EIRP 2024

THE 19TH EDITION OF THE INTERNATIONAL CONFERENCE
EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES

The New Paradigm of
FinTech and CyberSecurity

Vanet Security and Privacy – an Overview

Veranda Syla[1], Algenti Lala[2], Aleksandër Biberaj[3]

Abstract: While vehicular ad-hoc networks (VANETs) offer substantial benefits to society, they also present numerous challenges, particularly in terms of security and privacy. Given the significant impact of VANETs on modern transportation systems, ensuring robust security and safeguarding user privacy are paramount. This paper provides an overview of VANET security and privacy, exploring fundamental challenges, state-of-the-art solutions, and emerging trends in this field. By examining the unique characteristics of VANETs, such as dynamic topology and resource constraints, this paper highlights the vulnerabilities inherent in these networks and the potential threats they face, including malicious attacks and privacy breaches. Additionally, the paper explores the intricate balance between security and privacy requirements, highlighting the trade-offs involved in deploying protective measures while preserving user anonymity and data confidentiality. Finally, the paper discusses future research directions and open challenges, advocating for interdisciplinary approaches and innovative solutions to address the evolving landscape of VANET security and privacy. This paper aims to provide researchers, practitioners, and policymakers with a nuanced understanding of the complex interplay between security, privacy, and attacks in VANET environments.

Keywords: VANET Attacks; Security; Privacy Preservation

1. Introduction

As the world moves towards more interconnected and intelligent transportation systems, Vehicular Ad-hoc Networks have emerged as a pivotal technology in enhancing vehicular communication, safety, and operational efficiency. VANETs, comprising vehicles connected by wireless networks, facilitate a multitude of applications ranging from traffic management to emergency response and multimedia transmissions (Khan, et. al., 2021). However, the increased connectivity and data sharing inherent in VANETs also introduce significant security and privacy challenges. These networks are particularly susceptible to a range of security threats that could compromise personal privacy, data integrity, and the

[1] PhDc. Veranda Syla, Polytechnic University of Tirana, Tirana, Albania, Address: Sheshi Nënë Tereza 4, Tiranë 1010, Albania, E-mail: vsyla@fti.edu.al.

[2] Prof. Assoc. Algenti Lala, Polytechnic University of Tirana, Tirana, Albania, Address: Sheshi Nënë Tereza 4, Tiranë 1010, Albania, E-mail: alala@fti.edu.al.

[3] Prof. Dr. Aleksandër Biberaj, Polytechnic University of Tirana, Tirana, Albania, Address: Sheshi Nënë Tereza 4, Tiranë 1010, Albania, E-mail: abiberaj@fti.edu.al.

overall reliability of transportation systems. Ensuring the security and privacy of VANETs is crucial due to the potential consequences of cybersecurity threats which could range from minor disruptions to catastrophic incidents affecting life and property.

In recent years, due to economic and population growth, a rapid increase has been observed in the numerous vehicles. This has automatically increased the chances of road accidents. According to The Global Status Report on Road Safety, 2023 shows that the number of annual road traffic deaths has fallen slightly to 1.19 million (World Health Organization, 2023). The report shows that efforts to improve road safety are having an impact and that significant reductions in road traffic deaths can be made if proven measures are applied. Despite this, the price paid for mobility remains too high. Road traffic injuries remain the leading killer of children and young people aged 5-29 years.

Furthermore, VANETs command a unique grade of requirements to maintain the liability and accountability of drivers involved in accidents, traffic violations, emission norms, and irregularities to take punitive actions if a driver commits any crime. Besides that, location and context-aware services require pinpoint user location and preferences to provide the most specific, exact, and comprehensive list of personalized information (Mansour, et. al, 2018). Despite that, communication of such information raises significant privacy issues that cannot be neglected. Also, privacy concerns in vehicular communications are necessary to protect user data from profiling and tracking.

This paper explores the security and privacy landscape of VANETs, delves into specific vulnerabilities and threats, and reviews the state-of-the-art security measures and privacy-preserving techniques currently employed. We also look into the future, discussing emerging trends and the ongoing research aimed at fortifying the resilience of VANETs against evolving cybersecurity risks. This paper is organized as follows: the second section describes related work on security and privacy in VANETs. Section three provides an overview of the security and privacy requirements versus the state-of-the-art approaches proposed for VANET security and privacy. In Section Four, we discuss the types of VANET attacks. Finally, Section five concludes the paper, and section six describes future work.

