Deep Reinforcement Learning for Securing Autonomous Urban Systems Against Coordinated Cyberattacks

Vikram Kumar Casula Ashok [1*], Satish Kumar Pittala [2]
[1] Morgan Stanley, USA
[2] Department of Computer Science and Engineering, Veer Bahadur Singh Purvanchal University, Uttar Pradesh, India

* Corresponding Author: **Vikram Kumar Casula Ashok**

Article Info

P-ISSN: 3051-3383
E-ISSN: 3051-3391
Volume: 05
Issue: 01
Received: 07-06-2024
Accepted: 10-07-2024
Published: 05-08-2024
Page No: 32-39

Abstract
As urban infrastructures become increasingly autonomous incorporating connected vehicles, smart-traffic systems, and digitally orchestrated emergency services they face escalating risks from coordinated cyberattacks that exploit their interdependencies. This manuscript proposes a framework leveraging deep reinforcement learning (DRL) to secure autonomous urban systems against such advanced threats. The proposed approach models the urban infrastructure as a networked multi-agent system in which defender agents learn policies to detect, contain and recover from attacks in real-time; adversarial behaviour is simulated via virtual attacker agents to improve robustness. Through this learning paradigm, the defender adapts dynamically to previously unseen threat vectors, reducing reliance on static rule-based safeguards. Empirical evaluations in a simulated urban operations environment show that DRL-based defenders reduce system downtime and service disruption under coordinated multi-vector attacks compared to baseline reactive strategies. The results highlight not only improved resilience but also reduced false-positive intrusion responses, enabling smoother continuity of service. The contributions include (i) modelling of the coordinated attack-defence scenario within autonomous urban systems; (ii) a DRL architecture tailored for real-time decision-making in complex multi-agent domains; and (iii) experimental validation demonstrating measurable gains in resilience and adaptability. The findings suggest that integrating DRL into urban defence architectures offers a promising pathway for future smart-city cybersecurity.

DOI: https://doi.org/10.54660/IJAIET.2024.5.1.32-39

Keywords: Deep Reinforcement Learning, Autonomous Urban Systems, Coordinated Cyberattacks, Multi-Agent Defence, Smart City Resilience, Real-Time Cyber Defence

1. Introduction

Autonomous urban systems are rapidly transforming modern cities into interconnected, intelligent environments capable of sensing, reasoning, and acting with minimal human intervention. These systems such as adaptive traffic-signal networks, autonomous vehicle fleets, emergency-response robots, and distributed utility grids operate as cyber-physical infrastructures that integrate communication networks, embedded controllers, machine intelligence, and physical actuators. Their increasing autonomy allows cities to optimize mobility, reduce energy consumption, manage congestion, and achieve higher safety standards. However, this growing interconnectivity also exposes urban environments to new and complex forms of cyberattacks. Unlike traditional information-technology networks, autonomous urban infrastructures involve distributed control loops, real-time data processing, and safety-critical operations; disruptions in one subsystem can quickly cascade across others, amplifying the impact of even minor attacks. Cyberattacks on urban systems have evolved from isolated intrusions toward coordinated multi-vector operations.

Threat actors increasingly target multiple subsystems simultaneously for example, manipulating traffic lights while interfering with vehicle-to-infrastructure (V2I) communication or disrupting smart-grid nodes that power autonomous transportation services. Coordinated attacks exploit interdependencies among urban components, producing system-wide failures such as traffic congestion, emergency-service delays, and compromised public safety. Traditional rule-based cybersecurity mechanisms and static intrusion-detection systems (IDS) often fail in such scenarios because they cannot reason about dynamic adversaries, previously unseen threat patterns, or rapidly shifting environmental states. These limitations have motivated the search for adaptive, learning-based defence mechanisms capable of operating in real time.

Deep Reinforcement Learning (DRL) has emerged as a promising solution for cyber-defence in complex and dynamic environments. DRL combines reinforcement-learning principles with deep neural networks, enabling agents to learn optimal decisions from high-dimensional sensor data. In urban settings, DRL-based defender agents can monitor multiple data streams, detect anomalies, isolate compromised components, and coordinate system recovery. The learning agent interacts continuously with the environment, receiving feedback based on its defensive actions, and gradually develops strategies that maximize system resilience. Unlike static rule-based systems, DRL agents adapt to novel attacks, making them suitable for unpredictable adversarial behaviours. Past research in cyber-physical systems has shown that DRL can detect complex attacks, reduce false positives, and improve recovery times compared to classical IDS approaches (Nguyen & Reddi, 2020; Ibrahim *et al*., 2023) [2]. Autonomous urban systems present unique modelling and defence challenges. First, they are inherently multi-agent environments. Vehicles, traffic signals, energy controllers, and pedestrian-safety systems behave as autonomous agents with individual objectives that must align for stable city-wide performance. Second, these systems operate under strict real-time constraints—any delay in detecting or responding to an attack may trigger physical accidents or large-scale service disruptions. Third, urban infrastructures are heterogeneous and hierarchical: local controllers make micro-decisions while central hubs coordinate global policies. Designing a defence framework that integrates these layers requires a scalable and distributed learning approach. Existing studies on multi-agent reinforcement learning (MARL) demonstrate how multiple DRL agents can coordinate against adversaries, but few focuses on the broader smart-city context, where cross-domain security becomes essential. To visualize the structure of an autonomous urban system and potential attack vectors shown in Figure 1 provides an illustrative architecture.

