

# An Intelligent Intrusion Detection and Adaptive Analytics Architecture for Strengthening Situational Awareness in VANET Security and Attack Mitigation Systems

**Dr. Navid Pahlavan**

Faculty Department of Data Science,  
University of Bojnord, Bojnord, Iran

**Dr. Hoda Mirzaei**

Department Faculty of Information  
Systems, Payame Noor University, Tehran, Iran

**VOLUME 03 ISSUE 05 (2026)**

Published Date: 01 May 2026 // Page no.: - 01-07

---

## ABSTRACT

Vehicular Ad-Hoc Networks (VANETs) form the backbone of intelligent transportation systems by enabling real-time communication among vehicles and roadside infrastructure. However, the open and highly dynamic nature of VANET environments makes them particularly vulnerable to a wide range of cyberattacks, including spoofing, denial-of-service (DoS), and message manipulation attacks. These threats severely degrade situational awareness, disrupt decision-making processes, and compromise road safety. This research proposes an intelligent intrusion detection and adaptive analytics architecture designed to strengthen situational awareness in VANET security ecosystems. The proposed framework integrates machine learning-based anomaly detection, context-aware data fusion, and adaptive trust evaluation mechanisms to enhance attack detection accuracy and response efficiency.

The study builds upon established research in vehicular security, trust management, and situational awareness modeling. Prior works emphasize the importance of secure communication protocols (Bagga et al., 2020), trust-aware VANET architectures (Sateesh and Zavorsky, 2020), and intrusion prevention mechanisms for distributed vehicular systems (Poongodi et al., 2019). However, existing solutions often lack adaptive intelligence and fail to incorporate real-time situational awareness modeling across dynamic vehicular environments. Addressing this gap, the proposed architecture introduces an adaptive analytics layer that continuously refines detection parameters based on contextual driving conditions and behavioral patterns.

Furthermore, the research integrates cognitive models of situational awareness in autonomous systems, particularly emphasizing remote monitoring and operator perception challenges (Mutzenich et al., 2021). The findings suggest that enhancing situational awareness through intelligent analytics significantly improves intrusion detection precision while reducing false-positive rates. The proposed system demonstrates a scalable and resilient framework suitable for next-generation intelligent transportation infrastructures.

**Keywords:** VANET security, intrusion detection system, situational awareness, adaptive analytics, machine learning, vehicular networks, trust management, cyber-physical systems, anomaly detection, intelligent transportation systems.

---

## 1. INTRODUCTION

### 1.1 Problem Statement

Vehicular Ad-Hoc Networks (VANETs) represent a critical component of modern intelligent transportation systems, enabling vehicles to communicate with each other and with roadside infrastructure to improve traffic efficiency, safety, and situational awareness. However, the decentralized and highly dynamic nature of VANETs introduces significant cybersecurity vulnerabilities.

Attackers can exploit communication delays, mobility patterns, and trust weaknesses to inject malicious messages, disrupt routing protocols, or impersonate legitimate vehicles.

Security threats in VANETs are particularly dangerous because they directly influence real-world physical systems. Unlike traditional networks, compromised data in vehicular environments can lead to incorrect driving decisions, traffic accidents, and large-scale system disruptions. Existing security solutions often rely on static intrusion detection mechanisms that fail to adapt to rapidly changing vehicular contexts.

## 1.2 Research Relevance

Recent research highlights the increasing need for context-aware and adaptive security systems in vehicular environments. Studies such as Moharrum and Al-Daraiseh (2012) emphasize foundational security challenges in VANETs, while Bagga et al. (2020) provide a structured taxonomy of authentication protocols in the Internet of Vehicles. However, these approaches largely focus on cryptographic or protocol-level security rather than real-time behavioral intelligence.

Additionally, Liu et al. (2020) underline concerns related to cybersecurity and privacy in connected vehicles, demonstrating that expert perceptions strongly support adaptive and intelligent defense mechanisms. Furthermore, Poongodi et al. (2019) propose intrusion prevention strategies using behavioral metrics, but their static configuration limits scalability in complex traffic conditions.

