II. Attacks In Vanet

Malware Attack— Malware attack in vanet posses significant risks to both vehicle safety and network integrity . In the VANET, vehicles communicate with each other and with infrastructure to enhance safety, traffic management and infotainment services. Malware attacks hits with various strategies like data manipulation is a big issue now a days , such as altering messages like traffic updates or safety warnings, leading to potential accidents. Also intercepting communication to gather sesnsitve information, about vehicle location and habits. Impacting in safety risks compromised communication can lead to accidents or dangerous situation on the road. Also drivers may become hesitant to rely on Vanet services if the security is not ensured. Mitigating it we can use secure communiction like implement encryption and authentication to ensure the integrity and authenticity of the messages. Also we can deploy IDS (Instruction Detection System) to monitor network traffic for anomalies indicative of malware activities.

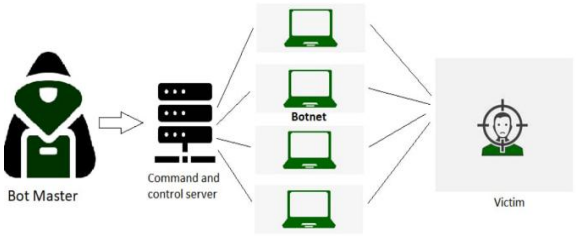


Jamming Attack— A jamming attack in vanet involves an attacker deliberately disrupting communication between vehicles and infrastructure by emitting radio frequency signals. This can lead to significant safety risks as vehicles rely on timely information for navigation and collision avoidance ,with the different types of jamming attacks there are constant jamming,intermittent jamming ,deceptive jamming and a lot more. the constant jamming continues transmission of noise on a specific frequency , with the intermittent jamming signals are sent sporadically making detection harder and with the deceptive jamming there is mimicking legitimate signals to confuse reccivers as with the impact of jamming attacks there becoming more of safety risks , disruption in traffic management and a lot more.

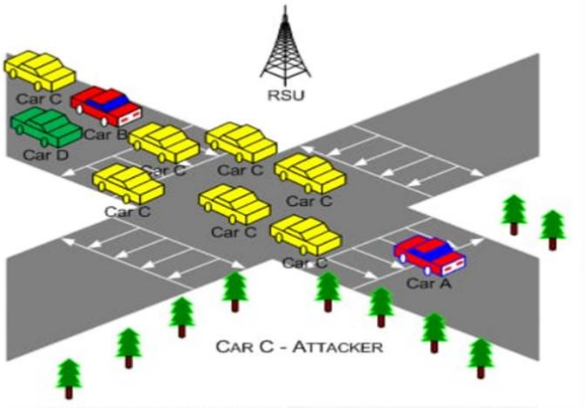


DOS Attack— A Denial of Service attack in a vanet aims to disrupt communication between vehicles or between vehicles and infrastructure, rendering the network inoperable or significantly degrading its performance, with the dos attacks there is traffic overload which is destroying the network with excessive messages overwhelming the available bandwidth also there is the resource exhaustion which is targeting the specific nodes to drain the processing power of battery life and another type of dos attack is" route table poisoning "which helps in sending false information to corrupt the routing tables, causing miscommunication impacting in traffic inefficiency making delay disruption of critical safety messages can lead to acciddents.

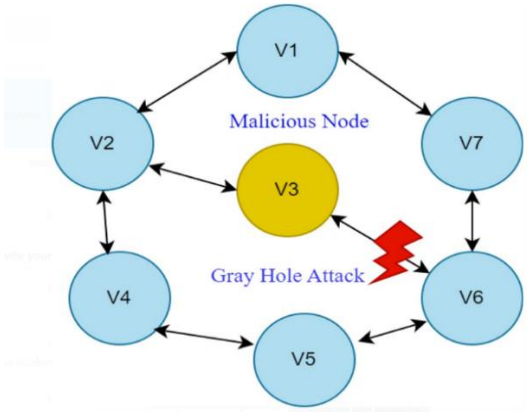
International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 06, June 2026)



