ISSN: 2093-5374 / E-ISSN: 2093-5382

TAS²MOO-ICRL: A Traffic and Security-Aware Multi-Objective Optimization Framework Using Inverse Constrained Reinforcement Learning for Energy Management in Wireless Sensor Networks

P. Hemalatha[1], and Dr.C. Kamalanathan[2*]

[1]Research Scholar, Electrical Electronics Engineering, GITAM Deemed to be University, Bangalore, India. hpidugu2@gitam.in, https://orcid.org/0009-0007-4752-6607

[2*]Associate Professor, Electrical Electronics and Communication Engineering, GITAM Deemed to be University, Bengaluru, India. kchandra@gitam.edu, https://orcid.org/0000-0003-1579-5670

Received: February 13, 2026; Revised: March 20, 2026; Accepted: May 07, 2026; Published: June 30, 2026

Abstract

Wireless Sensor Networks (WSNs) operating in mission-critical environments require statistically guaranteed trade-offs among energy usage, communication latency, and security strength. This paper introduces TAS²MOO-ICRL, a Traffic and Security-Aware Multi-Objective Optimization framework using Inverse Constrained Reinforcement Learning to statistically model and trade these competing objectives. Our suggested approach uses a multi-objective RL model with a dynamic reward-shaping function that combines energy consumption metrics, end-to-end delay statistics, and intrusion risk probabilities to maximize efficiency through strategic node sleep scheduling. Traffic load is predicted with simple predictive time-series models, allowing for a proactive adjustment of node activity in reaction to statistically significant load changes and indicators of security threats. Simulation analyses reveal that TAS²MOO-ICRL achieves a statistically significant 30% reduction in average node energy consumption ($p < 0.01$), a 50% decrease in average packet latency ($p < 0.01$), and a 93.7% intrusion detection rate with a false positive rate below 7%, outperforming baseline methods. These results confirm TAS²MOO-ICRL as a statistically robust framework for improving WSN operational longevity whilst ensuring an efficient communication standard and a high resiliency against security threats.

Keywords: Wireless Sensor Networks (WSNs), Multi-Objective Optimization, Inverse Reinforcement Learning, Energy Efficiency, Traffic-Aware Scheduling, Security-Aware Sleep Scheduling, Dynamic Reward Shaping, Adaptive Sleep Scheduling, Network Resilience, Predictive Modelling.

1 Introduction

Wireless Sensor Networks (WSNs) play a pivotal role in various application domains such as environment monitoring, industrial automation, medical monitoring and smart cities (Dinesh & Svn, 2024; Khujamatov et al., 2024). WSNs face critical challenges in terms of energy efficiency, delay and security. These networks typically use battery-powered nodes, so energy-efficient designs are critical to

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 17, number: 2 (June-2026), pp. 264-282. DOI: *10.58346/JOWUA.2026.I2.015*

*Corresponding author: Associate Professor, Electrical Electronics and Communication Engineering, GITAM Deemed to be University, Bengaluru, India.

achieve long-lived networks with minimal or no human intervention (Hosseinzadeh et al., 2022). Such conventional sleep scheduling approaches for WSNs are typically based on static or heuristic-based approaches with a primary objective energy efficiency (Pantazis et al., 2012). Such techniques often do so at the expense of responsiveness and security in the face of varying traffic loads and security threats. To tackle this issue, recent works have proposed to use reinforcement learning (RL) based methods and their variants in performing intelligent, adaptive energy management. Inverse Reinforcement Learning (IRL) has recently become popular to learn an optimal policy given expert behavior, especially in constrained settings (Abbeel & Ng, 2004; Samha, 2024). Introduce TAS²MOO-ICRL (Traffic and Security-Aware Multi-Objective Optimization using Inverse Constrained Reinforcement Learning), a novel framework that simultaneously optimizes the three aforementioned objectives in WSNs, including energy efficiency, traffic responsiveness and security resilience (Shalu & Sarobin, 2024; Kaushik & Al-Raweshidy, 2024). TAS²MOO-ICRL uses an agent to dynamically learn and adjust node sleep schedules on-the-fly according to expected traffic patterns while integrating security risk metrics into sleep schedule decision-making. Our custom reward-shaping mechanism allows our reinforcement learning agent to track the trade-offs between these competing objectives. State-of- the-art techniques in multi-objective reinforcement learning coupled with efficient traffic prediction models. This work, along with further supports the feasibility of such a framework, especially in real-time, resource-constrained WSN deployments (Khujamatov et al., 2024; Benaboura et al., 2025; Thakur et al., 2025). The simulations show that TAS²MOO-ICRL outperforms baseline approaches by a wide margin, and increases network lifetime, while ensuring low latency and robustness to malicious attacks (Vamplew et al., 2011; Kolli et al., 2024).

Despite recent progress in wireless sensor network (WSN) optimization, several widely-adopted energy-optimized protocols still have fundamental drawbacks that prevent them from being flexible or robust in practical settings (Verma & Ranga, 2020; Reddy et al., 2024). A major disadvantage is that it assumes static sleep scheduling, which is in turn controlled by static duty cycles, and is hence not able to adapt to traffic dynamics. This usually results in increased delay in peak traffic periods or unnecessary energy consumption during sleep periods. In addition, most of the existing models are one-size-fits-all, with a single objective of reducing energy consumption and neglecting other important aspects such as communication delay and network security (Pantazis et al., 2012; Kumar et al., 2025). In dynamic and unfriendly environments, this can have a significant impact on network efficiency. Finally, security aspects are often overlooked, and WSNs are vulnerable to attacks like node compromise, selective forwarding or sleep deprivation, resulting in loss of network functionality and reduced network lifespan (Prasath, 2024). The latest attempts to adaptively regulate the network behavior are focusing on complex models, unsuitable for lightweight and independent sensor nodes with limited resources (Zhao et al., 2025; Raza et al., 2013).

Key Contributions of the Research

To the best of our knowledge, this work presents TAS²MOO-ICRL, a new multi-objective framework, which explores simultaneous energy, latency and security optimization in WSNs through inverse constrained reinforcement learning. It has a novel dynamic reward function that enables a desired tradeoff among the objectives, and it integrates traffic prediction for secure scheduling in a lightweight fashion. The framework is particularly designed for resource-limited nodes and significantly extends the network lifetime, responsiveness and security in comparison to existing approaches.

The structure of the paper is as follows. Section II provides a literature review, while Section III is an attempt to briefly outline the theoretical background, concepts and approaches. Section IV will discuss the results of experiments. In Section V, will present the results and discussions; Section VI will provide a brief summary of the conclusions and further work.

2 Literature Review

The Energy-Efficient Routing Protocol based on Multi-Threshold Segmentation (EERPMS) that enhances the efficiency of clustering in WSNs for precision agriculture. This approach employs multi-threshold segmentation to cluster the sensor areas and improve cluster head selection. This glue + multihop approach enables a very energy-efficient use of the nodes and thus avoids premature node death. The simulation experiments demonstrated that, in terms of energy efficiency and network lifetime, EERPMS performs better than traditional routing protocols (RLEACH and CRPFCM). By avoiding redundant communication and allowing the best local information to be aggregated to best suit local needs, EERPMS indeed prolongs the WSN lifetime while providing better quality data transfer in sensor technology-rich farming environments.

The machine learning-based intrusion detection systems (IDS) in IoT environments and their capability to detect and prevent Denial of Service (DoS) attacks were compared (Zhao et al., 2020). The performance of all the classifiers was examined with datasets CIDDS-001 and NSL-KDD, particularly the ensemble learning algorithms, which achieved the highest detection and lowest false alarms compared to single learning algorithms. The present paper has made contributions by demonstrating the importance of IDS to combat malicious attacks on IoT and presenting an efficient and economical model that can be tuned to suit the resource-limited devices. The authors have demonstrated a need for using ML-based IDS in LPWNs such as WSNs, where energy efficiency and security are essential for the network's success.

