Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 4 (2024)

Cryptanalysis of Authentication Schemes in Heterogeneous Vehicular Networks

Kamal Kumar[1], Vinod Kumar[2,*], Renu[1], Rajiv Kumar[3]
[1]Department of Mathematics, Baba Mastnath University, Rohtak – 124021, India
[2]Department of Mathematics, Shyam Lal College, University of Delhi, New Delhi-110032, India
[3]Department of Computer Science and Engineering, Baba Mastnath University, Rohtak – 124021, India
**: Corresponding author*

Abstract:- The rapid evolution of Heterogeneous Vehicular Network (HetVNETs) has introduced complex challenges in securing communication between vehicles and infrastructure. One of the most critical aspects of security in these networks is authentication, which ensures that only trusted entities can participate in vehicular communication. The use of various communication technologies in HetVNETs, including networks like 4G, 5G, and dedicated short-range communication systems, makes these systems vulnerable to different cryptographic issues. This paper provides a detailed analysis of current authentication methods in HetVNETs, highlighting their weaknesses against several types of attacks, such as replay, man-in-the-middle, and impersonation attacks. We evaluate the performance, scalability, and resilience of these methods under different attack scenarios. Based on our findings, we propose ways to enhance the security of authentication protocols in HetVNETs to ensure safe and reliable communication for future vehicular networks.

Keywords: *Authentication, Security Attacks, Vehicular Networks, Vulnerability.*

1. Introduction

Heterogeneous Vehicular Networks (HetVNETs) are a cornerstone of modern Intelligent Transportation Systems (ITS), facilitating seamless communication between vehicles, roadside infrastructure, and cloud services. By integrating various communication technologies like 4G, 5G, and Dedicated Short-Range Communication, HetVNETs support a wide range of applications, from security alerts to entertainment and traffic control. However, the diversity and complexity of HetVNETs also present significant security challenges, particularly in the area of authentication. Authentication methods are essential for ensuring that only trusted vehicles and infrastructure can participate in network communications. Any issues with authentication can allow unauthorized access, enabling attackers to launch attacks that threaten the safety, privacy, and reliability of vehicular communication. In this context, cryptanalysis, the study of weaknesses in cryptographic systems, becomes crucial for evaluating the effectiveness of the authentication protocols used in HetVNETs.

This paper aims to analyze current authentication methods in HetVNETs, identifying cryptographic vulnerabilities and assessing their susceptibility to attacks. We examine the strengths and weaknesses of these protocols in real-world scenarios, taking into account the unique characteristics of different network types. By providing a detailed cryptanalysis, we hope to offer insights that will contribute to the development of more secure and reliable authentication methods for future vehicular networks.

1.1 How HetVNETs work

HetVnets refer to network of communications between vehicles, roadside infrastructure and cloud-based system, which combine multiple type of communication. Over the past decade, traffic congestion and accidents, as well as environmental pollution have become important global issue in the transportation industry. In order to

overcome these common issue, intelligent transportation systems (ITSs) and vehicular networks have been widely studied these days. It is based on dedicated short range of communication DSRC. As shown in Figure 1, the integration of DSRC or Wi-Fi (short range and less time consuming in sharing data), cellular based communication (wide area network coverage), MM wave communication (high bandwidth but more time consuming in sharing data), and satellite communication (ensure global connectivity below technologies) provides more efficient communication. After blending these technologies in HetVNETs, it provides more efficient and flexible communication. So, vehicles can easily move from one to another cellular networks for long-range communications. Vehicles can switch to short range communication network of wide range communication network.

For information exchange depending on situation. This technology provides 360-degree awareness of surrounding risk, which improves performance and safety. The main objective of this communication technology is to eliminate costly and life threatening traffic collisions and improve road safety (generate cost savings) and infrastructure management. Each technology comes with its own set of standards, process and constraints. It is essential to have a unified architecture that can coordinate in better way. However, the current network architecture of HETVNET cannot efficiently deal with the increasing demands of the rapidly changing network landscape. Additionally, the wide range of nature of the network gives more task of managing security, quality of service (QoS), and mobility, especially vehicles travel from different network environments. But these challenges, HetVNETs see as opportunity for future intelligent transportation systems (ITS), providing better way to increase road safety, reduced traffic problems, and easy path for fully autonomous vehicles.

1.2 Motivation

The idea of HetVNETs embraces as an integral part of smart transport systems and self-driving technologies, which promote road safety, the management of traffic flows, and the efficacy of transport in general. Nevertheless, it is precisely the synergy that poses unique challenges in security due to the diversity of the environment, including 5G, dedicated short-range communication, etc. While this communication occurs across disparate platforms of vehicles, roadside infrastructure, and cloud infrastructure, it is imperative to manage such interactions in a manner that only bona fide participants take part in such interactions for the reasons of security and trust within the network.