SYBIL ATTACK— A sybill attack in vanet occurs when a malicious node creating multiple false identities to gain disproportionate influence over the network. This can disrupt communication compromise data integrity and lead to false routing information or traffic patterns. The one of the main sybil attack is the spoofing in which attackers generate multiple identities, making it difficult to distinguish legitimate nodes from malicious ones also there is impact on trust where trust based protocols can be undermined, as attackers can sway decisions or mislead other vehicles. The impacts of sybil attack are like data integrity copromises in which attackers can create multiple false identities, leading to misinformation about traffic conditions, accidents or road hazards, also there is network congestion in which generating excessive messages, a sybil attack can overwhelm the network, causing delays and reducing communication efficiency.

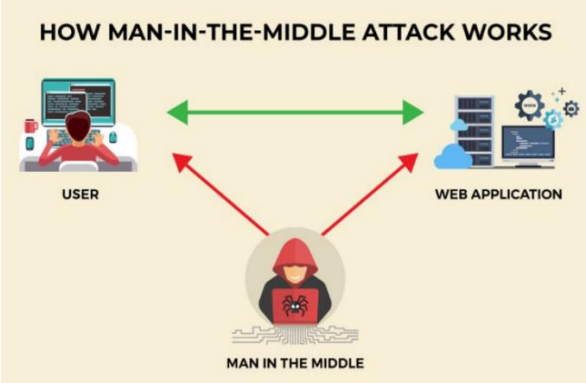


Grey Hole Attack— A Grey Hole Attack in vanet refers to a security threat where a malicious vehicle selectively drops certain messages while forwarding others. This behaviour is a deceptive because the attacker to be a legitimate participant in the network, making it difficult to detect, one of the main of the gray hole attack is selective dropping where the attacker may drop critical safety messages while allowing non-ccritical messages to pass through. The another one is impact on safety where they suppress important information, the attack can lead to dangerous situations, compromising the safety of drivers and pedestrians. The impact of grey hole attacks being increasing in accidents like they will drop critical safety messages (collision warnings or hazard alerts), the attacker ca lead to potentially fatal accidents, also there is communication disruption where there is attacker can lead to potentially fatal accidents, also there is communication disruption where there is loss of critical information where the attackers disrupts the flow of essential traffic information.

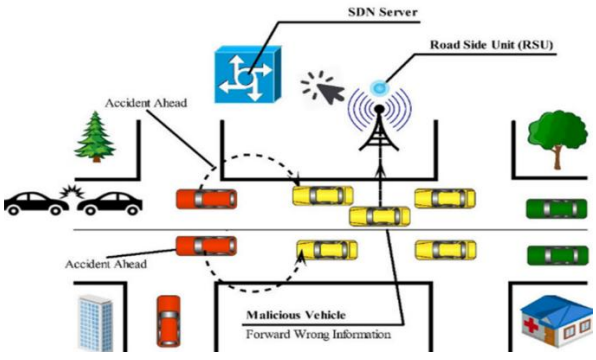


MAN In The Middle Attack— A Man in the Middle attack IN VANET occurs when a malicious entity intercepts alters or relays communication between two legitimate vehicles without their knowledge , this type of attacks can have serious consequences for the safety and security of the network .In the man in the middle attack there is interception of communication where the attacker can eavesdrop on sensitive information , such as location data , navigation instructions or safety messages , also there is message alternation in this the attacker can modify messages being sent between vehicles , potentially causing confusion or leading to dangerous situations. There are several impacts of mitm attack like compromised situational awareness for drivers, leading to poor decision making. also there is trust erosion where they diminished trust among vehicles in the network as messages may be viewd with suspicion resulting in establishing reliable communication channels.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 06, June 2026)

