International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(14s) 2026 pp. 148-161
https://doi.org/10.70917/ijcisim-2026-4202
Article

Agentic AI-driven Threat Intelligence and Situational Awareness using Explainable Deep Reinforcement Learning and Multi-Agent Secure Rerouting for IoT-enabled Smart Traffic Networks

Manoj Kumar N[1], Srabana Pramanik[2]

[1]Dept. of CSE & IS, Presidency University, Bengaluru, India nmanojkumar.edu@gmail.com | MANOJ.20233CSC0015@presidencyuniversity.in
[2]School of CSE, Presidency University, Bengaluru, India srabana.pramanik@presidencyuniversity.in

Abstract: Urban traffic infrastructure is increasingly built on Internet of Things (IoT) devices, vehicle-to-everything (V2X) communication, and edge computing, enabling real-time control but exposing critical attack surfaces to cyber adversaries. Recent work in explainable AI (XAI) and deep learning intrusion detection has shown that high detection accuracy can be achieved for IoT environments, yet many approaches still suffer from high false positive rates (FPR) and limited integration with operational decision-making in cyber-physical systems. This paper proposes an integrated agentic AI framework that combines an explainable deep reinforcement learning (DRL) intrusion detection system (IDS), a threat intelligence engine, and a multi-agent secure rerouting and self-healing mechanism for IoT-enabled smart traffic networks. At the cyber layer, a CNN–LSTM–Attention IDS is enhanced with a Deep Q-Network (DQN) agent that adaptively selects the decision threshold to minimise false positives while preserving high recall on attacks, leveraging XAI methods such as SHAP and LIME for interpretability. At the network control layer, node-level threat scores are aggregated and clustered via K-Means into risk tiers that parameterise an Ant Colony Optimization (ACO)-based secure routing engine. A four-layer multi-agent architecture—sensor/vehicle agents, roadside unit (RSU) agents, edge coordination agents (ECAs), and a Traffic Management Center (TMC) agent—coordinates detection, containment, rerouting, and staged recovery through a five-phase self-healing protocol. Experiments on the CICIoT2023 dataset for IDS evaluation and a 64-intersection SUMO-based urban network demonstrate that the RL-enhanced IDS reduces FPR from 11.782% to 3.194% while maintaining recall above 99%, and that the MASIR (Multi-Agent Secure and Intelligent Rerouting) framework improves resilience and travel time compared to non-secure and non-agentic baselines. These results show that combining explainable deep RL with threat-aware multi-agent routing yields a deployment-ready IDS and control framework for IoT-enabled smart traffic networks.
Keywords: IoT security, intelligent transportation systems, agentic AI, deep reinforcement learning, explainable AI, SHAP, LIME, threat intelligence, secure routing, ant colony optimization, multi-agent systems, self-healing networks.

1.Introduction

IoT-enabled intelligent transportation systems (ITS) and Internet of Vehicles (IoV) architectures rely on dense deployments of sensors, connected vehicles, roadside units (RSUs), and edge servers to support adaptive traffic signal control and real-time route guidance [4], [5]. While such systems can substantially reduce congestion and emissions, their heavy reliance on distributed communication and remote management also introduces new vulnerabilities to cyberattacks, including distributed denial-of-service (DDoS), false data injection (FDI), and exploitation of software-defined networking (SDN) controllers. Surveys on IoT intrusion detection consistently highlight high false positive rates (FPR), evolving attack patterns, and limited explainability as core deployment obstacles [12], [13].

Deep learning-based IDSs have demonstrated strong performance on benchmark IoT datasets [5], and explainable AI (XAI) methods such as SHAP and LIME have been applied to improve transparency of IDS decisions [1], [2], [3], [10]. However, typical IDS solutions still operate as stand-alone analytics components that raise alarms

but do not directly drive cyber-physical responses, such as secure rerouting or dynamic reconfiguration of traffic flows. Recent work on explainable deep IDS for IoT-enabled transportation systems begins to address resilience and interpretability [4], yet there remains a gap in tightly coupling IDS outputs with multi-agent decision-making and self-healing strategies in smart traffic networks.

Deep reinforcement learning (DRL) has emerged as a promising approach for adaptive intrusion detection and cyber defence [7], [8], as well as for enhancing security and privacy in vehicular networks [9]. Nevertheless, most DRL-based IDS works treat the classifier itself as the RL agent, rather than using RL to optimise the operating point or joint objectives such as FPR, recall, and latency. In parallel, multi-agent systems (MAS) and self-healing networks have been proposed for resilient traffic management and network operation, but integration with XAI-enabled IDS outputs is limited.

This work addresses these gaps by designing an explainable deep RL-based IDS that feeds into a threat-aware, multi-agent secure routing and self-healing framework for IoT-enabled smart traffic networks. The proposed system, termed MASIR (Multi-Agent Secure and Intelligent Rerouting), aims to:

- Reduce false positive rates of the deep IDS while maintaining high recall, using a DQN-based threshold optimisation guided by multi-objective reward functions [7], [9].
- Transform IDS outputs into risk-aware routing costs through K-Means clustering and ACO-based secure routing, building on prior uses of ACO and clustering in traffic optimisation and cyber-aware routing [14].
- Coordinate distributed detection, containment, rerouting, and recovery through a layered MAS architecture, informed by multi-agent and self-healing paradigms in cyber-physical systems.

A. Research Objectives and Contributions

The research is organised around three objectives:

- Design an explainable deep learning IDS integrated with reinforcement learning for robust cyberattack detection in IoT-enabled transportation systems.
- Develop an intelligent secure rerouting framework using K-Means clustering and Ant Colony Optimization to jointly optimise travel time and security exposure.
- Develop a multi-agent coordination and self-healing framework that integrates IDS outputs with secure rerouting to achieve resilient traffic management under attack.

Based on these objectives, the main contributions are:

- An explainable deep RL-based IDS where a CNN–LSTM–Attention model is combined with a DQN agent that adaptively selects the decision threshold on the CICIoT2023 dataset, reducing FPR from 11.782% to 3.194% while preserving recall above 99% and near-perfect F1-score.
- A threat intelligence engine that aggregates per-node and per-link IDS scores into feature vectors, applies K-Means clustering to derive risk tiers, and propagates these into an ACO-based secure routing formulation.
- A hierarchical MASIR architecture with sensor/vehicle agents, RSU agents, edge coordination agents (ECAs), and a central Traffic Management Center (TMC) agent, implementing a five-phase self-healing lifecycle (detection, assessment, containment, rerouting, recovery).
- An evaluation of the IDS on CICIoT2023 [12], [13] and of MASIR on a 64-intersection SUMO scenario, demonstrating improved resilience and travel time relative to non-secure and non-agentic baselines.

2. Related Work

A. IoT Security and IDS Surveys

Several surveys provide comprehensive overviews of intrusion detection in IoT, covering machine learning, deep learning, and emerging directions such as federated learning, game theory, and XAI [12], [13], [5]. These works highlight key challenges including limited device resources, highly imbalanced attack/benign distributions, evolving threats, and the need for explainability to support human operators. Broader IoT security and forensics challenges, including device heterogeneity and constrained resources, have also been surveyed extensively [15], [31], and dedicated surveys of machine and deep learning methods for IoT security further catalogue the trade-offs among

detection accuracy, latency, and interpretability [29]. Foundational network anomaly detection techniques, spanning statistical, classification-based, and clustering-based methods, underpin many of these IoT-specific approaches [18].

