Mapping Extended Reality Threats in Connected Vehicles with Attack-Defense Tree

Mujtabaa Adam, Muhammad Baqer Mollah, and Kyu In Lee
Dept. of Information Science Technology, University of Houston, Houston, TX 77204 USA
Emails: {madam, mmollah, klee49}@uh.edu

***Abstract*—Extended Reality (XR), encompassing Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR), is rapidly transforming multiple industries by enabling immersive and context-aware user experiences. In the automotive domain, modern vehicles are increasingly equipped with rich sensing and computation capabilities through Advanced Driver Assistance Systems (ADAS), which are creating a strong foundation for vehicle-centric XR applications. By leveraging multi-modal sensor data, real-time perception algorithms, and software-defined vehicle architectures, XR can enhance situational awareness, navigation, and human–vehicle interaction. However, the integration of XR into connected vehicular systems introduces significant security challenges, as these systems rely heavily on accurate perception, reliable data processing, and trustworthy communication. To this end, in this paper, we present a systematic security threat modeling for XR-enabled connected vehicles using attack–defense tree model. In particular, we identify critical attack surfaces across sensing, perception, data processing, and XR rendering layers, and map how adversaries can manipulate XR-driven decision-making processes. We then incorporate the corresponding defense mechanisms within the attack–defense tree model to systematically evaluate the structured reasoning about security risks and mitigation strategies.**

***Index Terms*—Extended reality, Connected vehicles, Cyber security, threat modeling, attack-defense tree.**

I. Introduction

Extended Reality (XR), which includes Augmented Reality (AR), Virtual Reality (VR), and Mixed Reality (MR), is rapidly changing in education, training, manufacturing, and remote assistance to enable more interactive and immersive experiences. At the same time, modern vehicles already have the necessary sensors, computing power, and communication systems to support XR applications [1], [2]. More specifically, today's vehicles are increasingly equipped with Advanced Driver Assistance Systems (ADAS), which integrate a diverse set of sensors such as cameras, LiDAR, radar, and ultrasonic devices to continuously capture real-time information about the surrounding environment [3], [4]. These sensor streams are processed using advanced algorithms, including computer vision and deep learning techniques, to perform object detection, semantic segmentation, and depth estimation. For example, drivers in certain vehicles already utilize augmented reality through narrow field-of-view (FOV) head-up displays (HUDs), which deliver intuitive assistance features that improve situational awareness and overall driving experience.

As automotive architectures evolve toward software defined vehicles [5], data collected from multiple subsystems can be abstracted through standardized interfaces, such as an XR Software Development Kit (XR SDK), enabling developers to build XR applications on top of vehicle-generated insights. These applications can augment the driver's perception of the environment by overlaying contextual information directly onto their field of view, thereby improving reaction time and decision-making. Unlike traditional interfaces, XR systems tightly couple physical-world perception with digital augmentation, making them highly sensitive to data integrity and system reliability.

Despite these advancements, the integration of XR into connected vehicular environments introduces new and complex security challenges [6], [7]. XR systems depend on accurate sensing, trustworthy data processing, and consistent environmental understanding. Any compromise in these components can directly affect the correctness of XR outputs, potentially leading to hazardous situations. For example, adversarial manipulation of sensor inputs or perception algorithms may result in incorrect object representation, while falsified contextual information could mislead drivers and degrade situational awareness.

Given the safety-critical nature of vehicular systems, there is a pressing need for systematic threat modeling and security evaluation methodologies for XR-enabled vehicles. Specifically, traditional cyber security approaches are insufficient to capture the tight coupling between perception, decision-making, and user interaction inherent in XR systems. To address this gap, in this paper, we adopt attack-defense tree as a structured tool to model potential attack vectors and corresponding countermeasures, where a hierarchical decomposition of complex attack scenarios along with simultaneously incorporating defensive strategies would provide a comprehensive view of system vulnerabilities and protections. In summary, this work aims to (i) identify key attack surfaces across sensing, processing, and XR rendering stages, (ii) systematically map defense mechanisms to mitigate these threats, and (iii) provide a foundation for evaluating security risks in safety-critical XR applications.

