M.J. Hornos et al. (Eds.)

doi:10.3233/AISE240008

Cyber Resilience in Autonomous Vehicles: Defending Against Emerging Threats

Karel VEERABUDREN and Visham RAMSURRUN
Middlesex University Mauritius
ORCiD ID: Karel Veerabudren https://orcid.org/0009-0009-6432-6062

Abstract. Autonomous vehicles (AVs) represent a transformative shift in transportation, promising faster transit, enhanced safety, and reduced accidents. Leveraging the Vehicular Ad-Hoc Network (VANET) for communication among vehicles and roadside units, AVs exchange critical information to optimize driving conditions. However, the constant communication necessitates robust security measures to safeguard both the network and the vehicles themselves. This paper delves into the various cyber threats facing AVs and proposes countermeasures to mitigate them. A comparative analysis identifies prevalent attacks such as Denial of Service (DoS), Sybil, Spoofing, Replay, and Blackhole attacks as the most prominent in AV environments. Subsequently, protocols aimed at thwarting these common attacks are examined. However, it is noted that these protocols may fall short in cases where physical tampering compromises the vehicle's systems. To address this vulnerability, a novel countermeasure involving cryptographic key management for system access control is proposed and discussed. Additionally, the reliability of each countermeasure is evaluated to ensure robust protection against evolving threats.

Keywords. autonomous vehicles, VANET, security, attacks, countermeasures, autonomy levels, analysis, reliability, CIA

1. Introduction

Autonomous vehicles (AVs) boast a rich history, tracing back to the groundbreaking work of German computer scientist Ernst Dickmanns and his team in the 1980s, culminating in developing a van capable of autonomous highway driving [1]. Since then, advancements in AV technology have been fueled by the promise of enhancing road safety, efficiency, and sustainability [2]. Studies underscore human error as a primary contributor to accidents, citing factors such as speeding, distractions, and impaired driving [3]. AVs hold the potential to mitigate accidents and fatalities by eliminating human-related driving behaviours while also enhancing fuel efficiency and alleviating traffic congestion through optimized driving and improved coordination [4]. However, concerns about cybersecurity vulnerabilities have emerged as AVs increasingly rely on software. While strides are being made to address these risks through evolving security standards [5], challenges persist in ensuring robust cybersecurity practices across the automotive industry.

This paper aims to delve into the mechanics of AVs, scrutinize security risks and objectives, and propose defences against potential cyber threats. The research goals are to examine the security challenges autonomous vehicles face comprehensively and eview various countermeasures and protocols developed to detect and prevent these attacks in VANETs. Subsequent sections will provide an overview of standard AV terminology,

review relevant research, analyze attack scenarios, conduct a comparative analysis, and discuss defense strategies. Through this comprehensive examination, we seek to contribute meaningfully to the ongoing discourse surrounding the reliability and security of autonomous vehicle systems.

2. Background

2.1. Autonomy levels

The Society of Automotive Engineers (SAE) International has delineated six levels of driving automation systems, ranging from level 0 to level 5 [6]. These levels are summarized in Table 1, illustrating that as autonomy increases, so does the vehicle's ability to operate independently. This advancement is facilitated by various technologies within the vehicle, enabling seamless wireless interaction with the surrounding environment. These interconnected devices form what is known as vehicular ad hoc networks (VANETs). With each escalation in autonomy level, there is a corresponding increase in reliance on connected technologies. Consequently, the security surrounding the exchange of data among computer systems becomes increasingly critical as vehicles become more autonomous.

2.2. Vehicular Ad Hoc Networks (VANETs)

A study [7] defines VANET as a wireless network that interconnects a group of moving or stationary vehicles with other devices in their vicinity. Vehicles are equipped with an onboard unit (OBU) to facilitate communication, enabling seamless integration into the VANET network. Acting as nodes, vehicles and devices exchange information to enhance safety and optimize traffic flow. Despite its open nature, allowing nodes to join and leave at will [8], VANETs are susceptible to security issues that can impact the exchange of data among vehicles and devices. VANET communication primarily comprises three types: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-infrastructure (I2I).Vehicle-to-Vehicle (V2V) Communication: V2V communication involves data exchange among different vehicles, enabling the sharing of crucial information like speed and location [9]. This allows vehicles to detect potential risks and threats posed by other vehicles and respond accordingly. Employing a mesh topology, each vehicle is directly connected to others in the network, ensuring resilience even if a node fails. Given the critical nature of communication in AVs, maintaining uninterrupted service is paramount to avoid potential disasters.