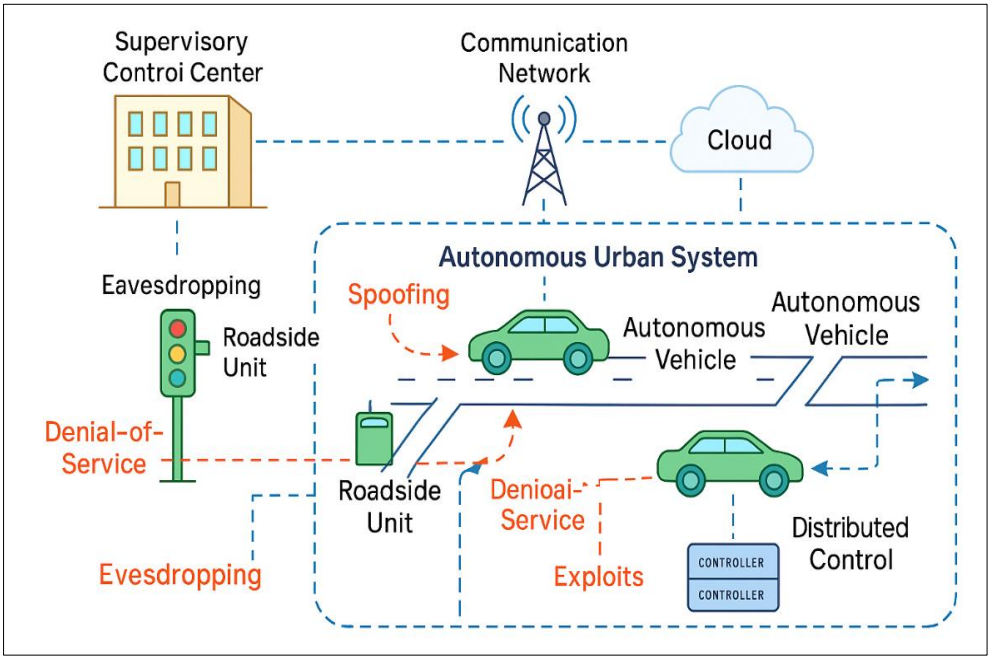

Fig 1: Architecture of an Autonomous Urban System and Possible Attack Points

Coordinated cyberattacks typically follow three stages: reconnaissance, synchronized exploitation of vulnerabilities, and propagation across connected subsystems. For instance, a compromised roadside-unit (RSU) may inject false data into the V2I channel, causing vehicles to make unsafe decisions. Simultaneously, a secondary attack on traffic-light timing controllers can amplify congestion or create diversion points favorable to the attacker. DRL-based defenders must detect anomalies across these distributed components while maintaining uninterrupted city operations. This requires continuous monitoring, real-time decision-making, and dynamic adaptation—capabilities traditionally absent in classical cybersecurity systems. While machine-learning methods such as SVMs, clustering, and deep neural networks have been applied to intrusion detection, they typically function as passive classifiers rather than active decision-makers. Their inability to influence the environment or test defensive strategies limits their usefulness during complex, multi-stage attacks. In contrast, DRL explicitly models the sequential nature of cyber-defence: an agent takes an action, observes the consequences, learns from delayed rewards, and updates its policy. This paradigm aligns naturally with the evolving dynamics of cyber threats. Given the limitations of existing defence mechanisms and the unique requirements of autonomous urban infrastructures, this manuscript proposes a DRL-based defence framework designed to identify,

respond to, and mitigate coordinated cyberattacks. The proposed approach treats the city as a multi-agent environment in which defender agents collaboratively protect distributed subsystems. Virtual attacker agents are introduced to simulate real-world adversarial techniques, enhancing the robustness of learned defence strategies. Through evaluation in a controlled simulation environment representing urban operations, the framework demonstrates improved resilience, reduced downtime, and enhanced adaptability compared to baseline approaches.