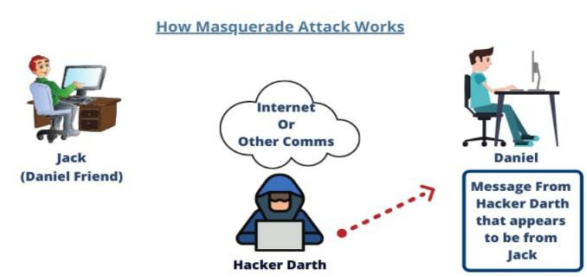


Black Hole Attack— Blackhole attacks result in packet losses in the network and it could affect life-or-death decisions where safety-related applications cannot send or receive critical data. For instance, a vehicle which is involved in a traffic accident should propagate warning messages, but an attacker could prevent others from receiving the warning by misrouting packets.:- Blackholes attack in VANET is a denial of service attack by a node or router traffic is redirected in a blackhole area in VANET. Data packets are directed to the malicious vehicle with the promise of having the shortest route. In AODV (It is a routing protocol, employed in VANET where the route gets active only when the source node wants to transmit data packets to other nodes.) protocol the attackers take advantage of the AODV property of having the highest sequence number for a new route. A malicious node introduce itself as having the shortest route to the destination and cheats the AODV protocol.

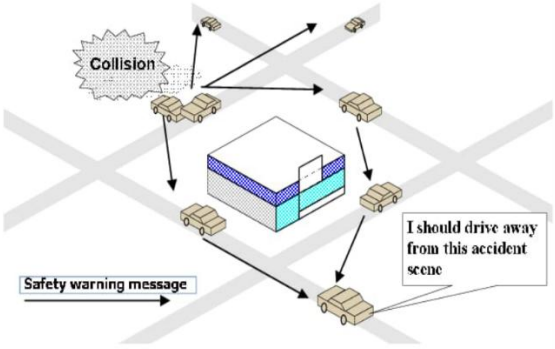


Masquerading— In this attack, one attacker is defined by false identification and visibility as a legitimate node by another vehicle. The attacker behaves like a man in the central middle and spoofs them as the second vehicle as all vehicles interact in the process. This also done deliberately attack to change the results.

Like for example first, they would create a fake website that looks indistinguishable from the real one. Then, they'd launch an email campaign, trying to trick the users to go to the fake website and enter their credentials. Once the hacker has the user credentials, they can log into the target network. They can exploit software bugs to eavesdrop on communications trying to intercept and modify the message before passing it on to the original recipient.



Illusion Attack— In Vehicular Ad Hoc Network an Illusion attack can happens when aa malicious node can enters to mislead other vehicles infrastructure . An illusion attack may occurs due to many of the reasons like fake location information in which a vehicle may broadcast incorrect location data , causing others to misinterpret its position and possibly leading to acccidents or traffic jams also with the identity spoofing attaackers csn impersonate legitimate vehicles to manipulate the network ,gain authorized access or disrupt communication. Also there are several impacts of illusion attack like traffic disruption in which false data can cause inefficient routing congestion and increasd travel times . Repeated illusion attacks can cause accidents . Drivers may make sudden or inappropriate maneuvers based on false information, increasing the risk of accidents.

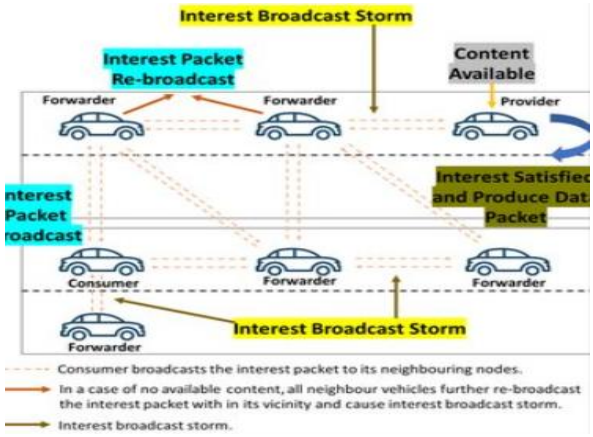


Greedy Behaviour Attack— Greedy behaviour attack in vaanet iinvolve malicious nodes attempting to exploit the network for their own benefit, often at the expense of others.

