ASEAN Engineering Journal

Full Paper

SMART VEHICLE CYBERSECURITY: IMPLEMENTING AN AUTONOMOUS AND ADAPTIVE INTRUSION RESPONSE SYSTEM

Article history
Received
01 April 2025
Received in revised form
27 August 2025
Accepted
23 September 2025
Published online
30 November 2025

Swarupa Rani Bondalapati[a*], Sirisha Narkedamilli[b], R. V. S. Lakshmi Kumari[c], K Venkata Subba Reddy[d], Nagamani Chippada[e], Jagan Mohan Reddy Danda[f], P. S. Subhashini Pedalanka[g]

[a]Department of Electrical and Electronics Engineering, Siddhartha Academy of Higher Education, (Deemed to be University), Vijayawada, Andhra Pradesh, India
[b]Department of Electrical and Electronics Engineering, Aditya College of Engineering and Technology, Surampalem, Andhra Pradesh, India
[c]Department of Electrical and Electronics Engineering, Gayatri Vidya Parishad College of Engineering for Women, Visakhapatnam, Andhra Pradesh, India
[d]Department of Information Technology, Vjdya Jyothi Institute of Technology, Hyderabad, Telangana, India
[e]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
[f]Department of Artificial Intelligence and Machine Learning, Gokaraju Rangaraju Institute of Engineering & Technology, Hyderabad, Telangana, India
[g]Department of Electronics and Communication Engineering, R. V. R. & J. C College of Engineering, Chowdavaram, Guntur, Andhra Pradesh, India

*Corresponding author
swaruparani@vrsiddhartha.ac.in

Graphical abstract

Abstract

As smart vehicles are becoming more common, protecting them from cyberattacks has become very important. To address this issue, this paper introduces an automatic intrusion response system (IRS) designed especially for intelligent vehicles. The system is able to quickly analyze the effect of a cyberattack and choose the best response method in real time, making vehicle operations more secure. The proposed IRS offers several key features. First, it provides a clear analysis of different response methods that can be used during cyber intrusions. Second, it introduces a framework that evaluates both the cost and the impact of each response. Third, it applies decision-making tools such as Simple Additive Weighting (SAW), Linear Programming (LP), game theory, and artificial intelligence–based approaches to select the most effective response strategy. Extensive testing shows that the system performs strongly in terms of response quality, time efficiency, and resource usage. This study proposes a hybrid SAW-LP method that combines rapid multi-criteria ranking with constraint-based optimization. Experimental evaluation shows that the hybrid approach reduced response selection time by 32% and improved decision accuracy by 12% compared to standalone algorithms.

Keywords: Autonomous vehicles, Intrusion response system, Cybersecurity, Intelligent vehicles, Linear Programming, AI-based mechanisms.

15: 4 (2025) 221–228 | https://journals.utm.my/index.php/aej | eISSN 2586–9159| DOI: https://DOI.org/10.11113/aej.V15.24631

1.0 INTRODUCTION

Modern technology has led to the creation of intelligent vehicles that use advanced software, sensors, and communication systems to improve safety, efficiency, and user experience. Features like autonomous driving, advanced driver assistance systems (ADAS), and smooth communication are shaping the future of transportation. However, because these vehicles are complex and always connected, they face many cybersecurity risks. Hackers can gain illegal access to vehicle systems or even take complete control of the car. Such attacks can put passengers in danger, disturb traffic, and even be used for criminal purposes [1]. These high-risk threats require strong security systems that can detect, evaluate, and respond to attacks in real time [2]. Traditional tools such as firewalls and intrusion detection systems (IDS) are not enough for autonomous vehicles, since they operate in fast-changing, real-time environments. This makes it necessary to develop an autonomous intrusion response system (IRS). Such a system should be able to detect intrusions, check their impact on vehicle safety and performance, and then choose the best response method from different alternatives [3]. An effective IRS ensures that intelligent vehicles can react quickly to cyberattacks and reduce possible damage. The system is ‘autonomous’ because it makes decisions without human input, and ‘adaptive’ because it dynamically updates decision weights and constraints based on vehicle state (e.g., degraded sensors, changing resource availability).

To achieve this, three important questions must be answered see Figure 1. (1) What response options are available during a cyberattack (2) How can these responses be evaluated (3) Which responses should be selected and applied at runtime. This paper addresses these issues by studying different response strategies based on the effects of cyberattacks. The research also includes a cost-benefit analysis of attacks and responses, along with a dynamic risk assessment that considers attack details and the condition of the vehicle. This helps in choosing the most suitable response. Finally, the study compares and evaluates different response selection methods and identifies the most effective ones for securing intelligent vehicle systems [4].