- The capabilities of HetVNETs as applied in Integrated Transport Systems ITS and autonomous driving systems do not coincide, which demonstrates that developed systems need account security. This aggravation may be partly explained by the fact that no existing authentication protocols in HetVNETs provides optimum security levels.

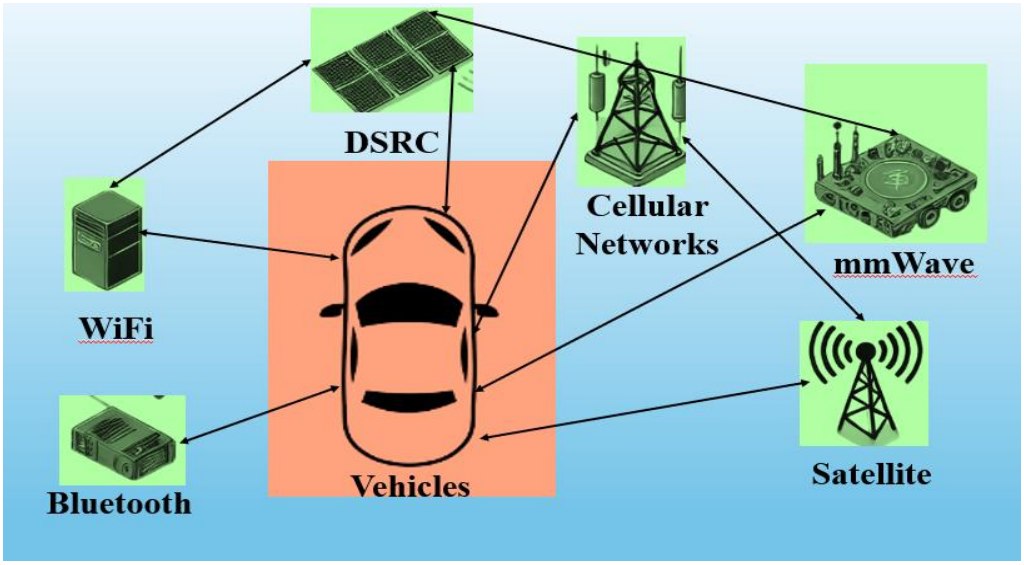

Figure 1: HetVNETs

- Communication networks have a wide range of safety issues, and the current authentication models' focus is mainly on safe critical applications such as collision avoidance, emergency braking, and platooning.
- An increased number of vehicles, in addition to rapid data exchanges, has left an increasing need for lightweight authentication protocols in Het VNETs that provide both security and efficiency. The volatile situation calls for the authentication to be both dynamic and resilient, which allows key exchanges to take place—often and with different interfaces of the system.
- Though vehicular networks include a number of authentication methods, not all of them have been able to withstand a practical attack-oriented cryptoanalysis.
- As such, while vehicular networks are undergoing a paradigm shift to be fully autonomous, there is greater reliance on the trust and security of all components. Effective measures on advancing the security mechanisms of trust in the authentication process in HetVNETs will promote secure communication within the next generation of transportation systems.

1.3 Contribution

This research paper contributes the following notable developments in the domain of security in vehicular networks, particularly towards the authentication schemes in HetVNETs. The paper presents the following key points in vehicular networks:

- We carry out a comprehensive cryptological analysis of the existing various authentication schemes used in HetVNETs with respect to replay attacks, man-in-the-middle attacks, impersonation attacks, Sybil attacks, denial-of-service attacks, and other attacks.
- Our research addresses concerns regarding the emergence of new vulnerabilities in the bio integration of various communication technologies in HetVNETs. We offer several examples of how these hetero-architectural strategies create new types of attacks that are not properly handled by conventional authentication mechanisms.
- We make certain recommendations in terms of bolstering and expanding the existing authentication framework in HetVNETs.
- In the course of this work, we construct an architecture that should be followed for the further development and assessment of authentication protocols in HetVNETs. Security or effectiveness may not be the criteria for the desired outcome, and so versatility comes into play that allows addressing the more complex issues of constructing authentication mechanisms in highly dynamic and heterogeneous vehicular networks.
- To show that the suggested protocol is more secure and efficient than existing methods in digital twin vehicular communication, it is compared to several competing contemporary protocols [1, 2, 3, 4].
- The proposed system can withstand various security attacks, as shown by the informal security assessment, which enables its application in a real-world digital twin vehicular communication.