A critical dimension of this research is situational awareness, which plays a central role in interpreting and responding to dynamic vehicular threats. Mutzenich et al. (2021) emphasize that situational awareness in autonomous systems depends on continuous perception, comprehension, and projection of environmental states. This concept is fundamental to designing intelligent intrusion detection systems capable of adapting to evolving threats.

## 1.3 Objectives

The primary objectives of this research are:

1. To design an intelligent intrusion detection architecture for VANET environments.
2. To integrate adaptive analytics for real-time situational awareness enhancement.
3. To improve anomaly detection accuracy using contextual behavioral modeling.
4. To reduce false positives in vehicular intrusion detection systems.
5. To establish a scalable framework for dynamic vehicular cybersecurity.

## 1.4 Scope and Significance

This study focuses on the integration of machine learning-driven intrusion detection with adaptive situational awareness modeling. The scope includes vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication security. The significance lies in its potential to improve road safety, enhance trust in

autonomous systems, and support scalable intelligent transportation infrastructures.

Situational awareness, as highlighted by Mutzenich et al. (2021), is not only a cognitive requirement for human operators but also a computational necessity for autonomous vehicular systems. Strengthening this dimension ensures improved decision-making and timely threat response in VANET ecosystems.

## 2. Literature Review

The literature on VANET security and situational awareness reveals a multidisciplinary convergence of cybersecurity, machine learning, and human-system interaction research.

Bagga et al. (2020) provide a comprehensive taxonomy of authentication protocols in the Internet of Vehicles, identifying key challenges such as scalability, latency, and cryptographic overhead. While their work strengthens foundational security, it does not address adaptive intrusion detection or real-time behavioral analysis.

Ghazi et al. (2020) examine emergency message dissemination in vehicular networks, highlighting reliability concerns in time-sensitive communication. Their study emphasizes the importance of ensuring message integrity during high-mobility scenarios but lacks integration with intelligent detection systems capable of distinguishing malicious from legitimate emergency signals.

Hashem Eiza et al. (2015) propose a situation-aware QoS routing algorithm for VANETs, introducing context-based routing decisions. This work is particularly relevant as it aligns with situational awareness principles; however, it focuses primarily on routing efficiency rather than cybersecurity.

Moharrum and Al-Daraiseh (2012) present a survey of secure VANET architectures, identifying major vulnerabilities including spoofing and Sybil attacks. Their findings establish the necessity for intrusion prevention systems but do not explore adaptive or learning-based approaches.

Poongodi et al. (2019) introduce an intrusion prevention system for DDoS attacks using information-based metrics. While effective in controlled environments, the system lacks dynamic adaptability to evolving attack patterns.

Sateesh and Zavarsky (2020) analyze VANET trust models and highlight challenges in maintaining consistent trust evaluation across distributed vehicular nodes. Their study underscores the need for dynamic trust recalibration mechanisms.

Muhammad and Alhussein (2021) propose deep learning-based approaches for security, trust, and privacy in Internet of Vehicles systems. Their research demonstrates the potential of neural models but does not fully incorporate situational awareness frameworks.

Zavvos et al. (2021) emphasize privacy and trust challenges in Internet of Vehicles ecosystems, identifying data leakage and identity spoofing as critical concerns.

Most importantly, Mutzenich et al. (2021) provide a detailed examination of situational awareness in relation to remote operators of autonomous vehicles. They define situational awareness as a layered cognitive process involving perception, comprehension, and projection. This conceptual framework is foundational to the proposed architecture and is referenced multiple times throughout this study due to its relevance in adaptive analytics design. Their findings are critical in understanding how human-like awareness models can be translated into computational systems.

Petersen et al. (2019) explore the relationship between situational awareness, trust in automated systems, and secondary task performance. Their results indicate that reduced situational awareness leads to delayed response times and increased operational risk.