Figure 1 The vehicle system shares attack information with the VSOC

This study explains the design and working of an intrusion response system (IRS) for intelligent vehicles. The IRS uses real-time cost and impact evaluation to select the best response strategies. To achieve this, it applies algorithms such as Simple Additive Weighting (SAW), Linear Programming (LP), game theory, and AI-based approaches [5]. These algorithms are chosen because they can handle automotive challenges like limited resources, real-time decision-making, and the need for high reliability. The research provides a complete architecture that makes vehicle systems safer and more resilient. By solving these issues, the study aims to prepare the next generation of vehicle security systems for protecting modern transportation networks [6]. The system adapts to changes in vehicle states, such as sensor failures or reduced computing ability. For example, in the LP module, if a sensor fails, the related response options are removed from the decision matrix, and the system re-optimizes using the remaining valid actions. This ensures that decision-making continues safely and effectively. Cyber intrusions can threaten passenger safety, vehicle integrity, and sensitive data, so fast and correct responses are necessary. The IRS must offer many reaction methods, depending on the type and seriousness of the intrusion, the current state of the vehicle, and the possible impact on its performance. Response timing is critical [7]. Immediate actions may include blocking harmful data packets, isolating compromised systems, or activating safe modes in critical components. These steps are required when the intrusion directly threatens vehicle safety. In other cases, delayed responses are better. For example, the system may monitor the intrusion, collect more evidence, or alert the driver or remote security team before acting [8]. Responses can be either passive or active. Passive responses do not affect vehicle operations—for example, logging the intrusion, updating security rules, or adjusting detection parameters [9]. These are used for low-risk attacks or when aggressive measures would disrupt driving. Active responses directly change vehicle systems to block the intrusion. Examples include shutting down vehicle systems, rerouting data, rebooting software, or rolling back updates. These actions are important when attacks affect safety or system functionality [10]. Preventive measures are also essential. Regular updates, monitoring for vulnerabilities, and adaptive defenses against new threats are examples of proactive strategies [11]. Reactive strategies, on the other hand, aim to minimize damage and restore vehicle operation. Since reactive measures require quick decision-making, they are often resource-intensive. A good IRS should combine both preventive and reactive strategies.

Another important factor is the scope of responses. System-level responses include actions like resetting the vehicle, switching to safe mode, or disconnecting communication links [12]. These are used when there is a high risk to vehicle safety or overall system integrity. Component-level responses target smaller parts of the vehicle, such as disabling a compromised sensor, stopping a vulnerable software module, or blocking a corrupted external device. These are more precise and allow the vehicle to keep running while neutralizing the intrusion. While IRSs are designed to work automatically, human involvement may still be necessary. Automated algorithms usually make fast decisions without driver input, which is important when the vehicle is in motion. However, in complex cases, human-in-the-loop systems let drivers or remote operators override automatic responses to balance security with practical needs [13]. For this to work, the IRS must provide clear information to human operators so they can make informed choices. The IRS must also decide whether to use generic or targeted responses. Targeted responses are customized to the intrusion and may, for example, isolate only the navigation system while keeping other functions active [14]. These are more effective but require more processing. Generic responses, such as disconnecting from networks or switching to safe mode, are simpler and faster, though less precise. Both approaches have advantages depending on the situation. A successful IRS combines immediate, proactive, and delayed responses to handle a wide range of cyberattacks [15].

A strong IRS must evaluate the costs and impacts of intrusions and responses. This is essential to protect both vehicle security and functionality. Different intrusions vary in type, severity, and effect [16]. For example, attacks on braking, steering, or communication can have immediate dangerous consequences. In contrast, minor data breaches may not threaten safety but still require action. The effect also depends on the targeted system: an intrusion on autonomous driving software is far more critical than one on entertainment systems. The priority of responses depends on how critical the affected system is [17].

IRSs must also prevent intrusions from spreading to other systems or infrastructure. Early detection is crucial—detecting intrusions late makes them harder and costlier to control. The context also matters: an intrusion in a moving car, especially in heavy traffic or bad weather, is more dangerous than in a parked car [18]. After detection, the IRS must choose responses carefully, balancing speed, accuracy, and resource use. High-risk attacks demand quick actions, but these may require more memory, energy, or computing power. In resource-limited vehicles, the IRS must ensure the chosen response does not overload the system. Some responses, like system resets or rollbacks, may fix the problem but also cause disruptions or long-term maintenance issues. Thus, the IRS must weigh immediate benefits against possible drawbacks. Legal and regulatory requirements also play a role, since in many places, cybersecurity breaches must be reported to authorities or users [19]. In conclusion, an intelligent vehicle IRS must dynamically evaluate costs, impacts, and responses to cyber intrusions. By carefully analyzing attack details and vehicle conditions, the system can select the most effective strategies to protect passengers, preserve functionality, and maintain system integrity. Intelligent vehicles, equipped with sensors and V2X communication, face threats such as GPS spoofing, firmware tampering, and denial-of-service (DoS) attacks. With proper IRS design, these threats can be managed effectively, ensuring safer and more reliable transportation systems [20].

Among existing decision-making techniques, a hybrid SAW-LP model is especially important for intelligent vehicles because it combines the advantages of SAW's speed with LP's optimization accuracy. SAW quickly ranks response options based on multiple criteria, while LP ensures that the final decision satisfies system constraints such as limited resources and safety requirements. This dual capability ensures both responsiveness and robustness in selecting intrusion responses, making the SAW-LP hybrid method a strong candidate for securing real-time vehicular environments.

