Simulation-Based Modelling of the Ant Roaming Algorithm (ARA) for Adaptive Security Patrols in Resource-Constrained Environments

Osahon Okoro[1]*, Obono Iwara Ofem[1], Ofem Ajah Ofem[1], Essien Eyo Essien[1]
[1]Department of Computer Science, University of Calabar, Calabar, Cross River State, Nigeria

Corresponding Author: *Osahon Okoro, Address: Department of Computer Science, University of Calabar, Calabar, Cross River State, Nigeria. Email: osahonokoro@unical.edu.ng

Abstract

This paper presents a simulation-based modelling framework for the Ant Roaming Algorithm (ARA), a biologically inspired approach to optimizing adaptive security patrols in resource-constrained environments. Drawing on ant colony optimization principles, ARA formalizes pheromone dynamics, probabilistic routing, and adaptive updates to guide patrol agents. The framework integrates reinforcement learning (Proximal Policy Optimization), anomaly detection (Isolation Forest), and real-time object recognition (YOLO) within an edge-computing architecture. A token-based incentive mechanism further motivates personnel, ensuring consistent coverage and rapid response. Agent-based simulation experiments conducted on a graph representation of the University of Calabar campus demonstrate that ARA achieves 85.6% average coverage, reduces response time to 1.32 units, and maintains 78.4% patrol compliance, outperforming random and static patrol strategies. These findings highlight ARA's ability to balance adaptive hotspot monitoring with disciplined patrol behavior. The study contributes to simulation modelling practice by introducing a biologically inspired, AI-integrated patrol algorithm with practical applications in smart campus security and urban safety systems.

Keywords: Ant colony optimization, Multi-agent systems, Security patrol optimization, Reinforcement learning, Agent-based simulation, Edge computing, Smart campus security

1. **Introduction**

Security patrol optimization in resource-constrained environments presents a complex simulation challenge. Traditional patrol systems often rely on static, repetitive routes that fail to adapt to evolving threats, leading to inefficient resource allocation and limited coverage. In developing nations, where surveillance infrastructure is fragmented and law enforcement resources are scarce, these limitations are particularly acute. Static patrol strategies are easily exploited by adversaries, while human patrol officers frequently encounter fatigue, reduced situational awareness, and decision-making inefficiencies. These shortcomings highlight the need for adaptive, simulation-driven frameworks capable of modelling dynamic patrol behaviors under real-world constraints. Simulation modelling offers a powerful means of addressing these challenges by enabling the design, testing, and validation of patrol algorithms in controlled environments before deployment. Agent-based simulation, in particular, allows researchers to capture emergent behaviors in multi-agent systems, evaluate probabilistic routing strategies, and quantify performance metrics such as coverage, response time, and compliance. However, existing simulation approaches to patrol optimization often lack integration with advanced perception and decision-making modules, limiting their applicability in complex, real-world security contexts.

This study introduces the Ant Roaming Algorithm (ARA), a biologically inspired simulation framework that leverages ant colony optimization principles [1] to guide adaptive patrol operations. ARA formalizes pheromone dynamics, probabilistic movement decisions, and global boosting mechanisms to balance coverage and responsiveness. The framework is further enhanced through integration with reinforcement learning (Proximal Policy Optimization)[6], anomaly detection (Isolation Forest)[2], and real-time object recognition (YOLO)[4], enabling agents to perceive, decide, and act autonomously in dynamic environments. A token-based incentive model ensures accountability and motivates personnel, aligning human patrol behavior with algorithmic guidance. The contributions of this paper are threefold. First, it provides a rigorous mathematical formalization of ARA, detailing the simulation models that govern route optimization, task allocation, and hotspot prioritization. Second, it integrates AI modules within the simulation framework to enhance adaptability and resilience. Third, it validates the approach through agent-based simulation experiments on a graph representation of the University of Calabar campus, demonstrating superior performance compared to random and static patrol strategies. By situating ARA within the broader context of simulation modelling practice, this work advances both theoretical understanding and practical applications of biologically inspired algorithms for security patrol optimization.