II. Related Works and Motivation

Security threat modeling in cyber-physical systems (CPS), including connected vehicles, has received significant attention due to the safety-critical nature of these systems. Threat modeling basically provides a systematic methodology to identify, analyze, and mitigate potential vulnerabilities to enable proactive security assurance. Traditional approaches,

such as attack trees [8] and their extensions, including attack-defense trees [9], have been widely adopted to represent adversarial goals and corresponding countermeasures in a hierarchical structure that essentially allows both qualitative and quantitative risk analysis. These methods have proven effective in modeling complex attack paths and evaluating system resilience, particularly in CPS environments where cyber and physical components are tightly coupled.

In the automotive specific domain, several studies have explored threat modeling for connected and autonomous vehicles. The authors in [10] has highlighted the need for combining multiple modeling techniques to capture diverse attack surfaces in modern vehicles. Similarly, the work in [11] has emphasized on constructing attack paths and corresponding countermeasures to present the importance of systematic threat analysis in vehicular systems. In another work in [12], a broader perspectives on safety risks in heterogeneous vehicular systems has presented, however, they have primarily focused on traffic-level risks rather than XR-specific cyber threats.

Recent advances have also introduced intelligent and automated threat modeling techniques. For instance, Salek et al. [13] have utilized large language models to identify attack vectors and countermeasures with reduced expert intervention to get improved scalability and adaptability in complex CPS environments. In other works in [14], [15], the authors have been focused on assessing system vulnerabilities, such as quantitative cyber security analysis approach for CPS and risk scoring as well as prioritization of critical components, respectively. Although these approaches enable more rigorous evaluation but often lack specific modeling of perception-driven systems like XR-based systems.

Besides these works, XR security has been studied in other domains as well. For example, Anjum et al. [16] have highlighted more about emerging threats related to user privacy, data leakage, and immersive system manipulation. In an another work [17], the authors have first illustrated how adversarial inputs might disrupt CPS operations, and then emphasized the necessity of robust threat modeling in safety-critical environments.

Despite these advances, existing work largely treats perception, computation, and user interaction as separate components, without fully addressing their tight integration in XR-enabled vehicular systems. In particular, there is a lack of structured threat modeling approaches that are able to capture how compromised perception and data processing directly affect XR outputs and user decision-making. And, to bridge this gap, this paper focuses on attack-defense tree modeling particularly for vehicular XR systems, where we systematically map threats across sensing, processing, and XR layers and incorporate corresponding defense mechanisms for comprehensive security analysis.

One comparison table!

III. System Description and Cyber Threats

In this section, we present the system description and outline the recent cyber threats related to XR-enabled connected vehicles.

A. System Description

We consider a connected vehicular XR system having three logical layers, such as the sensing layer, the ADAS-driven data processing and fusion layer, and the XR application and device layer, which are supported by vehicle-to-everything (V2X) communication, cloud, and edge computing services. These layers enable the transformation of vehicular data into immersive and context-aware XR representations and form a tightly integrated cyber-physical system. The details of these layers are discussed as follows.

First, the sensing layer consists of heterogeneous on-board sensors that continuously capture both vehicle state information and environmental context. These include vision sensors, such as monocular and stereo cameras that provide near 360-degree visual coverage, as well as ranging sensors including LiDAR, radar, and ultrasonic devices for accurate depth and distance estimation. In addition, localization sources such as GPS and inertial measurement units (IMUs) provide spatial positioning, while internal vehicle data, including speed, steering angle, acceleration, and CAN bus signals, offer insights into vehicle dynamics. Particularly, these sensing modalities enable comprehensive surround perception and environment understanding, which form the foundation for XR content generation.