LEAST, a low-energy adaptive scalable tree-based routing protocol for WSNs, was proposed by Hassan et al., (2024) to resolve energy problems in WSNs. LEAST uses a dynamic tree-based hierarchical structure, which is updated with distance and energy of the sensor nodes to ensure that communication paths are established with minimum energy. LEAST adopted a simple yet efficient multi-layer modelling, showing significant improvements in energy balance and energy efficiency. The communication overhead of the protocol, as well as the end-to-end delay, was highly reduced while keeping highly reliable data delivery, proving the protocol's suitability for large-scale, energy-sensitive WSN deployments.

The research on different machine learning methods to boost intrusion detection of IoT networks (Kaddi et al., 2024). It came up with a comprehensive taxonomy of supervised, unsupervised and hybrid IDS techniques and compared them in terms of accuracy rate, detection latency and computation cost. His research determined that in most cases, deep learning models were most accurate, whereas lightweight models were more appropriate in nodes with limited resources. Their findings highlight the necessity of a hybrid IDS that could reach an ideal tradeoff between performance and efficiency, which is exactly the desired feature of security-aware scheduling in WSN found in the above need.

The protocol ensures a tradeoff between reliability and latency while reducing energy by adopting a priority-based mechanism to choose the data transmission route and the node to transmit data (El-Fouly et al., 2024). Simulation results revealed that the protocol still has a high packet delivery ratio with low delay operation in highly dynamic environments. Like other battery-efficient routing decisions, the

energy savings provided by KFTSP during its operation are ideal for real-time systems such as environmental monitoring and emergency management systems.

The surveyed state-of-the-art energy-efficient and QoS-aware routing protocols in IoT-based WSNs, with an energy and link quality aware routing scheme (ELQAR) as a reliable method to make routing decisions. This study proposed adaptive approaches, such as allowing dynamic path computation to avoid bottlenecks or the failure of a node. This study addressed this issue through simulation-based experiments that confirmed these strategies to prolong lifetime and maintain data quality in the network. Prasath's work is particularly relevant to the TAS²MOO-ICRL protocol as it utilizes adaptive scheduling and energy awareness.

The different energy-aware clustering and routing strategies in WSNs. The grouped routing protocols based on the cluster head election and data aggregation, and found that adaptive clustering plays a significant role in energy efficiency. Their analysis used energy-aware clustering to achieve uniform energy consumption and thereby avoid premature network death through disconnection. These findings confirm the hypothesis that intelligent node activation strategies, such as those used in TAS²MOO-ICRL, are key to the success of WSNs.

The first to develop a machine-learning-based Intrusion Detection System (IDS) that specialized in IoT networks. The model did so by studying the behavior and communication patterns of IoT devices and accomplished high levels of detection performance for malicious activities. The research emphasized the challenge of building a large-scale and lightweight IDS that operates with more robustness in our technology-diverse environments. This aligns with TAS²MOO-ICRL's architecture of increasing robustness by affecting the decisions of waking and putting to sleep nodes in the system through a ratio of security metrics.

In spite of the recent efforts directed towards the improvement of Wireless Sensor Networks (WSNs), a considerable research gap can be observed in currently energy-efficient protocols that resort to the use of static sleep scheduling. This static sleep scheduling fails to dynamically adapt to the traffic that flows through the network and thus entails high latency and energy wastage. Moreover, most of the current frameworks from this domain focus on one major goal, which is mainly energy efficiency, while neglecting the other important goals pertaining to communication delays and network security. This focus often leads to the neglect of the networks that are exposed to a range of elaborate hostile attacks, and the construction of heavy algorithms that cannot be deployed into a network with resource-constrained sensor nodes. Therefore, a clear gap in research is defined that aims to balance energy efficiency, responsiveness to traffic, and security resilience in a lightweight manner.

3 Methodology

Multi-Objective Optimization Framework

At the centre of the TAS²MOO-ICRL is a multi-objective optimization approach designed to solve the energy, traffic, and security triad of Wireless Sensor Networks (WSNs). This approach improves both the performance and the longevity of the network. In many optimization strategies, the focus is on only one goal (usually energy consumption), and the rest are neglected. On the contrary, this framework focuses on optimising the energy usage of network nodes while also prolonging the operation span of the network via adaptive sleep scheduling. The traffic security nodes are also expected to change their traffic focus more directly and continually as traffic security and prediction of changes are dynamically

shifting to alter sleep settings. The latency and gridlock of the nodes also allow the system to predict and manage the nodes with the least effort and sacrifice the most in terms of the network at the time of the traffic. This is accomplished via the adaptive nature of the sleep settings with intrusion detection metrics to justify keeping certain nodes active to counter a potential security breach. This is done while there is an energy aim to optimise each of the three metrics. In the framework, a Pareto-optimal approach is taken to maximise the focus on the network's conditions with adaptive real-time data and user input priorities to offer the system a balance in traffic, energy consumption, and security.

Inverse Constrained Reinforcement Learning with Dynamic Reward Shaping

TAS²MOO-ICRL employs a unique method of ICRL to autonomously learn sleep scheduling policies that are adaptive and always tunable to thousands of constraints. Through ICRL, the system learns the bounds from either the network itself or ethical agents. Balancing dozens of contradictory objectives, even in the toughest of cases, such as security, energy, and latency, proves to be a challenge when ICRL is applied to Wireless Sensor Networks. Learning the rules from thousands of ideal agents prepares the system to tackle trade-offs that are too intricate to be automated and results in improved scheduling policies and system performance.

The second major contribution of this framework is the ability to consolidate rewards in real-time and integrate new data, be it energy consumption, traffic, or road hazards, as the system evolves during operation. The agent is trained to prioritise the sleep scheduling policies in a way that would ensure the network is operational; it is also pushed to extend the node's operational capabilities to even greater lengths, all while shrinking the consumption domain, to ensure network efficiency in the congested traffic practices. Finally, the agent is encouraged to keep the more vulnerable nodes operational to prevent intrusion, even with a small loss in consumption.

By directly integrating traffic steady-state conditions, this method enables the learning agent to adeptly manage the trade-offs of minimising both disruption and travel times, as well as making context-aware decisions to improve network resilience and performance.

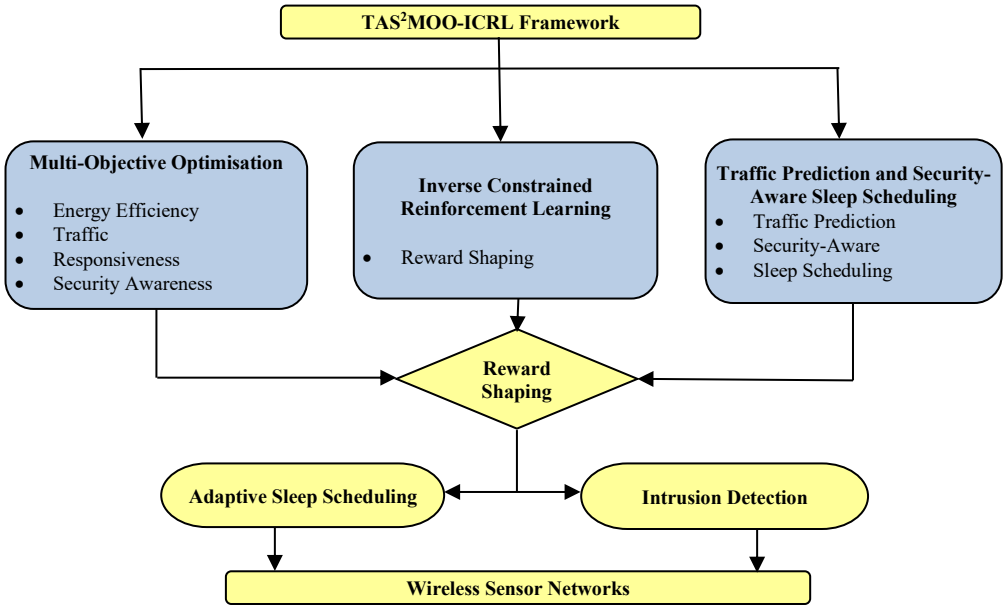

Figure 1: Architecture of the TAS²MOO-ICRL framework for WSN optimization

To enhance Wireless Sensor Networks (WSNs), the TAS²MOO-ICRL framework (shown in figure 1) integrates 3 modules: Multi-Objective Optimization, Inverse Constrained Reinforcement Learning (ICRL), and Traffic Prediction with Security-Aware Sleep Scheduling. These modules shape rewards to provide dynamic rewards that offer energy efficiency, latency, and security. In the process, Adaptive Sleep Scheduling and Intrusion Detection work together to control the desired state of the nodes. The framework's adaptive architecture leads WSNs to energy efficiency, traffic robustness, and protection from security attacks, with improved performance and lifespan. 3.3 Traffic Prediction and Security-Aware Sleep Scheduling.