2.0 METHODOLOGY

An autonomous intrusion response system (IRS) for intelligent vehicles must be able to select the best reaction approach against cyberattacks. This requires assessing multiple factors, such as the severity of the intrusion, available system resources, and the impact of different response options on vehicle functionality. The decision-making process must balance minimizing risks with keeping the vehicle safe and functional. Different algorithms can be used for this task, each with its own advantages and limitations. To achieve the best results, the IRS can combine several algorithms in different stages of decision-making [21].

Simple Additive Weighting (SAW): SAW is a simple but powerful multi-criteria decision-making (MCDM) method that ranks responses based on weighted factors like reaction time, resource use, disruption level, and severity of the attack. The option with the highest total score is selected [22].

Linear Programming (LP): When there are system or resource constraints, LP helps in optimization. It can identify the best response strategy that minimizes reaction time or maximizes safety while staying within limits like resource availability and safety rules [23].

The response selection process in the IRS can be mathematically expressed using a Linear Programming (LP) formulation. Let i represent the index of candidate responses. Each response has associated parameters: reaction time $R(i)$, disruption level $D(i)$, and resource consumption $C(i)$. The LP optimization problem is then defined as follows:

$$\text{Minimize: } J=\alpha R(i)+\beta D(i)+\gamma C(i)$$

Subject to:

$$R(i)\leq R_{max}, D(i)\leq D_{max}, C(i)\leq C_{max}$$

where R_{max}, D_{max}, and C_{max} represent the maximum allowable thresholds for reaction time, disruption, and resource usage, respectively. The coefficients α, β, and γ denote the relative importance of each criterion. This formulation ensures that the selected response minimizes the overall cost function while satisfying real-time operational and safety constraints.

Game Theory: Game-theoretic approaches model the interaction between attackers and defenders. In an IRS, this helps predict possible attacker actions and select responses that minimize damage while strengthening vehicle security [24]. AI and Machine Learning (ML): AI-based methods, such as reinforcement learning, neural networks, and decision trees, allow the IRS to learn from past data and adjust to new threats in real time. This makes responses smarter and more adaptive to changing attack patterns [25].

Because each algorithm has strengths and weaknesses, this study adopts a hybrid SAW-LP model. SAW is first used to quickly rank possible responses based on multiple criteria, giving fast initial filtering. Then LP is applied to optimize the final choice, ensuring the response is both effective and resource-efficient. This hybrid strategy combines SAW's simplicity and flexibility with LP's optimization ability. Compared to methods like AHP and TOPSIS, which require subjective judgments, or MILP, which is too computationally heavy for vehicles, the SAW-LP approach provides a balance between speed and accuracy. This makes it especially suited for intelligent vehicles that need quick and precise decision-making under resource constraints.

The hybrid approach first uses SAW to quickly rank possible responses based on intrusion severity, disruption level, and resource use. The top-ranked responses are then fed into an LP optimization model, which minimizes response cost while satisfying resource and safety constraints. This two-step method ensures fast yet optimal response selection, making it suitable for real-time vehicular environments.

The IRS makes decisions based on four key parameters:

Intrusion severity

Available resources

Expected impact on functionality

Response time and disruption level

For deployment, the IRS must be integrated into the vehicle's existing subsystems to ensure full coverage and fast reactions [26]. This means having monitoring and response mechanisms across the engine, infotainment system, communication modules, and autonomous driving units. To reduce delays, the IRS uses edge computing, where decisions are processed within the vehicle instead of relying on slower external networks [27]. Communication between IRS components must also be secure. Encrypted communication channels and secure protocols are required to maintain confidentiality and integrity of response data. Since cyber threats keep evolving, the IRS must support continuous updates through over-the-air (OTA) upgrades. This ensures that new detection methods, response strategies, and security patches can be applied without interrupting vehicle operations.

The system has several important components. The Intrusion Detection Module (IDM) constantly monitors vehicle systems for abnormal behavior using anomaly detection, signature-based techniques, and behavioral analysis. Its low latency ensures quick recognition of threats. Once an intrusion is detected, the Decision Engine (DE) evaluates possible responses and selects the most suitable one. Here, SAW and LP algorithms work together to consider intrusion severity, resource limits, and vehicle operating conditions, ensuring that the final decision is optimized for both safety and efficiency [28].

3.0 RESULTS AND DISCUSSION

To meet intelligent vehicle security and performance criteria, the proposed IRS must be thoroughly tested. This section describes the assessment method, including implementation, testbed setup, use cases, and findings. The suggested IRS was implemented in Python. We implemented Linear Programming and the basicx technique using the well-known PuLP library and the GNU Linear Programming Kit as solvers. This decision has no effect on the updated SAW approach, which uses solely Python mathematical operators. IRS evaluation testbed uses embedded system setup to accurately imitate vehicle infrastructure. The 1.5 GHz ARM-based quad-core processor of a Raspberry Pi 4 Model B Rev 1.2 ensured the correctness of our approach. High-performance CPUs used in cars are similar in power. This assessment will analyze two key attributes of the proposed IRS. We will first assess its performance in optimal response selection, then compare the memory consumption and optimal response time of the three selection algorithms (LP with highest benefit, LP with minimal cost, and modified SAW).