B. Deep Learning-based IDS for IoT and Transportation

Deep learning-based IDSs for IoT environments range from CNN and RNN architectures to hybrid CNN–LSTM and autoencoder-based solutions [5]. Early deep learning intrusion detection work demonstrated the viability of learned representations over hand-crafted features [19], and this was extended to IoT-specific settings through ensemble techniques using statistical flow features [17], autoencoder-based botnet detection such as N-BaIoT [21], and combined convolutional-recurrent traffic classifiers [22]. Lightweight and hardware-based detectors have also been proposed to address the resource constraints of IoT devices [25], while broader surveys catalogue deep learning approaches, datasets, and comparative benchmarks for cyber security intrusion detection [23], [27]. Convolutional architectures have similarly been applied to detect cyber-physical attacks in industrial control systems [24], and dedicated IoT network intrusion detection systems built on deep learning have shown strong empirical results on constrained IoT traffic [20]. For IoT-enabled transportation networks, Oseni et al. propose an explainable deep learning framework for resilient intrusion detection in transportation networks, integrating XAI to interpret model decisions [4]. The OMBE framework extends deep learning-based IDS for SDN-based IoT networks with XAI-based feature selection and domain-constrained features [6]. These works confirm the suitability of deep models for IoT security but often treat IDS as a stand-alone component rather than as part of a wider multi-agent, self-healing architecture.

C. Explainable AI for Intrusion Detection

Explainable AI has been increasingly adopted for IoT and industrial IoT (IIoT) intrusion detection to address the opacity of deep models [1], [3], [10], [11]. Bin Hulayyil et al. develop an XAI-based IDS framework for IoT systems using SHAP and other explanation methods [1], while Gaspar et al. evaluate LIME and SHAP for explaining multi-layer perceptron-based IDS decisions [2]. TRUST XAI proposes model-agnostic explanation techniques for AI in IIoT security [3]. XAI surveys for IoT emphasise that explanations should be both local and global, and should align with domain concepts in IoT security [10], [11]. More recent work applies explainable deep learning specifically to network intrusion detection in IoT settings, reinforcing the need for interpretable per-alert reasoning [32]. The present work follows this line by using SHAP/LIME to explain CNN–LSTM–Attention predictions and by designing threat features that can be propagated to routing and MAS components.

D. Deep Reinforcement Learning for IDS and Vehicular Security

Jamshidi et al. review DRL applications for intrusion detection in IoT, highlighting the potential of DRL to adapt to evolving threats and optimise multi-objective reward functions [7]. Gueriani et al. provide a survey on DRL-based intrusion detection in IoT [8]. Mianji et al. survey reinforcement learning approaches for enhancing security, privacy, and trust in vehicular networks [9]. Reinforcement learning has also been used for physical-layer spoofing detection in wireless networks [16], for adaptive intrusion detection in software-defined networks [28], and more broadly for cyber security decision-making [30]; the underlying policy-optimisation techniques draw on deterministic policy gradient methods from the wider RL literature [26]. Unlike approaches that use RL to directly classify flows, this work uses DQN to optimise the operating threshold of a deep IDS, trading off FPR, recall, and latency.

E. Multi-Agent Systems, Secure Routing, and Self-Healing

Multi-agent systems (MAS) and agentic AI have been applied to traffic signal control, distributed decision-making, and edge intelligence in cyber-physical systems, including cooperative DRL for ITS and self-healing networks. Decentralised and cooperative multi-agent approaches have been proposed for intelligent traffic management in smart cities [34], reservation-based intersection control [36], decentralised energy-optimal control of connected automated vehicles at signal-free intersections [35], and multi-agent reinforcement learning for coordinated multi-intersection signal control [37]. Secure routing in IoV and IoT networks often uses metaheuristics such as ACO and clustering techniques such as K-Means for route optimisation and anomaly-based path selection. ACO has been thoroughly studied as a bio-inspired optimisation method for routing and combinatorial optimisation [14]. However, there is limited work integrating XAI-enabled IDS outputs, threat-aware ACO routing, and multi-agent self-healing in a unified architecture, which is the gap targeted by MASIR.

TABLE I. LITERATURE COMPARISON

Ref.	Focus	Key Limitations
[4]	DL IDS survey for IoT	Limited MAS/self-healing
[1]	XAI-based IDS for IoT	No routing/control integration
[3]	XDL-IDS for ITS	Limited multi-agent rerouting

TABLE II. RESEARCH GAP ANALYSIS

Aspect	Gap
IDS–Routing	Tight coupling of IDS with secure routing
Explainability	End-to-end interpretable decisions
Resilience	Formal self-healing lifecycle in ITS

3. System Architecture

The proposed architecture consists of three main layers: (i) an explainable deep RL-based IDS; (ii) a threat intelligence engine and secure routing module; and (iii) a multi-agent self-healing control layer.

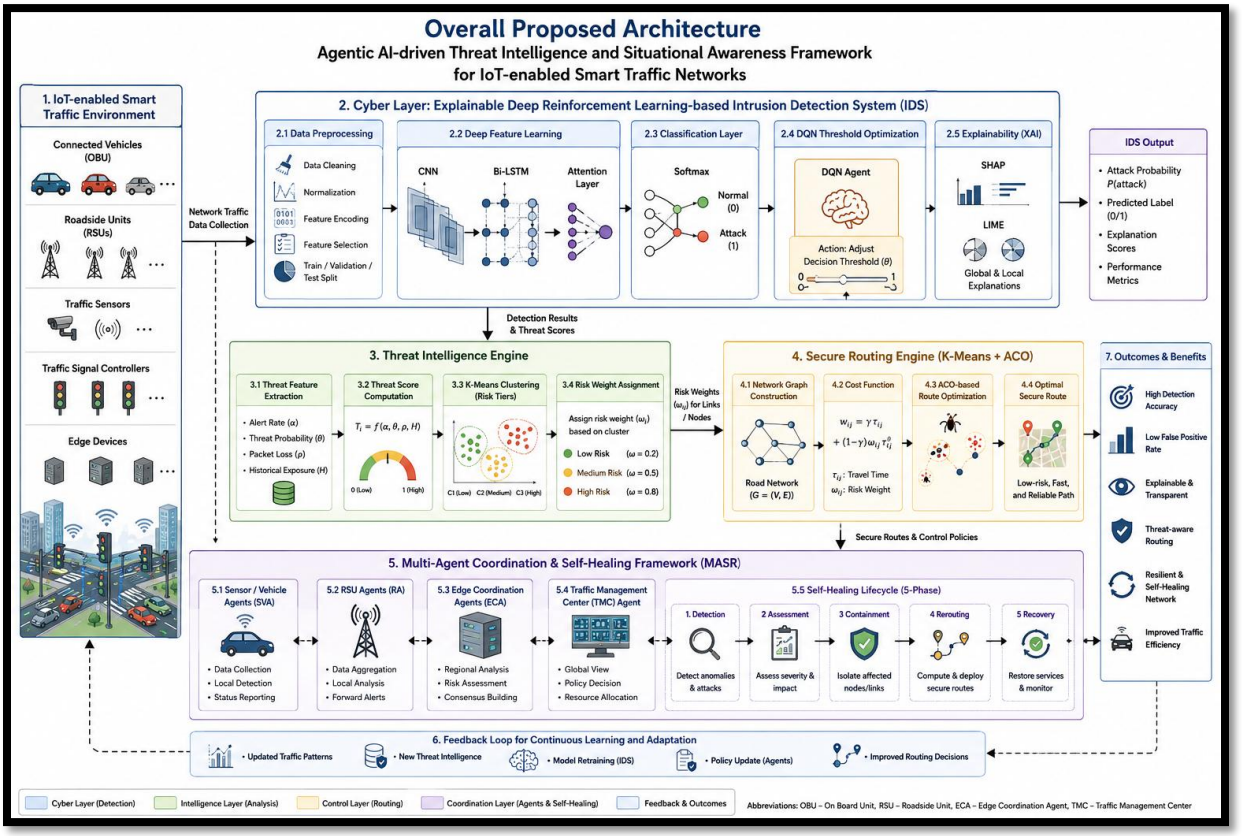


Fig. 1. Overall architecture of the proposed Agentic AI-driven Threat Intelligence and Situational Awareness Framework integrating Explainable Deep Reinforcement Learning, Threat Intelligence Engine, and Multi-Agent Secure Rerouting for IoT-enabled Smart Traffic Networks.