2.2.1. Vehicle-to-infrastructure (V2I): V2I communication facilitates interaction between vehicles and surrounding infrastructure, including traffic lights, signage, and cameras [10]. This communication enables adaptive traffic control, such as adjusting speed limits to prevent accidents based on weather conditions and sending warning messages to vehicles to adjust their speed based on traffic conditions [11]. Additionally, connected infrastructure units can serve as intermediaries to facilitate long-range communication between vehicles that are too far apart [12].

2.2.2. Infrastructure-to-Infrastructure (I2I): I2I communication involves interactions between roadside units connected to the internet, which gather and share data on current traffic conditions [12]. When a vehicle approaches a roadside unit, it sends a signal requesting information, which the unit authenticates using a digital signature algorithm and generates a unique key. Information is exchanged as the vehicle moves within range of other roadside units to maintain continuous service.

2.3. Controller Area Network

In modern vehicles, electronic control units (ECUs), equipped with microprocessors, facilitate communication throughout the vehicle and are enabled by the Controller Area Network (CAN) protocol. CAN ensures reliable data transfer at speeds of up to 1 Mb/s [13, 14]. Described as a "multi-master message broadcast system," CAN allows any connected ECU to broadcast messages to all nodes on the network when the bus is idle [15]. CAN messages include Data frames, Remote frames for requesting data, Error frames to address data frame errors, and Overload frames to request additional delays [16, 17]. While these messages primarily operate internally within the vehicle, safeguarding them is essential. Messages from the On-Board Unit (OBU) are processed, and the vehicle's in-built computer compares values with those from the CAN bus. Without protection, malicious messages received by the OBU could traverse the CAN bus, potentially causing the vehicle to malfunction.

3. Related Works

Several types of research have been conducted on the different security issues in AVs. However, little work has been done to determine the most common attacks in AVs. A previous study [18] discussed the different communication layers in AVs. Moreover, a taxonomy of the security threats was performed. Nevertheless, little analysis was carried out to determine the common attacks. Countermeasures and defence techniques were not discussed. In another research [19], different attacks were summarised, and proposed countermeasures for navigation was given. The research ended with a new spoofing attack against GPS navigation. However, the defence techniques were little discussed. In a different paper [20], security issues about VANET were reviewed and discussed. The security requirements were also analyzed. However, little research has focused on identifying common attacks. The previous research [21] reviewed different challenges VANET network faced. The issues regarding authentication, availability, privacy, integrity, and non-repudiation were discussed. The authors described the types of attackers and made a taxonomy of them before going into the different attacks. Nonetheless, the paper did not touch on the defence mechanism in the VANET network or the vehicle's system.

4. Methodology

In pursuit of the study's objectives, a meticulous methodology was employed to select and analyze pertinent research papers. The process commenced with a comprehensive search across leading databases, including IEEE Xplore Digital Library, ACM Digital Library, Google Scholar, and ScienceDirect. Focused on recent advancements, the search was confined to publications spanning from 2017 to 2022, ensuring the inclusion of up-to-date insights into AV threats.

Strategic keyword combinations such as "AV attacks," "AV vulnerabilities," "VANET attacks," and "AV network defence" were employed to retrieve relevant papers. Subsequently, a rigorous filtering process was implemented to ascertain each paper's alignment with the study's focus on AV security. Only papers directly addressing AV threats and defence mechanisms were considered for further analysis.