Second, the ADAS-based data processing and fusion layer transforms raw sensor inputs into structured and semantically meaningful representations using computer vision, signal processing, and machine learning techniques. Core functionalities include object detection and classification for identifying vehicles, pedestrians, and obstacles; semantic segmentation for scene understanding; depth estimation and three-dimensional scene reconstruction; and driving context inference such as lane detection, traffic sign recognition, and road condition assessment. To improve robustness and accuracy, multi-modal sensor fusion is employed, combining complementary data from cameras, LiDAR, radar, and localization systems to ensure consistent perception even under adverse conditions such as low visibility or partial sensor degradation. Processing is primarily performed within the vehicle using domain controllers or consolidated computing units in software-defined vehicles (SDVs). However, due to computational limitations and latency constraints, the selected tasks are offloaded to edge or cloud infrastructure for large-scale computation or to XR devices for rendering and lightweight processing. The output of this layer is an abstracted environmental model containing object-level metadata, spatial relationships, and contextual information, which can be directly consumed by XR applications.

Third, the XR application and device layer utilizes the processed data to generate context-aware XR experiences. An XR Software Development Kit (XR SDK) abstracts the underlying sensing and perception pipeline, enabling developers to access real-time environmental representations, object metadata, spatial coordinates, and user or device context

through standardized interfaces. XR applications can augment the real-world environment with virtual elements or generate immersive representations based on vehicle perception data. These applications are rendered on various XR-capable devices, including in-vehicle displays such as augmented reality head-up displays (HUDs), personal devices like smartphones and tablets, and wearable XR devices such as AR glasses or head-mounted displays. Given the safety-critical nature of many vehicular XR use cases, the system operates under strict latency and reliability requirements, requiring tight synchronization between sensing, processing, and rendering components.

Finally, the overall system is supported by the V2X connectivity for data exchange among vehicles (V2V), infrastructure (V2I), and cloud or edge servers (V2N). This connectivity basically supports cooperative perception, remote processing, and system updates, thereby enhancing the capabilities of XR applications.

B. Cyber Threats in Vehicular XR Systems

The integration of XR into connected vehicular systems introduces a wide range of cyber-physical threats [18], [19], as adversaries can target multiple layers of the system to manipulate perception, disrupt communication, or compromise system integrity. These threats are particularly critical because they can directly influence XR-driven decision-making and potentially lead to unsafe driving conditions. In this work, we categorize the threats according to the system layers defined above.

At the sensing layer, the primary vulnerabilities arise from attacks that manipulate raw data inputs, thereby corrupting the foundation of XR perception. Sensor spoofing attacks can inject fabricated inputs into cameras, LiDAR, or radar systems, while replay attacks reuse previously recorded sensor data to mislead real-time perception. GPS spoofing can manipulate localization information, resulting in incorrect spatial alignment of XR overlays. Additionally, adversarial perturbations can be crafted to deceive machine learning models used in perception tasks. The impact of these attacks is significant, as they can lead to incorrect environment reconstruction, causing false object detection or omission in XR representations.

In the ADAS processing and fusion layer, attacks target the data processing pipelines and machine learning models responsible for generating environmental understanding. Adversaries may inject false objects or remove legitimate ones by manipulating detection outputs, or conduct model poisoning attacks by compromising training data or learned parameters. Sensor fusion inconsistency attacks exploit discrepancies between different sensing modalities, while computation offloading attacks target data exchanged with edge or cloud services. These attacks undermine the trustworthiness of perception outputs, directly affecting the accuracy and reliability of XR content.

The XR application layer introduces threats that directly affect user perception and interaction. Malicious XR content injection can result in unauthorized virtual objects being displayed within the scene, while overlay misalignment attacks disrupt the spatial consistency between virtual and real-world elements. User interface manipulation attacks can alter visual cues in ways that mislead users, and data integrity attacks can compromise the outputs of the XR SDK. Such threats are particularly dangerous because they influence how users interpret their environment, potentially leading to incorrect decisions and unsafe actions.