2. Literature survey

Vehicular ad hoc networks (VANETs) play a key role in assuring safe communication within HetVNETs, yet they continue to exist unguarded to a range of safety and security challenges. A huge variety of cryptographic techniques and methods have been evolved to address the bottom line of the matter of authentication, integrity, and confidentiality in these networks. Although, due to the diverse nature of vehicular communication, where disparate cryptographic systems (such as identity-based cryptosystems and public key infrastructures) accompany, extra complications arise. In the 2014, Liu et al. upgraded upon Shim's authentication scheme by enhancing safety and security against the selected message attacks. They recognized the actuality that Shim's original evidence was not sufficient and provided a more stronger batch verification process, decrease the rate of error in signature validation [1]. To improve the robustness of safety and security measures in VANETs, various schemes combine extra layers of defense. In the year 2017, Sedjelmaci et al. introduced the invasion of detection methodology to

mark the risks like Sybil attacks, depending on game theory to forecast hostile behavior before it happens [2]. Later, in year 2019, Zhou et al. introduced the bi-directional signcryption methodology for safeguard vehicular communications in HetVNETs. These plans aid batch verification and ensure confidentiality, integrity, and non-repudiation of messages by decreasing computational costs [3].

In year 2020, Ali et al. introduced the theory which is based on bilinear pairing to safeguard data exchange between vehicles and infrastructure, providing conditional privacy preservation and batch unsigncryption for performance upgradations [4]. Correspondingly, another study by Ali et al. presented uncertified public key infrastructure-based hybrid signcryption model that focused on the address efficiency issues by decreasing the computational overhead without increasing communication costs [5]. Ali et al. also offered an ECC-based hybrid signcryption protocol that effectively protects communications between infrastructure and automobiles, reducing the burden of both computational as well as communication overheads [6]. In 2021, Altaf and Maity introduced PLHAS, a scheme for privacy-preserving localized hybrid authentication that disperse essential management across hoc and vehicular networks. By protecting long term secret keys from side-channel assaults and reducing centralized dependencies, the plan addressed the issues of large- VANETs' high mobility and bandwidth limitations [7]. Despite of all these improvements, performance issues persist in many current methods, especially where there is a requirement for real-time authentication or significant mobility. Utilizing hybrid cryptographic models, such as elliptic curve cryptosystems, has stated that they have potential in addressing these problems. Shawky et al. created a cross-layer authentication system in year 2023 that very much lowers overheads by optimizing authentication at various level of vehicular communication. Overall, even though a number of cryptographic techniques and methods have been put forth to safeguard authentication in HetVNETs, further study is required in this area to overcome the challenges related to computational efficiency, real-time processing, and privacy preservation. Table 1 summarizes the comparison of different kinds of vehicle networks.

Table 1: Comparison of vehicular networks

Network Type	Key Features	Advantages	Limitations
Cluster-based HetVNET (C-HetVNET) [8]	Focuses on intracluster and intercluster communication using LTE and DSRC, utilizes Markov queuing models	Optimizes uplink transmission and reduces queuing delays	Limited to specific vehicle densities and data arrival rates
Software-defined HetVNET (SD-HetVNET) [9]	Integrates cellular base stations and RSUs with multicast technology for content delivery	Enhances efficiency and reduces content delivery costs through double auction game	Network stability relies heavily on RSU availability
Vehicular Ad Hoc Networks (VANETs) [10]	Uses DSRC for direct vehicle-to-vehicle communication	Provides efficient real-time data exchange in localized areas	Limited coverage and prone to fragmentation in larger networks
Reputation-based HetVNET (TrustV) [11]	Utilizes game theory to assess vehicle trustworthiness and detect malicious nodes	Effectively identifies black hole and grey hole attacks	Dependent on the accuracy of reputation systems
6G-Enabled HetVNET [12]	Uses 6G network infrastructure (satellites, drones) for edge computing and service customization	Reduces communication overhead and provides personalized services	Complex infrastructure and high implementation costs

3. HetVNETs

These are internet-based vehicular networks that are the next level in the development of vehicular communication systems and incorporate many different technologies to satisfy the requirements of the new vehicular networks.

HetVNETs are more advanced technologies integrating cellular, short-range, and other available means of communication that are instrumental in the evolution of more intelligent and autonomous future transport systems. This is made possible by the reliance on various communication protocols, such as:

- **Cellular networks:** These are the ones that provide the best connectivity over a large area for two-way communication with minimum lag. For example, 4G or 5G.
- **DSRC:** Dedicated Short-Range Communication (DSRC), designed for the purpose of vehicle-to-vehicle or vehicle-to-infrastructure communication system.
- **Wi-Fi (802.11p)**: This primarily facilitates short-range low-latency transmission, in particular for vehicle-to-vehicle (V2V) applications.
- **Millimeter-Wave (mmWave) technology**: Short range but very high bandwidth technology, particularly useful for self-driving cars.
- **Satellite Communication**: Non-obstructed communication that enables a vehicle in the remote region to connect.
- **Bluetooth and Zigbee**: Used for low power and short range communication in certain vehicular applications.