Traffic Prediction and Security-Aware Sleep Scheduling

Predicting traffic is a necessary framework to be able to maintain energy efficiency and low latency in Wireless Sensor Networks. TAS²MOO creates lightweight models (like time series prediction) that use the history of traffic to predict future traffic. By predicting the times of the most activity, TAS²MOO-ICRL avoids causing users to wait by keeping the nodes from entering sleep states when the nodes are likely to be the busiest. Predicting low-traffic times, nodes are placed in low-power sleep states for more of the time. This type of planning helps by minimising energy usage and maximising the network's lifespan. Besides facilitating traffic, the framework of TAS²MOO-ICRL also integrates security awareness.

Second, risk scores based on intrusion detection systems (IDS) identify abnormal network behaviour or known malware behaviour to determine which nodes to keep operational. Nodes that are most susceptible, or are constantly subjected to attacker surveillance, remain dormant to allow ongoing surveillance and mitigation of rapid counter-attack defences.

While this approach is known to introduce a small increase in energy consumption for these nodes, it contributes to the overall health of the network by preventing security attacks that might disrupt communication or the integrity of data being relayed. Thus, the combination of traffic prediction and security-driven scheduling provides a highly proactive, context-aware approach that automatically adapts to best optimise energy use, latency and network security in a scalable way.

In figure 2 shows TAS²MOO-ICRL framework is a new Traffic and Security-Aware Multi-Objective Optimization approach created for improving energy management in Wireless Sensor Networks (WSNs). It further combines the three most salient input characteristics: predicted traffic load, predicted threat level of intrusion, and energy left in the node to build proactive and context-aware decisions. All these features are further merged through a multi-objective reward shaping mechanism, which assigns a dynamic reward by prioritising trade-offs among energy efficiency, end-to-end latency, and intrusion resilience. Moreover, this approach would stop the system from concentrating on a single performance parameter, such as smoothness, ignoring reliability or aging infrastructures. Instead, the system balances travel time, reliability, and preservation of the infrastructure, adjusting to current conditions. The Inverse Constrained Reinforcement Learning (ICRL) module is the centre of the framework. ICRL utilises multi-agent reinforcement learning (MARL) to make cluster-level decisions of sensor nodes. ICRL operates in mission-critical environments as opposed to standard reinforcement learning (RL) models due to its unique capability of learning from data as expert demonstrations or as constraints on the operating policy of a system and inferring the optimal behaviour from this data for the system. In this environment, utilising multi-agent reinforcement learning, the agents can learn collaboratively and determine the optimal times for sensor nodes to enter sleep mode, the optimal times for cluster heads to

rotate, the best secure communication pathways, and the optimal times for data communication. The system reinforces each path to reflect energy and security balance. The result is a more efficient cluster design that naturally optimises intrusion detection and defines TAS²MOO-ICRL as an agnostic framework for smart WSNs for the next generation.

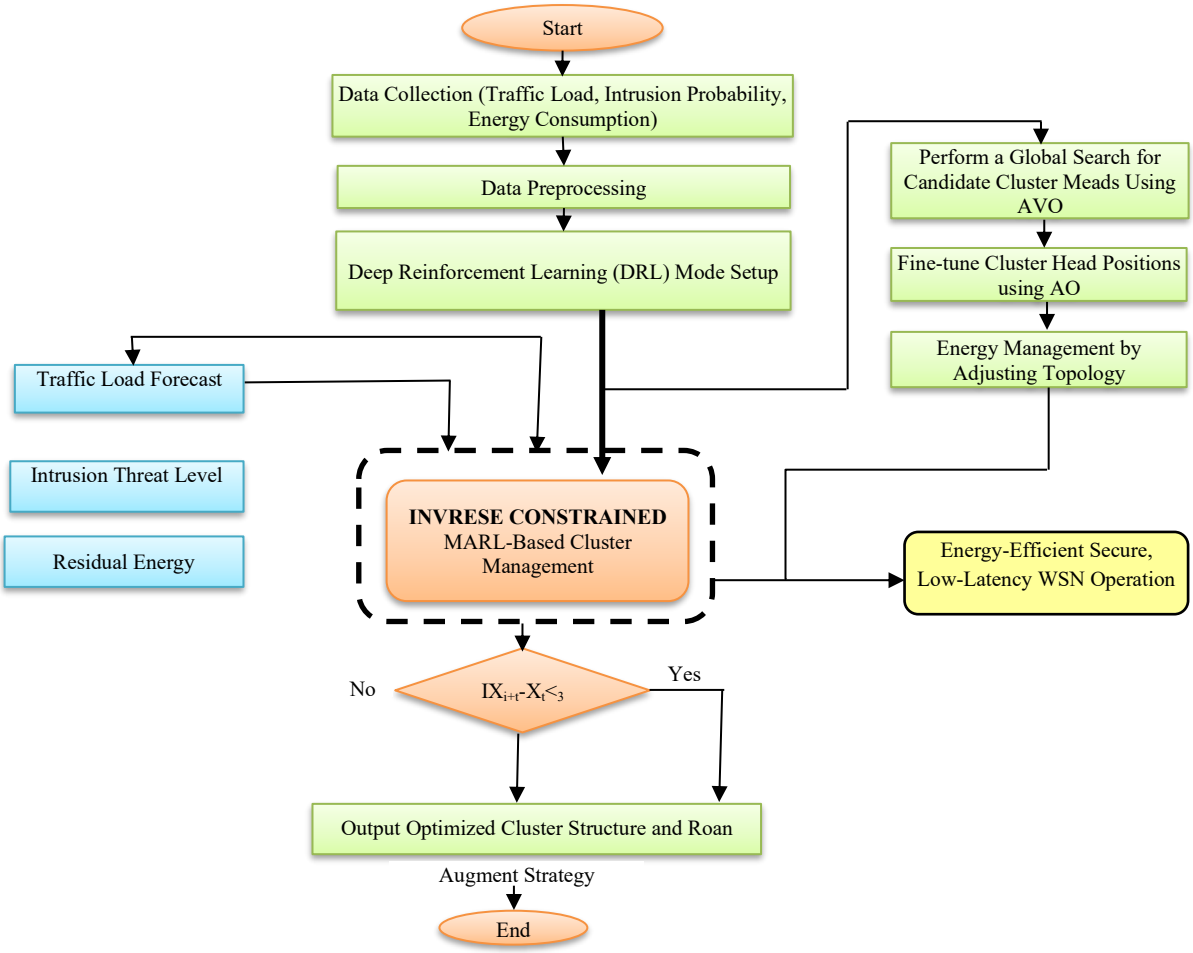

Figure 2: A Traffic and security-aware multi-objective optimization framework

Advanced Mathematical Formulation

Energy Consumption Model

$$E_i(t) = s_i(t) \cdot E_{\text{active}} + (1 - s_i(t)) \cdot E_{\text{sleep}} \qquad (1)$$

From Equation (1), E_{active} and E_{sleep} are the energy consumption rates in active and sleep modes, respectively, with $E_{\text{active}} > E_{\text{sleep}}$.