Finally, communication-related threats arise due to the reliance on V2X connectivity. These might include false data injection in vehicular messages, Sybil attacks involving multiple fake identities, and denial-of-service (DoS) attacks that disrupt communication channels. These attacks can compromise the availability, authenticity, and timeliness of shared information, thereby affecting cooperative perception and synchronization across XR systems.

TABLE I: Summary of defense mechanisms in the Attack–Defense Tree for XR-enabled connected vehicular systems.

$\mathcal{D}$	**Descriptions**
d_1	Cryptographic solutions
d_2	Intrusion detection and monitoring systems
d_3	Sensor redundancy and basic calibration checking
d_4	Robust sensor fusion with adversarial-resilient perception models
d_5	Physics-based consistency validation
d_6	GNSS filtering and assisted localization
d_7	Multi-modal fusion
d_8	Model retraining and data augmentation
d_9	Adversarially trained AI models
d_{10}	Cross-frame temporal consistency checks
d_{11}	Consensus-based perception across sensors and time
d_{12}	XR SDK access control and application sandboxing
d_{13}	Calibration and pose estimation correction
d_{14}	Spatial consistency monitoring between rendered & sensed world
d_{15}	Real-time drift correction algorithms
d_{16}	Adaptive resilient communication scheduling

IV. Modeling of Attack-Defense Tree

In this section, we present the attack-defense tree model and a structured analytical evaluation for security threats in XR-enabled connected vehicular systems.

A. Attack–Defense Tree for Vehicular XR

In this work, we adopt a cyber security modeling approach inspired by [20], which represents as hierarchical structures, where the root node captures the adversary's ultimate objective and the leaf nodes denote atomic attack actions required to achieve that objective. Furthermore, the intermediate nodes describe sub-goals or attack steps that collectively contribute to the realization of the root objective. The logical operators, such as AND and OR are used to model the relationships among these nodes to offer the representation of multiple attack strategies and dependencies within complex systems.

By extending it to the context of XR-enabled vehicular systems, this approach enables us to develop a systematic representation of multi-layer attack surfaces spanning sensing, data processing, and XR application layers. As discussed the

potential cyber threats in prevision section, we now construct the attack-defense tree in the context of XR-enabled vehicles as presented in Fig. 1. Here, the tree incorporates attacks targeting sensing spoofing, threats against ADAS system, compromising in XR application layer, and intrusions in V2X interface along with their individual attacks paths and corresponding countermeasure. We then summarize the set of defense strategies considered in this work in Table I, where the complete set of defenses are denoted by $\mathcal{D}$.

B. Mathematical Modeling

For further quantitative evaluation, we formulate a mathematical model, which allows us to evaluate both the likelihood and impact of potential attacks, as well as the effectiveness of deployed defense mechanisms. This quantitative approach supports risk-aware decision-making by enabling security analysts to rank threats and prioritize mitigation strategies based on their severity and system-wide consequences. For that, let the vulnerability score associated with an attack leaf node $\mathcal{A}_i$ be denoted $V(\mathcal{A}_i)$. This score is defined formally as:

$$V(\mathcal{A}_i) = \begin{cases} \max\left\{w_c \cdot \left(1 - \frac{d_i}{D_{max}}\right), w_c \cdot \max(\lambda)\right\}, & \text{if } w_c > 0 \\ \frac{1}{3} \cdot \max\left\{\left(1 - \frac{d_i}{D_{max}}\right), \max(\lambda)\right\}, & \text{if } w_c = 0 \end{cases} \tag{1}$$

where w_c represents the weighting factor associated with the level of defensive deployment at the attack leaf, and λ denotes the effectiveness scores of individual defense mechanisms applied at that node. The parameter d_i corresponds to the number of implemented defenses for attack node $\mathcal{A}_i$, while D_{max} represents the maximum allowable number of defenses (set to 5 to reflect practical deployment constraints). The vulnerability score $V(\mathcal{A}_i)$ is normalized within the range $[0, 1]$, where a value of 0 indicates a fully secured node and a value of 1 represents maximum vulnerability.