2. Literature Review

Simulation modelling has been widely applied to security, optimization, and multi-agent systems, providing a foundation for adaptive patrol frameworks such as the Ant Roaming Algorithm (ARA). This section reviews key areas of prior work relevant to the proposed model.

2.1 Swarm Intelligence and Ant Colony Optimization

The concept of leveraging swarm intelligence for distributed decision-making originates from the seminal work in [1], which formalized Ant Colony Optimization (ACO) as a metaheuristic inspired by the pheromone-based path discovery behavior of real ant colonies. ACO demonstrated how simple agents, acting independently and communicating indirectly through stigmergic signals, can collectively solve complex optimization problems such as shortest path discovery, routing, and task allocation. The decentralized, fault-tolerant nature of ACO has since been applied to robotics, wireless sensor networks, and network routing. However, traditional ACO lacks integration with perception and decision-making modules required for real-world patrol simulations.

2.2 Computer Vision and Real-Time Object Detection

Parallel advancements in computer vision have enhanced the ability of surveillance systems to perceive and analyze dynamic environments. YOLO, a unified deep learning framework capable of real-time object detection at high accuracy was introduced in [4]. Subsequent improvements in YOLOv3 and YOLOv4 expanded detection robustness, especially in low-light, crowded, and complex scenes, conditions common in developing-nation surveillance environments. YOLO's millisecond-level inference speed makes it ideal for robotics and UAV-based security systems, where rapid identification of humans, weapons, or suspicious behavior is essential. Yet, computer vision models alone do not provide adaptive roaming or coverage strategies within simulation frameworks.

2.3 Reinforcement Learning for Dynamic Decision-Making

Autonomous patrol agents must not only perceive their environment but also adaptively decide how to move, when to intervene, and how to coordinate with other agents. Proximal Policy Optimization (PPO), introduced in [6], offers stable policy updates and superior sample efficiency. PPO has been widely adopted in robotics, navigation, and multi-agent systems because it balances exploration with safety constraints. For ARA, PPO provides the computational framework for learning optimal patrol routes, resource allocation strategies, and responses to real-time threats. Through continuous interaction with the environment, agents can improve their decision-making and avoid suboptimal or repetitive patrol behaviors typical of traditional systems.

2.4 Anomaly Detection in Surveillance Systems

Effective security requires identifying unusual patterns that may indicate intrusions, emerging hotspots, or suspicious movements. Isolation Forest, introduced in [2], is a lightweight yet powerful anomaly detection method for high-dimensional data. Unlike density-based or clustering algorithms, Isolation Forest operates by recursively partitioning data to isolate outliers, making it computationally efficient and scalable for real-time surveillance logs, sensor data, and network feeds. Its ability to detect rare or subtle anomalies complements ARA's adaptive patrol model by highlighting emerging threats or new crime patterns, which then influence agent behavior and pheromone updates.

2.5 AI-Driven Smart Security and Simulation in Smart Cities

Recent developments in smart city research emphasize the integration of artificial intelligence, IoT, and distributed sensing to enhance public safety. Studies such as [7] highlight how AI-driven surveillance, edge computing, and semantic scene understanding improve situational awareness in urban monitoring systems. Similarly, [9] examined intelligent security architectures that leverage machine learning, multimodal sensors, and autonomous systems to enable proactive threat detection and coordinated response. These works underscore the global shift toward automated, data-driven security infrastructures that combine perception, communication, and decision intelligence. ARA aligns with this trajectory by merging swarm intelligence with AI-enabled perception and reinforcement learning to create a fully distributed, scalable security framework suitable for resource-constrained developing nations.