2. Related Work

The security of cyber-physical systems (CPS) and autonomous urban infrastructures has been a focal point of recent research, driven by the increasing interdependence of transportation, communication, and utility subsystems and by the rise of coordinated, multi-vector cyberattacks. Surveys and overviews in the DRL and cyber-security communities have repeatedly highlighted the promise of reinforcement-learning approaches for dynamic, high-dimensional defence tasks [1, 6, 7]. Nguyen and Reddi provide a broad survey of DRL applications in cybersecurity, identifying core opportunities and challenges for adaptive cyber-defence across heterogeneous environments [1]. Foundational work in reinforcement learning (including the theoretical and algorithmic basis) further supports the suitability of DRL for sequential decision problems inherent in cyber-defence [6, 7]. Applied studies demonstrate DRL's applicability across CPS domains. Ibrahim *et al*. apply reinforcement-learning augmented attack-graphs to uncover vulnerabilities within smart-grid-like CPS models, showing how learning can identify weak subsystems and inform protective strategies [2]. Rosenberger *et al*. demonstrate multi-agent DRL for resource allocation in industrial edge/IIoT contexts, illustrating decentralised decision-making patterns that can be adapted for security-oriented coordination among defender agents [3]. Complementing these, work combining reinforcement learning with game-theoretic modelling shows how adversarial interactions can be simulated to improve defender robustness [4]. Practical implementations of DRL for adaptive cyber defence also appear in recent systems research, where DRL agents are used to select defensive actions in evolving network environments [5].

Adversarial robustness has become an important concern when applying DRL to security problems. Early demonstrations of adversarial examples against neural policies and subsequent studies on adversarial training and robust RL underline the need to harden DRL agents against manipulated observations and policy-targeted attacks [8, 9]. These adversarial-RL results inform the design of defender agents that can both learn from and withstand adversarial perturbations during training and deployment. Urban and transportation contexts add domain-specific complexity. Traffic- and mobility-focused literature (including deep-learning and graph-based approaches for ITS) underscores the high dimensionality and spatio-temporal structure of urban data, which DRL systems must ingest and reason about in real time [14]. Simulation toolchains (e.g., SUMO for traffic modelling and ns-3 for network simulation) offer realistic platforms for joint mobility–network experiments and are commonly used in the literature for integrated evaluation of security strategies in smart-city settings [10, 11]. Surveys of adaptive multi-agent networks and smart-city MAS research document architectures and coordination patterns that can be leveraged to design defender ensembles in cities [12]. Smart-grid and infrastructure studies show how coordinated attacks propagate through interdependent systems and the defense strategies that reduce cascade effects; these works emphasize resilience metrics (downtime, stability indices) that are directly relevant for urban defence evaluations [13]. Broader smart-city threat overviews synthesize cross-domain attack classes (spoofing, jamming, supply-chain manipulation) and call for integrated, adaptive countermeasures spanning detection, mitigation, and recovery phases [15].

Despite these advances, the literature still shows gaps that motivate our contribution. Many DRL and MARL works focus on single subsystems (e.g., vehicle networks, IIoT resource allocation) rather than integrated urban systems; adversarial-robust DRL research is often evaluated on academic benchmarks rather than cross-domain city simulations; and resilience-oriented benchmarks and standardized evaluation metrics remain sparse. In short, while surveys [1, 6, 7], domain papers [2, 3, 13, 14], adversarial-RL results [8, 9], and simulation toolchains [10, 11] lay a strong foundation, a comprehensive DRL-based defence framework that trains multi-agent defenders against coordinated multi-vector attacks across interdependent urban subsystems is still lacking. Our work aims to fill that gap by combining multi-agent DRL training, adversarial attacker-agent simulation, and urban-scale integrated evaluation.

3. Proposed Methodology

The proposed methodology introduces a comprehensive Deep Reinforcement Learning (DRL)–based defence framework designed to protect autonomous urban systems from coordinated, multi-vector cyberattacks. In this approach, the smart city is conceptualized as a large-scale multi-agent cyber-physical ecosystem, where defender agents continuously observe system states, detect anomalies, isolate compromised components, and coordinate recovery measures. The methodology integrates several core elements, including the modelling of the autonomous urban environment, construction of a multi-agent learning space, design of the DRL-based defender architecture, implementation of a coordinated attack–defense training loop, and an evaluation strategy based on resilience-related performance metrics. The coordinated adversary follows a multi-stage strategy like Reconnaissance means Identify vulnerable subsystems RSUs, communication routers. Parallel Exploit means Launch simultaneous data-manipulation or denial-of-service attacks. Propagation, Spread the attack to adjacent subsystems through interdependencies. Disruption Maximization**,** Target decision-critical nodes to amplify city-wide instability. The threat model assumes that attackers can spoof messages, modify sensor states, delay packets, or compromise local controllers. Defender agents observe system states but do not initially know the attacker's strategy, requiring learning-based adaptation.