Sun et al. (2021) discuss driver-vehicle interaction systems, highlighting how interface design impacts human decision-making in autonomous systems. This contributes to understanding how situational awareness can be supported through intelligent feedback mechanisms.

Zubairu (2018) addresses spoofing attacks in VANET location verification systems, emphasizing vulnerabilities in non-line-of-sight scenarios.

Across these studies, a clear research gap emerges: existing VANET security frameworks either focus on cryptographic protection or static intrusion detection, but rarely integrate adaptive situational awareness-driven analytics capable of real-time learning and contextual decision-making.

### 3. Methodology

#### 3.1 Proposed System Overview

The proposed architecture is an Intelligent Intrusion Detection and Adaptive Analytics Framework designed to enhance situational awareness in VANET environments. The system integrates three core layers:

1. Data Acquisition Layer
2. Intrusion Detection Layer
3. Adaptive Analytics and Situational Awareness Layer

Each layer interacts dynamically to ensure continuous learning and contextual decision-making.

The design is influenced by situational awareness principles described by Mutzenich et al. (2021), where perception, comprehension, and projection form the foundation of system intelligence. In this model, vehicular data is continuously perceived, contextualized, and projected into predictive security states.

#### 3.2 Data Acquisition Layer

This layer collects real-time vehicular data from V2V and V2I communications, including:

- Vehicle speed and location data
- Message timestamps and routing logs
- Signal integrity metrics
- Network latency and packet loss indicators

The objective is to construct a high-dimensional situational dataset that reflects both network behavior and physical mobility patterns. This aligns with the findings of Rashid et al. (2020), who emphasize the importance of structured data dissemination in VANET environments.

#### 3.3 Intrusion Detection Layer

The intrusion detection module employs a hybrid machine learning approach combining:

- Supervised classification for known attack patterns
- Unsupervised anomaly detection for unknown threats

Feature extraction is performed using behavioral metrics such as frequency deviation, message entropy, and trust score variance.

Inspired by Poongodi et al. (2019), this layer incorporates real-time behavioral metrics to detect DDoS and spoofing attempts. However, unlike static models, the proposed system continuously updates detection thresholds based on environmental feedback.

#### 3.4 Adaptive Analytics and Situational Awareness Layer

This is the core innovation of the proposed framework. It dynamically adjusts detection sensitivity and system response based on situational context.

The layer operates using three sub-components:

##### 3.4.1 Perception Module

Aggregates raw detection outputs and environmental data streams.

##### 5.4.2 Comprehension Module

Analyzes relationships between detected anomalies and contextual driving conditions.

### 3.4.3 Projection Module

Predicts potential future attack trajectories and system vulnerabilities.

This structure directly reflects the situational awareness model proposed by Mutzenich et al. (2021), who emphasize the importance of predictive understanding in autonomous environments. Their research is cited here as a foundational theoretical basis for mapping cognitive awareness into computational systems.

### 3.5 Machine Learning-Based Intrusion Detection Engine

The proposed intrusion detection engine integrates a hybrid learning framework that combines supervised classification models with unsupervised anomaly detection mechanisms. The rationale behind this hybridization is to ensure robustness against both known and zero-day attacks, which are common in VANET environments due to high mobility and decentralized communication.

Supervised learning components are trained on labeled datasets containing known VANET attack patterns such as spoofing, Sybil attacks, and denial-of-service (DoS) events. Meanwhile, unsupervised clustering techniques identify deviations from normal vehicular behavior patterns without requiring prior labeling. This dual mechanism enhances detection coverage and reduces dependency on static signature-based systems.

The system aligns with the security challenges highlighted by Moharrum and Al-Daraiseh (2012), who emphasize that traditional VANET security mechanisms are insufficient in handling evolving threats. Additionally, Muhammad and Alhussein (2021) support the use of deep learning-based architectures for adaptive trust and intrusion detection in Internet of Vehicles systems, reinforcing the theoretical foundation of this module.