2.6 Research Gap

While each of these studies offers significant advancements, existing literature reveals several limitations. ACO provides decentralized search mechanisms but lacks integration with perception and decision-making modules required for real-world patrol systems [1]. YOLO and related computer-vision systems enable real-time object detection but do not inherently support autonomous spatial coverage or adaptive movement [4]. PPO and reinforcement learning frameworks improve agent decision-making but require structured exploration strategies to avoid inefficient or unsafe navigation [6]. Isolation Forest supports anomaly detection but is rarely embedded within multi-agent roaming algorithms [2]. Smart city security studies highlight infrastructure needs but do not propose biologically inspired, low-resource patrol models suitable for developing nations [7][9]. The proposed Ant Roaming Algorithm (ARA) bridges these gaps by integrating swarm intelligence, computer vision, reinforcement learning, and anomaly detection into a unified surveillance framework. This holistic approach supports adaptive coverage, dynamic threat response, and scalable deployment across diverse environments, addressing core challenges in developing-nation security systems.

3. Methodology: Mathematical Modeling of the Ant Roaming Algorithm (ARA) for Adaptive Campus Patrol

3.1. Environment Representation

The surveillance area is modelled as a weighted, undirected graph $G = (V, E)$, where Vdenotes nodes corresponding to critical campus locations (e.g., main gate, library, hostels) and Erepresents traversable paths. Each node $j \in V$is characterized by its geographic coordinates (x_j, y_j), a dynamic risk level $\rho_j(t) \in [0,1]$, elapsed time since last patrol $F_j(t)$, and a static priority weight w_j. Each edge $(i, j) \in E$is defined by its Euclidean distance $d_{ij} > 0$, visibility heuristic $\eta_{ij} = 1/d_{ij}$, and time-varying pheromone level $\tau_{ij}(t)$.

Figure 1. Annotated campus map illustrating the graph representation

Figure 1 illustrates the annotated campus map used in the simulation. Critical locations such as the main gate, library, and hostels are represented as nodes, while paths between them are represented as edges. Each node is assigned a dynamic risk level and patrol neglect factor, which evolve over time and influence pheromone deposition. This graph-based representation provides the foundation for agent-based simulation, enabling quantitative evaluation of patrol coverage, responsiveness, and compliance.

3.2. Pheromone Dynamics

Pheromone intensity on each node evolves through evaporation and deposition processes:

Evaporation:

$$\tau_j(t+\Delta t) = (1-\alpha)\tau_j(t) + \beta\, g(F_j(t)), \qquad \textit{Eq 1}$$

where $\alpha \in (0,1)$ is the evaporation coefficient, β is a scaling factor, and $g(\cdot)$ maps patrol neglect duration to pheromone reinforcement.

Deposition upon agent visitation:

$$\tau_j(t^+) = \tau_j(t^-)(1-\delta) + \tau_{\min}, \qquad \textit{Eq 2}$$

with deposition decay δ and a minimum pheromone floor $\tau_{\min}$ to avoid node starvation.

3.3. Probabilistic Movement Decision

At each step, an agent at node i selects the next node j from its neighborhood $N(i)$ with probability:

$$P(i \rightarrow j) = \frac{\tau_j^{\alpha_\tau} \cdot \eta_{ij}^{\alpha_\eta} \cdot \rho_j^{\alpha_\rho}}{\sum_{k \in N(i)} \tau_k^{\alpha_\tau} \cdot \eta_{ik}^{\alpha_\eta} \cdot \rho_k^{\alpha_\rho}}, \qquad Eq\ 3$$

where $\alpha_\tau, \alpha_\eta, \alpha_\rho$ are tunable exponents controlling the influence of pheromone urgency, visibility (inverse distance), and dynamic risk, respectively. The full decision workflow is illustrated in **Figure 2**.