2. Related Work

The research landscape on VANET security and privacy is both broad and diverse, reflecting the complexity and critical nature of the issues involved. Prior works in this field have primarily focused on developing robust cryptographic protocols to ensure secure communication among vehicles.

The study (Al-Qutayri, et. al, 2010) demonstrated that identity-based cryptography (IBC) is particularly suited for VANETs due to it is lightweight nature, which aligns well with the network's infrastructure-less setup and the need for high-speed, real-time responses. It highlighted the unique properties, security, and privacy challenges presented by such mobile ad hoc networks. Furthermore, the study investigated three main cryptographic schemes: public key, symmetric key, and identity-based cryptography. It identified the advantages and disadvantages of these schemes and how they correspond with the characteristics of VANETs, concluding that IBC is the most viable option for securing these networks.

The paper (Maxim, et. al, 2007) provides a comprehensive threat analysis and proposes a security architecture tailored to VANETs. The authors discuss the importance of privacy protection alongside ensuring robust security measures. They highlight the dual need to establish driver liability in incidents while protecting individual privacy, suggesting a set of security protocols designed to safeguard against various threats, including attacks on data integrity and privacy. Their proposed solutions involve identity-based cryptography as a means to secure communication without infringing on user privacy.

This choice is favored due to its efficiency in environments characterized by high mobility and dynamic network changes, which are typical in VANETs. Their work is foundational in setting the direction for subsequent research on VANET security, aiming to balance effective threat mitigation with minimal impact on system performance and user convenience.

In the comprehensive study (Xiaodong, et. al, 2008) on vehicular ad hoc networks, the authors focus on the pivotal aspects of security and privacy within Wireless Access in Vehicular Environments (WAVE). Their research underscores the critical challenges and presents innovative solutions necessary for enhancing certificate revocation processes and achieving conditional privacy preservation. They propose a suite of novel security mechanisms specifically designed to ensure robust protection and privacy, adaptable to the high-speed and dynamic nature of VANETs. This research plays a crucial role in advancing the field by addressing both practical implementation challenges and the theoretical foundations of secure and private vehicular communications.

The study (Mintemur, et. al, 2017) analyzes security vulnerabilities within Vehicular Ad Hoc Networks by testing four types of attacks—blackhole, dropping, flooding, and bogus information—on Ad-Hoc on on-demand Distance Vector Routing Protocol (AODV) and Greedy Perimeter Stateless Routing Protocol (GPSR) routing protocols using simulations on realistic road maps. Their findings reveal significant impacts on network communication, highlighting the urgent need for robust security solutions tailored to the dynamic nature of VANETs. This research contributes substantially to understanding and mitigating potential threats in vehicular networks.

The related work in the realm of VANET security and privacy underscores the vital importance of robust cryptographic solutions and network security architectures. Studies have explored identity-based cryptography for its suitability in VANETs, emphasizing its efficiency in high-mobility environments. Other research has focused on threat analyses and the enhancement of security protocols, including certificate revocation and privacy preservation, to protect against varied network attacks. These collective efforts highlight the dynamic challenges of VANETs and the ongoing need for innovative security mechanisms tailored to their unique characteristics.

3. Security and Privacy Requirements in VANETs

3.1. Authentication and Authorization

Ensuring that communication between vehicles and infrastructure is conducted by verified and trustworthy sources. Authentication and authorization are critical for securing vehicular ad hoc networks. These processes ensure that only legitimate users and devices can access network resources and communicate securely. Authentication in VANETs typically involves verifying the identities of vehicles and infrastructure components using digital certificates and asymmetric cryptography methods. This process helps mitigate various security threats such as impersonation and man-in-the-middle attacks (Maxim & Hubaux, 2005).

Authorization, on the other hand, ensures that once authenticated, entities are permitted to perform only those actions that are allowed based on predefined policies. It is crucial for enforcing control over access to network services and sensitive information, thus safeguarding against unauthorized data manipulation and ensuring the privacy of users. Effective authorization mechanisms contribute to maintaining operational integrity and trust in VANET environments (Papadimitratos, et. al, 2008). These security measures are essential not only for protecting the network against unauthorized access and attacks but also for ensuring the privacy and safety of the users in dynamic vehicular environments.