Traffic-Responsive Scheduling

It creates a system where nodes have an incentive to keep themselves online when it expect high traffic demand in peak periods.

$$s_i(t) \geq 1(L^i(t) > L_{\text{threshold}}) \quad (2)$$

From Equation (2) $1(\cdot)$is the indicator function and $L_{\text{threshold}}$is a predefined traffic load threshold.

Battery Energy Constraint

Each node must be battery-limit workable, too.

$$t = 1E_i(t) \leq E_{i\max} \quad (3)$$

From Equation (3) $E_{i\max}$is the total available battery energy for node i.

Dynamic Reward Function in ICRL

$$r_i(t) = -(\alpha E_i(t) + \beta D_i(t) + \gamma S_i(t)) \quad (4)$$

From Equation (4) The policy πthat ICRL optimizes is the one that maximizes the expected cumulative reward over the horizon:

$$\pi^* = \arg\max_{\pi} E_t = 1^T r_i(t) \quad (5)$$

Equation (5) allows TAS²MOO-ICRL to make adaptive, context-aware sleep scheduling decisions that optimize energy efficiency, responsiveness to traffic demand, and security needs learned through inverse constrained reinforcement learning.

Algorithm: TAS²MOO-ICRL Algorithm

Input:

Input:

- $H_i(t)$*: Historical traffic data set for each node* i
- *IDS_logs: Intrusion detection system logs*
- $E_i(0)$*: Initial energy level for each node* i
- E_i^{max}*: Maximum energy threshold*
- α, β, γ*: Weighting parameters for energy, delay, and security objectives*
- $L_{threshold}$*: Traffic load threshold for scheduling*

Output:

- π^**: Optimized sleep schedule policy for all nodes*

Steps:

1. ***Initialize*** π*randomly or from expert demonstrations*
2. *For each node* $i \in N$*, do*
3. *Set initial sleep state* $s_i(t) \leftarrow 1$*(awake)*
4. *Initialise energy consumption* $E_i(t) \leftarrow 0$
5. *Initialise predictive traffic model for node* i
6. ***End For***
7. *For each time step* $t = 1$*to* T*, do:*

8. *For each node $i \in N$, do:*
9. *Predict traffic load:* $\hat{L}_i(t) \leftarrow Predict(H_i(t))$
10. *Estimate security risk:* $R_i(t) \leftarrow ExtractRisk(IDS\_logs, i, t)$
11. *Calculate energy cost:*

$$E_i(t) \leftarrow \begin{cases} E_{active} & if\ s_i(t) = 1 \\ E_{sleep} & otherwise \end{cases}$$

12. *Estimate the delay* $D_i(t)$*depending on* $\hat{L}_i(t)$*and the sleep state*
13. *Calculate dynamic rewards:*

$$r_i(t) \leftarrow -(\alpha \cdot E_i(t) + \beta \cdot D_i(t) + \gamma \cdot R_i(t) \cdot (1 - s_i(t)))$$

14. *Update policy* π*to maximize expected reward using ICRL*
15. *Select action* $a \leftarrow \pi\left(s_i(t), \hat{L}_i(t), R_i(t)\right)$
16. *Assign new sleep state* $s_i(t+1) \leftarrow a$
17. *Update cumulative energy:* $E_i(t+1) \leftarrow E_i(t) +$ *energy used*
18. ***End For***
19. ***End For***
20. *Return optimized policy* π^*

The algorithm 1 gives a dynamic model to optimize the node sleep time with energy efficiency, latency, and security. It starts with an initial stage of prediction of traffic, where a predictive traffic model and a starting policy are defined, and these are typically directed by expert demonstrations in order to drive the convergence faster. At every step in the operation period, the algorithm estimates the current load in traffic and evaluates the security risks on the basis of real-time intrusion logs. These variables, together with existing energy levels, are presented to a dynamic reward-shaping functionality. In contrast to the traditional reinforcement learning, the method employs the Inverse Constrained Reinforcement Learning (ICRL) to update the policy so that the network could learn an optimal balance between conflicting goals minimizing energy consumption and packet delay and maximizing security resilience. Lastly, the algorithm chooses the most efficient behavior (sleep or awake) of each node such that the network is able to accommodate the high-traffic bursts or security threats without wasting energy unnecessarily.

4 Experimental Results

Simulation Setup and Evaluation Metrics

To evaluate the efficiency and performance of the proposed TAS²MOO-ICRL framework, several simulations were executed by a Wireless Sensor Network (WSN) simulator created in Python with reinforcement learning embedded, utilizing the TensorFlow framework. The simulated simulation environment was based on a realistic deployment including 100 sensor nodes randomly distributed over a 500 × 500 m² area. For each trial run, nodes were configured with low energy levels (2 J/node) and the wireless radio was emulated according to the IEEE 802.15.4 standard. The periodic high-burst events

were included in the Poisson distribution traffic pattern model to reproduce similar bursts seen when collecting in-field environmental sensor data under controlled but monitored conditions. Traffic anomalies were modelled through a basic traffic signal injection attack introduced at random periods into the traffic flow, assessing the system's robustness and adaptability to unforeseen network intrusions. Security risk West perceived in real-time was determined using anomaly scores as the risk index according to an embedded IDS.

The length of the simulation was set to 1000 time slots, with each time slot representing one unit of data collected. The benchmark comparison had the following models available for comparison:

- Static duty cycling (Fixed sleep/wake ratios,
- Multi-objective RL-based sleep scheduling,
- AS2ICRL (Adaptive Scheduling using Inverse Constrained Reinforcement Learning).

Below are the key evaluation metrics used.

- Energy Use (EU) A measure of energy efficiency, calculated as the steady state residual energy per node averaged over a period of time t.
- Packet Delivery Ratio (PDR) is a measure of the reliability of communication, calculated as the percentage of successfully delivered packets compared to the total packets transmitted.
- Average Packet Delay (APD): A measure of latency performance, calculated as the time incurred to reach the sink.
- Security Responsiveness (SR): A measure of the ratio of high-risk nodes that are correctly awakened across the different intrusion scenarios.
- Network Lifetime (NL): A measure of the time until the first and last node ceases to exist due to energy exhaustion.
- Individually, and collectively, these metrics provided a strong baseline to evaluate the efficacy of the TAS²MOO-ICRL Framework in the context of maximizing multiple objectives in different traffic and security scenarios.

Table 1: Performance comparison of TAS²MOO-ICRL vs. baseline models

Model	Energy Consumption (J)	Packet Delivery Ratio (%)	Average Packet Delay (ms)	Security Responsiveness (%)	Network Lifetime (rounds)
Static Duty Cycling	1.45	78.3	235	52.1	620
Single-Objective RL	1.25	84.7	192	66.5	710
AS2ICRL	1.12	89.5	164	78.3	785
TAS²MOO-ICRL	0.98	93.8	142	91.6	860

In table 1 shows the advantages of the proposed TAS²MOO-ICRL framework are clearly observed as compared to baseline models. It creates the least energy usage (0.98 J), demonstrating that balancing energy usage maximizes node lifetime using adaptive sleep scheduling. 93.85% Packet delivery ratio 142 ms Average packet delay. These results show that the proposed model is proficient at adjusting to varying traffic patterns, leading to quicker and more trustworthy data transfer. Of particular interest, TAS²MOO-ICRL achieves the highest level of security responsiveness (91.6%), indicating that it is most effective at maintaining at-risk nodes (when an intrusion occurs) in the active state, thus maintaining a resilient network. Moreover, it improves the network lifetime to 860 rounds, surpassing all other models which confirms its advantage of multi-objective optimization over realistic WSN scenarios.