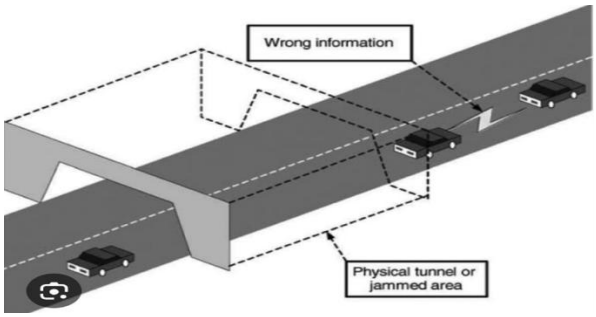
International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 06, June 2026)

Greedy Behaviour Attack can manifest in various forms such as like "packet dropping", in packet dropping malicious vehicles may selectively drop packets that are meant for other nodes , prioritizing their own data transmission instead, also like data spoofing is involve in this attack where attackers is trying to inject false information (e.g. – misleading traffic conditions or safety warnings) to manipulate the decision of other vehicles, results in impacting decreased network performance like malicious nodes monopolizing resources can lead to increased latency and reduced throughput for legitimate users , compromising overall communication efficiency also increasing in safety risks.

Broadcast Tampering — Broadcast Tampering in Vehicular Ad-Hoc Network involves malicious alternation of messages transmitted between vehicles , which can disrupt traffic safety and efficiency . This can lead to accidents or miscommunication between vehicles and infrastructure. Broadcast Tampering in VANET typically occurs when an attacker intercepts and modifies message sent between vehicles or from vehicles to infrastructure .The attacker can manipulate data , such as changing speed limits or vehicle positions , leading to dangerous situations. This is often done using techniques like spoofing or replay attacks , where the attacke either impersonates a legitimate vehicle or resends previously captured messages with altered information .

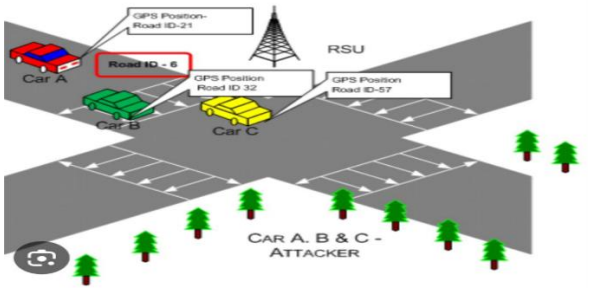


Tunneling Attack— A Tunneling attack in vanet involves an attacker creating a virtual tunnel to redirect or manipulate data traffic between vehicles. This can lead to several security issues, like data interception where the attacker can capture sensitive information being transmitted between vehicles not only data interception but also data manipulation in which controlling the traffic , the attacker can inject false information, leading to confusion or unsafe driving conditions, impacting in Personal information about vehicles locations and movement can be exploited through tunneling attack. There increases a more about safety risks in which manipulating or intercepting communications, attackers can mislead the driveers and there increases a more of safety risks also manipulated data could affect traffic signal timings and routing algorithms, causing congestion or dangerous situations.

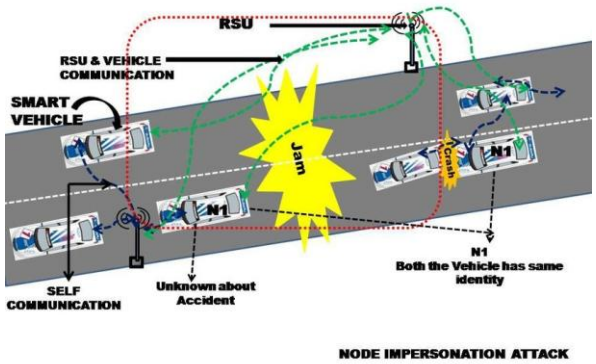


International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 06, June 2026)