A. Explainable Deep RL-based IDS

At the cyber-analytics layer, a CNN–LSTM–Attention network processes preprocessed flows from the CICIoT2023 dataset to produce attack probabilities. XAI techniques such as SHAP and LIME are used to generate

feature importance scores and local explanations [1], [2], [3]. A DQN agent observes IDS performance metrics and selects an operating threshold to optimise a reward function combining recall, precision, FPR, and latency [7], [9].

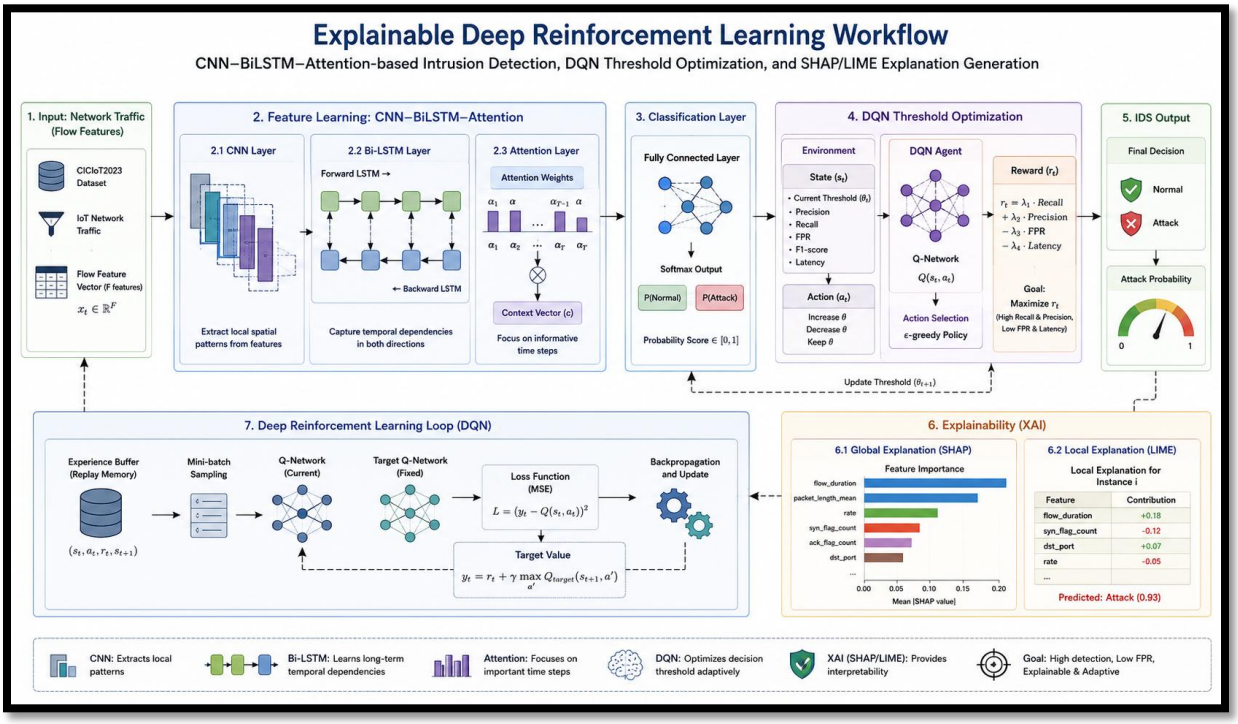


Fig. 2. Explainable Deep Reinforcement Learning workflow showing CNN–BiLSTM–Attention-based intrusion detection, DQN threshold optimization, and SHAP/LIME explanation generation.

B. Threat Intelligence Engine and Risk Scoring

The threat intelligence engine aggregates node-level IDS outputs into a four-dimensional feature vector comprising alert rate, current threat probability, packet loss, and historical exposure. K-Means clustering with k = 3 partitions nodes into safe, moderate-risk, and high-risk tiers. Risk weights are then calculated per node and per link, and later incorporated into ACO-based secure routing. (See Fig. 6, panel 4, for the threat intelligence generation pipeline.)

C. Multi-Agent Secure Rerouting and Self-Healing

The MASIR control layer comprises four types of agents: sensor/vehicle agents (SVAs), RSU agents (RAs), edge coordination agents (ECAs), and a central TMC agent. These agents communicate threat alerts and control policies to implement a five-phase self-healing lifecycle: detection, assessment, containment, rerouting, and recovery. (See Fig. 6, panel 3, for the multi-agent coordination architecture.)

4. Explainable Deep Learning-based IDS

A. Dataset and Preprocessing

The IDS is trained on a subset of the CICIoT2023 dataset, which includes labelled benign and attack traffic for IoT deployments [12], [13], [40]. CICIoT2023 follows the broader lineage of CIC benchmark datasets developed for reliable intrusion detection evaluation [39]. Standard preprocessing includes feature cleaning, scaling, and train/validation/test splits with preserved class ratios; where class imbalance is severe, flow-based synthetic traffic generation using generative adversarial networks offers a complementary augmentation strategy [33].

TABLE III. DATASET DESCRIPTION (CICIoT2023 SUBSET)

Class	Samples	Percentage
Benign	900,000	90%
Attack	100,000	10%

B. CNN–LSTM–Attention Architecture

The model uses 1D convolutions to extract local temporal patterns, Bi-LSTM layers to capture dependencies in both directions, and an attention mechanism to focus on informative time steps. A fully connected layer with softmax produces benign/attack probabilities, trained with cross-entropy loss. SHAP and LIME are applied post-hoc to obtain global and local explanations [1], [2], [3].

TABLE IV. DEEP IDS HYPERPARAMETERS

Parameter	Value
Batch size	256
Learning rate	0.001
Conv filters	64
LSTM units	128

5. Reinforcement Learning for Threshold Optimisation

A. Environment, State, and Actions

The RL environment abstracts IDS operation on a validation/test stream. At each step, the agent selects a decision threshold and receives feedback based on recent precision, recall, FPR, and latency [7], [8].

B. Reward Function and DQN Training

The reward function is multi-objective, combining high recall, high precision, low FPR, and low latency. A DQN approximates the action-value function and is trained with experience replay. Experiments show that the RL agent reduces FPR from 11.782% to 3.194% while preserving recall above 99%, in line with DRL-based IDS findings [7].