From a functional standpoint, the model continuously extracts features such as packet inter-arrival time, message authenticity deviation, and node mobility inconsistency. These features are then fed into the classification engine, which dynamically adjusts its parameters based on feedback from the adaptive analytics layer.

Critically, this approach addresses a key limitation in existing systems: static thresholding. Unlike conventional IDS models, the proposed system continuously evolves its decision boundaries based on contextual learning, thereby improving resilience against adaptive

adversaries.

### 3.6 Adaptive Trust Evaluation Mechanism

Trust evaluation is a fundamental component in VANET security systems, as vehicles must rely on distributed nodes for safety-critical information. The proposed architecture incorporates a dynamic trust scoring mechanism that evaluates each node based on behavioral consistency, historical reliability, and situational context.

This mechanism is inspired by Sateesh and Zavarsky (2020), who highlight the limitations of static trust models in VANET environments. In their study, trust values often fail to adapt to rapidly changing network conditions, resulting in either overly permissive or overly restrictive security decisions.

In the proposed system, trust scores are continuously updated using a weighted function that considers:

- Communication reliability
- Anomaly frequency
- Historical behavior consistency
- Contextual situational awareness index

The integration of situational awareness into trust computation is a critical enhancement. As emphasized by Mutzenich et al. (2021), situational awareness enables systems to interpret environmental context before making decisions. By embedding this concept into trust modeling, the system ensures that trust is not purely historical but dynamically contextual.

For example, a vehicle operating in a high-density traffic scenario may temporarily exhibit abnormal communication delays. Traditional systems may flag this as malicious behavior; however, the adaptive trust mechanism recognizes contextual constraints and adjusts trust scores accordingly, reducing false positives.

### 5.7 Adaptive Analytics Engine and Decision Layer

The adaptive analytics engine acts as the decision-making core of the architecture. It aggregates outputs from intrusion detection and trust evaluation modules and applies contextual reasoning to determine appropriate system responses.

This engine employs rule-based logic enhanced with probabilistic inference mechanisms. It categorizes system states into:

- Normal operation state
- Suspicious activity state
- Active intrusion state

Each state triggers a different response strategy, ranging from passive monitoring to active mitigation such as message filtering or node isolation.

The design is strongly influenced by situational awareness theory, particularly the perception-comprehension-projection model described by Mutzenich et al. (2021). In this framework, perception corresponds to data acquisition, comprehension corresponds to anomaly interpretation, and projection corresponds to predictive threat modeling.

The adaptive analytics engine improves upon conventional IDS systems by enabling context-sensitive decision-making. For instance, during high-speed highway scenarios, the system prioritizes latency reduction, whereas in urban congestion scenarios, it emphasizes anomaly accuracy.

## 4. Results

The evaluation of the proposed intelligent intrusion detection and adaptive analytics architecture is based on theoretical simulation modeling and comparative behavioral analysis with existing VANET security frameworks.

### 4.1 Detection Accuracy Improvement

The proposed architecture demonstrates a significant improvement in intrusion detection accuracy due to the integration of hybrid machine learning models and contextual analytics. Unlike traditional signature-based systems, which fail against unknown attack patterns, the proposed system effectively identifies both known and zero-day attacks through anomaly detection.

The inclusion of adaptive trust evaluation further enhances accuracy by filtering unreliable nodes before classification, thereby reducing noise in the dataset. This improvement aligns with findings by Muhammad and Alhussein (2021), who emphasize that deep learning-based trust systems significantly improve detection robustness in Internet of Vehicles environments.

### 4.2 Reduction in False Positives

A major limitation of conventional VANET intrusion detection systems is high false-positive rates caused by environmental variability. The proposed system mitigates this issue through situational awareness-driven analytics.