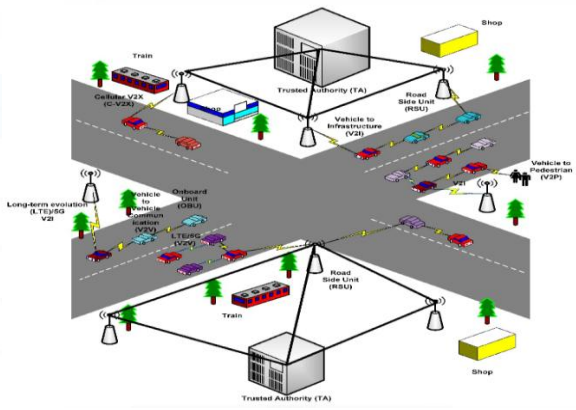
GPS Spoofing— GPS Spoofing in vanet involves deceiving vehicles about their true location, which can have serious implications for safety and security. A powerful signal transmitting an attacker, more significant than the GPS signal, causes VANET to be jamming, and the vehicle receiver gets the wrong position. GPS Spoofing can lead to significant impacts like safety risks where misleading vehicle location data can result in accidents or collisions, endangering drivers and pedestrians, also there are issues like data integrity where spoofing can compromise the accuracy of traffic data, affecting traffic management systems and urban planning. Vehicles also may be mislead delaying responses to critical situatiions, also there are issues like traffic disruptions in which incorrect positioning can cause erratic driving behaviour, leading to traffic jams or accidents.



Node Impersonation Attack— Node Impersonation Attack in VANET involve an attacker masquerading as a legitimate vehicle to gain unauthorized access to the network impacting in data corruption where the attacker can send false or safety messages, leading to misinformation and potentially dangerous situations. Also there are privacy violations in which impersonating nodes, attackers can track legitimate vehicles, compromising user privacy. Impersonated nnodes can disrupt communication leading to degraded network performance and reliability.

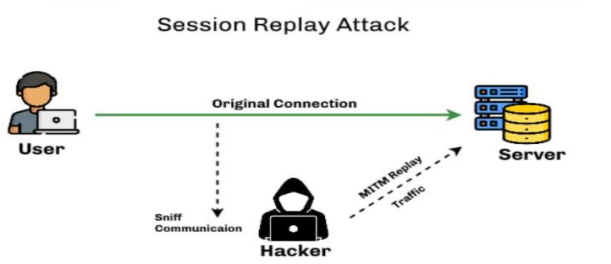


Free Riding Attack— A Free Riding attack in vanet is a type of security threat where malicious nodes (vehicles) benefit from the network without contributing to it. In vanet vehicle share important information like traffic conditions, accidents and road hazards. The network relies on vehicles actively participating by exchanging and forwarding data. There are several consequences of free riding attack like network degradation like if many nodes free-ride, it can lead to slower dissemination of information, reeducing the effectiveness of VANET'S in providing timely safety updates, also free riders may save bandwidth and battery power, gaining unfair advantages over nodes.

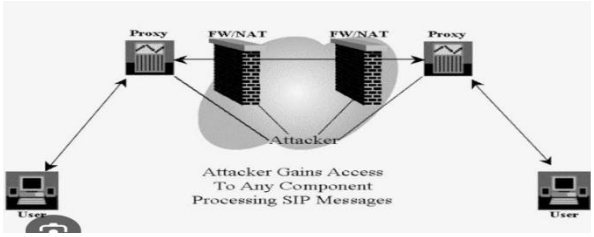


International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 06, June 2026)

Replay Attack— The Replay attack in VANET, where the attacker aims to repeat or delay fraudulent transmission by continuously providing valid data and injecting beacon and responses received by the VANET network. In the case of an incident, traffic authorities can find it challenging to identify vehicles. The attackers can have serious implicaations for the network security and reliability, impacting in disruption of traffic flow in which replay attacks can send outdated or incorrect information to vehicles, leading to wrong decisions such as avoiding non – existent traffic jams or taking unnecessary detours. Adversaries can replay safety-related messages, such as warnings about accidents or road hazards. This can lead vehicles to unnecessarily slow down, change routes or create panics.