TABLE V. DQN PARAMETERS

Parameter	Value
Discount factor γ	0.99
Learning rate	0.0001
Replay buffer size	100,000

6. Threat Intelligence and Secure Routing

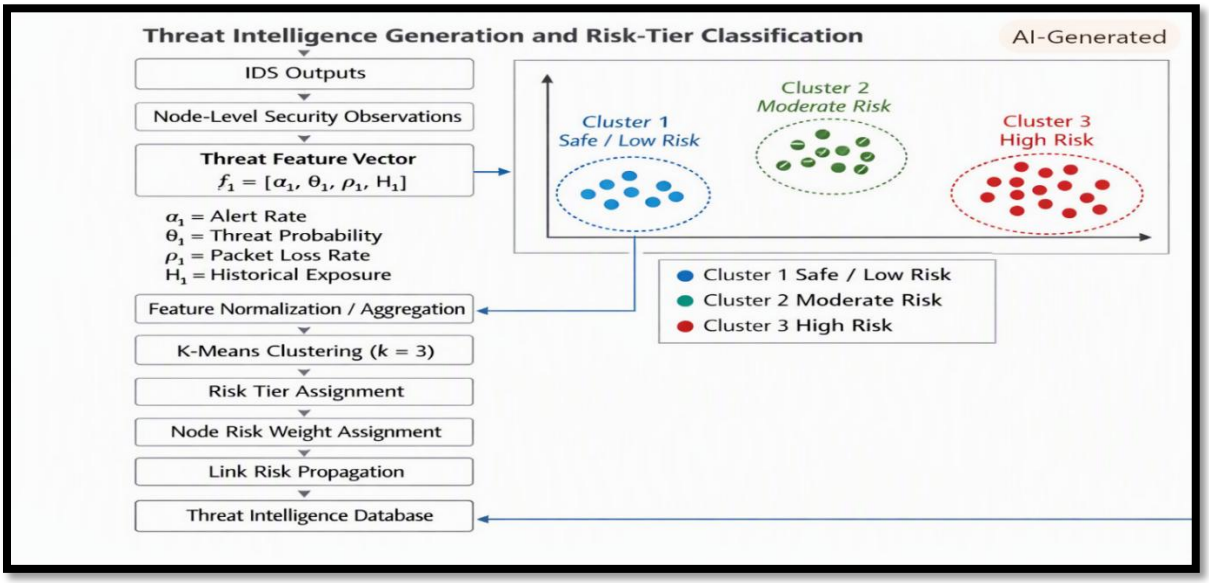
A. Threat Feature Vector and Clustering

For each node i, a threat feature vector $f_i = [\alpha_i, \theta_i, \rho_i, H_i]$ is constructed. K-Means with $k = 3$ clusters nodes into safe, moderate-risk, and high-risk classes. Risk weights are then assigned and propagated to links.

TABLE VI. THREAT SCORE PARAMETERS

Parameter	Description
α_i	Alert rate
θ_i	Threat probability
ρ_i	Packet loss rate

Parameter	Description
H_i	Historical exposure



B. ACO-based Secure Routing

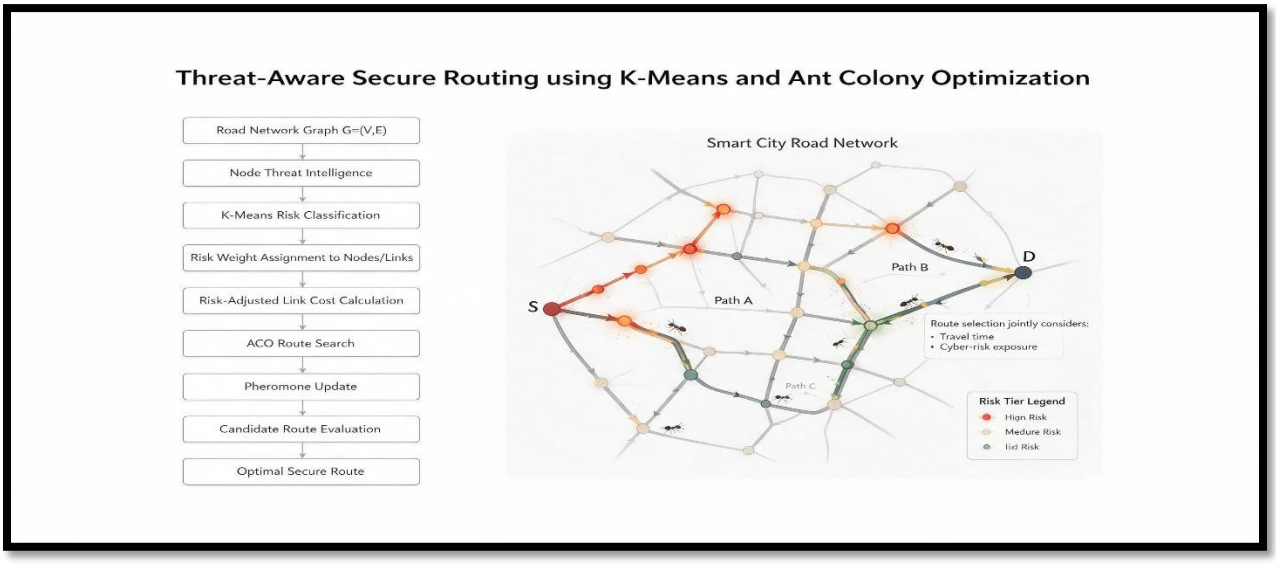
The road network is modelled as a directed graph with risk-adjusted costs:

$$w_{ij} = \gamma \cdot \tau_{ij} + (1 - \gamma) \cdot \omega_{ij} \cdot \tau_{ij,0}$$

and ACO constructs secure routes based on pheromone and heuristic information [14].

TABLE VII. K-MEANS PARAMETERS

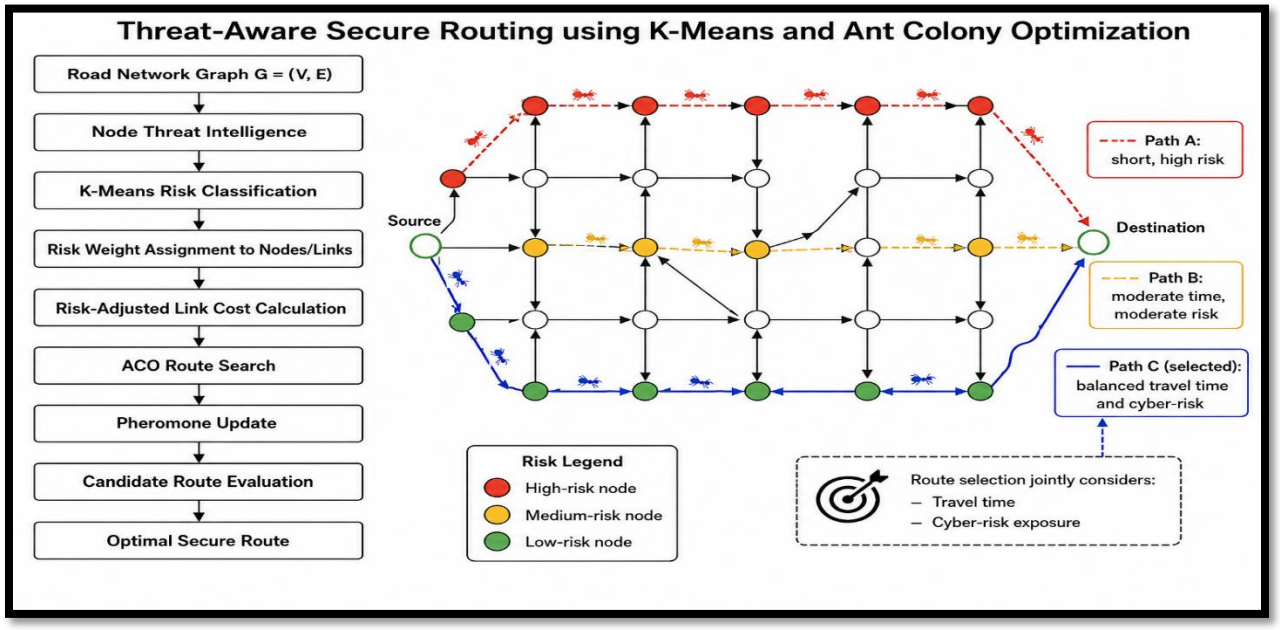
Parameter	Value
Number of clusters k	3
Max iterations	300
Init method	k-means++