The weighting factor w_c is determined based on the extent of countermeasure deployment at each attack node. We present the considered conditions in Table II. Specifically, if no countermeasures are implemented, the node is assigned the highest weight, reflecting maximum exposure. If at least one countermeasure is present, the weight is reduced to indicate partial protection. When three or more countermeasures are deployed, the weight is set to zero, representing a sufficiently hardened node with minimal residual vulnerability. This formulation captures the intuitive relationship between defense coverage and system robustness, while allowing flexibility in incorporating different types of security mechanisms. Furthermore, considering the necessity of intrusion detection and monitoring capability in XR-enabled vehicular systems, we consider different levels as presented in III to incorporate defensive capabilities into our evaluations, where each configuration is associated with a weighting factor, denoted by β, which reflects its relative effectiveness in mitigating attacks.

TABLE II: Defense coverage conditions and corresponding weight assignments for attack leaf nodes in vehicular XR systems.

Condition	**Defense Coverage at Attack Leaf**	w_c
Condition 1	No defense mechanism is applied to the attack leaf, or existing protection is ineffective against the considered threat (e.g., unprotected sensor input, unauthenticated data, or lack of validation in XR rendering).	1.00
Condition 2	Partial defense is present, where at least one mitigation mechanism is implemented (e.g., basic input validation, single-layer authentication, or isolated sensor verification), but the protection is insufficient against advanced or multi-vector attacks.	0.50
Condition 3	Strong and multi-layered defense is implemented, combining three or more complementary countermeasures (e.g., sensor fusion validation, secure communication, integrity verification, and runtime monitoring), providing robust protection against the attack.	0.00

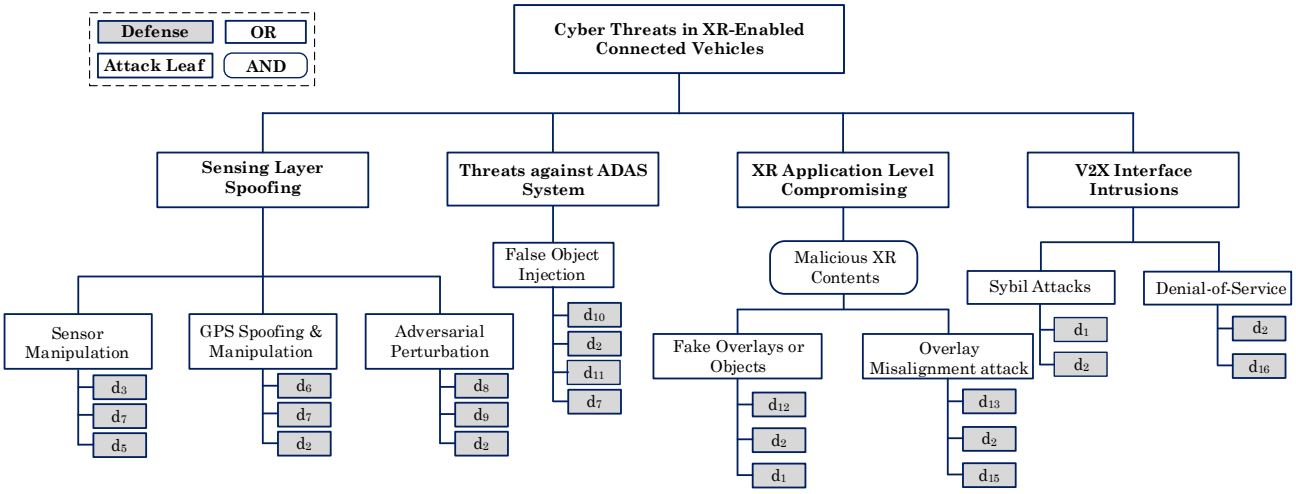
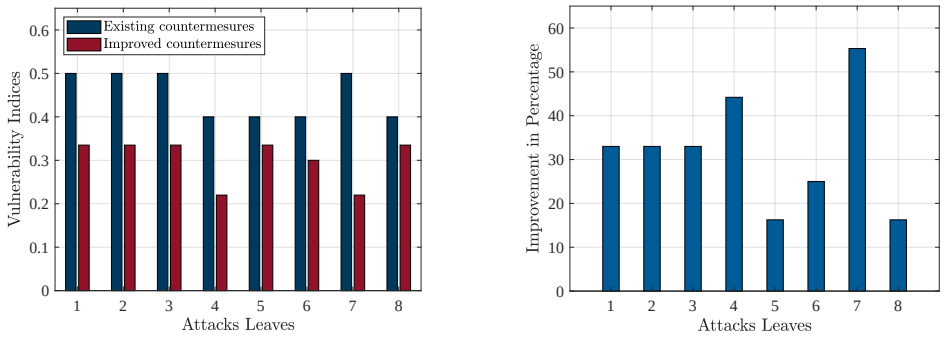