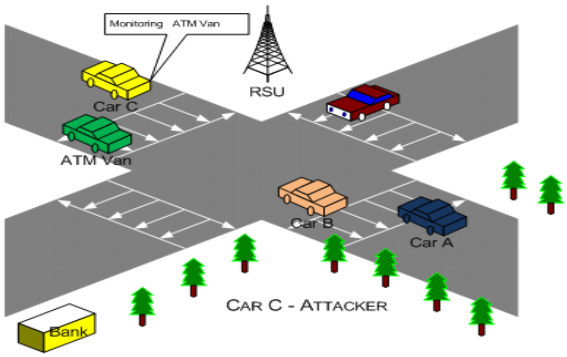


Message Tampering Attack— A message tampering attack in VANET involves an adversary intercepting, altering, or manipulating legitimate messages exchanged between vehicles to deceive or disrupt the system. This attack ca severely , compromise the safety, reliability and efficiency of VANET'S as the exchanged messages are crucial for real-time decision-making ,impacting in several causes like dissemination of false information where altered messages may provide incorrect traffic or safety information.This can cause chaos on the road, mislead drivers, and lead to inefficient traffic flow, also malicious actors can tamper with safety – critical messages such as collision warnings , speed limits or emergency vehicle alerts.

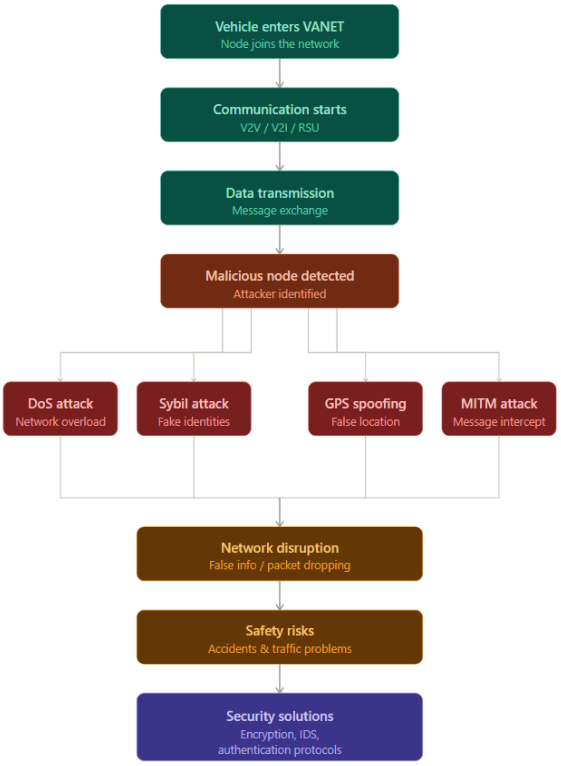


Eavesdropping Attack— An eavesdropping attack in VANET occurs when an attacker intercepts the communication between vehicles and roadside units without altering the messages.

The attacker listens to sensitive information bbeing exchanged in the network, which can lead to a variety of security and privacy risks. There are several impacts of eavesdropping like " privacy breach "where VANET'S transmits a variety of data including vehicle locations, routes, and driving behaviours. Attackers can intercept this information and use it to track drivers , leading to serious privacy violaations. Over time, they can build patterns of a vehicle's movement , which can be exploited for stalking or monitoring.



III. FLOWCHART OF VANET



- *Teal nodes* — normal network operation phases
- *Red nodes* — the four key (DoS, Sybil, GPS Spoofing, MITM) attack types branching out
- *Amber nodes* — consequences of those attacks
- *Purple node* — security countermeasures at the end

IV. Conclusion

This comprehensive survey systematically examined critical security vulnerabilities and attack mechanisms threatening Vehicular Ad Hoc Networks (VANETs) in Intelligent Transportation Systems. VANETs face diverse threats ranging from passive eavesdropping to active attacks including Denial of Service, Sybil, Black Hole, GPS Spoofing, and Man-in-the-Middle attacks. Each attack vector poses significant risks to vehicular safety and network integrity, causing communication failures, false information dissemination, unauthorized tracking, and accidents. VANET's inherent characteristics—high node mobility, dynamic topology, decentralized architecture, and open wireless channels—create complex security challenges. Traditional security solutions prove insufficient. Emerging countermeasures including cryptographic protocols, Intrusion Detection Systems (IDS), trust-based authentication, and blockchain-integrated architectures demonstrate promising potential in mitigating identified threats and advancing VANET security research.