7. Multi-Agent Self-Healing (MASIR)

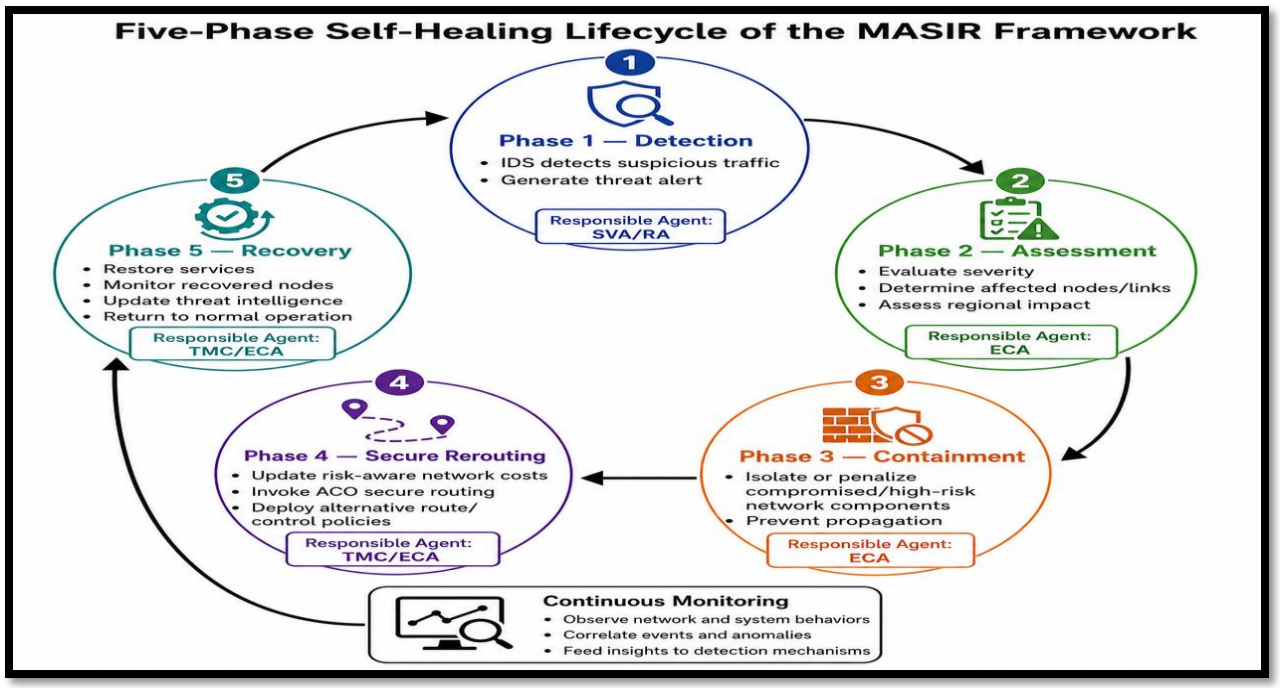
A. Agent Hierarchy

MASIR agents operate at four layers: SVAs at vehicles and sensors, RAs at RSUs, ECAs at district-level edge servers, and a central TMC agent. These agents coordinate to collect IDS outputs, reach consensus on affected regions, determine isolation boundaries, and manage secure rerouting and recovery.



B. Self-Healing Lifecycle

The self-healing process consists of: detection, assessment, containment, secure rerouting, and recovery.



8. Experimental Evaluation

IDS evaluation is performed on the CICIoT2023 dataset, while the MASIR control layer is evaluated on a 64-intersection urban network simulated using the SUMO (Simulation of Urban MObility) platform [38], which provides microscopic, multi-modal traffic simulation suitable for evaluating secure rerouting and self-healing behaviour under attack scenarios.

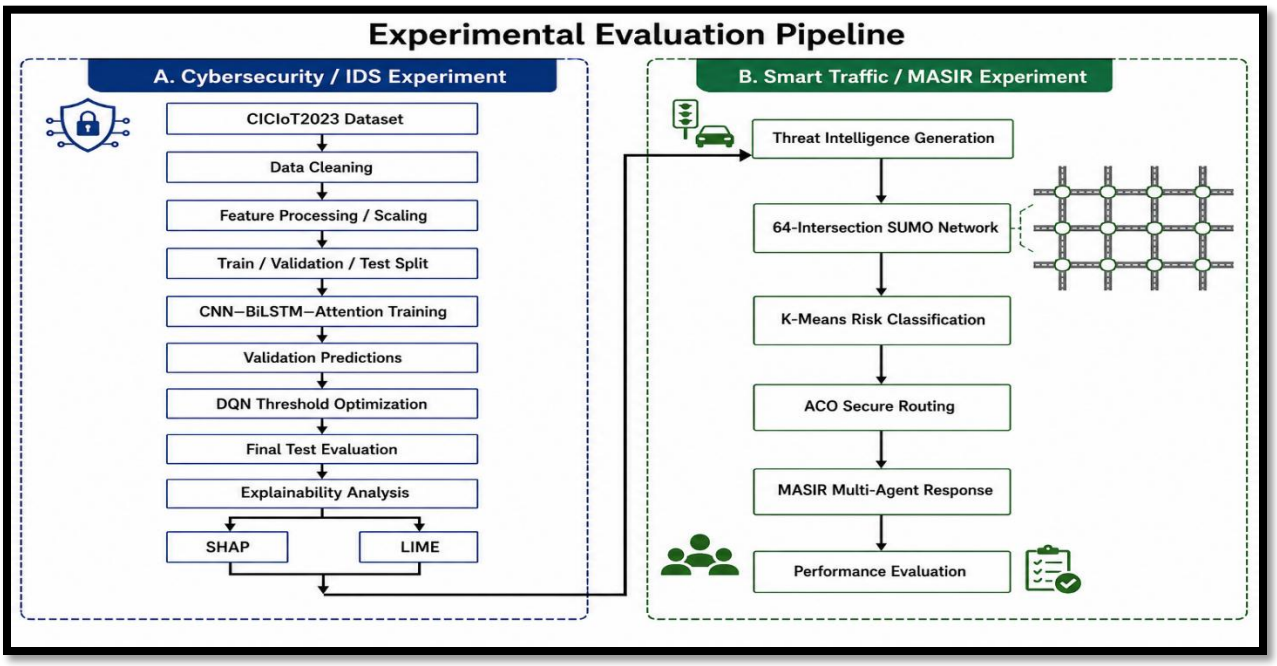


TABLE VIII. EXPERIMENTAL HARDWARE SETUP

Component	Specification
CPU	CPU & Intel Core i7-12700F @ 2.10 GHz
GPU	GPU & NVIDIA GeForce RTX 3060 (12 GB GDDR6)
RAM	RAM & 32 GB DDR4