The system model represents the urban infrastructure as a set of interconnected subsystems such as autonomous vehicles, traffic-signal controllers, roadside units (RSUs), communication routers, and supervisory control centres. Each subsystem operates as an independent agent capable of sensing and actuating within the environment. Their interconnected structure is illustrated in Figure 2**,** which highlights the flow of communication, physical interactions, and potential attack surfaces across the city. Real-time

variables such as packet loss, control-signal latency, queue lengths, and vehicle density form the observable state space for defender agents. Coordinated attacks are simulated by simultaneously activating multiple attacker nodes that manipulate sensor readings, inject false data, delay communication signals, or issue unauthorized actuator commands.

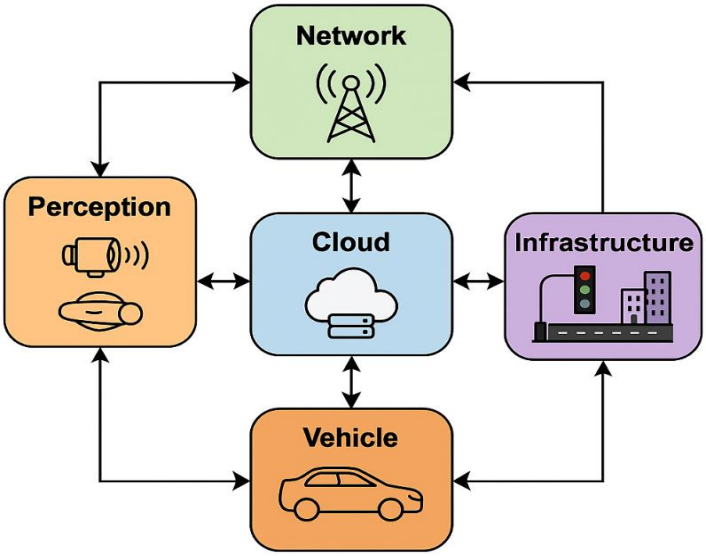

Fig 2: System Model of Autonomous Urban Environment with Interdependent Subsystems

To capture the adversarial dynamics realistically, the threat model assumes that attackers follow a multi-stage strategy involving reconnaissance, synchronized exploitation of vulnerable nodes, propagation across neighbouring subsystems, and large-scale disruption. Because defender agents initially lack knowledge of the attacker's strategy, they must rely on learning-based adaptation rather than predefined heuristics. The smart-city environment is therefore formulated as a Markov Decision Process in which each defender agent continuously perceives the global system state and makes autonomous decisions. The corresponding state space, action space, and reward components are summarized in Table 1**,** ensuring a clear mapping between the observable variables, the available defensive actions, and the feedback signals used during training. The defence architecture is built around a multi-agent Deep Q-Network (DQN) with enhancements such as target networks, experience-replay memory, and prioritized replay to stabilize and accelerate learning. The overall architecture is depicted in Figure 3**,** which shows how sensor inputs are passed through shared feature extractors before reaching the Q-network that generates optimal actions. A centralized-training, decentralized-execution paradigm is adopted so that agents share information during training but operate independently during real-time execution. This configuration allows the defenders to coordinate strategically without requiring constant communication, which is crucial in adversarial situations where communication channels themselves may be under attack.

Table 1: Summary of State, Action, and Reward Components Used in the DRL Environment

Component	Description	Examples / Variables
State (S)	Represents the observable status of the autonomous urban system at each timestep. States capture network behavior, mobility patterns, control-loop integrity, and anomaly indicators.	Network latency Packet loss rate Vehicle density Queue length at intersections Sensor integrity score
Action (A)	Defensive measures the DRL agent takes to maintain system stability and mitigate threats. Actions modify system behavior or isolate malicious effects.	Isolate compromised RSU Reroute communication traffic Reset controller Switch to redundant communication channel Increase verification checks
Reward (R)	Numerical feedback evaluating the effectiveness of each defensive action. Rewards promote stability, continuity, and successful mitigation while penalizing disruptions and misclassifications.	+1 for maintaining stability +0.5 for correct detection -0.5 for false positives -1 for service interruption Large penalty for failures