3.2. Confidentiality

Protecting sensitive information from unauthorized access to preserve the privacy of drivers and passengers. Confidentiality in VANETs is paramount to protect sensitive information transmitted between vehicles and infrastructure. This includes location data, travel routes, and personal information of drivers and passengers. Encryption plays a crucial role in achieving confidentiality. Techniques such as symmetric and asymmetric encryption are employed to ensure that data transmitted over VANETs cannot be accessed by unauthorized entities. For example, the Advanced Encryption Standard (AES) provides strong encryption to secure communication channels, preventing eavesdropping and ensuring that personal and operational data remain confidential (Qi & Gao, et. al, 2023).

Maintaining confidentiality also helps in building trust among users, which is essential for the widespread adoption of VANET technologies. The implementation of effective encryption protocols and confidentiality measures ensures that only intended recipients can access and interpret the data transmitted, which is critical in preserving the privacy and security of vehicular communications (Gerlach, et. al, 2007).

3.3. Integrity

Safeguarding data from alterations during transmission, ensuring the accuracy and reliability of exchanged messages. Integrity in VANETs ensures that data transmitted between vehicles and infrastructure remains unchanged and trustworthy. Mechanisms like digital signatures and hash functions are pivotal in maintaining data integrity, verifying that the data has not been altered from its original form. This is crucial for applications such as emergency vehicle notifications and cooperative collision avoidance, where receiving accurate and unmodified information is essential for safety. For instance, the use of Secure Hash Algorithms (SHA) provides a means to verify data integrity, ensuring that any alteration in the communication can be detected (Parno, Bryan & Perrig, 2005).

3.4. Non-Repudiation

Providing proof of communication and data transactions to prevent denial of involvement by the parties. Non-repudiation in VANETs ensures that every communication or transaction within the network is attributable, preventing any dispute over the authenticity of transmissions. This attribute is crucial in VANETs where evidence of misconduct or a breach could be pivotal in legal scenarios, such as resolving disputes following accidents or breaches of traffic laws. The implementation of robust cryptographic techniques, such as digital signatures combined with public key infrastructures (PKIs), is fundamental. These systems not only authenticate the source of the message but also ensure that the sender cannot deny their actions later. Advanced mechanisms like timestamping and secure logging further enhance non-repudiation by providing a verifiable trail of communications and operations, crucial for forensic analysis and establishing liability in vehicular networks (Zhang, 2011).

3.5. Availability

Ensuring reliable and continuous service, especially for critical safety applications in vehicular environments. Availability in VANETs is essential for ensuring that vehicular network services are consistently accessible to all users, supporting critical functionalities like safety communications and traffic management. To improve availability, VANETs employ various strategies such as network redundancy, where multiple communication paths and nodes are available, thus ensuring that the network can still function even if parts of it fail. Additionally, deploying fault-tolerant protocols helps in quickly recovering from node or link failures, crucial in maintaining uninterrupted service (Abdelkader, 2017).

Another aspect of enhancing availability involves addressing the scalability of the network to handle high densities of vehicles without degradation in performance. Techniques such as load balancing and adaptive data dissemination are used to manage network load effectively and prevent service outages. This is particularly important in urban environments where the concentration of vehicles can be very high, requiring robust mechanisms to ensure that data flows remain smooth and uninterrupted (Rawat, et. al, 2011).

Moreover, proactive security measures such as intrusion detection systems (IDS) and regular network health checks can preemptively identify and mitigate potential threats that may impact availability. These systems are designed to detect anomalies and potential cyber-attacks early, allowing for swift responses to avoid widespread network disruption (Ryma, 2019).

3.6. Anonymity and Privacy

Maintaining user anonymity to protect personal and location information against tracking and profiling, while still allowing for accountability in the event of disputes or investigations. Anonymity and privacy are paramount in VANETs, requiring robust mechanisms to protect user identities while allowing vehicles to communicate securely and effectively. Anonymization techniques such as changing pseudonyms at strategic locations or time intervals minimize the risk of user tracking, enhancing privacy without compromising the functionality of the network. The implementation of cryptographic protocols ensures that only authorized parties can access or decrypt transmitted data, which is crucial for maintaining the confidentiality of user information (Gerlach, 2006; Freudiger, 2007).