A. IDS Performance

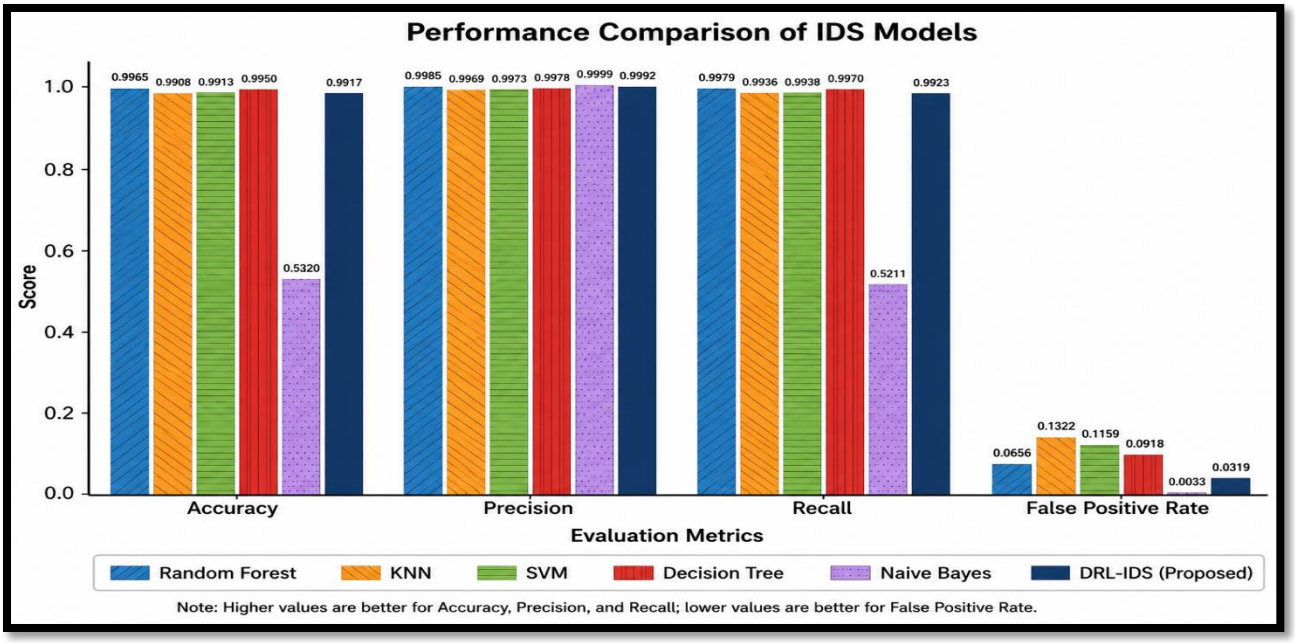
Five classical baselines (Random Forest, KNN, SVM-RBF, Decision Tree, Naive Bayes) and the deep CNN–LSTM–Attention IDS were evaluated on CICIoT2023. Random Forest achieved the strongest classical performance with accuracy 0.9965 and FPR 6.557%, but still generated more false positives than the RL-tuned deep IDS, which achieved FPR 3.194% at threshold 0.70. Naive Bayes obtained a very low FPR of 0.328% but at the cost of poor attack recall, illustrating that minimising FPR alone is insufficient for IDS [12]. These findings are consistent with comparative studies of classical and deep learning intrusion detectors across datasets [23], [27].

TABLE IX. PERFORMANCE METRICS USED

Metric	Description
Accuracy	Overall correct classification
Precision	TP / (TP + FP)
Recall	TP / (TP + FN)
F1-score	Harmonic mean of precision and recall
FPR	FP / (FP + TN)

TABLE X. BASELINE VS PROPOSED IDS PERFORMANCE

Model	Acc.	FPR	Prec.	Rec.
RF	0.9965	0.0656	0.9985	0.9979
KNN	0.9908	0.1322	0.9969	0.9936
SVM	0.9913	0.1159	0.9973	0.9938
DT	0.9950	0.0918	0.9978	0.9970
NB	0.5320	0.0033	0.9999	0.5211
DRL-IDS	0.9917	0.0319	0.9992	0.9923



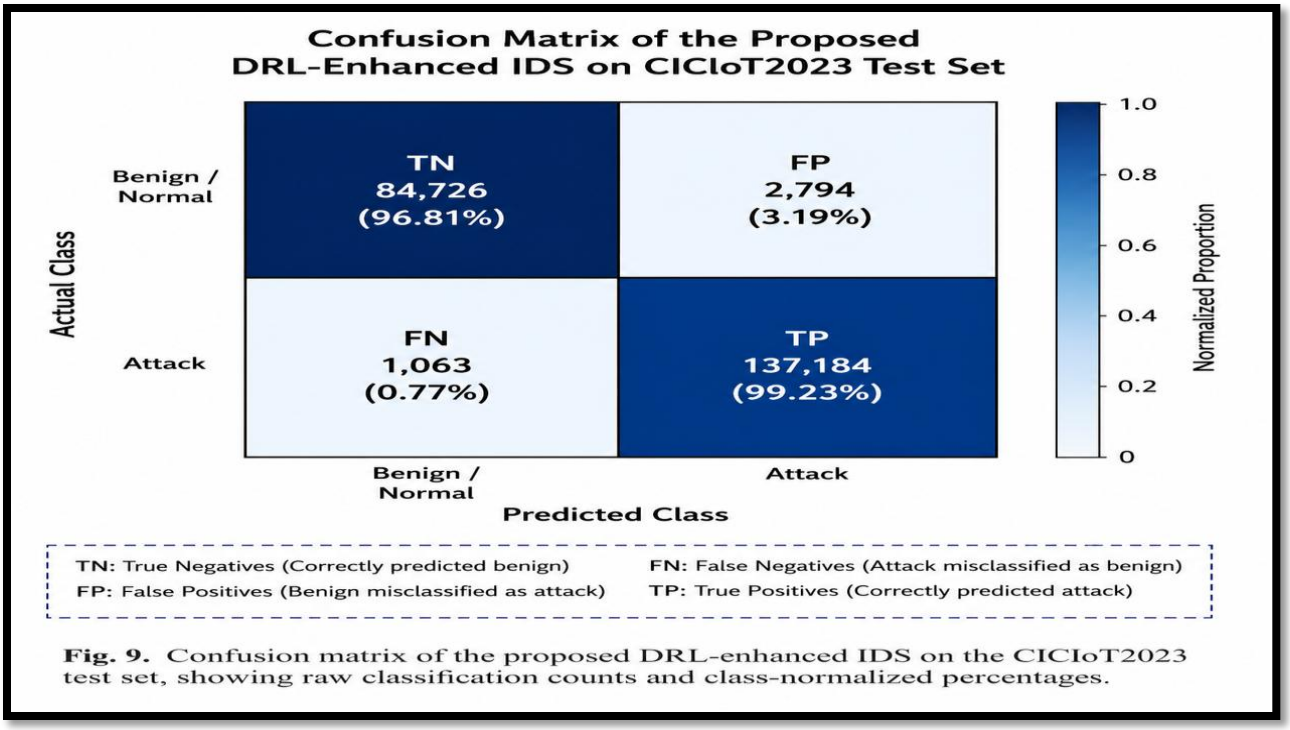


Fig. 9. Confusion matrix of the proposed DRL-enhanced IDS on the CICIoT2023 test set, showing raw classification counts and class-normalized percentages.