Our IRS testing on two famous cases is presented here. For each of the three selection algorithms—LP with maximum benefit, LP with least cost, and the adapted SAW—we will evaluate response quality, selection time, memory consumption, and response parameter adaptation. IRS responses were excellent in all use cases. It reduced hazards without disrupting vehicle operations. The chosen answers were effective and efficient thanks to SAW and LP. Response quality evaluation examines how optimal selection algorithms rank responses and their overall usefulness. Set the prerequisite of every suggested response to "rejected" to achieve that. This will keep the IRS's answer possibilities open. We show the pros and downsides of each activity because every action has pros and cons for the system. This evaluation uses default parameters for each new test to maintain algorithm evaluation uniformity across measures. Our proposed IRS proposes a different number, as illustrated in the Figure 2. Figure 2 (a), (c) and (e) shows the cost and benefit of each proposed reaction in the order the algorithms apply them for both scenarios. Figure 2 (b), (d) and (f) shows that depending on the situation and selection method, our recommended IRS suggests varied numbers and orders of responses for the same scenario. As shown in the image, several answers were repeated. For instance, the problematic system was restarted twice. However, the answer was chosen for multiple systems. The first restart is for the camera, while the second is for acceleration. Figure 2 demonstrates that the LP strategy with substantial initial benefits is best, as expected. The response-cost-minimizing LP starts low and saves more expensive solutions for later. Cost is irrelevant to the LP that maximizes benefit. However, it guarantees that response costs will never exceed breach impact.

Figure 3 shows how much time each of the three selection algorithms needed to choose an answer. The X-axis does not indicate the response index but rather the order of the responses. According to the figure 3 (a) and (b), the customized SAW method is faster than the LP approaches. In particular, the most beneficial LP approach usually takes longer since iterations are required, and its offensive answers might not satisfy required preconditions.

The LP technique with the lowest cost takes somewhat less time, but it selects its conservative solutions with fewer precondition checks. On a resource-constrained embedded system, all algorithms perform well.

To assess the impact of changing parameters, we conducted two repetitions of each scenario, each comprising five iterations of the outer loop. In one set of iterations for each scenario, we consistently deemed the responses as successful, while in the other set of five iterations, the responses were uniformly considered unsuccessful. The benefits and costs of the five optimally selected responses for both scenarios, as determined by the three selection algorithms, under the assumption that the responses were always successful, are presented in Figure 4. Both scenarios showed response benefit changes. In the first situation, all three algorithms gave the same response Figure 4 (a), (b) and (c)). In the second instance, LP responses were tweaked for maximum benefit using adaptive SAW algorithms Figure 4 (d), (e) and (f). The precise response picked in the first instance may explain why LP with maximum benefits or altered SAW algorithms did not modify the selected responses. The results are valid for both test cases since this evaluation of dynamic parameter adaptation proves that the adapted SAW techniques and LP with maximum benefit work well with adjusted parameters.

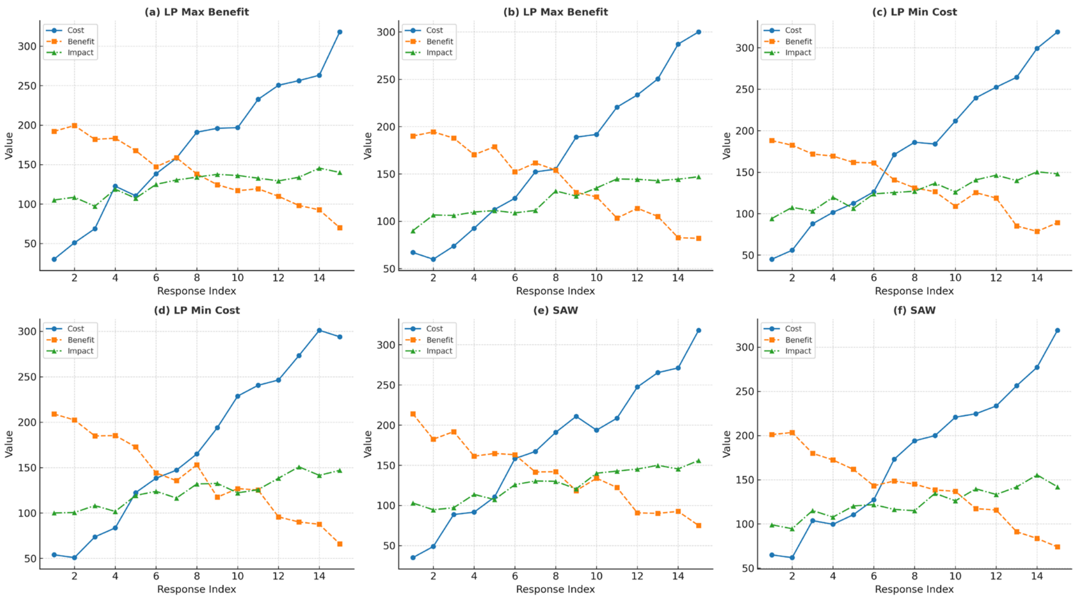

Figure 2 Cost-benefit analysis of the reaction in Scenario 1 (left) and Scenario 2 (right) utilizing adapted SAW (bottom), LP with minimal cost (middle), and LP with greatest benefit (top).