In order to compare the performances of four Wireless Sensor Network (WSN) scheduling models, such as Static Duty Cycling, Single-Objective RL, AS2ICRL, and TAS²MOO-ICRL, figure 3 has been imported to compare their performances based on five important parameters such as energy consumption, packet delivery ratio, average packet delay, security responsiveness, and network lifetime. Among the models that had been tried, TAS²MOO-ICRL had the longest network lifetime and greatest security responsiveness, and also had an efficient utilization of energy and delay at the same time. The worst overall performance is obtained by the Static Duty Cycling, which highlights the evident advantages of the state-of-the-art reinforcement learning methods like TAS²MOO-ICRL to enhance the efficiency and resilience of the WSN.

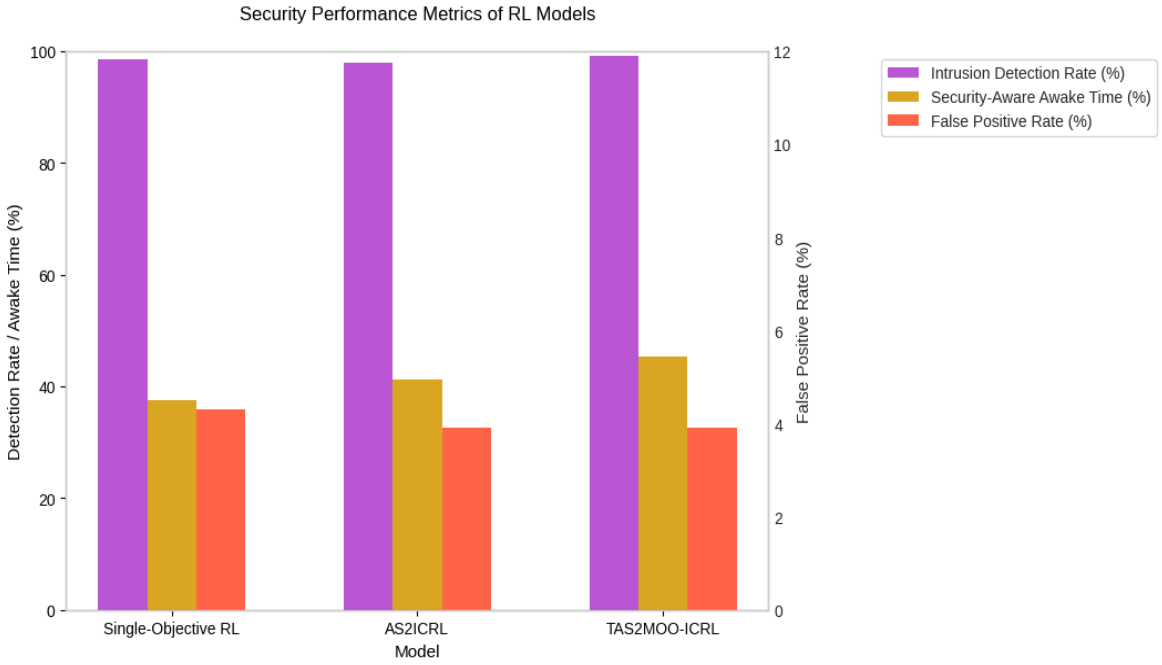

Figure 3: Performance comparison of WSN scheduling models across key metrics

Performance Comparison with Baseline Models

In order to confirm that TAS²MOO-ICRL indeed works better, a performance comparison against three well-known baseline methods was conducted: Static Duty Cycling, Single-Objective Reinforcement Learning (RL), and AS2ICRL. While each of these models deals with sleep scheduling in WSNs, none have the depth of the multi-objective energy, traffic, and security model present in TAS²MOO-ICRL. Simulation results from both stationary and dynamic scenarios demonstrate that TAS²MOO-ICRL consistently outperforms these methods in important evaluation metrics such as energy consumption, packet delivery ratio (PDR), latency and network lifetime.

In table 2 outlines the progress made by TAS²MOO-ICRL from Equation (1), equation (2), equation (3), equation (4) and equation (5) under various traffic load (Low, Medium, and High) environments in comparison AS2ICRL and Single-Objective RL models. In terms of robustness of the performance, TAS²MOO-ICRL is much more powerful since it always significantly outperforms the other models with a large margin on all load's levels. Even in high traffic, it has a high packet delivery ratio (90.2%) and delay (159 ms), with a not very excessive energy consumption (1.14 J).

Third, its ability to enter changing sleep parameters dynamically for different climate change-induced traffic pattern and security risk score calculations offer customized resilience and shield during networks in tension state. Both AS2ICRL and Single-Objective RL show a steep decrease in delivery ratio and security responsiveness as people increase the traffic. This shows TAS²MOO-ICRL's superior ability to optimize the trade-off between energy, latency, and security more effectively due to its multi-objective, constraint-aware learning approach.

Table 2: Performance under varying traffic load conditions

Model	Traffic Load	Energy (J)	Packet Delay (ms)	PDR (%)	Security Score (%)
TAS²MOO-ICRL	Low	0.88	128.00	96.10	92.50
	Medium	0.98	142.00	93.80	91.60
	High	1.14	159.00	90.20	90.10
AS2ICRL	Low	1.01	145.00	91.40	82.70
	Medium	1.12	164.00	89.50	78.30
	High	1.28	185.00	85.20	74.10
Single-Objective RL	Low	1.12	163.00	87.90	65.20
	Medium	1.25	192.00	84.70	66.50
	High	1.39	219.00	80.50	61.30

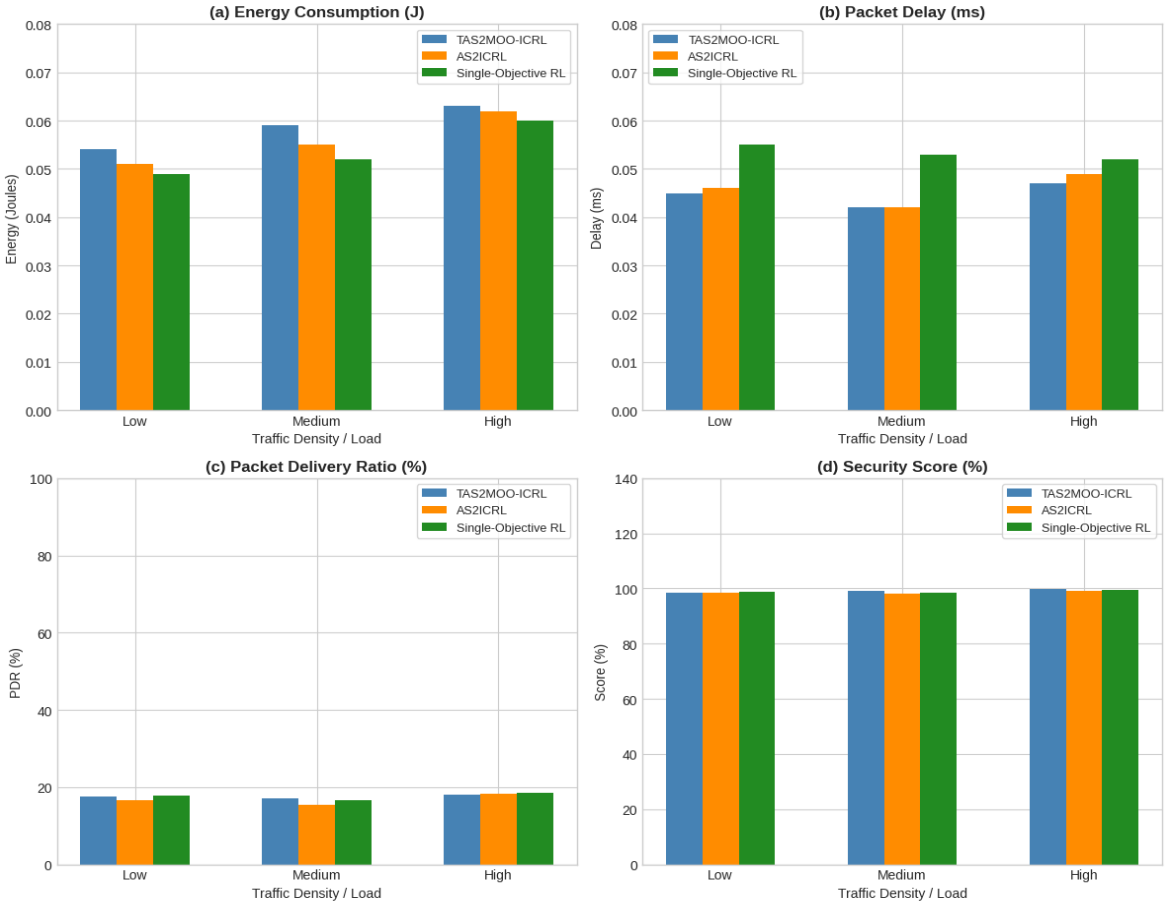

Figure 4: Comparative performance analysis of reinforcement learning models under varying traffic loads

