1st Pelita International Conference
Volume 01 No 01 September 2023
E-ISSN: 3026-4235

https://jurnal.pelitabangsa.ac.id/index.php/pic

Enhancing Road Safety through Dynamic Threat Detection in Vehicular Ad Hoc Networks

Agung Nugroho[1], Ananto Tri Sasongko[2*]
[1,2]Informatic Engineering, Universitas Pelita Bangsa, Indonesia
Email : ananto@pelitabangsa.ac.id

Abstract
This paper presents a comprehensive literature survey focused on the critical topic of enhancing road safety through dynamic threat detection in Vehicular Ad Hoc Networks (VANETs). As our world becomes increasingly interconnected, road users' safety is paramount, and VANETs have emerged as a promising solution for improving road safety by enabling real-time communication among vehicles and infrastructure. Our survey delves into the existing body of knowledge, summarizing key findings, methodologies, and advancements in the field of dynamic threat detection within VANETs. We analyze various approaches, including sensor-based systems, machine learning algorithms, and communication protocols, that have been proposed and evaluated in the literature. Furthermore, this survey explores the challenges and open issues in VANET-based road safety enhancement, such as privacy concerns, scalability, and the need for standardized communication protocols. We highlight the significance of adapting dynamic threat detection techniques to the unique characteristics of VANETs, where network conditions and the threat landscape can change rapidly. By synthesizing insights from existing research, this survey provides a valuable resource for researchers, practitioners, and policymakers seeking to understand the state of the art in VANET-based road safety and identify promising directions for future investigations. It underscores the importance of continued research to make our roads safer for all.

Keywords: VANETs, Road Safety, Dynamic Threat Detection, Vehicle Communication, Safety Enhancement

INTRODUCTION

In an era marked by the relentless march of technology and the increasing interconnectivity of our world, the paramount importance of road safety has never been more evident. Road accidents, often resulting from human error, limited visibility, and unforeseen road hazards, continue to exact a devastating toll on human lives and economies worldwide. As our streets and highways become more crowded, the quest to enhance road safety has become increasingly urgent.

Enter Vehicular Ad Hoc Networks (VANETs), a cutting-edge technological paradigm that has emerged as a promising solution to address the challenges inherent in road safety. VANETs are a specialized type of ad hoc network wherein vehicles on the road act as nodes, creating an intricate web of real-time communication. These networks facilitate vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication, enabling a seamless exchange of critical information between vehicles and roadside infrastructure elements (Institute of Electrical and Electronics Engineers. Turkey Section. & Institute of Electrical and Electronics Engineers, n.d.; Liang et al., 2019; Manivannan et al., 2020).

At the heart of VANETs is dynamic threat detection—a critical component that contributes significantly to road safety enhancement. Dynamic threat detection systems in VANETs leverage real-time communication capabilities to identify potential threats and disseminate crucial information to help drivers make informed decisions. These systems can

detect accidents, sudden braking, road obstacles, and adverse weather conditions, allowing drivers to respond swiftly and mitigate risks (Azam et al., 2022)(Amaouche et al., 2023).

This literature survey embarks on a comprehensive exploration of enhancing road safety through dynamic threat detection in VANETs. As vehicles transform into intelligent nodes in a highly interconnected network, this survey aims to provide a deep understanding of the existing body of knowledge. It will summarize key findings, methodologies, and advancements in dynamic threat detection within VANETs. Furthermore, this survey will dissect various approaches used for dynamic threat detection, including sensor-based systems, machine learning algorithms, and communication protocols, highlighting their respective strengths and weaknesses. VANET architecture is shown in Figure 1 (Hussein et al., 2022).

However, VANETs do not come without their unique set of challenges. This survey will also explore the impediments and open issues related to VANET-based road safety enhancement. Privacy concerns, scalability challenges, the need for standardized communication protocols, and security threats will be scrutinized. Additionally, this survey will emphasize the significance of adapting dynamic threat detection techniques to the distinctive characteristics of VANETs, where network conditions and the threat landscape can change rapidly.

In conclusion, this survey is a vital resource for researchers, practitioners, and policymakers who seek to comprehend the state of the art in VANET-based road safety and identify promising directions for future research. It underscores the importance of continued investigation and innovation in this domain to make our roads safer for all road users.