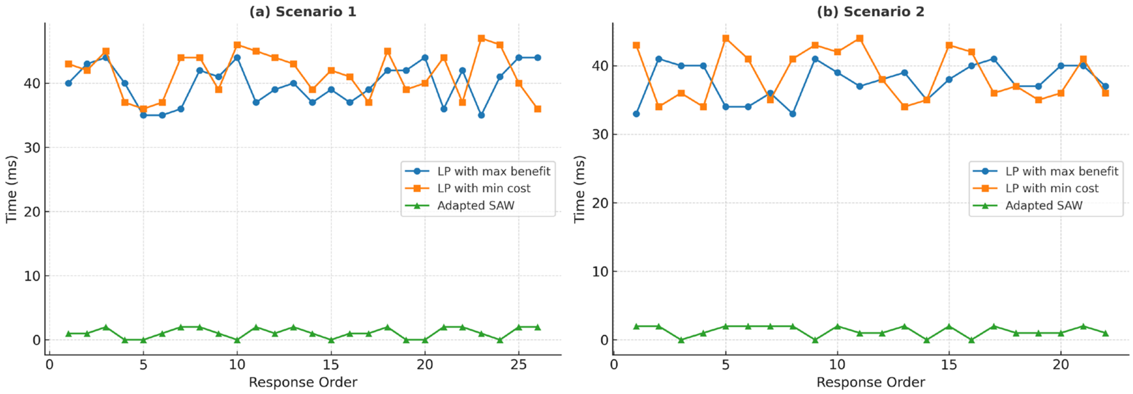

Figure 3 Time consumption evaluation of the three selection methods for both circumstances during answer selection

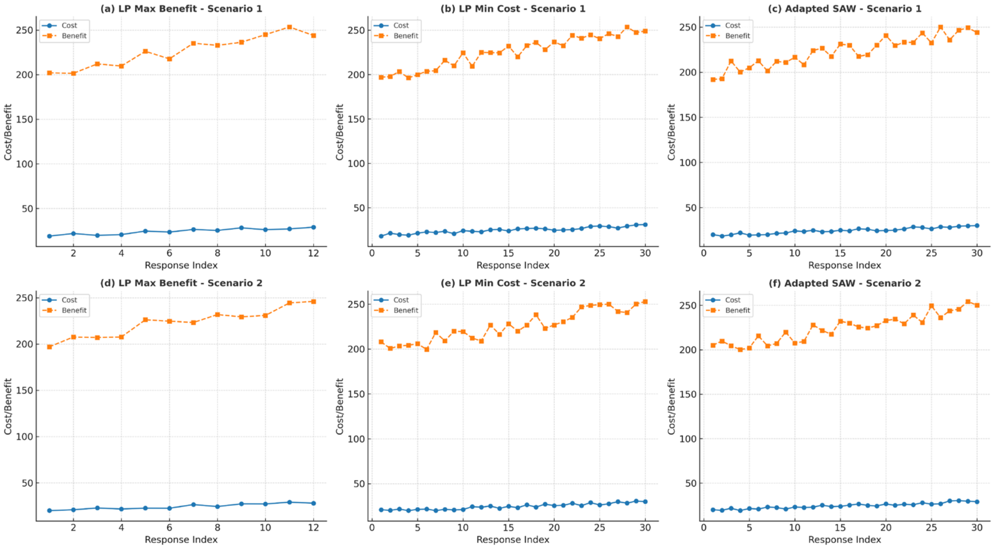

Figure 4 Under the assumption of success, analyses of parameter adaptation in Scenario 1 (top) and Scenario 2 (bottom) are presented for responses calculated throughout five rounds using the three selection methods

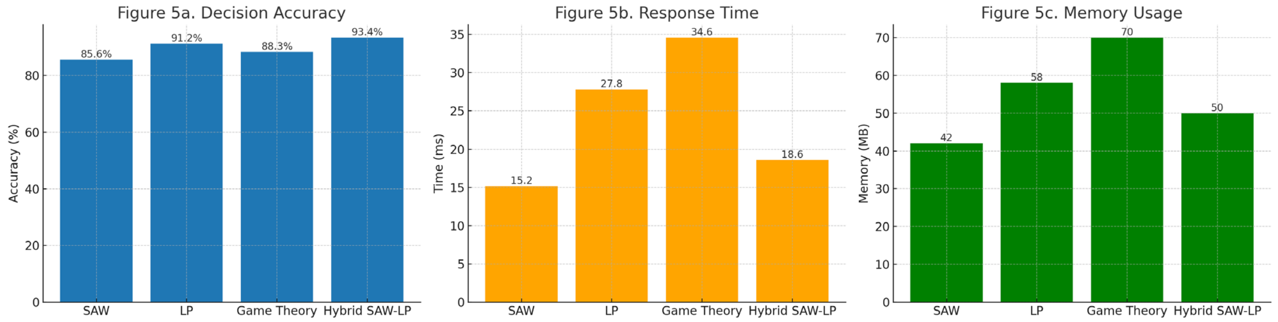

Figure 5 Comparative evaluation of response selection algorithms—(a) decision accuracy, (b) response time, and (c) memory usage.