Fig. 1: The developed attack-defense tree for XR-enabled vehicular system with example attacks and defenses.



(a) Vulnerabilities at each leaf

(b) Vulnerability improvement in percentage

Fig. 2: Vulnerability evaluating of connected vehicles in quantitative manner.

TABLE III: Levels of intrusion detection and monitoring capability in XR-enabled vehicular systems.

Level	Intrusion Detection and Monitoring Capability	λ
Level 1	**No Monitoring Capability** The system lacks any form of intrusion detection or runtime monitoring across sensing, communication, or XR processing layers (e.g., no mechanisms are deployed to detect malicious sensor inputs, abnormal perception outputs, or network anomalies).	1.00
Level 2	**Basic Monitoring** Limited intrusion detection is available, typically focused on a single layer (e.g., network traffic or system logs). Detection is primarily rule-based or signature-driven, with limited capability to identify novel or cross-layer attacks.	0.67
Level 3	**Multi-Layer Monitoring** The system incorporates intrusion detection across multiple components, such as sensing validation, ADAS processing, and communication monitoring. A combination of rule-based and anomaly-based techniques is used to improve detection coverage.	0.33
Level 4	**Adaptive and Intelligent Monitoring** A comprehensive monitoring framework is deployed, integrating cross-layer intrusion detection with learning-based methods for identifying previously unseen attacks. The system should supports real-time analysis and adaptive response across sensing, processing, and XR application layers.	0.00

C. Threats Evaluation and Resutls

To support the evaluation, the attack leaf nodes identified from the attack–defense tree along with their corresponding defense mechanisms are summarized in Table IV. This structured mapping enables a detailed study on how individual attack points are being mitigated within the system. In addition, we extend the baseline defense configurations by incorporating enhanced countermeasures, including strengthened validation mechanisms and intrusion detection capabilities at each attack leaf. This improvement allows for a comparative analysis between the original and improved defense strategies that eventually facilitate a clearer understanding of how additional protections influence overall system security.

The resulting threat assessments for each attack leaf calculated by Eq. (1) are presented in Fig. 2 through a bar chart to offer a concise visualization of the system's security performance before and after the implementation of enhanced defenses. This comparison highlights the relative reduction in vulnerability achieved through the proposed improvements and helps identify residual weak points that may require further attention.