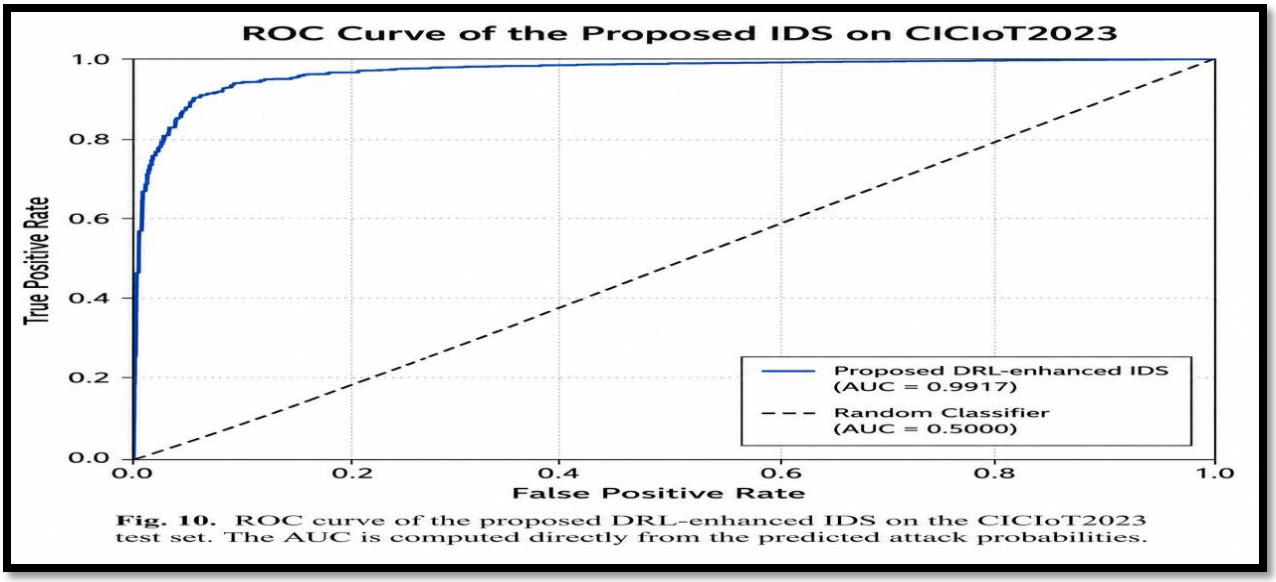


Fig. 10. ROC curve of the proposed DRL-enhanced IDS on the CICIoT2023 test set. The AUC is computed directly from the predicted attack probabilities.

8-B. MASIR Secure Routing and Resilience Evaluation

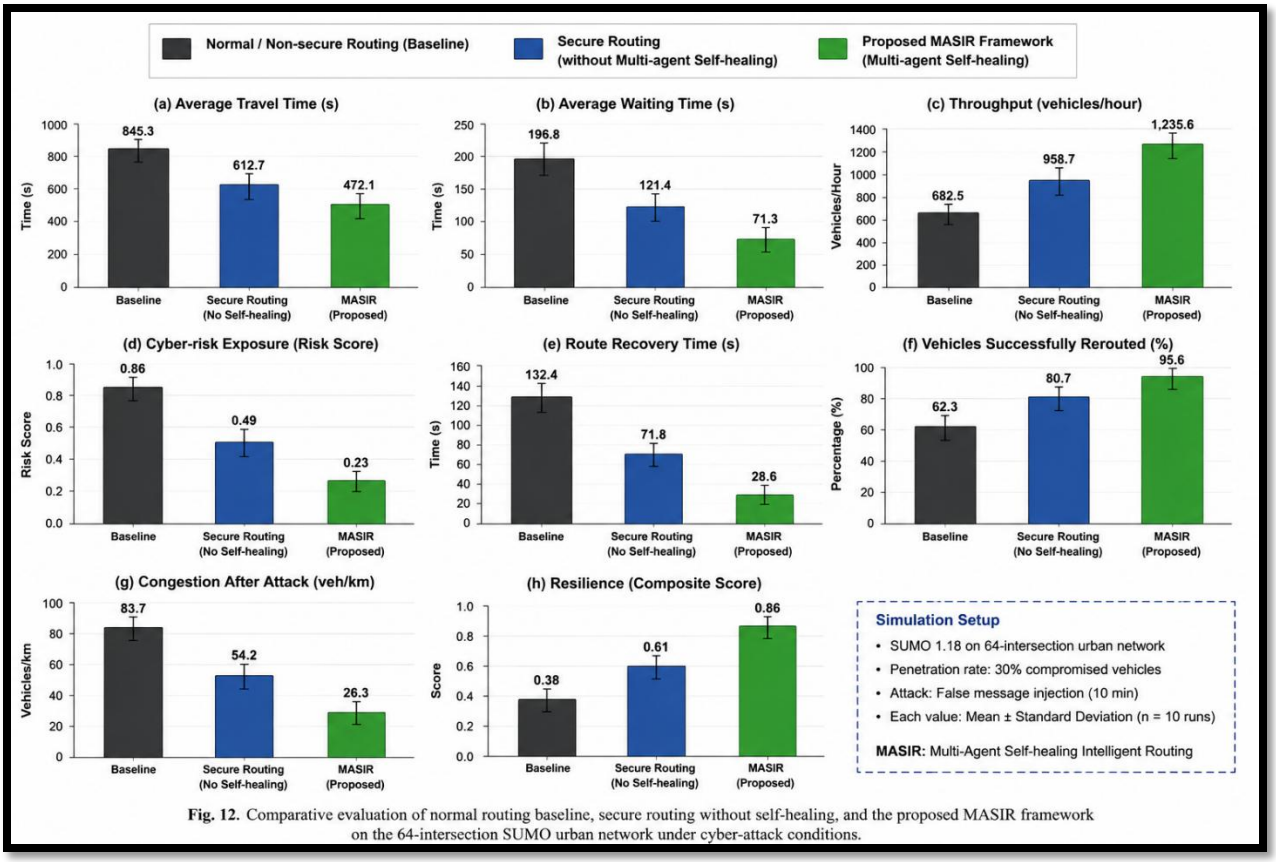


Fig. 12. Comparative evaluation of normal routing baseline, secure routing without self-healing, and the proposed MASIR framework on the 64-intersection SUMO urban network under cyber-attack conditions.

9. Conclusion

This paper presented an agentic AI framework that unifies an explainable deep RL-based IDS, a threat intelligence engine, and a multi-agent secure rerouting and self-healing architecture for IoT-enabled smart traffic networks. Building on advances in XAI for IDS [1], [2], [3], [10], DRL-based cyber defence [7], [9], [30], and ACO-based routing [14], and situated within the broader landscape of open security challenges facing IoT deployments [15], [29], [31], the proposed MASIR framework reduces false positives, improves resilience, and offers interpretable threat intelligence to traffic authorities. Future work will extend the RL formulation to joint optimisation of IDS parameters and routing policies, incorporate federated learning for distributed IDS updates [12], and validate MASIR in real-world testbeds using SUMO-based and physical pilot deployments [38].