Following the selection process, the content of the chosen papers underwent meticulous scrutiny. Each paper was thoroughly examined to identify prevalent threats and corresponding countermeasures. Notably, threats discussed in more than 50% of the reviewed papers were prioritized for in-depth analysis. Additionally, proposed defence mechanisms were scrutinized to assess their efficacy in mitigating identified threats. Finally, based on the findings, a tentative approach to address physical tampering vulnerabilities was proposed, aiming to bolster the overall security posture of autonomous vehicle systems.

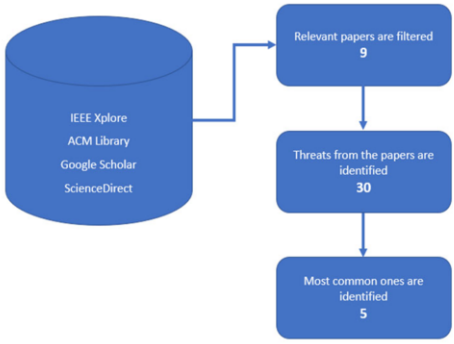

Figure 1. Research Methodology to identify the most common threats

5. Comparative Analysis of AVs attacks

In this section, nine research papers discussing the different attacks are analyzed. The papers are Nanda et al. [18], Kaur et al. [20], Junaid et al. [21] Cui et al. [22], Upadhyaya and Shah [23], Chowdhury et al. [24], Ghori et al. [25], Sirola et al. [26] and Samara [27]. In total, 30 unique attacks were reviewed in these studies.

The attacks from each paper were written down. Then, the number of times those attacks appeared in the different papers were noted. The attacks with more than 60% of occurrence are considered the most common in AVs. Table 2 shows the list of all attacks and their occurrences.

From Table 2, it can be seen that five attacks are discussed in most of the papers reviewed. Two of them have been in all the papers: DoS and Sybil attack. The other three attacks are GNSS Spoofing, replay and blackhole, which appeared in six papers out of the nine reviewed. Thus, the most common attacks in AVs are DoS, Sybil, GNSS spoofing, replay and blackhole.

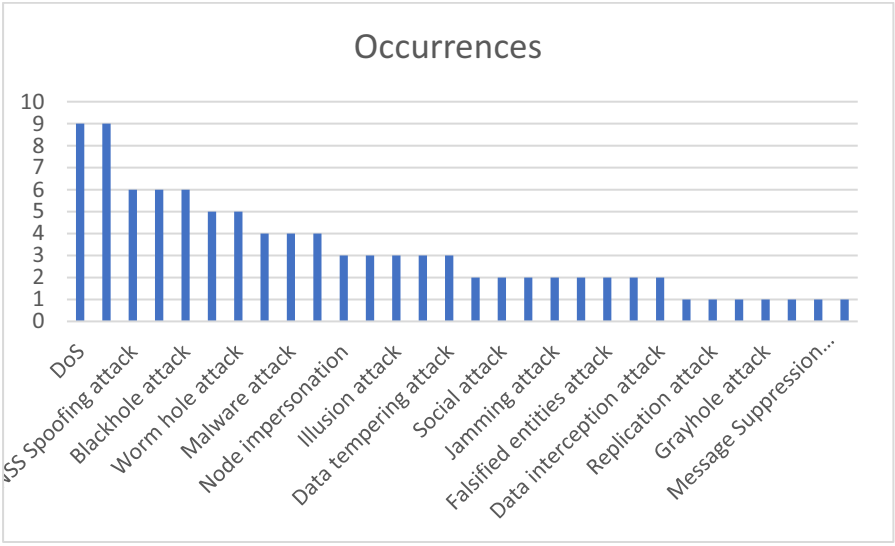

Figure 2. Occurrences of attacks from the different papers

Table 1. Taxonomy of Avs Attack

Attack	Type	CIA Triad	Description
Denial of Service	Network Disruption	Availability	Rendering the network unavailable to users by overwhelming it with excessive messages.
Sybil Attack	Identity Spoofing	Confidentiality	Creating false identities deceives the network into believing there are multiple vehicles.
GNSS Spoofing	Location Spoofing	Integrity	Falsifying the location of a vehicle in the GNSS network leads to incorrect localization.
Replay Attack	Message Manipulation	Integrity	Resending previously transmitted information to exploit timing vulnerabilities.
Blackhole Attack	Routing Manipulation	Availability	Deceiving users into sending packets through a malicious node, which drops the packets.