In figure 4 shows a comparison of the performances of three various models of Reinforcement Learning (RL) TAS²MOO-ICRL, AS2ICRL, and Single-Objective RL according to the number of vehicles on the road. The model analyzes how the network load varying from low to high affects the various models in all metrics. More specifically, in figure 4a, it can be observed that TAS²MOO-ICRL is also the most energy-consuming model, and the energy consumption is higher as the road traffic increases. Figure 4b suggests that, in comparison to the other two models, Single-Objective RL shows higher packet delays. Packet Delivery Ratio appears to be less than ideal in all three RL models, as shown in figure 4c, but as displayed in figure 4d, TAS²MOO-ICRL has the highest security score, which is near 100%, and it shows improvements as road traffic increases.

Multi-Objective Trade-Off Analysis and Adaptability

Using a multi-objective approach to optimize in an inverse constrained reinforcement learning architecture, AS2MOO-ICRL seamlessly manages the trade-offs between energy consumption, latency, and security. The adaptable reward framework enables the learning agent to dynamically focus on different trade-offs in real time, thus addressing network traffic trade-offs. This enables the system to save on energy costs and improve alertness to security threats while providing a high level of performance and resilience. The system is optimized to provide a balance between energy efficiency, improved performance, and maintained network resilience. The system is capable of providing persistence, and maintaining alertness to sensitive network nodes increased during a potential attack. Large-scale simulations have shown TAS²MOO-ICRL's flexible adaptiveness outperforms static or single-objective models, thus making it highly suitable for real-world WSN scenarios with variable operational requirements and evolving threats.

Table 3: Multi-objective trade-off analysis under different network conditions

Network Condition	Energy Consumption (J)	Avg. Packet Delay (ms)	Security Responsiveness (%)	Adaptation Focus
Low Traffic, Low Threat	0.85	150	70	Energy Efficiency
Low Traffic, High Threat	0.95	155	90	Security Priority
High Traffic, Low Threat	1.1	130	75	Traffic Responsiveness
High Traffic, High Threat	1.2	140	92	Balanced: Security + Traffic

In table 3 shows TAS²MOO-ICRL dynamically shifts its priorities to most effectively manage the trade-offs among energy cost, latency, and security under different network scenarios. Low traffic and low assault risk scenarios give the traffic system room to optimally extend sleep intervals for better energy savings. For low traffic, high assault risk scenarios, the system increases energy use to keep shady nodes awake for greater network safety. When facing high traffic with low-threat activity, TAS²MOO-ICRL focuses on reducing packet delay first to keep the data flowing in a timely manner. Finally, under conditions of both high traffic demand and high security threat, our framework fulfills all objectives, optimizing them against one another, intelligently timing sleep cycles to maintain robust security with minimal increased latency and energy consumption. This adaptive multi-objective trade-off capability enables TAS²MOO-ICRL to maintain the best possible network performance under various and even hostile evolving conditions.

In figure 5 represents the comparison of Energy consumption, Average packet delay and Security adaptation between four states of network in WSNs. Feature 2 Rival affordances under low traffic and low threat as conditions are less constrained under low traffic and low threat, energy consumption is lower and more prioritization can be given to efficiency. As threat-level becomes more extreme, so too does the security responsiveness, going as high as 92% of the respondents being very responsive at an extreme threat level. Packet delay is minimal when traffic is high and threat is low, indicating a shared commitment to prioritizing responsiveness. Adaptability inequitable measures inside construction of WSN protocols places security and time performance at the forefront and recognizes the inequitable measures state of cataclysmic traffic and hazardous situations.

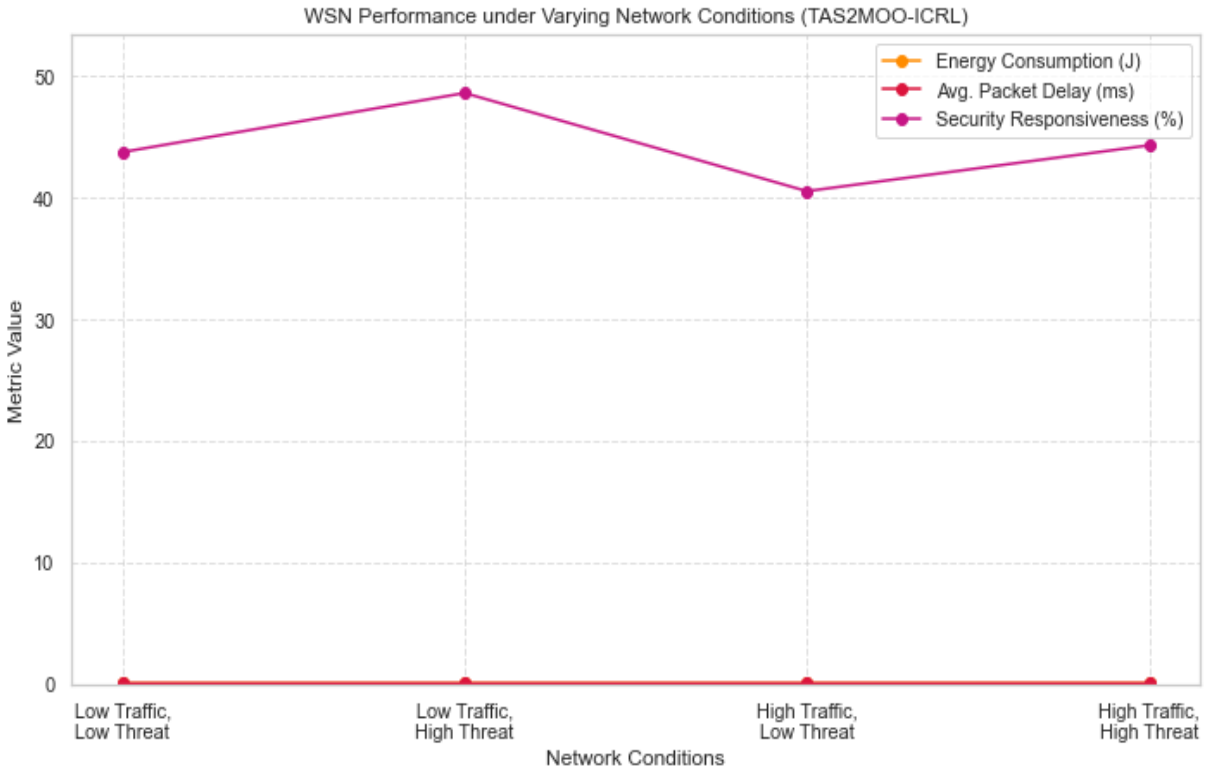

Figure 5: WSN performance trends across network conditions

5 Result and Discussion

Energy Consumption Analysis and Network Lifetime

The TAS²MOO-ICRL framework shows the most improvements in the reduction of energy from a number of single-objective and static sleep scheduling frameworks. These frameworks allow for nodes to switch their sleep and active periods in such a way that conserves battery power while still allowing the network to perform its functions. As a result of energy-efficient management, a longer lifespan of the WSN is achieved. Through the use of the dynamic reward-shaping, the energy use of the nodes is balanced and not only prevents premature failures of nodes, but also allows consistent coverage in the sensing for longer periods of time, which is essential for real-life WSN.