3.1 Key Features of HetVNETs

HetVNETs represent a combination of several wireless communication technologies to support effective and uninterrupted vehicular communication. These networks are very important for Intelligent Transportation Systems (ITS), as they aim satisfy the need of real-time data exchange, traffic management, and safety enhancement. Other key features of HetVNETs are the following:

- **Multi-Access technology integration:** HetVNETs merge the technologies such as Dedicated Short Range Communication (DSRC), cellular networks (3G/4G/LTE), and Wi-Fi to give effective connectivity and meet different type of vehicular communication needs. Hence, the network is able to provide optimal long-range communication and optimal short-range communication while considering the context and optimum location of service delivery.
- **Always Best Connected (ABC) paradigm:** HetVNETs make sure the vehicles are attached to the best available network by integrating the coverage from various communication channels. This model allows for continuous access to the adopted network even while traveling in and out of regions that have unrestricted and varied networks.
- **Real-time traffic management and service delivery:** HetVNETs facilitates real-time communication of data, including vehicular security related information. This is achieved through synergies between vehicles and infrastructure, where a number of technologies integrate with each other [13].
- **Support for diverse QoS requirements:** HetVNETs perform real-time vehicular services such as transmission of safety and traffic data. This elasticity permits HetVNETs to prioritize crucial communications, securing authentic data transmission under dynamic network situation [14].
- **Security and trust mechanisms:** Due to the combination of various networks, HetVNETs face significant security challenges, particularly related to trust and data integrity. The solutions such as reputational systems pose game theory help to find the vicious nodes, ensuring safeguard the data exchange around the network.
- **Adaptive network selection and handover:** In order to maintain the uninterrupted communication, HetVNETs recruit intelligent network selection algorithms. Such algorithms permit the vehicles to swap between contrary networks established on the basis of network, infrastructure and servers' performance, eliminating the performance lags in the communication process [15].

3.2 Applications of HetVNETs

HetVNETs have appeared to be new emerging novel system components in contemporary Intelligent Transportation Systems. Such integration of different wireless network technologies enables HetVNETs to

address concerns such as road safety as well as increase the efficiency of traffic management. Some of the relevant areas for HetVNETs are summarized below:

- **Traffic management and road safety:** With the help of various applications like accident detection and crowding management, HetVNETs can provide the means for vehicles to communicate with each other and also with the infrastructure with the help of a broadband network and a requiem-subscriber-tower communication. By the way of integrating LTE and DSRC networks, HetVNETs provides advanced traffic management services [16].
- **Cooperative driving and vehicle clustering:** HetVNETs enables the cooperative clustering of vehicles for traffic management and thus alleviates the pressure on the LTE networks while enhancing efficiency on the exchange of data. Non-cooperative strategic game-theoretic models will also promote collaboration among stringent users of vehicular data to increase vehicular clustering and reduce the expense of data [17].
- **Infotainment services and content delivery:** As different networks can be integrated with each other, HetVNETs are able to provide high bandwidth applications like video streaming, internet and multimedia content ensuring users are actively connected with the content and not stranded. Vehicular users are subject to the least time lags due to content caching in the form of Wi-Fi hotspots and in the long-term evolution base stations while driving [18].
- **Mobility and handoff management:** Heterogeneous wireless vehicular networks will allow one to access the internet wherever he or she is located due to transfer between different networks (Wi-Fi LTE) seamlessly. Such systems enable the vehicles, passengers, and public transport users to maintain uninterrupted communication flow even while traversing around city landscapes.
- **Edge caching for delay minimization:** Edge caching in HetVNETs saves the popular files as close to the user as possible in order to save the overhead on the network and speed up the delivery process. Such a system could be very useful for low latency applications such as traffic and navigation [19].

4. Cryptanalysis of authentication schemes in HetVNETs

In HetVNETs, security defenses to attacks such as unauthorized access are addressed by proving authentication which without a doubt has become one of the most secure methods ever used. (VANETs) or vehicular ad hoc networks provide means of information exchange between vehicle to vehicle and to any infrastructure support and control traffic and improve road safety. However, these networks are highly vulnerable to many attacks due to their nature of being open, free and wireless. The main challenges in HetVNET authentication schemes are discussed as follows:

- **Message integrity and authentication**: The general hot topic in HetVNET seems to be focused on authentication schemes where in both from and to a message is sent, its integrity, confidentiality, and non-repudiation during its transmission must be satisfied. Cryptanalysis of these schemes often reveals vulnerabilities in the protection against message interception or forgery attacks, which can undermine trust within the network.
- **Heterogeneity and compatibility**: In HetVNETs, it is frequent that Public Key Infrastructure (PKI), Identity-based Cryptography (IBC) and other cryptographic standards are implemented in different devices and networks. A problem is how to construct such schemes that function efficiently across these systems without compromising the security. For instance, hybrid signcryption schemes based on bilinear pairing are to provide secure message exchange to systems using different cryptographic primitives. Yet these schemes have systemic limitations when applying them to transitions between the systems. In this case, performing several systems computationally with the same security exposure normally limits performance blocking this alternating strategy.
- **Efficiency and scalability**: High computational overhead and delay are common concerns, especially as HetVNETs grow in scale and the number of vehicles get larger. For example, schemes that depend on

batch verification may break down under heavy load due to non-negligible errors during the verification procedure, reducing the scheme's overall reliability.