V. Conclusion

As vehicles evolve into sensor-rich, software-defined platforms capable of supporting immersive XR applications, ensuring security of the underlying system components becomes critically important. In this paper, we have presented a structured approach to security threat modeling for XR-enabled connected vehicular systems using attack–defense tree. Through a systematic way, we have identified the key attack vectors spanning sensor manipulation, perception interference, data processing vulnerabilities, and XR output distortion. And, then we have showed how potential threats can be mitigated through different countermeasure strategies by embedding corresponding defense mechanisms within the thee. Finally, we presented how we can facilitate qualitative risk evaluation by capturing the relationships between attack feasibility, defense effectiveness, and safety impact. We believe this work will provide a comprehensive foundation for future works on understanding, analyzing, and mitigating security threats in emerging XR-assisted vehicular systems.

Acknowledgments

This work was supported by the US Department of Transportation (USDOT) Tier 1 University Transportation Center (UTC) Transportation Cybersecurity Center for Advanced Research and Education (CYBER-CARE) (Grant No. 69A3552348332); and the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. RS-2024-00463802).

References

[1] I. Argui, M. Gueriau, and S. Ainouz, "Advancements in mixed reality for autonomous vehicle testing and advanced driver assistance systems: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 12, pp. 19 276–19 294, 2024.

TABLE IV: Attack-Defense mapping for XR-enabled connected vehicular systems with existing countermeasures, detection strategies, and improved defenses.

Attack Leaves	Descriptions	Existing Countermeasures	Intrusion Detection / Monitoring	After Improvement
1	Sensor spoofing (camera, LiDAR, or radar manipulation)	Sensor redundancy and basic calibration checks	No deployed mechanism to detect malicious sensor inputs	Robust sensor fusion with adversarial-resilient perception models Physics-based consistency validation
2	GPS spoofing and localization manipulation	GNSS filtering and assisted localization	Lack of spoofing and manipulation monitoring	Multi-source localization fusion (GPS + IMU + vision SLAM) Trajectory anomaly detection and map deviation monitoring
3	Adversarial perturbation in perception models	Model retraining and data augmentation	No mechanisms to detect abnormal perception outputs	Adversarially trained AI models Confidence score monitoring and uncertainty estimation
4	False object injection or removal in ADAS system	Cross-frame temporal consistency checks	Rule-based object validation	Consensus-based perception across sensors and time Trust-weighted fusion mechanisms
5	Fake overlays or objects injections	XR SDK access control and application sandboxing	Visual anomaly detection (overlay mismatch vs sensor reality)	Cryptographically signed XR content and overlays
6	Overlay misalignment attack (AR–real world mismatch)	Calibration and pose estimation correction	Spatial consistency monitoring between rendered and sensed world Continuous spatial re-registration using sensor fusion	Real-time drift correction algorithms Learning-based real-time alignment correction engine
7	Sybil attacks	PKI-based authentication for vehicular communication	Absent of network behavior analysis tools	Blockchain-assisted trust management Lightweight reputation-based identity validation Rule- and anomaly-based tools
8	Denial-of-Service (DoS)	Rate limiting and basic firewall configured	Traffic anomaly detection and latency monitoring	Adaptive resilient communication scheduling

[2] A. Manzoor, Y. Iqbal, A. Ortis, S. Livatino, and S. Battiato, "Xr-vits: Extended reality vehicle intelligent tracking system for smart transportation," *Array*, p. 100748, 2026.

[3] A. Manila, S. Negi, C. Nowakowski, and P. Reilhac, "Unlocking immersive driving experiences with automotive sensor-powered extended reality (xr)," in *IET Conference Proceedings CP887*, vol. 2024, no. 10. IET, 2024, pp. 15–22.

[4] D. M. Doe, D. Chen, K. Han, J. Xie, and Z. Han, "Enhancing ar/vr performance via optimized edge-based object detection for connected autonomous vehicles," in *2024 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2024, pp. 2841–2847.

[5] J. Stümpfle, J. Sigel, M. Weiß, B. C. Gül, F. Dettinger, N. Jazdi, M. Hoßfeld, and M. Weyrich, "The software-defined vehicle: A comprehensive study on current trends and challenges," *IEEE Engineering Management Review*, 2025.