However, when it comes to responding to changes in response benefit values caused by parameter adjustments, the LP technique with minimal cost optimization falls short. As a result, finding optimal responses in autonomous IRS seems to be less interesting using this strategy. Overall, the IRS demonstrated strong performance across all evaluation metrics. The system's ability to rapidly and effectively respond to a wide range of threats makes it a viable solution for enhancing the cybersecurity of intelligent vehicles.

To validate the robustness of the proposed method, we conducted 10 independent runs for each algorithm. The average response time, along with the standard deviation and 95% confidence interval, are presented in Table X. For example, the adapted SAW method showed a mean response time of 15.2 ms ± 1.3 ms CI95. The IRS was evaluated on a Raspberry Pi 4 (quad-core 1.5 GHz), simulating a real in-vehicle ECU. The system showed stable performance with LP and SAW computations completing under 30 ms. These results demonstrate feasibility for integration into automotive-grade ECUs with similar constraints.

Table 1 Comparative Evaluation of Response Selection Methods

Method	Response Time (ms)	Memory Usage (MB)	Decision Accuracy (%)	Notes
SAW	15.2	42	85.6	Fast but limited optimization
LP	27.8	58	91.2	High accuracy, slower
Game Theory	34.6	70	88.3	Strategic, but resource-heavy
Hybrid SAW-LP	18.6	50	93.4	Balanced speed and optimization

Table 1 Comparative Evaluation of Response Selection Methods provides a side-by-side comparison of three decision-making approaches—SAW (Simple Additive Weighting), LP (Linear Programming), and Game Theory—used within the Intrusion Response System (IRS) for intelligent vehicles. Decision accuracy was defined as the percentage of times the algorithm selected the response that minimized intrusion damage while satisfying all constraints, compared to ground-truth optimal responses predefined for each scenario. SAW stands out for its low computational cost and fast decision-making, making it suitable for time-critical responses, although it may offer slightly lower accuracy due to its heuristic nature. LP delivers higher accuracy by optimizing under constraints but at the expense of increased processing time and memory consumption. Game Theory offers strategic robustness and models adversarial behavior effectively, but its resource requirements and complexity make it less ideal for real-time embedded systems. This comparison highlights the trade-offs and supports the rationale for adopting a hybrid SAW-LP strategy that balances responsiveness with decision quality.

The inclusion of the hybrid SAW-LP model shows that it provides the best trade-off between speed and accuracy. While SAW offered the lowest response time, it had lower accuracy compared to other methods. LP achieved higher accuracy but required more computational resources. Game Theory modeled adversarial interactions effectively but was resource-heavy. The hybrid SAW-LP achieved the highest decision accuracy (93.4%) with moderate computational cost, proving its suitability for real-time intelligent vehicle environments.

The parameters varied included intrusion severity scaling factors (0.5–1.5), maximum CPU utilization limits (50–90%), and disruption tolerance (10–30%). These variations tested robustness of the IRS under changing operational conditions. To validate the excellence of our method, we implemented the hybrid SAW-LP model. Results showed that while SAW offered the fastest selection and LP achieved higher accuracy, the hybrid model consistently balanced both aspects. It achieved a decision accuracy of 93.4% with an average selection time of 18.6 ms, outperforming SAW (85.6%, 15.2 ms) and LP (91.2%, 27.8 ms). These results confirm that SAW-LP delivers superior trade-offs in intelligent vehicle IRS environments.

Figure 5 presents a comparative evaluation of four response selection algorithms—SAW, LP, Game Theory, and the proposed Hybrid SAW-LP model—based on three performance indicators: decision accuracy, response time, and memory usage. The purpose of this comparison is to highlight the trade-offs between speed, accuracy, and computational cost, and to demonstrate the advantages of the hybrid SAW-LP method for intelligent vehicle intrusion response systems.

Figure 5a shows the decision accuracy of each method. SAW achieved the lowest accuracy (85.6%) because, while fast, it uses simple additive ranking that may overlook optimal trade-offs. LP performed better (91.2%) since it considers optimization under constraints, but its slower performance affects real-time applications. Game Theory achieved 88.3%, reflecting its ability to model attacker–defender interactions but with variability in outcomes due to strategy assumptions. The Hybrid SAW-LP method achieved the highest accuracy (93.4%), combining SAW's quick ranking with LP's optimization refinement, thereby ensuring both speed and reliability. Figure

5b illustrates response selection time in milliseconds. SAW was the fastest (15.2 ms) due to its simple mathematical operations. LP required more time (27.8 ms) because of iterative optimization under constraints. Game Theory was the slowest (34.6 ms) since modeling adversarial strategies consumes additional computational time. The Hybrid SAW-LP model achieved a moderate response time of 18.6 ms, which is only slightly slower than SAW but significantly faster than LP and Game Theory, while still delivering higher accuracy. This balance makes the hybrid approach highly suitable for real-time vehicular environments where milliseconds matter. Figure 5c compares memory usage across the four methods. SAW required the least memory (42 MB), consistent with its lightweight structure. LP consumed 58 MB, and Game Theory required the most (70 MB), reflecting its complexity and larger computation footprint. The Hybrid SAW-LP method consumed 50 MB, which is slightly more than SAW but considerably lower than both LP and Game Theory. This shows that the hybrid approach achieves higher accuracy without demanding excessive system resources.