- **Dynamic topology:** Differences across HetVNETs suffer as there are constant movements of vehicles consequently changing the topology as result. This fast-changing structure of the network hampers the establishment of persistent secure communications as there are delays and disturbance Cryptanalysis of this type focuses on understanding what kinds of compromises would allow an attacker to send a message to the network or cause an interruption in the communications in a useful manner.
- **Intrusion detection and privacy**: Great quantities of verification schemes fail to care for strong privacy protections, which are crucial in shield user namelessness. Cryptanalysis of these schemes often exposes flaws that leave networks at risk to invasion attacks, such as false alert and Sybil attacks, where poisonous entities impersonate multiple vehicles. Game theory-based detection method have been suggested to forecast and prevent mis-functioning vehicles, although the efficiency of such methods is still under evaluation.

Hybrid schemes strongest matches the PKI and IBC can improve efficiency while making the certain security. These approaches are designed to advocate bunch unsigncryption, enabling faster refining of multiple messages, although they still suffer from high calculation demands. Localized hybrid authentication schemes, which distribute key management among local roadside units (RSUs) rather than central authorities, reduce latency and improve scalability. This approach also mitigates vulnerabilities from single points of failure in the network.

5. Security issues in HetVNETs

The vehicular networks security in HetVNETs is paramount due to the sensitive nature of the data exchanged between vehicles, infrastructure, and external networks. One of the most critical components of security in these networks is authentication, ensuring that only genuine entities engage in vehicular communication. Authentication protocols in HetVNETs face numerous challenges because of the heterogeneity in communication technologies (e.g., 4G/5G, Wi-Fi, DSRC) and the dynamic nature of vehicular networks. Cryptanalysis plays a crucial role in identifying vulnerabilities within these authentication schemes by evaluating how resistant they are to various cryptographic attacks summarized in Figure 2.

- **Replay attacks**: Replay attacks occur when an attacker intercepts valid data (such as an authentication message) and replays it at a later time, potentially gaining unauthorized access to the network. In HetVNETs, the vehicles and roadside units (RSUs) frequently exchange authentication messages, and without proper protection mechanisms (e.g., timestamps or nonces), these messages can be captured and replayed by attackers. For instance, in some schemes, the authentication token issued to a vehicle or RSU may be valid for a certain period. If an attacker captures the message and replays it within the valid time frame, they can impersonate the vehicle and potentially disrupt communication. Some lightweight authentication schemes designed for low-latency communication are especially vulnerable because they often minimize the use of complex cryptographic operations, leaving them more exposed to replay attacks.
- **Man-in-the-Middle (MitM) attacks**: Man-in-the-Middle attacks implies expropriating communication between two entities and altering the messages. In the context of HetVNETs, where multiple communication technologies are used, MitM attacks can occur at different layers of communication. For example, in DSRC or Wi-Fi-based communications, if authentication schemes are not robust enough, an attacker can eavesdrop on the communication channel, modify the authentication data, and then forward it, making both parties believe they are communicating securely when in fact, the attacker is controlling the exchange. MitM attacks can be particularly damaging in safety-critical applications, such as emergency braking or collision warnings. An attacker could manipulate the data in real-time, causing accidents or system failures. Some cryptographic schemes attempt to prevent MitM attacks using mutual authentication, where both the vehicle and the infrastructure verify each other's identity. However,

vulnerabilities can still arise if the cryptographic keys used for authentication are weak or if the communication channel lacks end-to-end encryption.