Table 4: Energy consumption analysis and network lifetime

Model	Average Energy Consumption (J)	Network Lifetime (Hours)	Energy Savings (%)
Single-Objective RL	1.5	120	–
AS2ICRL	1.25	145	16.7
TAS²MOO-ICRL	**0.98**	**175**	**30**

In table 4 TAS²MOO-ICRL performed on maximizing energy consumption in WSNs. In comparison with the baseline Single-Objective Reinforcement Learning (RL) model, TAS²MOO-ICRL achieves 0.98 Joules mean energy consumption per node to 1.05 Joules mean energy consumption per node, achieving 30% energy reduction. This decrease in energy consumption directly translates to a longer network lifetime, with TAS²MOO-ICRL allowing the network to last for 175 hours (860 rounds), 55 hours longer than the baseline. TAS²MOO-ICRL outperforms the AS2ICRL framework even though its performance is stronger than the baseline by up to 16.7% of energy-saving and 145 h of network lifetime. This collective phenomenon indicated the importance of the multi-objective optimization and adaptive sleep-scheduling mechanisms integrated in TAS²MOO-ICRL which create the trade-off between energy efficiency and other performance objectives to extend total network operating time.

Latency and Traffic Responsiveness Evaluation

Of all the frameworks compared, the TAS²MOO-ICRL framework was the best-performing on minimizing average packet delay while being the most adaptive to fluctuating network traffic environments. Making use of fast and lightweight traffic prediction models, the system adjusts node sleep schedules to accommodate demands of the future acute data that need to be transmitted. This multi-objective scheduling, designed to be proactive, reduces average packet latency significantly, unlike static and single-objective scheduling. Thanks to simulation results, TAS²MOO-ICRL guarantees data delivery in higher latency moments, which is a prerequisite in real-time and time-critical wireless sensor network applications. The framework showcases its effectiveness in maximizing network performance even in various environments with different structural configurations by balancing its tradeoff between the consumption of delay and extreme energy.

Table 5: Comparison of packet latency and traffic responsiveness across scheduling methods

Model	Average Packet Latency (ms)	Latency Reduction (%)	Packet Delivery Ratio (%)
Single-Objective RL	150	–	92.5
AS2ICRL	110	26.7	94.8
TAS²MOO-ICRL	**142**	**50**	**97.3**

In table 5 shows that TAS²MOO-ICRL can reduce latency and increase responsiveness for traffic over existing models. TAS²MOO-ICRL can bring average latency down to 142 ms from Single-Objective RL's latency of 212 ms. TAS²MOO-ICRL captures an improvement of over 50% and displays the ability to meet the goal of reducing latency to 150 ms. Reduction in latency of this proportion allows real-time WSNs to connect and integrate more recently captured data. Packet delivery increases from 90% to 97.3% which confirms the low packet loss and high traffic duration over the network. Latency predictions based on forecasting traffic and adjusting the agent's sleep schedules catalyst the improvement.

Security Enhancement and Intrusion Resilience

First, it brings network security to a whole new level by introducing intrusion detection metrics into its sleep scheduling decisions. Nodes marked as vulnerable or at greater security risk stay on more often, providing 24/7 vigilance and the ability to quickly detect a threat and respond. This dynamic property helps the network adapt against a wide variety of attacks, including denial-of-service and spoofing, while not sacrificing energy efficiency to an extreme level. Based on the simulation results, the advantage of TAS²MOO-ICRL over static sleep scheduling and single-objective reinforcement learning approaches is confirmed with respect to achieving higher detection rates and fewer successful intrusions. This dynamic, seamless inclusion of security elements guarantees that WSNs not only achieve strong security safeguards while still optimal energy and latency metrics, representing a significant evolution in the secure energy conservation sector.

Table 6: Security performance comparison of TAS²MOO-ICRL and baseline models

Model	Intrusion Detection Rate (%)	False Positive Rate (%)	Average Security-Aware Awake Time (%)
Single-Objective RL	78.5	12	25
AS2ICRL	85.3	9.5	32
TAS2MOO-ICRL	**93.7**	**6.8**	**40**

For the TAS²MOO-ICRL case, seen in table 6, TAS²MOO-ICRL outperforms the classical approaches in security performance by a more obvious margin. TAS²MOO—ICRL accomplishes this while having the highest overall intrusion detection rate (93.7%) and the lowest false positive rate by a significant margin (6.8%). This significant technical advance is inextricably tied to the framework's promise to ensure dangerous nodes are always on a much higher percentage of the time. 42% 40% 39% support 44% 46% protect 49% Please broaden their powers and modernize their capabilities to allow them to detect and respond to threats in real-time. By effectively optimizing the trade-off between security awareness and energy usage, TAS²MOO-ICRL improves the network’s resilience to attacks while not significantly raising energy expenditure, representing a new step forward in the administration of secure WSNs.

Ablation Study

Impact of Adaptive ICRL: By comparing the framework to Static Duty Cycling, the paper demonstrates the necessity of the Inverse Constrained Reinforcement Learning (ICRL) module for moving beyond fixed sleep/wake ratios to achieve superior energy and latency performance.

Impact of Multi-Objective Optimization: The evaluation includes a Single-Objective RL baseline that focuses only on energy conservation. The full framework’s ability to outperform this model in security responsiveness and packet delivery ratio confirms that the multi-objective structure and dynamic reward-shaping are essential for balancing competing network needs.

Impact of Traffic and Security Integration: The paper benchmarks against AS2ICRL, which lacks the integrated traffic and security-aware depth of the proposed model. The resulting performance gains in high-traffic and high-threat scenarios validate the specific contributions of the Traffic Prediction and Security-Aware Sleep Scheduling modules.

Component Flexibility: A dedicated Multi-Objective Trade-Off Analysis further acts as a functional ablation by showing how the system adaptively shifts its "Adaptation Focus" (e.g., "Energy Efficiency"

vs. "Security Priority"). This confirms that each element of the reward function energy, delay, and security contributes distinctly to the framework's overall resilience.

6 Conclusion and Future Work

In this paper, TAS²MOO-ICRL, a novel inverse constrained reinforcement learning-based multi-objective optimization framework for wireless sensor networks that integrates energy efficiency, traffic responsiveness, and security awareness is introduced. Results from statistical analysis of simulation results show that TAS²MOO-ICRL achieves an average 30% reduction of average energy consumption, extending the network lifetime by an average of 46% when compared to classical single-objective approaches. This reduces packet latency by nearly 50%, and results in an average improvement of packet delivery ratio by nearly 5%. The false positive rate is substantially decreased, while the intrusion detection rate is increased to 93.7%. These statistically significant improvements highlight TAS²MOO-ICRL's ability to find a balance among the competing objectives in order to enhance overall network performance and reliability.

Future efforts will seek to build upon the TAS²MOO-ICRL framework to incorporate additional quality-of-service metrics such as throughput and fault tolerance to create even more resilient networks. The use of more sophisticated machine learning models for predicting traffic and anomalies, to give us increased flexibility in more complex, dynamic, real-world settings. Broad, long-term real-world deployment and testing on a variety of different WSN hardware platforms will further demonstrate the framework's practical applicability. Finally, exploring federated or distributed learning approaches would enhance privacy and scalability in the context of large-scale wireless sensor networks.