In November 2019, an incident unfolded concerning white hat hackers targeting Tesla S vehicles manufactured before 2018 [28]. Exploiting vulnerabilities via the Wi-Fi attack vector, these hackers raised significant concerns regarding the cybersecurity of connected vehicles. Specifically, the vulnerability, identified as CVE-2019-13582, was found within Tesla's Model X Wi-Fi connectivity modules.

CVE-2019-13582 constitutes a critical flaw characterized by a heap-based buffer overflow. This vulnerability enables attackers to manipulate Wi-Fi packets, potentially triggering a denial of service or facilitating the execution of arbitrary code within the affected vehicle's systems.

This case underscores the paramount importance of robust cybersecurity countermeasures within the automotive industry, particularly concerning connected vehicles. Without adequate defences, vehicles become vulnerable to exploitation by malicious actors, potentially resulting in severe consequences such as loss of control, compromise of sensitive data, or physical harm to occupants. Thus, proactive measures such as comprehensive vulnerability testing, routine software updates, and robust intrusion detection systems are imperative to safeguarding the integrity and security of connected vehicles against evolving cyber threats. Additionally, collaboration among automakers, cybersecurity experts, and regulatory bodies is essential to establish and enforce stringent security standards that mitigate the risk of similar vulnerabilities in the future.

6. Defence Mechanism

As seen previously, AVs are subject to attacks compromising confidentiality, integrity, availability, and authentication. This section reviews and discusses countermeasures for the attacks elaborated above in research papers.

6.1. Authenticated Routing for Ad-hoc Network (ARAN)

ARAN is a secure routing protocol that can be used in an open network like VANET. Cryptographic certificates are used to ensure authentication and non-repudiation. As a study [29] said, each node in the network is given a signed certificate by a third-party certificate authority. This signed certificate is then appended in packets sent by the node when requesting a route for a destination [30]. The certificate in the packet acts as a signature of the node [31]. ARAN ensures the authenticity of routing requests and responses by issuing signed certificates to each node from a trusted third-party certificate authority. This authentication mechanism mitigates the risk of attacks such as replay attacks, eavesdropping, and node impersonation, thus enhancing the reliability of route establishment and data transmission within the network.

6.2. Secure and Efficient Ad hoc Distance (SEAD)

SEAD is a protocol that was designed to be effective and simple. As a previous study [32] explained, SEAD can provide a low delay in the packet transfer in a dense environment. Furthermore, it also reduces the broadcast storm problem since each packet contains a unique ID consisting of the ID of the vehicle and the packet itself. Each time a message is received, the vehicle compares it with the received message buffer to see whether the same message was previously received and stored. If it was, then the

message is disregarded. The paper [32] explained further that only messages received from the vehicle in front are processed and analyzed, whereas messages from vehicles behind are only acknowledged. By efficiently managing packet transmission and reception, SEAD enhances the reliability of data delivery.

6.3. ARIADNE

ARIADNE is a routing protocol developed by Chun Hu et al. [33] which uses symmetric cryptography and message authentication code for authentication. The sender and the receiver choose two keys. One key is from sender to receiver and the second is from receiver to sender. The communicating node then sends its message, which includes a nonce like a timestamp, along the calculated message authentication code (MAC), encrypted by the sender's key. On the receiving side, the receiver can be sure the message is indeed sent from the sender because the message contains the MAC and a digital signature that confirms authenticity and non-repudiation. This robust authentication mechanism bolsters the reliability of route establishment and data exchange.