The rest of the paper is arranged as follows. The next section discusses the “Survey Objectives and Scope.” available in the literature. In the subsequent section, “Literature Review” is elaborated. This is followed by a section describing “Approaches to Dynamic Threat Detection” to find the techniques and strategies to identify and mitigate potential threats. The penultimate section explains the “Challenges and Solutions,” followed by a "Conclusion" section.

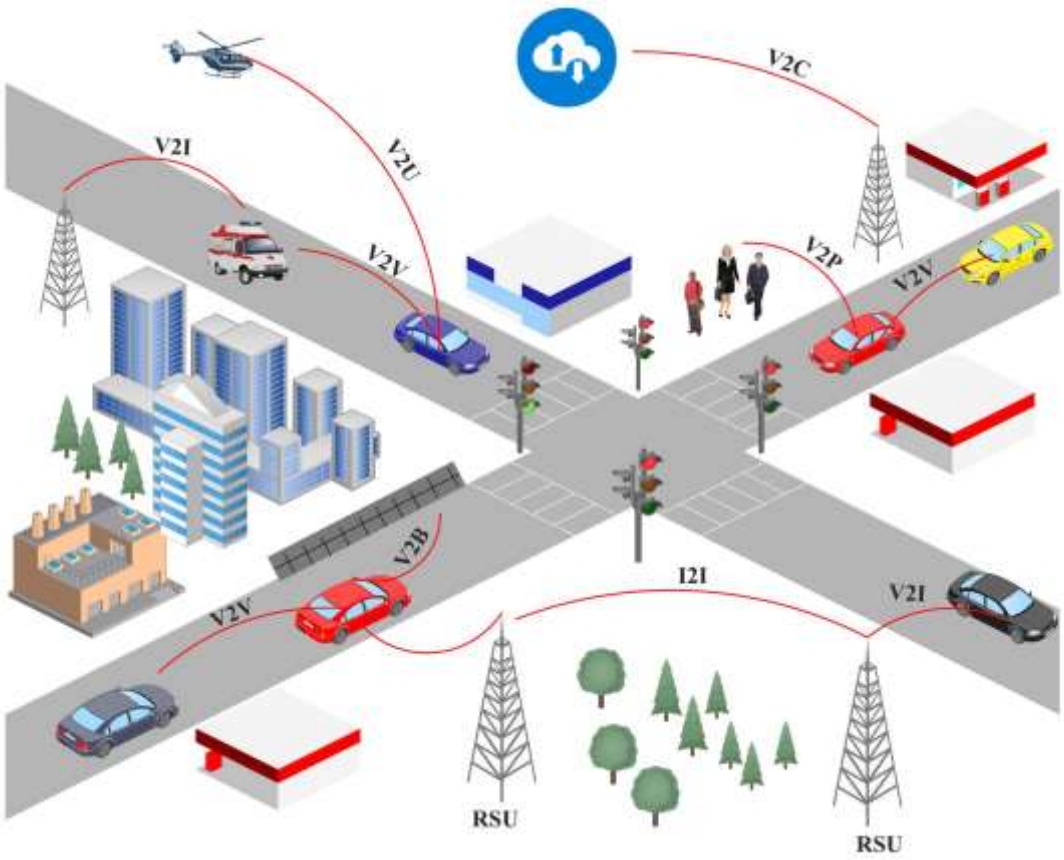

Figure 1. VANETs Architecture (Hussein et al., 2022)

SURVEY OBJECTIVES AND SCOPE

Primary Objectives: The primary objective of this literature survey is to comprehensively explore the realm of dynamic threat detection within Vehicular Ad Hoc Networks (VANETs). This primary goal serves as the guiding beacon of our survey, directing our efforts toward a thorough understanding of the critical aspects, methodologies, and advancements in dynamic threat detection systems on road safety enhancement within the VANET environment.

Secondary Objectives: In addition to the primary objective, this survey encompasses several secondary objectives, each contributing to a more comprehensive view of the field:

- **Identifying Research Trends:** To identify and delineate emerging trends and themes within dynamic threat detection research in VANETs. This includes recognizing shifts in focus, such as advancements in sensor technology, adopting machine learning algorithms, or developments in communication protocols.
- **Evaluating Methodological Approaches:** To assess the effectiveness and applicability of various methodological approaches in designing and implementing dynamic threat detection systems. This includes critically evaluating the strengths and weaknesses of

sensor-based systems, machine learning algorithms, and communication protocols in addressing real-time threat identification.