However, the challenge of achieving both security and efficiency in resource-constrained vehicular nodes remains unresolved. Future research must focus on lightweight cryptographic implementations, real-time anomaly detection algorithms, and scalable trust management frameworks specifically tailored for VANET deployments. Additionally, standardization of security protocols across vehicle manufacturers and infrastructure providers is essential to ensure interoperability and comprehensive network protection.

As vehicular networks become increasingly critical infrastructure supporting autonomous driving and smart cities, sustained investment in VANET security research is imperative to realize the full potential of intelligent transportation while safeguarding public safety and privacy.

REFERENCES

[1] F. Sakiz and S. Sen, "A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV," Department of Computer Engineering, Hacettepe University, Turkey.

[2] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, "Recent Advances in VANET Security: A Survey," Department of Electrical and Computer Engineering, Khalifa University, Abu Dhabi, United Arab Emirates.

[3] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET Security Surveys," *Computer Networks*, Département de Génie Informatique et Logiciel, École Polytechnique de Montréal, Montréal, QC, Canada.

[4] D. T. Le, K. Q. Dang, Q. L. T. Nguyen, S. Alhelaly, and A. Muthanna, "A Behavior-Based Malware Spreading Model for Vehicle-to-Vehicle Communications in VANET Networks," *Electronics*, vol. 10, p. 2403, 2021.

[5] L. Mokdad, J. Ben-Othman, and A. T. Nguyen, "DJAVAN: Detecting Jamming Attacks in Vehicular Ad Hoc Networks," LACL, University of Paris-Est, and L2TI, University of Paris 13, France.

[6] R. K. Patel and D. Kumar, "Detection of DoS Attack in VANETs," *Indian Journal of Science and Technology*, Dec. 2016, DOI: 10.17485/ijst/2015/v8i1/106865.

[7] B. Yu, C. X. Zu, and B. Xiao, "Detecting Sybil Attacks in VANET," Department of Electrical and Computer Engineering, Wayne State University, USA, and Department of Computing, Hong Kong Polytechnic University, Hong Kong.

[8] K. T. Gowdhami and D. Nithya, "Design and Analysis of Secure VANET Framework Preventing Sink Hole and Gray Hole Attack," Department of Information Technology, M.P.N.M.J Engineering College, Chennimalai, Erode, Tamilnadu, India.

[9] D. Javeed, U. M. Badamasi, C. O. Ndubuisi, F. Soomro, and M. Asif, "Man in the Middle Attacks: Analysis, Motivation and Prevention," Northeastern University, Shenyang, China, and Changchun University of Science and Technology, China.

[10] A. Malik, M. Z. Khan, M. Faisal, F. Khan, and J. T. Seo, "An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs," Department of Computer Engineering, Gachon University, Seongnam 13120, Korea.

[11] A. K. Malhi and S. Batra, "Genetic-Based Framework for Prevention of Masquerade and DDoS Attacks in Vehicular Ad Hoc Networks," Department of Computer Science and Engineering, Thapar University, Patiala, Punjab, India.

[12] P. Sirola, A. Joshi, and K. C. Purohit, "An Analytical Study of Routing Attacks in Vehicular Ad Hoc Networks (VANETs)," Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun, Uttarakhand, India.

[13] T. Ismail, N. Hajlaoui, and H. Touati, "A Fuzzy-Based Greedy Behaviour Attack Detection Approach in VANETs," *SN Computer Science*, vol. 5, p. 822, 2024.

[14] M. A. H. Al Junaid, S. A. A, M. N. M. Warip, K. N. F. Ku Azir, and N. H. Romli, "Classification of Security Attacks in VANET: A Review of Requirements and Perspectives," School of Computer and Communication Engineering, University Malaysia Perlis, Malaysia.

[15] B. Ying, D. Makrakis, and H. T. Mouftah, "Privacy Preserving Broadcast Message Authentication Protocol for VANETs," *Elsevier*, 2012, DOI: 10.1016/j.future.2012.05.013.