6.4. Non-Disclosure Method (NDM)

NDM protocol uses asymmetric encryption and a third-party agent to safeguard exchanged information. Communication between sender and receiver is passed through the third-party agent. Messages sent by the sender are encrypted using the agent's public key and sent to the agent. The agent knows all the addresses of the connected nodes in the network. Then, it encapsulates the message sent by the sender and sends it to the destination, encrypted with the receiver's public key. Using a third-party agent increases the security in terms of confidentiality, given that the agent is genuine [34]. This approach enhances the reliability of data confidentiality by mitigating the risk of unauthorized access and information disclosure, thereby bolstering trust and confidence in VANET communications.

7. Security Analysis

Table 2. Analysis of Defence Mechanism

Defense Mechanism	Strengths	Weaknesses	Attack Prevented
ARAN	• Robust authentication using cryptographic certificates • Minimizes risk of node impersonation and data tampering • Effective against Sybil attacks and replay attacks	• Limited effectiveness against sophisticated DoS attacks and GNSS spoofing • Primarily focuses on message authentication rather than traffic filtering or anomaly detection	Replay attack, Eavesdropping, node impersonation
SEAD	• Efficient packet structure and	• May lack adequate protection against GNSS spoofing and	DoS, Routing attack, node impersonation

	message buffering mechanism • Reduces impact of DoS attacks and blackhole attacks by minimizing network congestion	sophisticated replay attacks • Primarily focuses on optimizing packet delivery rather than cryptographic security	
ARIADNE	• Uses symmetric cryptography and MAC for message authenticity and integrity • Resilient against replay attacks and blackhole attacks	• May struggle to detect and mitigate DoS attacks and Sybil attacks effectively • Security mechanisms primarily focus on message authentication rather than traffic analysis or anomaly detection	DoS, Replay attack and node impersonation
NDM	• Enhances data confidentiality and integrity through asymmetric encryption and third-party agent-based approach • Effective against GNSS spoofing and certain DoS attacks	• May face challenges in addressing Sybil attacks and sophisticated replay attacks • Relies on secure message relay rather than extensive network verification or anomaly detection	Eavesdropping, Man-in-the-Middle, Identity Spoofing

Combining defence mechanisms such as ARAN and ARIADNE can significantly enhance the reliability and effectiveness of mitigating various attacks in VANETs. For instance, the combination of ARAN and ARIADNE can offer robust authentication and message integrity, complementing SEAD's efficient packet delivery mechanism to combat DoS attacks. Furthermore, integrating NDM's data confidentiality measures can further bolster security against GNSS spoofing and information disclosure threats. However, it's essential to acknowledge that no single solution can provide comprehensive protection against all attack vectors. This underscores the importance of adopting a layered defense strategy and continually researching to address evolving threats in VANET environments.

Moreover, ensuring the physical protection of the system is equally vital as securing the network. Unauthorized access to an AV's system compromises the integrity of messages exchanged and jeopardizes the confidentiality of information. It is imperative to implement measures to safeguard the system's physical components to mitigate this risk. However, it's crucial to strike the right balance between preventing access entirely, hindering maintenance, and leaving the system vulnerable to attacks.

One way to enhance physical security is to use asymmetric encryption to control vehicle ECU access. This enables engineers to inspect the system for potential vulnerabilities while thwarting unauthorized access. By employing cryptographic keys for system entry, attackers face significant obstacles in breaching the system. Additionally, implementing separate sets of cryptographic keys for read and write access ensures an added layer of security. With this approach, attackers would require distinct

sets of keys to access and modify the system, making unauthorized access exceedingly challenging.

8. Conclusion

In conclusion, this paper has thoroughly examined the security challenges confronting autonomous vehicles, with a particular emphasis on attacks such as Denial of Service (DoS), Sybil, Spoofing, Replay, and Blackhole attacks within the VANET network. Through a comparative analysis, these attacks have been identified as prevalent in existing research literature, highlighting their substantial impact on the confidentiality, integrity, and availability goals of the CIA triad. Additionally, we have reviewed various countermeasures and protocols designed to detect and mitigate these attacks in VANETs.