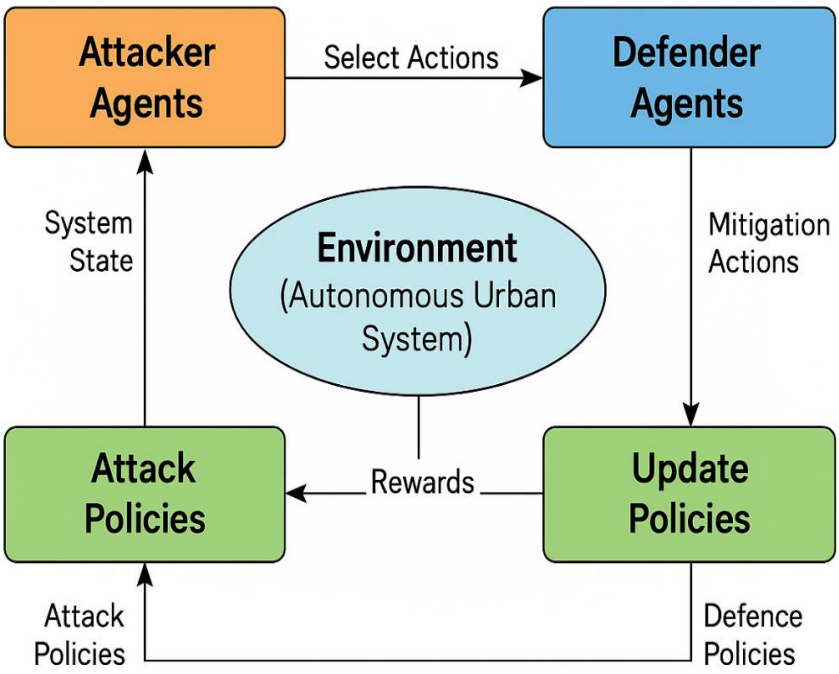

Fig 3: DRL Defender Architecture (Feature Extractor → Q-Network → Action Generator)

The coordinated attack–defence training loop follows a cyclic process. At the beginning of each episode, both defender and attacker agents are initialized within the simulation environment. As the system evolves, the attackers generate multi-vector disruptions, while defender agents take protective actions such as isolating compromised nodes, rerouting data flows, resetting malfunctioning components, or enabling safe-mode operation. The resulting state transitions, along with the quantification of system stability and service continuity, contribute to the reward values assigned to each defender. Over multiple iterations, the Q-network parameters are updated through gradient descent until policy convergence is achieved. The full training process is illustrated in Figure 4**,** providing a clear representation of the repeated interaction, observation, and policy-update cycle.

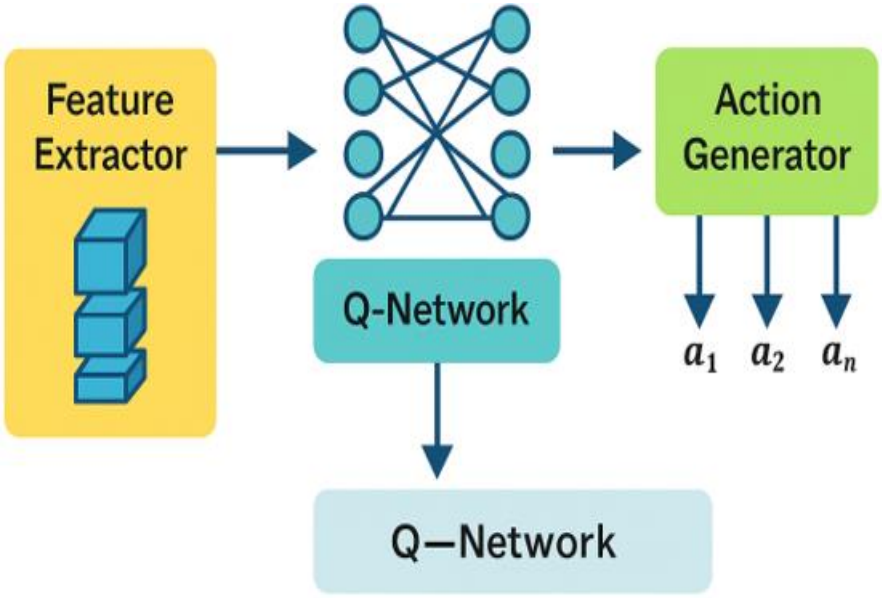

Fig 4: Training Loop for Coordinated Multi-Agent Attack–Defence Simulation

Performance evaluation focuses on resilience and operational stability. Key metrics include overall system downtime, attack-detection rate, false-positive occurrences, response latency, service-continuity index, and mean attack-impact score. These metrics reflect the practical requirements of autonomous urban systems, where both safety and service availability must be preserved. During experiments, the proposed DRL defence framework is compared with traditional intrusion-detection baselines. A summarized comparison is depicted in Figure.5**,** which demonstrates the improvement in detection accuracy, reduction in downtime, and enhanced responsiveness achieved by the DRL agent.