To further strengthen privacy, VANET systems can integrate mix-zones areas where vehicles change their pseudonyms in a coordinated manner to break the linkability of consecutive messages. Additionally, privacy-preserving authentication methods can verify the legitimacy of messages without revealing the sender's identity, thus maintaining both security and privacy. Techniques like zero-knowledge proofs provide an additional layer of security by allowing nodes to prove their authenticity without exposing their actual identities or credentials (Pravin, 2021). Ensuring that these privacy measures are compliant with regulatory requirements and effectively implemented is vital for fostering user trust and promoting widespread adoption of VANET technologies.

3.7. Scalability

Addressing the capacity to securely manage a vast number of vehicles moving at high speeds and changing network topologies frequently. Scalability is a critical aspect of VANETs, ensuring that the network can accommodate increasing numbers of vehicles and maintain performance without significant degradation. To address scalability challenges, VANETs employ various strategies, including efficient routing protocols, network management techniques, and resource allocation mechanisms.

One approach to improving scalability is the deployment of hierarchical or clustering-based routing protocols. These protocols organize vehicles into clusters, with each cluster having a designated cluster head responsible for managing communication within the cluster. This hierarchical structure helps reduce overhead and control message flooding, thereby improving the scalability of the network, particularly in large-scale deployments. Moreover, adaptive routing algorithms dynamically adjust the routing paths based on network conditions and traffic patterns, further enhancing scalability by optimizing resource utilization and minimizing congestion (Esteban, 2006).

Additionally, the utilization of cloud computing and edge computing paradigms can significantly enhance the scalability of VANETs. By offloading computation and storage tasks to centralized or distributed cloud infrastructure, VANETs can handle a larger number of vehicles and applications without overburdening onboard resources. Edge computing, on the other hand, leverages computational resources at the network edge, closer to the vehicles, to reduce latency and improve responsiveness, particularly for time-critical applications such as collision avoidance systems (Cui, et. al, 2020; Yousefi, et. al, 2006).

Ensuring the scalability of VANETs is essential for accommodating the growing number of connected vehicles and supporting the diverse range of applications and services envisioned for future intelligent transportation systems. Each of these requirements is critical for maintaining a secure and private network within the challenging and dynamic environment of VANETs.

These foundational elements guide the development of secure communication protocols and privacy-preserving strategies essential for the deployment and acceptance of VANET technologies.

4. Types of VANET Attacks

VANETs are susceptible to various types of attacks, each targeting different aspects of the network.

4.1. Eavesdropping Attacks

These attacks involve unauthorized interception of communications between vehicles, compromising the privacy and confidentiality of the data transmitted**.** Eavesdropping attacks in VANETs pose significant threats to the privacy and confidentiality of vehicular communications. These attacks involve unauthorized interception of data exchanged between vehicles, potentially exposing sensitive information such as location details, travel patterns, and personal data of passengers. To combat eavesdropping, VANETs employ robust encryption methods that ensure the data remains unreadable to unauthorized parties (Obaidat, et. al, 2020). Additionally, techniques such as secure key exchange protocols are crucial for maintaining secure communication channels, preventing attackers from gaining access to encryption keys used in data transmission.

Further enhancing security against eavesdropping, network designers can implement network segmentation strategies. These limit the scope of any single communication to a small geographic area, thus reducing the potential impact of intercepted communications. Advanced monitoring and anomaly detection systems also play a vital role in identifying unusual patterns that may indicate an eavesdropping attempt, enabling network administrators to react swiftly to secure the network.

4.2. Spoofing Attacks

Attackers impersonate another vehicle or infrastructure component to send false information or commands, leading to potential chaos in traffic management systems. Spoofing attacks in VANETs are particularly disruptive, as they involve an attacker masquerading as a legitimate network entity to send deceptive information or commands. This can lead to incorrect routing information, emergency system alerts, or false traffic updates, potentially causing chaos on the road. To mitigate these attacks, VANETs implement sophisticated authentication protocols that verify the identity of each communicating party (Baldini, 2022). Additionally, the integration of intrusion detection systems (IDS) can help identify and isolate spoofing attempts by analyzing patterns of communication and detecting anomalies that deviate from normal behavior.

Continuous improvements in cryptographic security, such as the adoption of more robust and dynamic cryptographic keys, are also vital in combating spoofing. These measures not only prevent unauthorized access but also ensure that any compromised data can be quickly identified and mitigated.