- **Impersonation attacks**: Impersonation attacks occur when an attacker successfully pretends to be a legitimate user or entity in the network. In HetVNETs, an attacker might impersonate a legitimate vehicle or roadside unit by forging an authentication token or manipulating identity verification mechanisms. One loophole in certain verification schemes is their assurance on static credentials or keys, which, if exposed, allow attackers to imitate sanctioned vehicles. For instance, some authentication treaty uses a pre-shared key system, where each vehicle is issued a unique key. If an attacker gets access to a vehicle's key, they can impersonate that vehicle and participate in the network, potentially dominating to the injection of malicious data. Cryptanalysis of these systems often unmasks that without frequent key updates, session-specific keys, or dynamic credential management, impersonation attacks are a real threat in HetVNETs.
- **Sybil attacks**: Sybil attacks include creation of numerous fake identities to undermining the control on the network, inundating the legitimate communication and potentially gaining majority of influence on network integrity. In the context of Het VNETs, Sybil attacks can have drastic upshots, as vehicles rely on realistic data from nearby junction for decision-making. For instance, a malicious vehicle could generate numerous fake nodes to create false clog alerts or disrupt traffic flow. Authentication schemes in Het VNETs must embody mechanisms to detect and avoid Sybil attacks. However, many schemes that depend on static identities or simple key-based authentication grapple to differentiate between legitimate and false nodes. Cryptanalysis uncovers that without proper identity authentic mechanisms, such as digital certificates issued by an assured authority or group-based authentication schemes, Sybil attacks can easily manipulate these exposures.
- **Denial-of-Service (DoS) attacks**: Denial-of-Service attacks results into the network impractical for authorized users. In Het VNETs, attackers can aim authentication schemes by flooding authentication servers with illegitimate requests, thus preventing valid users (vehicles and RSUs) from validating and participating in network communication. Lightweight authentication schemes, which aim to deteriorate computational complexity, are often more vulnerable to DoS attacks due to their limited volumes for handling large ratios of requests. One common cryptographic loophole that can be exploited in DoS attacks is deprivation of rate-limiting or request validation mechanisms. If an attacker can pass around these mechanisms, they can swamp the network with frequent authentication requests, effectively draining the network's resources. Robust cryptographic solutions must include mechanisms to discover and prevent these types of attacks, for instance CAPTCHA-like challenges or proof-of-work systems that scare off illegitimate requests [20].
- **False data injection:** This attack occurs when an attacker shots false information into the network, resulting to inaccurate traffic management measures, road safety cautions, or manipulation of vehicular sensor networks. Cryptanalysis aims to ensure the integrity of messages through rigorous authentication protocols, but some schemes may fail to properly validate the source and content of messages, opening up possibilities for such attacks [21]
- **Eavesdropping:** Due to the receptivity of wireless network connections, HetVNETs are vulnerable to eavesdropping, where attackers intercept and listen to vehicle-to-vehicle or vehicle-to-infrastructure communication. This can lead to the compromise of sensitive information such as location and personal data. To counter this, physical layer security mechanisms are implemented to secure the communication links [22].
- **Key management vulnerabilities**: The management and distribution of cryptographic keys are critical in securing authentication schemes. In HetVNETs, where vehicles move between different network environments, key management becomes particularly challenging. Cryptanalysis often reveals vulnerabilities in how keys are generated, distributed, and updated. For example, if a central authority issues keys and an attacker compromises this authority, the entire network's security can be jeopardized. Additionally, if vehicles are required to update their keys frequently, there must be a secure and efficient mechanism in place to ensure that the key update process is not vulnerable to attacks. One of the

vulnerabilities identified in certain authentication schemes is the reliance on static keys, which remain the same for extended periods. If these keys are not updated regularly, the risk of key compromise increases. Additionally, key exchange protocols that are not resistant to attacks, can expose the systems and network to many vulnerabilities.

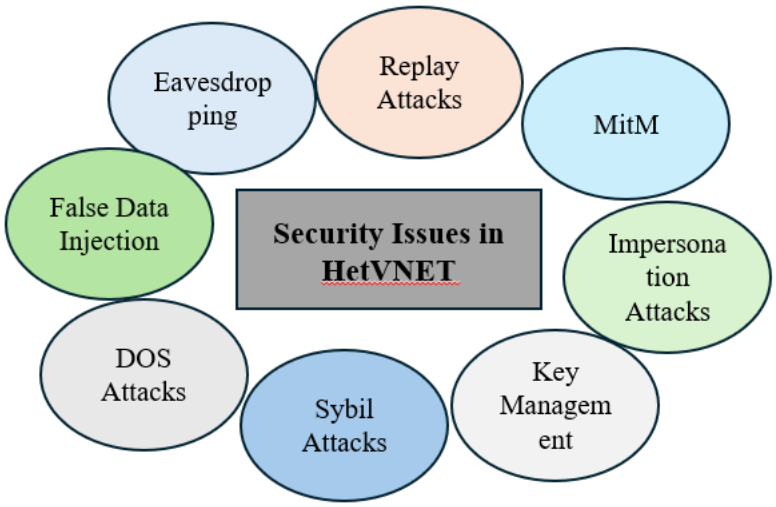

Figure 2: Security Issues in HetVNETs

6. **Critical improvement domains in HetVNETs**

Cryptanalysis plays a crucial role in improving the security of authentication schemes in HetVNETs. By identifying vulnerabilities in cryptographic methods, message validation, and system scalability, researchers can develop more robust solutions to protect vehicular networks from various types of attacks. Going forward, detection, hybrid cryptosystems, localized authentication methods, and game theory-based intrusion detection will be the main areas of focus for improving the security of HetVNETs.