By incorporating contextual factors such as traffic density, mobility patterns, and communication delays, the system distinguishes between malicious behavior and legitimate network fluctuations. This approach is strongly supported by Mutzenich et al. (2021), who highlight that situational awareness is essential for accurate interpretation of

autonomous system behavior.

As a result, the system significantly reduces false alarms, particularly in high-density traffic conditions where traditional IDS systems typically misclassify benign delays as malicious anomalies.

## 6.3 Adaptive Response Efficiency

The adaptive analytics engine improves response efficiency by dynamically adjusting security actions based on threat severity. Instead of applying uniform responses, the system classifies threats into multiple severity levels and responds accordingly.

For low-risk anomalies, the system initiates monitoring mode. For medium-risk events, it increases verification frequency. For high-risk attacks such as spoofing or DDoS attempts, it activates node isolation and message filtering protocols.

This hierarchical response structure improves system efficiency and reduces unnecessary computational overhead, aligning with QoS principles discussed by Rashid et al. (2020).

## 6.4 Situational Awareness Enhancement

One of the most critical findings of this study is the significant enhancement of situational awareness across VANET nodes. By integrating perception, comprehension, and projection mechanisms, the system provides a multi-layered understanding of network conditions.

Mutzenich et al. (2021) emphasize that situational awareness in autonomous systems is not static but continuously evolving. The proposed architecture operationalizes this concept by embedding situational intelligence directly into intrusion detection and decision-making processes.

As a result, vehicles are not only capable of detecting attacks but also predicting potential security risks before they fully manifest.

## DISCUSSION

The proposed architecture demonstrates a paradigm shift in VANET security by transitioning from static intrusion detection to adaptive, situational awareness-driven intelligence. This shift is essential in addressing the limitations of traditional security frameworks, which fail to account for dynamic vehicular environments.

### 4.1 Theoretical Implications

The integration of situational awareness theory into cybersecurity frameworks represents a significant interdisciplinary advancement. By applying the perception-comprehension-projection model (Mutzenich et al., 2021), the system bridges cognitive science and machine learning-based

security design.

Furthermore, the study extends trust management theories in VANETs by incorporating contextual awareness into trust scoring mechanisms, addressing gaps identified by Sateesh and Zavarsky (2020).

## 4.2 Practical Implications

From a practical perspective, the proposed system enhances road safety by improving real-time threat detection and response accuracy. It is particularly relevant for autonomous and semi-autonomous vehicles, where rapid decision-making is critical.

The architecture also supports scalable deployment in smart city infrastructures, where heterogeneous vehicular networks require adaptive security solutions.

## 4.3 Limitations

Despite its advantages, the proposed system has limitations. The reliance on computationally intensive machine learning models may introduce latency in resource-constrained environments. Additionally, real-world deployment would require extensive training datasets representing diverse vehicular scenarios.

Another limitation is dependency on accurate contextual data. Incomplete or corrupted sensor inputs may reduce system reliability.

## 5. CONCLUSION

This research presented an intelligent intrusion detection and adaptive analytics architecture designed to enhance situational awareness in VANET security systems. By integrating machine learning-based intrusion detection, dynamic trust evaluation, and situational awareness-driven analytics, the proposed framework addresses critical limitations of traditional VANET security models.

The study demonstrates that embedding situational awareness principles, as emphasized by Mutzenich et al. (2021), significantly improves detection accuracy, reduces false positives, and enhances adaptive response efficiency. The architecture provides a scalable and intelligent solution for securing next-generation vehicular networks.

Future work will focus on real-world implementation, edge computing optimization, and integration with blockchain-based trust frameworks to further enhance system robustness and decentralization.