It is essential to acknowledge that while these protocols are effective in safeguarding vehicle networks, their efficacy relies heavily on the physical integrity of the vehicle itself. Recognizing this limitation, our security analysis has explored potential measures to enhance the physical protection of computer systems within autonomous vehicles. By integrating network-level and physical security measures, we aim to enhance the overall resilience of autonomous vehicle systems against evolving cyber threats. Ultimately, these efforts are directed towards ensuring the safety and security of passengers and pedestrians, thereby bolstering the reliability of autonomous vehicle technology.

References

[1] M. Weber, “Where to? A History of Autonomous Vehicles - CHM,” CHM, May 08, 2014. https://computerhistory.org/blog/where-to-a-history-of-autonomous-vehicles/.

[2] J. S. Brar and B. Caulfield, “Impact of autonomous vehicles on pedestrians’ safety,” 2017 IEEE 20th International Conference on Intelligent Transportation Systems (ITSC), Oct. 2017, doi: 10.1109/itsc.2017.8317963.

[3] Matthew Lynberg, “Automated Vehicles for Safety,” NHTSA, Nov. 28, 2018. https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety.

[4] J. M. Anderson, N. Kalra, K. D. Stanley, P. Sorensen, O. A. Oluwatola, and Rand Corporation, Autonomous vehicle technology : a guide for policymakers. Santa Monica, Calif.: Rand Corporation, 2016.

[5] “Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices An independent study commissioned by.” [Online]. Available: https://www.sae.org/binaries/content/assets/cm/content/topics/cybersecurity/securing_the_modern_vehicle.pdf.

[6] Society Of Automotive Engineers, Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems. Warrendale, Pa: Sae International, 2014.

[7] “VANETs,” encyclopedia.pub. https://encyclopedia.pub/9694 (accessed Feb. 18, 2022).

[8] Sandeep N. Kugali, "Vehicular ADHOC Network (VANET):-A Brief Knowledge," International Journal of Engineering Research and, vol. V9, no. 06, Jun. 2020, doi: 10.17577/ijertv9is060784.

[9] F. Arena and G. Pau, “An Overview of Vehicular Communications,” Future Internet, vol. 11, no. 2, p. 27, Jan. 2019, doi: 10.3390/fi11020027.

[10] R. K. Jurgen, V2V/V2I communications for improved road safety and efficiency. Warrendale, Pa.: Sae International, 2012.

[11] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETS): status, results, and challenges,” Telecommunication Systems, vol. 50, no. 4, pp. 217–241, Dec. 2010, doi: 10.1007/s11235-010-9400-5.

[12] T. K, S. T M, B. M, and A. K H, “A Survey on Vanet Technologies,” International Journal of Computer Applications, vol. 121, no. 18, pp. 1–9, Jul. 2015, doi: 10.5120/21637-4965.