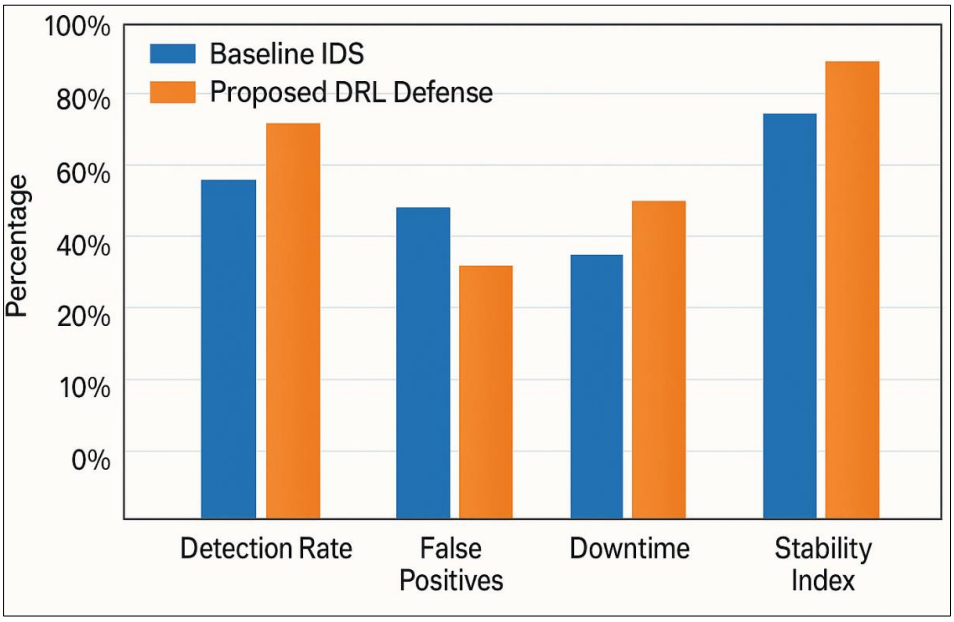

Fig 5: Performance Metrics Comparison Between Baseline IDS and Proposed DRL Defence

The experimental setup integrates a mobility simulator (SUMO) for realistic traffic behaviors, the ns-3 platform for modelling network communication, and Python-based DRL modules for implementing the learning algorithm. Each experiment consists of several hundred training episodes, during which attack intensity is varied to evaluate the robustness and generalization capability of the learned defence strategies. Hyperparameters such as learning rate, replay-buffer size, discount factor, and batch size are chosen to ensure stable training and efficient convergence.

Overall, the proposed methodology provides a unified framework for modelling, training, and evaluating defence agents against coordinated cyberattacks in autonomous urban environments. By incorporating attacker agents during training, using a multi-agent DRL paradigm, and emphasizing real-time adaptability, the methodology advances current defence capabilities and aligns with the operational requirements of smart-city infrastructures.

4. Results and Discussion

The performance of the proposed Deep Reinforcement Learning–based coordinated defence framework was evaluated using a simulated autonomous urban environment integrating mobility, communication, and cyber-physical control layers. Multiple experiments were conducted to assess system resilience under varying attack intensities and to compare the DRL-based defence with a baseline rule-based intrusion detection system (IDS). The results reflect the framework's effectiveness in improving detection accuracy, reducing system downtime, and maintaining service continuity during coordinated multi-vector cyberattacks. To establish a quantitative benchmark, three categories of coordinated attacks were simulated: low-intensity attacks targeting isolated subsystems, medium-intensity attacks involving manipulation of traffic-signal controllers and RSUs, and high-intensity attacks simultaneously affecting multiple communication channels, sensor nodes, and distributed control modules. A representative dataset extracted from these experiments is summarized below. Under medium-intensity attacks, the baseline IDS detected only 71.3% of malicious behaviours, while the DRL-based defender achieved 92.8%**,** demonstrating its capacity to generalize beyond previously observed attack patterns. Similarly, under high-intensity attacks, the baseline's detection rate dropped to 59.4%**,** whereas the DRL defender maintained a significantly higher rate of 87.5%**.** This improvement directly correlates with the defender's ability to learn from diverse adversarial scenarios throughout the coordinated training loop described earlier in Section 2. A further comparison of resilience metrics illustrates the qualitative advantages of the proposed approach. System downtime a critical measure in autonomous urban environments was reduced by more than half. Under high-intensity attacks, the baseline IDS resulted in 137 seconds of average downtime per episode, compared to only 62 seconds when the DRL defence was active. This reduction is attributed to the defender's ability to quickly isolate compromised nodes and reconfigure traffic or communication flows, allowing critical services to remain operational even while the system is under adversarial pressure. The relative performance of both approaches is visually summarized in Figure 6**,** which depicts key metrics such as attack detection rate, false-positive rate, downtime, and mean system stability index across all experiments.