[16] C. Vitale, N. Piperigkos, C. Laoudias, G. Ellinas, J. Casademont, J. Escrig, A. Kloukiniotis, A. S. Lalos, K. Moustakas, R. D. Rodriguez, D. Baños, G. R. Crusats, P. Kapsalas, K. P. Hofmann, and P. S. Khodashenas, "CARAMEL: Results on a Secure Architecture for Connected and Autonomous Vehicles Detecting GPS Spoofing Attacks."

[17] R. S. Raghav, R. Danu, A. Ramalingam, and G. Krishna Kumar, "Detection of Node Impersonation for Emergency Vehicles in VANET," Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry, and I.F.E.T College of Engineering, India.

[18] A. Nobahari, D. B. Avval, A. Akhbari, and S. Nobahary, "Investigation of Different Mechanisms to Detect Misbehaving Nodes in Vehicle Ad Hoc Networks (VANETs)," Islamic Azad University, Tehran, Iran, and Sakarya University, Turkey.

[19] Q. G. Fan, L. Wang, Y. N. Cai, Y. Q. Li, and J. Chen, "VANET Routing Replay Attack Detection Research Based on SVM," Xi'an Research Institute of High Technology, Xi'an 710025, China.

[20] T. M. Mohammed, I. Z. Ahmed, and R. A. Sadek, "Efficient VANET Safety Message Delivery and Authenticity with Privacy Preservation," Faculty of Computers and Artificial Intelligence, Helwan University, Cairo, Egypt.

[21] S. A. Soleymani, S. Goudarzi, M. H. Anisi, M. Zareei, A. H. Abdullah, and N. Kama, "Security and Privacy Scheme Based on Node and Message Authentication and Trust in Fog-Enabled VANET," Universiti Teknologi Malaysia, Johor, Malaysia, and University of Essex, Colchester, UK.

BIOGRAPHIES (Optional not mandatory)

Souvik Dey is a B.Tech Computer Science Engineering student at B.P. Poddar Institute of Management and Technology (3rd year), with hands-on project development experience across data science, machine learning, and full-stack applications. As a skilled developer, he has worked on multiple ML projects implementing supervised learning, deep neural networks (CNN, RNN, LSTM), and transformer-based models.

Technical stack proficiency includes Python, Java, JavaScript, C++, SQL, and modern frameworks (TensorFlow, PyTorch, Scikit-learn). His expertise encompasses data preprocessing, feature engineering, model optimization, deployment, and real-world AI implementation. These projects demonstrate capability in complex problem-solving, predictive analytics, and cybersecurity applications.

Key Projects: He developed an Intelligent Flight Ticket Price Prediction System utilizing data-driven machine learning models, implementing regression algorithms and feature engineering techniques to forecast dynamic pricing patterns. Currently developing research work on VANET security and network intrusion detection using machine learning, demonstrating capability in complex problem-solving and real-world AI implementation.

Swapnanil Mukherjee is a B.Tech Computer Science and Engineering student at JIS University (6th semester) with strong academic performance. His expertise spans Artificial Intelligence, Machine Learning, Data Analytics, Full-Stack Development, and Cyber Security. He has completed training in Mean Full Stack Development and Data Analytics & Big Data.

His research contribution includes publication of "Sentiment Analysis on Twitter: A Study of SVM and CNN Performance" through Springer. Key academic projects encompass E-Commerce Customer Behaviour Analysis, VANET-based security research, and multiple software development initiatives. Passionate about emerging technologies and innovation, he aspires to build a successful IT career through continuous learning and contributing to technological advancements via research and development.

Mr. Sudipta Kumar Dutta is an Assistant Professor in the Department of Computer Science and Engineering at BPPIMT, Kolkata Campus. He holds M.Tech and B.Tech degrees in Computer Science from JIS College of Engineering. His research expertise encompasses Artificial Intelligence, Machine Learning, and Data Mining. He actively contributes to innovative research and academic excellence, mentoring students in advanced computational methodologies and intelligent systems development.