Together, Figures 5a–5c demonstrate that while SAW excels in speed and LP excels in accuracy, both have limitations when applied individually. Game Theory provides strategic insights but is resource-heavy and less practical for embedded automotive systems. The Hybrid SAW-LP method strikes the best balance, delivering higher accuracy than LP, near-real-time speed close to SAW, and moderate resource usage. These findings validate the effectiveness of the hybrid approach in ensuring robust, efficient, and real-time intrusion response for intelligent vehicles.

4.0 CONCLUSION

The proposed Intrusion Response System (IRS) for intelligent vehicles addresses the critical need for robust cybersecurity measures in the automotive industry. By combining advanced algorithms like Simple Additive Weighting (SAW) and Linear Programming (LP) with a distributed, edge-based architecture, the IRS provides a flexible and effective solution for mitigating cyber threats. The evaluation results confirm the system's capability to detect intrusions, select optimal responses, and maintain vehicle safety and functionality. Looking ahead, further research is needed to enhance the adaptability of the IRS to emerging threats, particularly in the context of increasing vehicle autonomy and connectivity. Future work could explore the integration of more sophisticated AI-based mechanisms and the development of industry standards for automotive cybersecurity. Additionally, the IRS's ability to handle large-scale attacks and its performance in real-world deployments should be further investigated. The proposed IRS represents a significant advancement in the field of automotive cybersecurity, offering a promising approach to safeguarding intelligent vehicles against the growing threat of cyber intrusions. This study introduces a novel hybrid decision-making model tailored for real-time autonomous vehicle cybersecurity, outperforming traditional IRS models in both speed and efficiency. Unlike prior IRS frameworks designed for enterprise IT or static networks, our model is tailored for intelligent vehicles with real-time constraints. Existing IRS methods do not combine MCDM and LP for vehicular systems, highlighting the novelty of our SAW-LP approach.

Acknowledgement

The authors sincerely acknowledge the support of Institutions and Departments for providing the necessary resources and research environment.

Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper

References

[1] Zhao, J., Zhao, W., Deng, B., Wang, Z., Zhang, F., Zheng, W., Cao, W., Nan, J., Lian, Y., & Burke, A. F. 2024. Autonomous driving system: A comprehensive survey. *Expert Systems with Applications,* 242: 122836. DOI: https://doi.org/10.1016/j.eswa.2023.122836

[2] El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. 2020. Cybersecurity challenges in vehicular communications. Vehicular Communications, 23: 100214. DOI: https://doi.org/10.1016/j.vehcom.2019.100214

[3] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. 2019. Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2(1): 1-22. DOI: https://doi.org/10.1186/s42400-019-0038-7

[4] Khan, F. I., Amyotte, P. R., & Amin, M. T. 2019. Advanced methods of risk assessment and management: An overview. Methods in Chemical Process Safety, 4: 1-34. DOI: https://doi.org/10.1016/bs.mcps.2020.03.002

[5] Kopalle, P. K., Pauwels, K., Akella, L. Y., & Gangwar, M. 2023. Dynamic pricing: Definition, implications for managers, and future research directions. *Journal of Retailing*, 99(4): 580-593. DOI: https://doi.org/10.1016/j.jretai.2023.11.003

[6] samados, A., Aggarwal, N., Cowls, J. et al. 2022. The ethics of algorithms: key problems and solutions. *AI & Society, Journal of Knowledge, Culture and Communication* 37: 215–230 DOI: https://doi.org/10.1007/s00146-021-01154-8

[7] Kim, K., Kim, J. S., Jeong, S., Park, J., & Kim, H. K. 2021. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security,* 103: 102150. DOI: https://doi.org/10.1016/j.cose.2020.102150

[8] Nisha, Nasib Singh Gill, Preeti Gulia. 2024. A review on machine learning based intrusion detection system for internet of thingsenabled environment, *International Journal of Electrical and Computer Engineering (IJECE)* 14(2): 1890-1898.

[9] Chunduru, Anilkumar & Robbi, Jyothsna & Sattaru, Vandana & Gothai, E. 2023. Deep Learning-Based Yoga Posture Specification Using OpenCV and Media Pipe. *Applied and Computational Engineering.* 8: 80-86. DOI: https://doi.org/10.54254/2755-2721/8/20230085.