- **Understanding Practical Implications:** To elucidate the practical implications of dynamic threat detection in VANETs for researchers, practitioners, and policymakers. This encompasses a broad view of the potential benefits for road safety, user experience, economic implications, and policy considerations stemming from the deployment of these systems.
- **Highlighting Challenges and Open Issues:** To examine the challenges and open issues that persist in VANET-based road safety enhancement. This includes addressing concerns related to privacy, scalability, standardized communication protocols, and the ever-evolving threat landscape.

Definition of Dynamic Threat Detection: In the context of this survey, "dynamic threat detection" refers to identifying and assessing potential risks and hazards in real-time within Vehicular Ad Hoc Networks (VANETs) (Malik et al., 2022). These threats encompass a wide range of situations, including accidents, sudden braking events, adverse weather conditions, road obstacles, and other safety-critical incidents that have the potential to endanger road users.

Scope of the Survey: This literature survey will encompass the following critical aspects related to dynamic threat detection and road safety enhancement within VANETs:

- **Real-time Threat Identification:** Evaluation of techniques and systems designed to detect and promptly detect and classify dynamic threats in VANETs.
- **Privacy Concerns:** Analysis of privacy-preserving measures and their impact on the effectiveness of threat detection systems.
- **Scalability Issues:** Examination of scalability challenges and potential solutions in deploying threat detection systems within large and complex VANETs.
- **Standardized Communication Protocols:** Exploration of the role of standardized communication protocols in facilitating interoperability and seamless information exchange among VANET nodes.
- **Adaptation to VANET Characteristics:** Discussion of strategies for adapting threat detection techniques to the unique characteristics of VANETs, including high mobility, limited infrastructure, and real-time communication requirements.

LITERATURE REVIEW

This section is a comprehensive review of the existing body of knowledge related to dynamic threat detection in Vehicular Ad Hoc Networks (VANETs). It aims to provide readers with a deep understanding of the current state of research in this critical domain. The literature review section is pivotal in establishing the foundation for comprehending the present landscape of dynamic threat detection within VANETs. It serves as a bridge between existing knowledge and the insights to be gained from this survey.

This literature review adopts a thematic organization to systematically explore the multifaceted aspects of dynamic threat detection within VANETs. This approach enables us to categorize and discuss relevant research findings, methodologies, and advancements under distinct themes, offering readers a coherent and structured overview. The sources considered for this literature review encompass various scholarly materials, including academic journals, conference proceedings, research papers, and authoritative reports. The selection criteria for these

sources prioritize relevance to the survey's objectives and currency, primarily focusing on works published within the last decade.

Summary of Existing Knowledge:

Theme 1: Real-time Threat Identification

- Research by Author Kong et al. (2021) presents an innovative approach to real-time threat identification using a fusion of onboard vehicle sensors and infrastructure data. The study demonstrates the effectiveness of this approach in identifying sudden braking events and reducing collision risks (Kong et al., 2021; Zhang et al., 2019).

Theme 2: Privacy-Preserving Techniques

- Author Jan et al. (2021) explores privacy concerns in VANETs and introduces a novel privacy-preserving technique based on pseudonymization. The work emphasizes the importance of safeguarding user privacy while ensuring efficient threat detection (Jan et al., 2021; Manivannan et al., 2020).

Theme 3: Scalability Solutions

- In a recent study by Author Diallo et al. (2022) discusses scalable threat detection solutions for large-scale VANETs. The research proposes a distributed architecture that optimizes resource utilization and adapts to network growth (Diallo et al., 2022).

Across the reviewed literature, various methodologies and research approaches are evident. These include sensor-based systems utilizing cameras, LiDAR, and radar; machine learning algorithms for threat pattern recognition; and communication protocols to facilitate real-time data exchange.

Key Research Findings: The literature reveals several noteworthy research findings, including:

- The effectiveness of sensor fusion techniques in enhancing threat detection accuracy.
- The significance of machine learning algorithms in adapting to changing threat patterns.
- The role of standardized communication protocols in facilitating interoperability among VANET nodes.