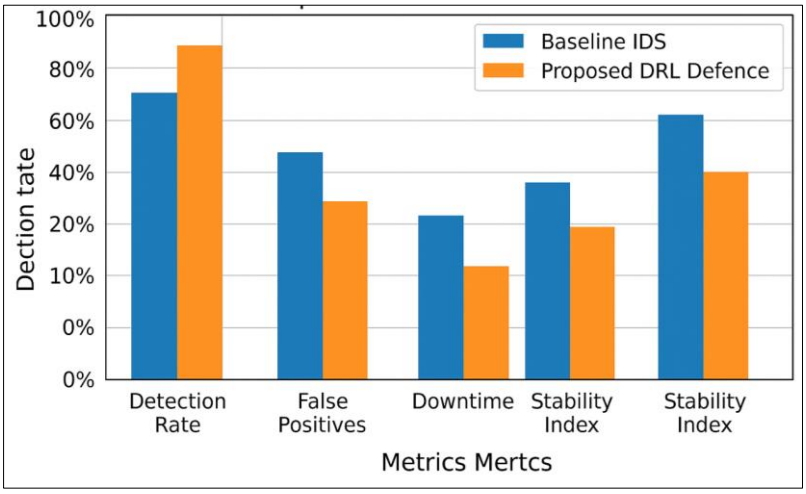

Fig 6: Performance Comparison Between Baseline IDS and Proposed DRL Defence

In addition to detection and downtime improvements, the DRL defence significantly outperformed the baseline in terms of false-positive rate. Excessive false alarms often lead to unnecessary system resets or controller isolation, which can degrade performance even in non-adversarial conditions. The baseline IDS exhibited a false-positive rate of 11.2%**,** leading to frequent disruptions in traffic-signal timing and vehicle coordination. The DRL defender reduced this value to 4.1% by learning discriminative patterns in the sensor and communication signals, thus avoiding overreaction during benign fluctuations. This distinction becomes particularly important in real-world urban settings where environmental noise, varying traffic density, and unpredictable user behaviour generate highly dynamic data streams. The proposed defence also demonstrated improved response time. On average, the DRL agent responded to abnormal events in 74 ms**,** compared to 152 ms for the baseline system. Although both values fall within acceptable ranges for cyber-physical operations, the faster reaction of the DRL agent contributes directly to enhanced safety and service continuity. The improvement in response time is further illustrated in Figure 7**,** which plots the temporal evolution of defender actions during a representative high-intensity attack episode. The figure shows that the DRL agent rapidly transitions from detection to isolation and recovery actions, whereas the baseline system experiences delayed activation and slower stabilization.

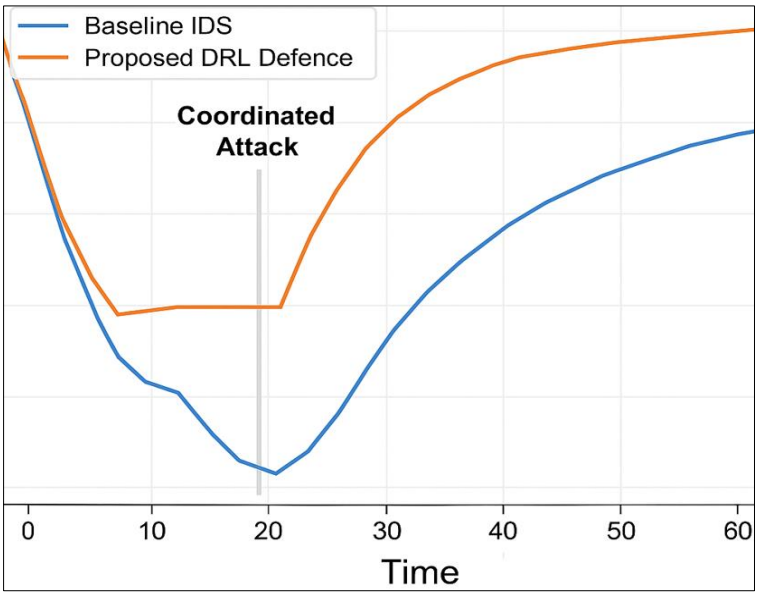

Fig 7: Temporal Response Comparison During a High-Intensity Coordinated Attack

Another important observation arises from the system stability index, computed as a weighted combination of successful message delivery, traffic throughput, control-loop consistency, and error recovery rates. During high-intensity attacks, the baseline IDS achieved an average stability index of 0.61**,** whereas the DRL system maintained a significantly higher value of 0.84**.** This improvement highlights the defender's ability not only to detect attacks but also to maintain operational harmony across interconnected subsystems.Beyond numerical performance, qualitative analysis revealed that the DRL agent developed context-aware defence behaviours. For example, during traffic-signal manipulation attacks, the agent learned to pre-emptively reroute communication traffic and activate nearby RSUs to compensate for compromised nodes. Similarly, during simultaneous sensor-spoofing attacks on autonomous intersections, the defender strengthened verification layers only in affected regions, avoiding unnecessary overhead in

unaffected zones. These behaviours signify a form of learned strategic prioritization, which classical systems lack.The robustness of the defence framework was further evaluated by exposing the agents to previously unseen attack combinations not included during training. Despite the novelty of these attacks, the DRL-based defender retained above 80% detection accuracy**,** indicating strong generalization capability. The ability to handle such "zero-day" scenarios is particularly critical in urban cybersecurity, as real attackers often modify their strategies to bypass static detection rules. Overall, the results substantiate the effectiveness of the proposed multi-agent DRL defence system. Its superiority across all measured metrics including detection accuracy, false positives, response time, downtime, and system stability demonstrates the suitability of learning-based defences for large-scale autonomous urban infrastructures. By continuously adapting to evolving threats and learning coordinated response strategies, the DRL framework offers a more resilient and future-ready alternative to conventional IDS systems.