- **Hybrid cryptosystems:** To solve the security issues with HetVNETs, hybrid cryptosystems which incorporate several cryptographic techniques like PKI and IBC, have been suggested. For instance, hybrid signcryption techniques based on bilinear pairing offer a consistent method for protecting communications between several platforms. These solutions are made to guarantee data security, confidentiality, and integrity all at once. Such systems could be improved in a number of ways, most notably in lowering the computing burden related to batch processing, as shown by cryptanalysis.
- **Localized authentication schemes:** Researchers have suggested localized authentication techniques that divide the key management responsibility across several semi-trusted roadside units (RSUs) in order to increase scalability and decrease delay. This lowers the possibility of single points of failure and lessens reliance on a single, reliable authority. Potential flaws in these systems communication with cars is revealed by cryptanalysis, but localized key management is still a viable way to address the scaling problems.
- **Batch verification techniques:** Batch verification is used in several contemporary techniques to authenticate numerous messages at once. Although the goal is to increase efficiency, cryptanalysis has revealed that these methods are prone to mistakes when handling incorrect signatures. In order to increase batch verification accuracy without raising computational costs, new methods are being developed.
- **Game theory-based intrusion detection:** Some intrusion detection systems employ game theory to forecast how possibly harmful cars would behave in the future. Researchers can detect and stop assaults before they happen by simulating the network as a strategic game. The goal of cryptanalysis of these systems is to decrease false positives and increase prediction accuracy.

7. Conclusion and future directions

For intelligent and autonomous transportation systems to be deployed successfully, authentication mechanisms in HetVNETs must be secure. We have discovered a number of weaknesses in current authentication systems through our cryptanalysis, especially in relation to replay, man-in-the-middle, and impersonation attacks. In addition to providing better functionality and coverage, the various communication protocols used in HetVNETs also create new attack surfaces that are frequently not fully addressed by existing approaches.

The security of HetVNETs can be improved in a number of ways based on the cryptanalysis of their authentication systems. To reduce the impact of key compromise, authentication protocols should first use dynamic key management, which involves regular key updates or session-based keys. Second, to defend against replay and man-in-the-middle attacks, mutual authentication and end-to- end encryption should be combined. Furthermore, to counter impersonation and Sybil attacks, sophisticated identity verification techniques like certificate-based authentication must be employed. Lastly, to protect against denial-of-service attacks and make sure the network is resilient even when there are a lot of requests strong rate-limiting techniques need to be put in place.

Our results highlight the need for more reliable, scalable, and contextual authentication algorithms designed to precisely address the special difficulties presented by HetVNETs. In order to secure real-time vehicular applications, future authentication frameworks must incorporate sophisticated cryptographic approaches that can withstand a diverse range of possible threats in heterogeneous situations. Additionally, these techniques must preserve efficiency and low latency. HetVNETs have the potential to serve as a safe basis for the upcoming autonomous driving and vehicular communication technologies by tackling these issues.

References

[1]: Liu, J.K., Yuen, T.H., Au, M.H., & Susilo, W. (2014). Improvements on an authentication scheme for vehicular sensor networks. Expert Syst. Appl., 41, 2559-2564. https://api.semanticscholar.org/CorpusID:28608695

[2]: Sedjelmaci, H., Senouci, S., & Bouali, T. (2017). Predict and prevent from misbehaving intruders in heterogeneous vehicular networks. Veh. Commun., 10, 74-83. https://api.semanticscholar.org/CorpusID:40439239.

[3]: Zhou, Li, & Ding (2019). Practical V2I Secure Communication Schemes for Heterogeneous VANETs. Applied Sciences, https://api.semanticscholar.org/CorpusID:201238758.

[4]: Ali, I., Lawrence, T., Omala, A.A., & Li, F. (2020). An Efficient Hybrid Signcryption Scheme With Conditional Privacy-Preservation for Heterogeneous Vehicular Communication in VANETs. IEEE Transactions on Vehicular Technology, 69, 11266-11280. https://api.semanticscholar.org/CorpusID:226229803.

[5]: Ali, I., Chen, Y., Ullah, N., Afzal, M., & He, W. (2021). Bilinear Pairing-Based Hybrid Signcryption for Secure Heterogeneous Vehicular Communications. IEEE Transactions on Vehicular Technology, 70, 5974-5989. https://doi.org/10.1109/TVT.2021.3078806.

[6]: Ali, I., Chen, Y., Pan, C., & Zhou, A. (2021). ECCHSC: Computationally and Bandwidth Efficient ECC-Based Hybrid Signcryption Protocol for Secure Heterogeneous Vehicle-to-Infrastructure Communications. IEEE Internet of Things Journal, 9, 4435-4450. https://doi.org/10.1109/jiot.2021.3104010.