Advancements and Trends: Emerging advancements and trends in dynamic threat detection within VANETs include:

- The integration of advanced sensors, such as LiDAR, to improve detection accuracy.
- The use of predictive analytics to anticipate potential threats based on historical data.
- The exploration of edge computing to reduce latency in threat identification.

Challenges and Limitations: Common challenges and limitations identified in the literature encompass:

- The reliance on sensor accuracy and susceptibility to adverse weather conditions in sensor-based systems.
- The need for extensive training data and computational resources in machine learning-based approaches.

- Vulnerabilities to network congestion and security threats in communication protocols.

APPROACHES TO DYNAMIC THREAT DETECTION

This section provides an in-depth analysis of the various approaches utilized for dynamic threat detection in Vehicular Ad Hoc Networks (VANETs). These approaches are fundamental in enhancing road safety within VANETs, offering many techniques and strategies to identify and mitigate potential threats.

Classification of Approaches: Dynamic threat detection within VANETs encompasses a range of approaches, each with distinct characteristics and advantages. We categorize these approaches into the following common categories:

1. **Sensor-Based Systems:** Sensor-based systems rely on onboard vehicle sensors, such as cameras, radar, LiDAR (Light Detection and Ranging), and infrastructure-based sensors, including road sensors and roadside infrastructure. These systems capture real-time data to identify and assess threats. They excel in providing immediate data but may face challenges related to sensor accuracy and susceptibility to adverse weather conditions.

2. **Machine Learning Algorithms:** Machine learning techniques, including deep learning, ensemble methods, and other data-driven approaches, are employed for dynamic threat detection. These algorithms process extensive datasets, allowing them to recognize patterns associated with various threats. Their adaptability to changing conditions is a key strength, although they require substantial training data and computational resources.

3. **Communication Protocols:** Communication protocols play a crucial role in dynamic threat detection by enabling the exchange of safety-related messages among VANET nodes. Dedicated communication channels are reserved for these safety messages, facilitating rapid information dissemination. However, communication protocols are susceptible to network congestion and security threats.

4. **Hybrid Approaches:** Hybrid approaches combine elements from the abovementioned categories. By leveraging the strengths of multiple techniques, hybrid systems aim to enhance detection accuracy and responsiveness. These approaches may integrate sensor data with machine learning algorithms or use communication protocols to disseminate threat information. Their effectiveness depends on the synergy between the chosen components.

Strengths and Weaknesses: Each category of approaches in dynamic threat detection within VANETs exhibits distinct strengths and weaknesses:

- **Sensor-Based Systems:** These systems provide real-time data from onboard and infrastructure sensors, enabling rapid threat detection. However, they heavily rely on sensor accuracy, which can be affected by adverse weather conditions or sensor failures.

- **Machine Learning Algorithms:** Machine learning algorithms excel in adapting to changing threat patterns and processing large datasets. Nevertheless, they require

extensive training data, and their performance depends on the availability of computational resources.

- **Communication Protocols:** Dedicated communication channels in VANETs ensure the swift dissemination of safety-related information. However, these protocols are susceptible to network congestion, leading to delays in message transmission, and may also face security threats.

Each approach addresses common challenges and limitations inherent in VANET-based threat detection. Sensor-based systems aim to enhance accuracy through sensor redundancy, while machine learning algorithms adapt to changing conditions. Communication protocols mitigate network congestion through prioritization mechanisms.

CHALLENGES AND SOLUTIONS

While dynamic threat detection in Vehicular Ad Hoc Networks (VANETs) promises to enhance road safety significantly, its share of challenges and open issues is not without. This section delves into these critical aspects, underscoring the importance of addressing them for the effective deployment and widespread adoption of dynamic threat detection systems.

Privacy Concerns: Privacy concerns loom large in the context of VANETs. The potential for unauthorized tracking of vehicles, data breaches, and collecting sensitive information raises significant apprehensions among users. Privacy concerns can deter individuals from participating in VANETs, leading to reduced data availability and potentially hampering the effectiveness of threat detection systems. Robust privacy-preserving techniques, such as pseudonymization, encryption, and access control, are essential to safeguard user privacy while allowing for effective threat detection.