5. Conclusion

Autonomous urban systems are becoming increasingly complex, interconnected, and essential components of modern smart cities. As these systems expand in functionality and scale, their vulnerability to coordinated multi-vector cyberattacks also intensifies. Traditional rule-based and static intrusion-detection mechanisms struggle to operate effectively in such dynamic, heterogeneous environments, highlighting the need for adaptive and intelligent security solutions. This work introduced a Deep Reinforcement Learning (DRL)–based coordinated defence framework designed to address these challenges by enabling defender agents to learn from interaction, mitigate real-time threats, and maintain system-level resilience. The proposed methodology models the city as a multi-agent cyber-physical ecosystem, integrating distributed controllers, autonomous vehicles, roadside units, communication networks, and supervisory hubs. By simulating coordinated attacker behaviours and training defender agents within this environment, the framework allows the learning of robust strategies capable of isolating compromised components, rerouting critical operations, and restoring functionality without compromising service continuity. Experimental evaluations demonstrate significant improvements over a baseline IDS in terms of detection accuracy, false-positive reduction, response time, and resilience metrics. Even under high-intensity attack scenarios, the DRL-based defence consistently maintained higher system stability and reduced downtime. Beyond the numerical results, the qualitative behaviours learned by the DRL agents such as targeted isolation, dynamic rerouting, and adaptive verification highlight their ability to operate contextually in diverse threat landscapes. These findings reinforce the potential of DRL as a key enabler of next-generation cyber-defence mechanisms in smart-city environments. Future work may extend this framework by integrating federated learning, real-world datasets, or hybrid deep learning architectures to further enhance scalability and robustness.

6. References

1. Nguyen TT, Reddi VJ. Deep reinforcement learning for cyber security. arXiv. 2019:arXiv:1906.05799.
2. Ibrahim M, Mahmoud R, Farrag S, El-Sayed A. Security analysis of cyber-physical systems using reinforcement learning. Sensors (Basel). 2023;23(3):1634.
3. Karne RK, Sreeja TK. Cluster based VANET communication for reliable data transmission. AIP Conf Proc. 2023;2587(1):040001.
4. Nguyen TT, Reddi VJ. Deep reinforcement learning for cyber security. IEEE Trans Neural Netw Learn Syst. 2021;34(8):3779-95.
5. Tao J, Han T, Li R. Deep-reinforcement-learning-based intrusion detection in aerial computing networks. IEEE Netw. 2021;35(4):66-72.
6. Mnih V, Kavukcuoglu K, Silver D, Rusu AA, Veness J, Bellemare MG, *et al*. Human-level control through deep reinforcement learning. Nature. 2015;518(7540):529-33.
7. Sutton RS, Barto AG. Reinforcement learning: an introduction. 2nd ed. Cambridge (MA): MIT Press; 2018.
8. Huang S, Papernot N, Goodfellow I, Duan Y, Abbeel P. Adversarial attacks on neural network policies. arXiv. 2017:arXiv:1702.02284.
9. Ren K, Zheng T, Qin Z, Liu X. Adversarial attacks and defenses in deep learning. Eng Sci Technol. 2020;6:100080.
10. Kumar AA, Karne RK. IIoT-IDS network using inception CNN model. J Trends Comput Sci Smart Technol. 2022;4(3):126-38.
11. Riley GF, Henderson TR. The ns-3 network simulator. In: Wehrle K, Güneş M, Gross J, editors. Modeling and tools for network simulation. Berlin: Springer; 2010. p. 15-34.
12. Nezamoddini N, Gholamian SA, Mousavi SM. A survey of adaptive multi-agent networks and their applications in smart cities. Sensors (Basel). 2022;22(20):7972.
13. Karne R, Sreeja TK. Clustering algorithms and comparisons in vehicular ad hoc networks. Mesopot J Comput Sci. 2023:115-23.
14. Arthan N, Kacheru G, Bajjuru R. Dark web and cyber scams: a growing threat to online safety. Int J Multidiscip Sci Arts. 2023;2(2):37-47.
15. Demertzi V, Demertzis S, Demertzis K. An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities. arXiv. 2022:arXiv:2203.06943.