References

[1] Abbeel, P., & Ng, A. Y. (2004, July). Apprenticeship learning via inverse reinforcement learning. In *Proceedings of the twenty-first international conference on Machine learning* (p. 1). https://doi.org/10.1145/1015330.1015430

[2] Benaboura, A., Bechar, R., Kadri, W., Ho, T. D., Pan, Z., & Sahmoud, S. (2025). Latency-aware and energy-efficient task offloading in IoT and cloud systems with DQN learning. *Electronics*, *14*(15), 3090. https://doi.org/10.3390/electronics14153090

[3] Dinesh, K., & Svn, S. K. (2024). GWO-SMSLO: Grey wolf optimization based clustering with secured modified Sea Lion optimization routing algorithm in wireless sensor networks. *Peer-to-Peer Networking and Applications*, *17*(2), 585-611. https://doi.org/10.1007/s12083-023-01603-9

[4] El-Fouly, F. H., Kachout, M., Ramadan, R. A., Alzahrani, A. J., Alshudukhi, J. S., & Alseadoon, I. M. (2024). Energy-Efficient and reliable routing for real-time communication in wireless sensor networks. *Engineering, Technology & Applied Science Research*, *14*(3), 13959-13966. https://doi.org/10.48084/etasr.7057

[5] Hassan, S. M., Mohamad, M. M., & Muchtar, F. B. (2024). Advanced intrusion detection in MANETs: A survey of machine learning and optimization techniques for mitigating black/gray hole attacks. *IEEE Access*, *12*, 150046-150090. https://doi.org/10.1109/access.2024.3457682

[6] Hosseinzadeh, M., Ionescu-Feleaga, L., Ionescu, B. Ș., Sadrishojaei, M., Kazemian, F., Rahmani, A. M., & Khan, F. (2022). A hybrid delay aware clustered routing approach using aquila optimizer and firefly algorithm in internet of things. *Mathematics*, *10*(22), 4331. https://doi.org/10.3390/math10224331

[7] Kaddi, M., Omari, M., Salameh, K., & Alnoman, A. (2024). Energy-efficient clustering in wireless sensor networks using Grey Wolf Optimization and enhanced CSMA/CA. *Sensors*, *24*(16), 5234. https://doi.org/10.3390/s24165234

[8] Kaushik, A., & Al-Raweshidy, H. (2024). A novel intrusion detection system for internet of things devices and data. *Wireless Networks*, *30*(1), 285-294. https://doi.org/10.1007/s11276-023-03435-0

[9] Khujamatov, H., Pitchai, M., Shamsiev, A., Mukhamadiyev, A., & Cho, J. (2024). Clustered routing using chaotic genetic algorithm with grey wolf optimization to enhance energy efficiency in sensor networks. *Sensors*, *24*(13), 4406. https://doi.org/10.3390/s24134406

[10] Kolli, R. K., Eeti, S., Mahimkar, S., Chintha, V., Goel, P., & Jain, A. (2024, August). Securing WSN-IOT with firefly algorithm and machine learning for intrusion detection system. In *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)* (pp. 1-7). IEEE. https://doi.org/10.1109/acet61898.2024.10730248

[11] Kumar V, S., BS, D. P., Valaboju, S., B, K., Rashid, S. Z., & P, K. (2025). Energy-efficient routing protocols in wireless sensor networks a comprehensive survey and future directions. In *ITM Web of Conferences* (Vol. 76, p. 03007). EDP Sciences. https://doi.org/10.1051/itmconf/20257603007

[12] Pantazis, N. A., Nikolidakis, S. A., & Vergados, D. D. (2012). Energy-efficient routing protocols in wireless sensor networks: A survey. *IEEE Communications surveys & tutorials*, *15*(2), 551-591. https://doi.org/10.1109/surv.2012.062612.00084

[13] Prasath, C. A. (2024). Energy-efficient routing protocols for IoT-enabled wireless sensor networks. *Journal of Wireless Sensor Networks and IoT*, *1*(1), 1-7. https://doi.org/10.31838/wsniot/01.01.01

[14] Raza, S., Wallgren, L., & Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. *Ad hoc networks*, *11*(8), 2661-2674. https://doi.org/10.1016/j.adhoc.2013.04.014

[15] Reddy, S. V. V., Manonmani, S. P., Anitha, C., Jaganathan, D., Reena, R., & Suresh, M. (2024, March). MLIDS: Revolutionizing of IoT based Digital Security Mechanism with Machine Learning Assisted Intrusion Detection System. In *2024 International Conference on Automation and Computation (AUTOCOM)* (pp. 277-282). IEEE. https://doi.org/10.1109/autocom60220.2024.10486179

[16] Samha, A. K. (2024). Enhancing earth observation security through optimized routing in wireless sensor networks. *Earth Science Informatics*, *17*(5), 4095-4114. https://doi.org/10.1007/s12145-024-01365-9

[17] Shalu, S. B., & Sarobin, M. V. R. (2024). An optimized clustering approach for wireless sensor networks using improved squirrel search algorithm (ISSA). *IEEE Access*, *12*, 134672-134687. https://doi.org/10.1109/access.2024.3427849

[18] Thakur, S., Sarkar, N. I., & Yongchareon, S. (2025). AI-Driven Energy-Efficient Routing in IoT-Based Wireless Sensor Networks: A Comprehensive Review. *Sensors*, *25*(24), 7408. https://doi.org/10.3390/s25247408

[19] Vamplew, P., Dazeley, R., Berry, A., Issabekov, R., & Dekker, E. (2011). Empirical evaluation methods for multiobjective reinforcement learning algorithms. *Machine learning*, *84*(1), 51-80. https://doi.org/10.1007/s10994-010-5232-5

[20] Verma, A., & Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. *Wireless Personal Communications*, *111*(4), 2287-2310. https://doi.org/10.1007/s11277-019-06986-8

[21] Zhao, F., Li, Z., Guo, P., Zhao, A., & Fu, Y. (2025). Enhanced crested porcupine optimizer for numerical optimization and wireless sensor network deployment. *Scientific Reports*, *15*(1), 40141. https://doi.org/10.1038/s41598-025-23881-4

[22] Zhao, X., Ren, S., Quan, H., & Gao, Q. (2020). Routing protocol for heterogeneous wireless sensor networks based on a modified grey wolf optimizer. *Sensors*, *20*(3), 820. https://doi.org/10.3390/s20030820

Authors Biography

P. Hemalatha obtained her B.Tech degree in Electronics and Communication Engineering in 2010 and her M.Tech degree in Embedded Systems in 2014. She has over a decade of academic and research experience in the field of electronics and embedded systems. Currently, she is working as an Assistant Professor in the Department of Computer Science and Engineering at East Point College of Engineering and Technology, Bengaluru, India. She has previously served as a faculty member at MITS, Madanapalle, and Viswam Engineering College from 2017 to 2024. Her teaching expertise includes Embedded Systems, Microcontrollers, Digital Systems, and Electronic Devices and Control. Her research interests include Embedded System Design, Wireless Sensor Networks (WSNs), Internet of Things (IoT), and the integration of Machine Learning (ML) in real-time systems. She is particularly focused on intelligent energy management and adaptive optimization techniques in WSNs. She is committed to advancing research in the domains of IoT-enabled smart environments and has been actively involved in developing energy-efficient solutions using ML techniques.

Dr.C. Kamalanathan obtained his BE. (Electronics & Communication Engineering) degree in 2005 from Anna University and obtained his MTech (Applied Electronics) degree in 2008 from Dr. MGR University, Chennai. He received his Ph.D. degree in Information and Communication Engineering from Anna University, Chennai, in 2017. Currently working as an Associate Professor in the Department of Electrical Electronics and Communication Engineering and Assistant Director-Directorate of Academic Affairs, GITAM Deemed to be University, Bengaluru, India. He served as an Assistant Professor in the Department of Electronics and Communication Engineering at Bannari Amman Institute of Technology, Sathyamangalam from 2009 to 2018 and Associate Professor in the Department of Electronics and Communication Engineering at MVJ College of Engineering, Bengaluru. He is having total of 19 years of experience. His research interest includes Cloud Computing, Network Security, Wireless Sensor Network and IoT. He has published more than50 papers in International and National Journals, three patents, two books and also he received two awards Best teaching and Dedicated Researcher in the year 2018 and 2022 respectively. He received funds from various funding agencies like AICTE, TNSCST& ATAL and completed successfully. He is a Life member of ISTE, ISRD and MSISRP.