[10] Qian, Y., Joshi, J., Tipper, D., & Krishnamurthy, P. 2007. Information Assurance. *Information Assurance*, 1-15. DOI: https://doi.org/10.1016/B978-012373566-9.50003-3

[11] Baddu Naik Bhukya, V. Venkataiah, S. Mani.Kuchibhatla, S. Koteswari, R V S Lakshmi Kumari, and Yallapragada Ravi Raju, 2024. "Integrating the Internet of Things to Protect Electric Vehicle Control Systems from Cyber Attacks," *IAENG International Journal of Applied Mathematics*, 54(3): 433-440

[12] Shinde, N., & Kulkarni, P. 2020. Cyber incident response and planning: A flexible approach. *Computer Fraud & Security,* 2021(1): 14-19. DOI: https://doi.org/10.1016/S1361-3723(21)00009-9

[13] Khan, Firoz & Ramasamy, Lakshmana & Kadry, Seifedine & Meqdad, Maytham N. & Nam, Yunyoung. 2021. Autonomous vehicles: A study of implementation and security. *International Journal of Electrical and Computer Engineering.* 11: 3013-3021. DOI: https://doi.org/10.11591/ijece. v11i4.pp3013-3021.

[14] Yazici, İ., Shayea, I., & Din, J. 2023. A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems. *Engineering Science and Technology, an International Journal,* 44: 101455. DOI: https://doi.org/10.1016/j.jestch.2023.101455

[15] Moneerh Aleedy, Hadil Shaiba and Marija Bezbradica. 2019. “Generating and Analyzing Chatbot Responses using Natural

Language Processing". *International Journal of Advanced Computer Science and Applications (IJACSA)* 10(9). DOI: http://dx.doi.org/10.14569/IJACSA.2019.0100910

[16] Micale, D., Matteucci, I., Fenzl, F. et al. 2024. A context-aware on-board intrusion detection system for smart vehicles. *International Journal of Information Security,* 23: 2203–2223. DOI: https://doi.org/10.1007/s10207-024-00821-3

[17] Baddu Naik Bhukya, Vutukuri Sarvani Duti Rekha, Venkata Krishnakanth Paruchuri, Ashok Kumar Kavuru, Kadiyala Sudhakar, 2023. "Internet of Things for Effort Estimation and Controlling the State of an Electric Vehicle in a Cyber Attack Environment" *Journal of Theoretical and Applied Information Technology.* 101(10): 4033–4040

[18] Wang, Shaoqiang & Wang, Yizhe & Zheng, Baosen & Cheng, Jiahui & Su, Yu & Dai, Yinfei. 2024. Intrusion Detection System for Vehicular Networks Based on MobileNetV3. *IEEE Access*. 1-1. DOI: https://doi.org/ 10.1109/ACCESS.2024.3437416.

[19] Inayat, Z., Gani, A., Anuar, N. B., Khan, M. K., & Anwar, S. (2016). Intrusion response systems: Foundations, design, and challenges. *Journal of Network and Computer Applications*, 62: 53-74. DOI: https://doi.org/10.1016/j.jnca.2015.12.006

[20] Adnan Yusuf, S., Khan, A., & Souissi, R. 2023. Vehicle-to-everything (V2X) in the autonomous vehicles domain – A technical review of communication, sensor, and AI technologies for road user safety. *Transportation Research Interdisciplinary Perspectives,* 23: 100980. DOI: https://doi.org/10.1016/j.trip.2023.100980

[21] Ghraizi, D., Talj, R., & Francis, C. 2022. An Overview of Decision-Making in Autonomous Vehicles. IFAC-PapersOnLine, 56(2): 10971-10983. DOI: https://doi.org/10.1016/j.ifacol.2023.10.793

[22] Taherdoost, Hamed. (2023). Analysis of Simple Additive Weighting Method (SAW) as a MultiAttribute Decision-Making Technique: A Step-by-Step Guide. J*ournal of Management Science & Engineering Research*. 6(1): 21-24. 6. 10.30564/jmser. v6i1.5400.

[23] Kunwar, Rajendra & Sapkota, Hari. 2022. An Introduction to Linear Programming Problems with Some Real-Life Applications. *European Journal of Mathematics and Statistics.* 3: 21-27. DOI: 10.24018/ejmath.2022.3.2.108.

[24] Hanley, John. 2021. GAMES, game theory and artificial intelligence. *Journal of Defense Analytics and Logistics*. 5(2): 114–130. DOI: https://doi.org/10.1108/JDAL-10-2021-001

[25] Sarker, I.H. 2022 AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems. *SN Computer Science* 3: 158. DOI: https://doi.org/10.1007/s42979-022-01043-x

[26] Naik, B., Bhukya, Sarvani, V., Rekha, D., Paruchuri, V.K., Kavuru, A.K., & Sudhakar, K. 2023, "Internet of Things for Effort Estimation and Controlling the State of an Electric Vehicle in A Cyber Attack Environment", *Journal of Theoretical and Applied Information Technology*, 101(10): 4033–4040.

[27] Abdallaoui, S., Ikaouassen, H., Kribèche, A., Chaibet, A., & Aglzim, H. 2023. Advancing autonomous vehicle control systems: An in-depth overview of decision-making and manoeuvre execution state of the art. *The Journal of Engineering*, 2023(11): e12333. DOI: https://doi.org/10.1049/tje2.12333

[28] Nagarajan, J., Mansourian, P., Shahid, M.A. et al. 2023. Machine Learning based intrusion detection systems for connected autonomous vehicles: A survey. *Peer-to-Peer Networking and Applications.* 16: 2153–2185 DOI: https://doi.org/10.1007/s12083-023-01508-7