[6] L. Schmidt and E. Yigitbas, "Taxonomy and analysis of security vulnerabilities, privacy violations and potential mitigation strategies to xr systems," in *Proceedings of the 18th ACM International Conference on PErvasive Technologies Related to Assistive Environments*, 2025, pp. 368–375.

[7] M. Hassan, S. S. Shraban, M. A. Islam, K. S. Basaruddin, M. F. Ijaz, N. S. B. Kamarrudin, and H. Takemura, "Integration of extended reality technologies in transportation systems: A bibliometric analysis and review of emerging trends, challenges, and future research," *Results in Engineering*, vol. 26, p. 105334, 2025.

[8] A.-M. Konsta, A. L. Lafuente, B. Spiga, and N. Dragoni, "Survey: Automatic generation of attack trees and attack graphs," *Computers & Security*, vol. 137, p. 103602, 2024.

[9] A. Birchler De Allende, B. Sultan, and L. Apvrille, "From attack trees to attack-defense trees with generative ai & natural language processing," in *Proceedings of the ACM/IEEE 27th International Conference on Model Driven Engineering Languages and Systems*, 2024, pp. 561–569.

[10] A. Yousseef, Y.-Z. Lin, S. Satam, B. S. Latibari, J. Pacheco, S. Salehi, S. Hariri, and P. Satam, "Autonomous vehicle security: Hybrid threat modeling approach," *IEEE Open Journal of Vehicular Technology*, 2025.

[11] M. B. Mollah, H. Wang, and H. Fang, "Evaluating vulnerabilities of connected vehicles under cyber attacks by attack-defense tree," in *2026 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2026, pp. 1–6.

[12] Z. Cheng, J. Zhu, Z. Feng, M. Yang, W. Zhang, and J. Chen, "Driving safety risk analysis and assessment in a mixed driving environment of connected and non-connected vehicles: a systematic survey," *IEEE Transactions on Intelligent Transportation Systems*, 2025.

[13] M. S. Salek, M. Chowdhury, M. B. Munir, Y. Cai, M. I. Hasan, J.-M. Tine, L. Khan, and M. Rahman, "A large language model-supported threat modeling framework for transportation cyber-physical systems," *IEEE Access*, 2025.

[14] A. Abdulhamid, S. Kabir, I. Ghafir, C. Lei, K. El Hindi, and M. Hammoudeh, "Quantitative cybersecurity analysis framework for cyber physical systems: A conceptual approach," *IEEE Open Journal of the Computer Society*, vol. 6, pp. 613–626, 2025.

[15] R. Alguliyev, R. Aliguliyev, and L. Sukhostat, "An approach for assessing the functional vulnerabilities criticality of cps components," *Cyber Security and Applications*, vol. 3, p. 100058, 2025.

[16] N. Anjum and M. R. Mahmud, "Beyond the headset: A systematization of knowledge on extended reality privacy and security in healthcare," in *Proceedings of the 2025 31st ACM Symposium on Virtual Reality Software and Technology*, 2025, pp. 1–12.

[17] S. K. Padisala, S. D. Vyas, and S. Dey, "Exploring adversarial threat models in cyber physical battery systems," *IEEE Journal of Emerging and Selected Topics in Industrial Electronics*, 2025.

[18] A. Qayyum, M. A. Butt, H. Ali, M. Usman, O. Halabi, A. Al-Fuqaha, Q. H. Abbasi, M. A. Imran, and J. Qadir, "Secure and trustworthy artificial intelligence-extended reality (ai-xr) for metaverses," *ACM Computing Surveys*, vol. 56, no. 7, pp. 1–38, 2024.

[19] K. Cai, J. Zhang, Y. Li, Z. Wang, X. Chen, T. Li, and Y. Tian, "From perception to protection: A developer-centered study of security and privacy threats in extended reality (xr)," *arXiv preprint arXiv:2509.06368*, 2025.

[20] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 40, no. 4, pp. 853–865, 2010.