4.3. Denial of Service (DoS) Attacks

These attacks aim to disrupt the network by overwhelming it with traffic, which can degrade performance or completely shut down communication channels. Denial of Service attacks in VANETs are critical threats that aim to disrupt the normal functioning of the network by overwhelming it with a flood of unnecessary requests (Krishna, et. al, 2022). This can incapacitate the network, preventing legitimate communications and potentially leading to hazardous situations on the roads. To defend against these attacks, VANETs utilize rate limiting and anomaly detection techniques to identify and mitigate unusual traffic patterns that may indicate a DoS attack. Additionally, implementing network segmentation can limit the spread of such attacks, confining their impact to smaller, manageable areas.

Further resilience against DoS attacks can be built by employing redundant communication paths and diversified network access technologies, ensuring that even if one part of the network is under attack, alternative channels remain available for critical communications.

4.4. Sybil Attacks

In this attack, a single node illegitimately takes on multiple identities. It can severely disrupt the trust and reputation systems within VANETs by skewing consensus or majority-based decisions. Sybil attacks pose a significant threat to the security of VANETs. In these attacks, a malicious vehicle or node creates multiple fake identities to gain a disproportionate influence over the network. This can disrupt various network operations, such as consensus mechanisms, reputation systems, and routing protocols, leading to false traffic reports, manipulated traffic flows, or even isolating legitimate vehicles from the network. To combat Sybil attacks, VANETs need robust identity verification mechanisms that can effectively authenticate and validate the identities of vehicles in real time.

One effective approach to mitigating Sybil attacks is the implementation of trust management systems. These systems evaluate the trustworthiness of each node based on their behavior and historical data, which helps in distinguishing legitimate nodes from malicious ones masquerading under multiple identities. Additionally, cryptographic techniques such as digital signatures and certificate authorities are used to ensure that each node in the network can be reliably authenticated, thus preventing the proliferation of fake identities (Douceur, 2002; Levine, et. al, 2006).

Further reinforcing the defense against Sybil attacks, some proposed methods include the use of decentralized solutions like blockchain technology, which can provide a transparent and tamper-proof system for managing identities and transactions within the network. By leveraging blockchain, VANETs can facilitate secure and immutable record-keeping of vehicle identities and their corresponding reputational scores, making it significantly harder for attackers to create and maintain multiple fake identities without being detected (Sanjeev, et. al, 2022).

4.5. Man-in-the-Middle (MitM) Attacks

Attackers intercept and potentially alter the communication between two parties without their knowledge, which could mislead the recipients or alter the behavior of vehicles. Man-in-the-middle (MITM) attacks in VANETs represent a significant security challenge due to their ability to intercept and alter communications between vehicles, potentially leading to misinformation and affecting the safety and efficiency of the transportation system. To address these issues, researchers have explored various strategies for mitigating the impact of MitM attackers in VANETs. These strategies focus on enhancing the security protocols to prevent attackers from successfully inserting themselves between communicating nodes.

One effective method to combat MitM attacks includes the implementation of advanced cryptographic solutions that ensure the integrity and confidentiality of the communications. By using both symmetric and asymmetric cryptography, VANETs can safeguard data against unauthorized access and tampering. Additionally, employing comprehensive network monitoring and anomaly detection systems can help in identifying and responding to MitM activities by analyzing unusual patterns in data transmission, which may indicate an interception attempt (Krzysztof, et. al, 2019).

Furthermore, the adaptation of blockchain technology has been proposed as a robust solution to enhance security in VANETs. Blockchain's decentralized nature helps reduce the risk of MitM attacks by eliminating the need for a central authority, thus making security management more resilient and less prone to attacks. The technology ensures that all transactions and data exchanges are recorded on a secure, immutable ledger, enhancing the overall trustworthiness of the communications within the network (Ahmad, et. al, 2018). This comprehensive approach to securing VANET communications is crucial for maintaining the integrity and reliability of vehicular communications, thereby supporting the safe operation of intelligent transportation systems. Understanding and addressing these vulnerabilities is crucial for enhancing the security and maintaining the integrity and privacy of VANET communications**.**

5. Conclusion

This paper has provided a comprehensive overview of the security and privacy challenges facing vehicular ad-hoc networks, elucidating the unique vulnerabilities and potential threats inherent to these networks. Through a detailed exploration of the fundamental security and privacy requirements, alongside a review of state-of-the-art solutions and emerging trends, this work has highlighted the complex interplay between security, privacy, and various types of attacks within VANET environments. By examining the security and privacy requirements and categorizing the types of VANET attacks, the paper has outlined effective strategies to mitigate these threats and enhance the resilience of VANETs against adversarial activities.