[7]: Altaf, F., & Maity, S. (2021). PLHAS: Privacy-preserving localized hybrid authentication scheme for large scale vehicular ad hoc networks. Veh. Commun., 30, 100347. https://api.semanticscholar.org/CorpusID:233847930.

[8]: Zheng, Q., Zheng, K., Sun, L., & Leung, V. (2015). Dynamic Performance Analysis of Uplink Transmission in Cluster-Based Heterogeneous Vehicular Networks. IEEE Transactions on Vehicular Technology, 64, 5584-5595. https://doi.org/10.1109/TVT.2015.2487682.

[9]: Hui, Y., Su, Z., & Luan, T. (2020). Collaborative Content Delivery in Software-Defined Heterogeneous Vehicular Networks. IEEE/ACM Transactions on Networking, 28, 575-587. https://doi.org/10.1109/TNET.2020.2968746.

[10]: Zheng, K., Zheng, Q., Chatzimisios, P., Xiang, W., & Zhou, Y. (2015). Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges, and Solutions. IEEE Communications Surveys & Tutorials, 17, 2377-2396. https://doi.org/10.1109/COMST.2015.2440103.

[11]: Quevedo, A., Quevedo, C., Gomes, R., Câmara, S., & Celestino, J. (2022). A Reputation and Security Mechanism for Heterogeneous Vehicular Networks. 2022 IEEE Symposium on Computers and Communications (ISCC), 1-6. https://doi.org/10.1109/ISCC55528.2022.9912844.

[12]: Hui, Y., Cheng, N., Su, Z., Huang, Y., Zhao, P., Luan, T., & Li, C. (2021). Secure and Personalized Edge Computing Services in 6G Heterogeneous Vehicular Networks. IEEE Internet of Things Journal, 9, 5920-5931. https://doi.org/10.1109/JIOT.2021.3065970.

[13]: Zheng, K., Zhang, L., Xiang, W., & Wang, W. (2016). Heterogeneous Vehicular Networks. https://doi.org/10.1007/978-3-319-25622-1.

[14]: El-Sayed, H., Sankar, S., Daraghmi, Y., Tiwari, P., Rattagan, E., Mohanty, M., Puthal, D., & Prasad, M. (2018). Accurate Traffic Flow Prediction in Heterogeneous Vehicular Networks in an Intelligent Transport System Using a Supervised Non-Parametric Classifier. Sensors (Basel, Switzerland), 18. https://doi.org/10.3390/s18061696.

[15]: Zhao, X., Li, X., Xu, Z., & Chen, T. (2019). An Optimal Game Approach for Heterogeneous Vehicular Network Selection with Varying Network Performance. IEEE Intelligent Transportation Systems Magazine, 11, 80-92. https://doi.org/10.1109/MITS.2019.2919563.

[16]: Silva, C., & Jr, W. (2015). Evaluating the Performance of Heterogeneous Vehicular Networks. 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), 1-5. https://doi.org/10.1109/VTCFall.2015.7390936.

[17]: Ahmad, I., Noor, R., Z'aba, M., Qureshi, M., Imran, M., & Shoaib, M. (2020). A Cooperative Heterogeneous Vehicular Clustering Mechanism for Road Traffic Management. International Journal of Parallel Programming, 1-20. https://doi.org/10.1007/s10766-019-00629-y.

[18]: Wu, H., Xu, W., Chen, J., Wang, L., & Shen, X. (2018). Matching-Based Content Caching in Heterogeneous Vehicular Networks. 2018 IEEE Global Communications Conference (GLOBECOM), 1-6. https://doi.org/10.1109/GLOCOM.2018.8647134.

[19]: Wu, H., Chen, J., Xu, W., Cheng, N., Shi, W., Wang, L., & Shen, X. (2020). Delay-Minimized Edge Caching in Heterogeneous Vehicular Networks: A Matching-Based Approach. IEEE Transactions on Wireless Communications, 19, 6409-6424. https://doi.org/10.1109/TWC.2020.3003339.

[20]: Alpcan, T., & Buchegger, S. (2011). Security Games for Vehicular Networks. IEEE Transactions on Mobile Computing, 10, 280-290. https://doi.org/10.1109/TMC.2010.146.

[21]: Shawky, M.A., Bottarelli, M., Epiphaniou, G., & Karadimas, P. (2023). An Efficient Cross-Layer Authentication Scheme for Secure Communication in Vehicular Ad-Hoc Networks. IEEE Transactions on Vehicular Technology, 72, 8738-8754. https://api.semanticscholar.org/CorpusID:258157671.

[22]: Wang, L., & Liu, X. (2018). Secure cooperative communication scheme for vehicular heterogeneous networks. Veh. Commun., 11, 46-56. https://doi.org/10.1016/j.vehcom.2018.01.001.