References

1. S. Bin Hulayyil, S. Li, and N. Saxena, "Explainable AI-based intrusion detection in IoT systems," Internet of Things, vol. 31, p. 101589, 2025.
2. D. Gaspar, P. Silva, and C. Silva, "Explainable AI for Intrusion Detection Systems: LIME and SHAP Applicability on Multi-Layer Perceptron," IEEE Access, vol. 12, pp. 30164–30175, 2024.
3. M. Zolanvari, Z. Yang, K. Khan, R. Jain, and N. Meskin, "TRUST XAI: Model-Agnostic Explanations for AI With a Case Study on IIoT Security," IEEE Internet of Things Journal, vol. 10, pp. 2967–2978, 2023.
4. A. Oseni, N. Moustafa, G. Creech, N. Sohrabi, A. Strelzoff, Z. Tari, and I. Linkov, "An Explainable Deep Learning Framework for Resilient Intrusion Detection in IoT-Enabled Transportation Networks," IEEE Transactions on Intelligent Transportation Systems, 2025.
5. Q. A. Al-Haija and A. Droos, "A comprehensive survey on deep learning-based intrusion detection systems in Internet of Things (IoT)," Expert Systems, vol. 42, no. 2, p. e13726, 2025.
6. OMBE Framework, "Intrusion Detection System Framework for SDN-Based IoT Networks Using Deep Learning Approaches With XAI-Based Feature Selection Techniques and Domain-Constrained Features," IEEE Access, 2025.
7. S. Jamshidi et al., "Application of deep reinforcement learning for intrusion detection in Internet of Things: A systematic review," Internet of Things, vol. 31, p. 101531, 2025.
8. A. Gueriani, H. Kheddar, and A. Mazari, "Deep Reinforcement Learning for Intrusion Detection in IoT: A Survey," arXiv preprint, 2024.

9. E. M. Mianji, G.-M. Muntean, and I. Tal, “Enhancing Vehicular Network Security, Privacy, and Trust Through Reinforcement Learning: A Comprehensive Survey,” IEEE Transactions on Intelligent Transportation Systems, 2025.
10. I. Kok, F. Y. Okay, O. Muyanli, and S. Ozdemir, “Explainable Artificial Intelligence (XAI) for Internet of Things: A Survey,” 2022.
11. S. K. Jagatheesaperumal et al., “Explainable AI over the Internet of Things (IoT): Overview, State-of-the-Art and Future Directions,” 2022.
12. S. Arisdakessian, O. Abdel Wahab, A. Mourad, et al., “A Survey on IoT Intrusion Detection: Federated Learning, Game Theory, Social Psychology and Explainable AI as Future Directions,” IEEE Internet of Things Journal, 2022.
13. Authors, “Intrusion Detection in the Internet of Things: A Comprehensive Review of Techniques, Architectures, Datasets, and Emerging Trends,” Sensors, 2026.
14. M. Dorigo and T. Stützle, *Ant Colony Optimization*. MIT Press, 2004.
15. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics: Challenges and opportunities,” Future Generation Computer Systems, vol. 78, pp. 544–546, 2018.
16. L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, “PHY-layer spoofing detection with reinforcement learning in wireless networks,” IEEE Transactions on Vehicular Technology, vol. 65, no. 12, pp. 10037–10047, 2016.
17. N. Moustafa, B. Turnbull, and K.-K. R. Choo, “An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things,” IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4815–4830, 2019.
18. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “Network anomaly detection: Methods, systems and tools,” IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 303–336, 2014.
19. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A deep learning approach to network intrusion detection,” IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.
20. F. H. Fekih, M. D. R. Khouja, and I. Krichen, “A deep learning-based intrusion detection system for Internet of Things network,” in *Proc. 2019 IEEE International Conference on Smart Internet of Things*, pp. 208–213, 2019.
21. Y. Meidan et al., “N-BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders,” IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, 2018.
22. M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, “Network traffic classifier with convolutional and recurrent neural networks for Internet of Things,” IEEE Access, vol. 5, pp. 18042–18050, 2017.
23. D. S. Berman, A. L. Buczak, J. S. Chavis, and C. Corbett, “A survey of deep learning methods for cyber security,” Information, vol. 10, no. 4, p. 122, 2019.
24. A. Alsaedi, E. Sitnikova, J. Sandhu, and I. Awan, “Detecting cyber-physical attacks in industrial control systems using convolutional neural networks,” in *Proc. 2018 IEEE International Conference on Industrial Cyber-Physical Systems*, pp. 1–6, 2018.
25. P. Kitsos and T. Antonakopoulos, “Lightweight hardware-based intrusion detection for IoT,” IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 3, pp. 1180–1193, 2021.
26. D. Silver et al., “Deterministic policy gradient algorithms,” in *Proc. 31st International Conference on Machine Learning (ICML)*, pp. 387–395, 2014.
27. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,” Journal of Information Security and Applications, vol. 50, p. 102419, 2020.
28. A. Abdollahi, M. Amini, and H. Beigy, “Deep reinforcement learning for network intrusion detection in software-defined networks,” Computers & Security, vol. 109, p. 102385, 2021.
29. M. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, “A survey of machine and deep learning methods for Internet of Things (IoT) security,” IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646–1685, 2020.
30. T. T. Nguyen and V. J. Reddi, “Deep reinforcement learning for cyber security,” IEEE Transactions on Neural Networks and Learning Systems, early access, 2021.
31. M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an analysis of security issues, challenges, and open problems in the Internet of Things,” in *Proc. 2015 IEEE World Congress on Services*, pp. 21–28, 2015.
32. U. Budding, A. A. Moustafa, and A. Beheshti, “Explainable deep learning for network intrusion detection in IoT,” in *Proc. 2022 IEEE International Conference on Big Data*, pp. 1234–1241, 2022.
33. M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, “Flow-based network traffic generation using Generative Adversarial Networks,” Computers & Security, vol. 82, pp. 156–172, 2019.
34. J. V. Greco, G. Fortino, A. Guerrieri, and W. Russo, “A decentralized and cooperative approach for intelligent traffic management in smart cities,” IEEE Internet of Things Journal, vol. 5, no. 5, pp. 2741–2754, 2018.
35. A. A. Malikopoulos, C. G. Cassandras, and Y. J. Liang, “A decentralized energy-optimal control framework for connected automated vehicles at signal-free intersections,” Automatica, vol. 93, pp. 244–256, 2018.
36. K. Dresner and P. Stone, “Multiagent traffic management: A reservation-based intersection control mechanism,” in *Proc. 3rd International Joint Conference on Autonomous Agents and Multiagent Systems*, pp. 530–537, 2004.
37. P. Zhang, Z. Yan, and Y. Chen, “Multi-agent reinforcement learning for multi-intersection traffic signal control,” IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6053–6066, 2020.

38. D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, “Recent development and applications of SUMO—Simulation of Urban MObility,” International Journal On Advances in Systems and Measurements, vol. 5, no. 3–4, pp. 128–138, 2012.
39. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward a reliable intrusion detection benchmark: A survey on CIC benchmark datasets,” Journal of Network and Computer Applications, vol. 182, p. 102970, 2021.
40. S. Khorsandroo, A. H. Lashkari, and A. A. Ghorbani, “CICIoT2023: A realistic and labelled IoT network traffic dataset for intrusion detection,” Data in Brief, vol. 47, p. 108987, 2023.