Moreover, the discussion on the necessary trade-offs involved in deploying protective measures, while preserving user anonymity and data confidentiality, emphasizes the delicate balance required to maintain both security and privacy. These efforts are crucial for fostering the acceptance and widespread deployment of VANET technologies, ensuring they enhance modern transportation systems without compromising user safety or privacy.

6. Future Work

The future work for enhancing VANET security and privacy should focus on several key areas to address ongoing challenges and leverage emerging technologies. Continued efforts are needed to develop more robust security solutions that can handle the high mobility and dynamic topology of VANETs. This includes refining cryptographic methods to ensure data integrity and confidentiality across varying network conditions.

Furthermore, the integration of artificial intelligence (AI) and machine learning techniques could significantly improve anomaly detection and response strategies, enabling the network to adapt to new threats proactively. This approach is crucial for managing the complexity of real-time data exchange and the varying security requirements of different vehicles and infrastructure components.

Additionally, the adoption of blockchain technology in VANETs presents a promising solution for achieving decentralized security management and enhancing trust among network participants. Blockchain can provide a reliable and transparent mechanism for handling transactions and data exchanges, ensuring integrity and non-repudiation.

Lastly, as VANETs become increasingly integrated with other components of intelligent transportation systems, such as connected and autonomous vehicles, there's a growing need to develop unified security frameworks that can seamlessly operate across different layers of the network infrastructure. This will involve close collaboration between industry stakeholders, researchers, and policymakers to establish standards and best practices that ensure the safety, privacy, and efficiency of future vehicular networks.

References

Abdelgader, A. M. S.; Shu, F.; Zhu, W. & Ayoub, K. (2017). Security challenges and trends in vehicular communications. *IEEE Conference on Systems, Process and Control (ICSPC)*. Melaka, Malaysia, pp. 105-110.

Ahmad, Farhan; Adnane, Asma; Franqueira, Virginia N. L.; Kurugollu, Fatih & Liu, Lu (2018). *Man in the Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies*. Retrieved from https://www.mdpi.com/1424-8220/18/11/4040.

Al-Qutayri, Mahmoud; Chan Yeun & Faisal, Al-Hawi (2010). Security and Privacy of Intelligent VANETs. *Computational Intelligence and Modern Heuristics*. InTech.

Cui, Jie; Lu, Wei; Hong, Zhong; Jing, Zhang; Yan, Xu & Lu, Liu (2020). Edge Computing in VANETs-An Efficient and Privacy-Preserving Cooperative Downloading Scheme. *IEEE Journal on Selected Areas in Communications*, Vol. 38, pp. 1191-1204.

Douceur, John R. (2002). *The Sybil Attack. International Workshop on Peer-to-Peer Systems*. Retrieved from https://api.semanticscholar.org/CorpusID:5310675.

Esteban, Egea López (2006). Simulation scalability issues in wireless sensor networks. *Journal Communications Magazine Publisher, IEEE Institute of Electrical and Electronics*.

Freudiger, Julien; Raya, Maxim; Félegyházi, Márk; Papadimitratos, Panos & Hubaux, Jean-Pierre (2007). Mix-Zones for Location Privacy in Vehicular Networks. Published in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems* (WiN-ITS), Vancouver, BC, Canada.

Gerlach, M. & Güttler, F. (22 April, 2007). Privacy in VANETs using Changing Pseudonyms - Ideal and Real. *Published in IEEE Vehicular Technology Conference Computer Science.*

Gerlach, Matthias (2006). *Assessing and Improving Privacy in VANETs*. Retrieved from https://api.semanticscholar.org/CorpusID:18699706.

Gianmarco, Baldini (2022). Detection of cybersecurity spoofing attacks in vehicular networks with recurrence quantification analysis. Computer Communications, Vol. 191, pp. 486-499.

Global status report on road safety *(*2023). *World Health Organization*.

Jaya Krishna, N. & Prasanth, N. (2022). An Insight View on Denial of Service Attacks in Vehicular Ad Hoc Networks. *Advances in Computational Intelligence and Communication Technology*, pp. 273–285.