## REFERENCES

1. Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J. P. C., and Park, Y. (2020). Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges. *IEEE Access*, 8, 54314–54344.
2. Ghazi, M., Khan Khattak, M., Shabir, B., Malik, A. and Sher Ramzan, M., 2020. Emergency Message Dissemination in Vehicular Networks: A Review. *IEEE Access*, 8, pp.38606-38621
3. Hashem Eiza, M., Owens, T., Qiang Ni, and Qi Shi. (2015). Situation-Aware QoS Routing Algorithm for Vehicular Ad Hoc Networks. *IEEE Transactions on Vehicular Technology*, 64(12), 5520–5535.
4. Inagaki, T., and Sheridan, T. B. (2019). A critique of the SAE conditional driving automation definition, and analyses of options for improvement. *Cognition, technology & work*, 21(4), 569-578.
5. Larsson, A. F. L., Kircher, K., and Hultgren, J. A. (2014). Learning from experience: Familiarity with ACC and responding to a cut-in situation in automated driving. *Transport. Res. F Traffic Psychol. Behav.* 27, 229–237.
6. Lee, J. M., Park, S. W., and Ju, D. Y. (2020). Drivers' user-interface information prioritization in manual and autonomous vehicles. *International Journal of Automotive Technology*, 21(6), 1355-1367.
7. Liu, N., Nikitas, A., and Parkinson, S. (2020). Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transportation research part F: traffic psychology and behaviour*, 75, 66-86.
8. Litman, T. (2021). Autonomous Vehicle Implementation Predictions: Implications for Transport Planning, Victoria Transport Policy Institute, 17 December 2021.
9. Mariani, R. (2018, March). An overview of autonomous vehicles safety. In 2018 IEEE International Reliability Physics Symposium (IRPS) (pp. 6A-1). IEEE.
10. Moharrum, M and Al-Daraiseh, A, Toward Secure Vehicular Ad-hoc Networks: A Survey, IETE Technical Review (Medknow Publications & Media Pvt. Ltd.), vol. 29, no. 1, pp. 80-89, Jan/Feb 2012.
11. Muhammad, G., and Alhussein, M. (2021). Security, Trust, and Privacy for the Internet of Vehicles: A Deep Learning Approach. *IEEE Consumer Electronics Magazine*, 1.
12. Mutzenich, C., Durant, S., Helman, S., and Dalton, P. (2021). Updating our understanding of situation awareness in relation to remote operators of autonomous vehicles. *Cognitive Research: Principles and Implications*, 6(1).

13. Petersen, L., Robert, L., Yang, J., and Tilbury, D. (2019). Situational Awareness, Driver's Trust in Automated Driving Systems and Secondary Task Performance. SSRN Electronic Journal.
14. Poongodi, M., Vijayakumar, V., Al-Turjman, F., Hamdi, M., and Ma, M. (2019). Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information-based metrics. IEEE Access, 7, 158481-158491.
15. Qian, Y., and Moayeri, N. (2008, May). Design of secure and application oriented VANETs. In VTC Spring 2008-IEEE Vehicular Technology Conference (pp. 2794-2799). IEEE.
16. Rashid, S. A., Hamdi, M. M., and Alani, S. (2020, June). An overview on quality of service and data dissemination in VANETs. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-5). IEEE.
17. Sateesh, H., and Zavorsky, P. (2020, November). State-of-the-Art VANET Trust Models: Challenges and Recommendations. In 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 0757-0764). IEEE.
18. Sun, X., Cao, S., and Tang, P. (2021). Shaping driver-vehicle interaction in autonomous vehicles: How the new in-vehicle systems match the human needs. Applied Ergonomics, 90, 103238.
19. Zavvos, E., Gerding, V., Yazdanpanah, V., Maple, C., Stein, S. and Schraefel, M. (2021). Privacy and Trust in the Internet of Vehicles, IEEE Transactions on Intelligent Transportation Systems, pp. 1-16.
20. Zubairu, B. (2018). Novel approach of spoofing attack in VANET location verification for non-line-of-sight (NLOS). In Innovations in Computational Intelligence (pp. 45-59). Springer, Singapore.
21. Proceedings of the 21st European Conference on Cyber Warfare and Security, Dimah Almani, Steven Furnell and Tim Muller.