[13] R. Toulson and T. Wilmshurst, Fast and Effective Embedded Systems Design. Elsevier, 2012.
[14] K. M. Zuberi and K. G. Shin, “Design and implementation of efficient message scheduling for controller area network,” IEEE Transactions on Computers, vol. 49, no. 2, pp. 182–188, 2000, doi: 10.1109/12.833115.
[15] S. Corrigan, “Introduction to the Controller Area Network (CAN) Application Report Introduction to the Controller Area Network (CAN),” 2002. [Online]. Available: https://www.ti.com/lit/an/sloa101b/sloa101b.pdf.
[16] J. Cook and J. Freudenberg, “Controller Area Network (CAN) EECS 461, Fall 2008 *,” 2008. [Online]. Available: https://www.eecs.umich.edu/courses/eecs461/doc/CAN_notes.pdf.
[17] H. Chen and J. Tian, “Research on the Controller Area Network,” 2009 International Conference on Networking and Digital Society, May 2009, doi: 10.1109/icnds.2009.142.
[18] A. Nanda, D. Puthal, J. J. P. C. Rodrigues, and S. A. Kozlov, “Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions,” IEEE Wireless Communications, vol. 26, no. 4, pp. 60–65, Aug. 2019, doi: 10.1109/mwc.2019.1800503.
[19] Q. Luo, Y. Cao, J. Liu, and A. Benslimane, “Localization and Navigation in Autonomous Driving: Threats and Countermeasures,” IEEE Wireless Communications, vol. 26, no. 4, pp. 38–45, Aug. 2019, doi: 10.1109/mwc.2019.1800533.
[20] R. Kaur, T. P. Singh, and V. Khajuria, "Security Issues in Vehicular Ad-Hoc Network(VANET)," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), May 2018, doi: 10.1109/icoei.2018.8553852
[21] M. A. Hezam Al Junaid, A. A. Syed, M. N. Mohd Warip, K. N. Fazira Ku Azir, and N. H. Romli, "Classification of Security Attacks in VANET: A Review of Requirements and Perspectives," MATEC Web of Conferences, vol. 150, p. 06038, 2018, doi: 10.1051/matecconf/201815006038.
[22] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, “A review on safety failures, security attacks, and available countermeasures for autonomous vehicles,” Ad Hoc Networks, vol. 90, p. 101823, Jul. 2019, doi: 10.1016/j.adhoc.2018.12.006
[23] A. N. Upadhyaya and J. S. Shah, “Attacks on VANET Security,” International Journal of Computer Engineering & Technology, vol. 9, no. 1, pp. 8–19, 2018.
[24] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, “Attacks on Self-Driving Cars and Their Countermeasures: A Survey,” IEEE Access, vol. 8, pp. 207308–207342, 2020, doi: 10.1109/ACCESS.2020.3037705.
[25] M. R. Ghori, K. Z. Zamli, N. Quosthoni, M. Hisyam, and M. Montaser, “Vehicular ad-hoc network (VANET): Review,” 2018 IEEE International Conference on Innovative Research and Development (ICIRD), May 2018, doi: 10.1109/icird.2018.8376311.
[26] P. Sirola, A. Joshi, and K. C. Purohit, “An AnalyticalStudy of Routing Attacks in Vehicular Ad-hoc Networks (VANETs),” International Journal of Computer Science Engineering (IJCSE), vol. 3, no. 4, pp. 210–218, 2014.
[27] G. Samara, W. A. H. Al-Salihy, and R. Sures, “Security Analysis of Vehicular Ad Hoc Nerworks (VANET),” IEEE Xplore, Sep. 01, 2010. https://ieeexplore.ieee.org/abstract/document/5635665 (accessed Mar. 09, 2021).
[28] Tencent Keen Security Lab (2020). Exploiting Wi-Fi Stack on Tesla Model S. [online] Keen Security Lab Blog. Available at: https://keenlab.tencent.com/en/2020/01/02/exploiting-wifi-stack-on-tesla-model-s/.
[29] R. Mishra, A. Singh, and R. Kumar, “VANET security: Issues, challenges and solutions,” IEEE Xplore, Mar. 01, 2016. https://ieeexplore.ieee.org/document/7754846 (accessed Aug. 05, 2021).
[30] W. S. Alnumay and U. Ghosh, “Secure Routing and Data Transmission in Mobile Ad Hoc Networks,” International journal of Computer Networks & Communications, vol. 6, no. 1, pp. 111–127, Jan. 2014, doi: 10.5121/ijcnc.2014.6108.
[31] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, “Authenticated routing for ad hoc networks,” IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598–610, Mar. 2005, doi: 10.1109/jsac.2004.842547.
[32] I. Achour, T. Bejaoui, A. Busson, and S. Tabbane, “SEAD: A simple and efficient adaptive data dissemination protocol in vehicular ad-hoc networks,” Wireless Networks, vol. 22, no. 5, pp. 1673–1683, Sep. 2015, doi: 10.1007/s11276-015-1050-9.
[33] Y.-C. Hu, A. Perrig, and D. B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” Wireless Networks, vol. 11, no. 1–2, pp. 21–38, Jan. 2005, doi: 10.1007/s11276-004-4744-y.
[34] M. N. Rajkumar, M. Nithya, and M. Krithika, “Security Requirements and Mechanisms in Vehicular Ad-Hoc Networks (VANET),” World Scientific News, pp. 200–207, 2016.