Khan, S.; Sharma, I.; Aslam, M.; Khan, M. Z. & Khan, S. (2021). S. Security Challenges of Location Privacy in VANETs and State-of-the-Art Solutions: A Survey. *Future Internet*, Vol. 13(4), p. 96.

Krzysztof, Stepień & Aneta, Poniszewska-Marańda (26–28 August, 2019). Security Measures in the Vehicular Ad-Hoc Networks – Man in the Middle Attack. *Mobile Web and Intelligent Information Systems: 16th International Conference, MobiWIS*, pp. 136–147.

Levine, Brian Neil, et. al. (2006). *A Survey of Solutions to the Sybil Attack*. Retrieved from https://api.semanticscholar.org/CorpusID:15204796.

Marvy, B. Mansour; Cherif Salama; Hoda, K. Mohamed & Sherif, A. Hammad (March, 2018). Vanet security and privacy – an overview. *International Journal of Network Security & Its Applications (IJNSA),* Vol. 10(2).

Maxim and Jean-Pierre Hubaux (2005). The security of vehicular ad hoc networks. *ACM Workshop on Security of Ad Hoc and Sensor Networks*.

Maxim, Raya & Jean-Pierre, Hubaux (2007). Securing vehicular ad hoc networks. IOS Press *Journal of Computer Security*, Vol. 15, pp. 39–68.

Mintemur, Ömer & Sen, Sevil (2017). Attack Analysis in Vehicular Ad Hoc Networks. *Proceedings of 7th International Conference on Computer Science, Engineering & Applications.* pp. 35-46.

Obaidat, M.; Khodjaeva, M.; Holst, J. & Ben Zid, M. (2020). *Security and Privacy Challenges in Vehicular Ad Hoc Networks*. In: Mahmood, Z. (eds) *Connected Vehicles in the Internet of Things*. Springer, Cham.

Papadimitratos, P.; Buttyan, L.; Holczer, T.; Schoch, E.; Freudiger, J.; Raya, M.; Ma, Z.; Kargl, F.; Kung, A. & Hubaux, J. P. (November, 2008). Secure Vehicular Communication Systems: Design and Architecture. *IEEE Communications Magazine*, Vol. 46(11), pp. 100—109.

Parno, Bryan & Adrian, Perrig (2005). Challenges in Securing Vehicular Networks. *Computer Science, Engineering.* Corpus.

Pravin, Mundhe; Shekhar, Verma & S. Venkatesan. (2021). A comprehensive survey on authentication and privacy-preserving schemes in VANETs. *Computer Science Review,* Vol. 41.

Qi, J.; Gao, T. & Zhao, C. (2023). An Efficient Privacy-Preserving Authentication Scheme Based on Shamir Secret Sharing for VANETs. *In: Barolli, L. (eds) Innovative Mobile and Internet Services in Ubiquitous Computing. IMIS 2023. Lecture Notes on Data Engineering and Communications Technologies,* Vol. 177. Springer, Cham.

Rawat, D. B.; Popescu, D. C.; Yan, G. & Olariu, S. (2011). Enhancing VANET Performance by Joint Adaptation of Transmission Power and Contention Window Size. *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22(9,) pp. 1528-1535.

Ryma, Abassi (04 January, 2019). *VANET security and forensics: Challenges and opportunities*.

Sanjeev Kumar Dwivedi; Ruhul Amin; Ashok, Kumar Das; Mark, T. Leung; Kim-Kwang, Raymond Choo & Satyanarayana, Vollala (2022). Blockchain-based vehicular ad-hoc networks: A comprehensive survey. *Ad Hoc Networks,* Vol. 137.

Xiaodong, Lin; Rongxing, Lu; Chenxi, Zhang; Haojin, Zhu; Pin-Han, Ho & Xuemin, Sherman (April, 2008). Security in vehicular ad hoc networks. *IEEE Communications Magazine*, vol. 46(4), pp. 88-95.

Yousefi, S.; Mousavi, M. S. & Fathy, M. (2006). Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives, *6th International Conference on ITS Telecommunications*. Chengdu, China, pp. 761-766.

Zhang, J. (2011). A Survey on Trust Management for VANETs. *IEEE International Conference on Advanced Information Networking and Applications*. Biopolis, Singapore, pp. 105-112.