Scalability Challenges: As VANETs grow in size and complexity, scalability challenges become increasingly prominent. The sheer number of vehicles on the road and the volume of data generated can strain communication networks and the computational resources needed for real-time threat detection. Maintaining system responsiveness in the face of escalating demands requires innovative solutions. Edge computing, distributed architectures, and efficient data aggregation methods are potential strategies to optimize resource usage and ensure scalability.

Standardized Communication Protocols: The absence of standardized communication protocols in VANETs poses a significant hurdle. Standardized protocols are imperative to ensure interoperability and seamless communication between different vehicle manufacturers and infrastructure providers. The lack of such standards can hinder the deployment of dynamic threat detection systems, as disparate systems struggle to communicate effectively. Ongoing standardization efforts in the VANET field, such as IEEE 802.11p and ETSI ITS-G5, aim to define communication standards that enhance interoperability and security.

Security Threats: VANETs are not immune to security threats. The potential for malicious attacks, data manipulation, and denial-of-service attacks poses significant risks. Security vulnerabilities can compromise the integrity of threat detection systems, potentially leading to false positives or negatives and endangering road safety. Robust security measures, including

intrusion detection systems and encryption, are essential to safeguard VANETs against these threats.

Impact on Deployment: These challenges and open issues can profoundly impact deploying dynamic threat detection systems in VANETs. Failure to address privacy concerns may result in user reluctance to participate in VANETs, limiting the availability of critical data. Scalability challenges can strain resources and lead to system inefficiencies. The absence of standardized communication protocols can hinder interoperability, and security threats can compromise the effectiveness of threat detection systems. Addressing these issues is pivotal for ensuring the widespread adoption and effectiveness of dynamic threat detection within VANETs.

Research and Innovation: The road to overcoming these challenges and open issues lies in ongoing research and innovation. Researchers and practitioners are actively exploring solutions to enhance privacy preservation, scalability, security, and interoperability within VANETs. Collaborative efforts to develop and implement robust privacy-preserving techniques, scalability solutions, and standardized communication protocols are at the forefront of advancements in this field. The commitment to innovation remains paramount in making VANETs safer and more effective for all road users.

Solutions to Address Challenges and Open Issues

This section delves into solutions and strategies to address the challenges and open issues associated with enhancing road safety through dynamic threat detection in Vehicular Ad Hoc Networks (VANETs). Recognizing the significance of these solutions is crucial for the successful deployment and effectiveness of threat detection systems.

Privacy Concerns:

Privacy-Preserving Techniques: Privacy concerns in VANETs can deter user participation and compromise the effectiveness of threat detection systems. Privacy-preserving techniques such as pseudonymization, encryption, and access control mechanisms have been proposed and adopted to mitigate these concerns. These techniques protect sensitive information while allowing effective threat detection and communication.

Scalability Issues:

Scalability Solutions: The scalability challenges arising from the growing number of vehicles in VANETs and the high volume of data generated demand for innovative solutions. Edge computing, for instance, involves processing data closer to the data source, reducing latency and alleviating the burden on central infrastructure. Distributed architectures and efficient data aggregation methods further optimize resource usage, ensuring that threat detection systems can scale effectively with network size and data volume.

Lack of Standardized Protocols:

Standardization Efforts: The lack of standardized communication protocols in VANETs can hinder interoperability and the widespread adoption of dynamic threat detection systems. Ongoing standardization efforts, such as IEEE 802.11p and ETSI ITS-G5, aim to define communication

standards that enhance interoperability, security, and reliability within VANETs. Standardization ensures that vehicles from different manufacturers and infrastructure providers can communicate seamlessly, fostering the deployment of effective threat detection systems.

Security Threats:

Security Measures: Security threats, including malicious attacks and data manipulation, pose significant risks to VANETs and their threat detection systems. Robust security measures, such as encryption, digital signatures, and intrusion detection systems, are essential to safeguard the integrity and authenticity of messages exchanged within VANETs. These measures ensure that threat detection systems can operate in a secure environment, free from external interference.

Impact on Deployment:

Policy and Regulation: Addressing the challenges and open issues discussed herein requires technological solutions and policy and regulatory frameworks. Governments, industry stakeholders, and standardization bodies must collaborate to establish guidelines and regulations that promote the deployment and operation of secure and privacy-respecting VANETs. These policies provide a conducive environment for deploying dynamic threat detection systems effectively.

Research and Innovation:

Continued Research and Innovation: As we navigate the complexities of VANETs and their unique challenges, one thing becomes evident: the journey is ongoing. The rapid evolution of technology, the emergence of 5G connectivity, vehicle-to-everything (V2X) communication, and the Internet of Things (IoT) present promising avenues for further research and innovation. To continue improving road safety through dynamic threat detection in VANETs, we must remain committed to pushing the boundaries of knowledge and actively contributing to this transformative field.

CONCLUSION

In conclusion, our exploration of enhancing road safety through dynamic threat detection in Vehicular Ad Hoc Networks (VANETs) has shed light on the pressing need for innovative solutions in the realm of transportation and technology. The challenges we have uncovered, from privacy concerns and scalability issues to the lack of standardized protocols and security threats, underscore the complexities of ensuring safe and efficient roadways in our interconnected world. Our analysis has revealed that while these challenges pose significant hurdles, they also present opportunities for solutions. Privacy-preserving techniques, scalable edge computing, standardized communication protocols, and robust security measures have emerged as critical components in addressing these issues. By proactively seeking solutions, we pave the way for the widespread deployment of dynamic threat detection systems in VANETs.

REFERENCES

Amaouche, S., Guezzaz, A., Benkirane, S., Azrour, M., Khattak, S. B. A., Farman, H., & Nasralla, M. M. (2023). FSCB-IDS: Feature Selection and Minority Class Balancing for Attacks Detection in VANETs. *Applied Sciences*, *13*(13), 7488. https://doi.org/10.3390/app13137488

Azam, S., Bibi, M., Riaz, R., Rizvi, S. S., & Kwon, S. J. (2022). Collaborative Learning Based Sybil Attack Detection in Vehicular AD-HOC Networks (VANETS). *Sensors*, *22*(18). https://doi.org/10.3390/s22186934

Diallo, E. hacen, Dib, O., & Al Agha, K. (2022). A scalable blockchain-based scheme for traffic-related data sharing in VANETs. *Blockchain: Research and Applications*, *3*(3). https://doi.org/10.1016/j.bcra.2022.100087

Hussein, N. H., Yaw, C. T., Koh, S. P., Tiong, S. K., & Chong, K. H. (2022). A Comprehensive Survey on Vehicular Networking: Communications, Applications, Challenges, and Upcoming Research Directions. In *IEEE Access* (Vol. 10, pp. 86127–86180). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2022.3198656

Institute of Electrical and Electronics Engineers. Turkey Section., & Institute of Electrical and Electronics Engineers. (n.d.). *HORA 2020 : 2nd International Congress on Human-Computer Interaction, Optimization and Robotic Applications : proceedings : June 26-27, 2020, Turkey.*

Jan, S. A., Amin, N. U., Othman, M., Ali, M., Umar, A. I., & Basir, A. (2021). A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues. *IEEE Access*, *9*, 153701–153726. https://doi.org/10.1109/ACCESS.2021.3125521

Kong, X., Wang, K., Wang, S., Wang, X., Jiang, X., Guo, Y., Shen, G., Chen, X., & Ni, Q. (2021). Real-Time Mask Identification for COVID-19: An Edge-Computing-Based Deep Learning Framework. *IEEE Internet of Things Journal*, *8*(21), 15929–15938. https://doi.org/10.1109/JIOT.2021.3051844

Liang, J., Sheikh, M. S., & Wang, W. (2019). A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs). In *Sensors (Switzerland)* (Vol. 19, Issue 16). MDPI AG. https://doi.org/10.3390/s19163589

Malik, A., Khan, M. Z., Faisal, M., Khan, F., & Seo, J. T. (2022). An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs. *Sensors (Basel, Switzerland)*, *22*(5). https://doi.org/10.3390/s22051897

Manivannan, D., Moni, S. S., & Zeadally, S. (2020). Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). In *Vehicular Communications* (Vol. 25). Elsevier Inc. https://doi.org/10.1016/j.vehcom.2020.100247

Zhang, X., Zhou, M., Qiu, P., Huang, Y., & Li, J. (2019). Radar and vision fusion for the real-time obstacle detection and identification. *Industrial Robot*, *46*(3), 391–395. https://doi.org/10.1108/IR-06-2018-0113