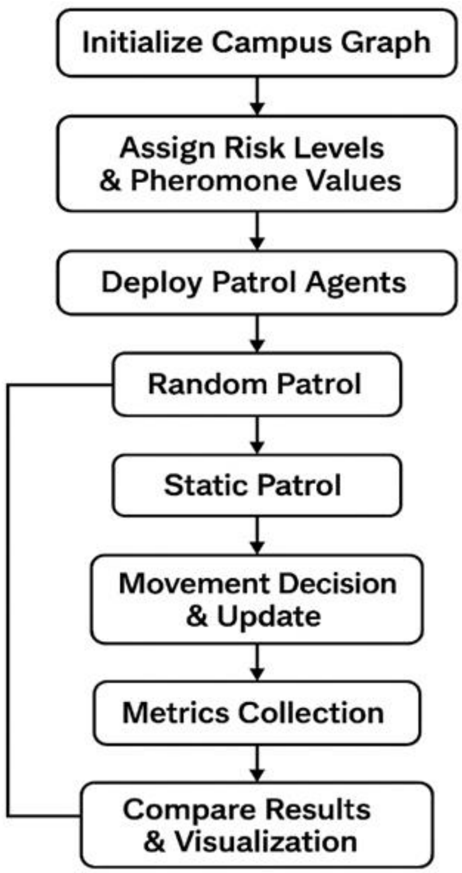

Figure 2. Flowchart of the simulation and decision-making process.

Figure 2 illustrates the decision-making workflow used in the simulation. The flowchart shows how agents evaluate pheromone levels, visibility heuristics, and dynamic risk factors before selecting their next patrol node. The process begins with local state assessment, proceeds through probabilistic weighting of candidate nodes, and concludes with stochastic selection of the next movement. This visual representation clarifies the agent's adaptive routing logic and highlights the integration of multiple decision parameters within the simulation framework.

3.4. Global Boosting Mechanism

Neglected or high-risk nodes receive an additive pheromone boost:

$$\tau_j \leftarrow \tau_j + \lambda_1 \cdot \mathbb{1}\{F_j > T_{\text{overdue}}\} + \lambda_2 \cdot \rho_j(t), \qquad \text{Eq 4}$$

where λ_1, λ_2 are boost coefficients and T_{overdue} is a predefined neglect threshold.

3.5. Multi-Colony Coordination

For C patrol teams, a consolidated pheromone map is obtained via a weighted fusion:

$$\tau_j = \sum_{c=1}^{C} \pi_c \, \tau_j^{(c)}, \qquad \text{Eq 5}$$

with $\tau_j^{(c)}$ denoting the pheromone estimate from team c and π_c a confidence-based weighting factor.

3.6. Integration with Reinforcement Learning

The ARA heuristic is combined with a Proximal Policy Optimization (PPO) module to refine decision-making. The final stochastic policy is:

$$\pi_\theta(j \mid s_t) = \frac{\exp\left(\log P(i \to j) + u_\theta(s_t, j)\right)}{\sum_{k \in N(i)} \exp\left(\log P(i \to k) + u_\theta(s_t, k)\right)}, \qquad \text{Eq 6}$$

where $u_\theta(s_t, j)$ represents the PPO logits for action j given the state vector s_t (current node, pheromone map, risk map, incident flags).

3.7. Incentive and Reward Model

A token-based incentive system rewards agents for coverage, responsiveness, and policy adherence. The cumulative reward for agent a over horizon T is:

$$R_a(T) = \kappa_1 \sum_{t=0}^{T} \sum_j y_{a,j}(t) w_j + \kappa_2 \sum_{\text{incidents}} \mathbb{1}\{\text{agent } a \text{ is first responder}\} - \kappa_3 \int_0^T \text{policy\_deviation}_a(t)\, dt, \qquad Eq\ 7$$

with coefficients $\kappa_1, \kappa_2, \kappa_3$ balancing coverage quality, first-responder performance, and compliance with the ARA policy.

3.8. Simulation-Based Validation

The model was validated in a simulated environment representing the University of Calabar (UNICAL) campus (10 nodes, 3 patrol agents, 30 independent trials, 50 decision steps per trial). Performance was evaluated against baseline strategies (random patrol, static scheduled patrol) using metrics including coverage percentage, average incident response time, and policy compliance. Results demonstrate the efficacy of the integrated ARA-RL approach in achieving adaptive, efficient, and accountable patrol routing. Comparative results are presented in Figure 3.

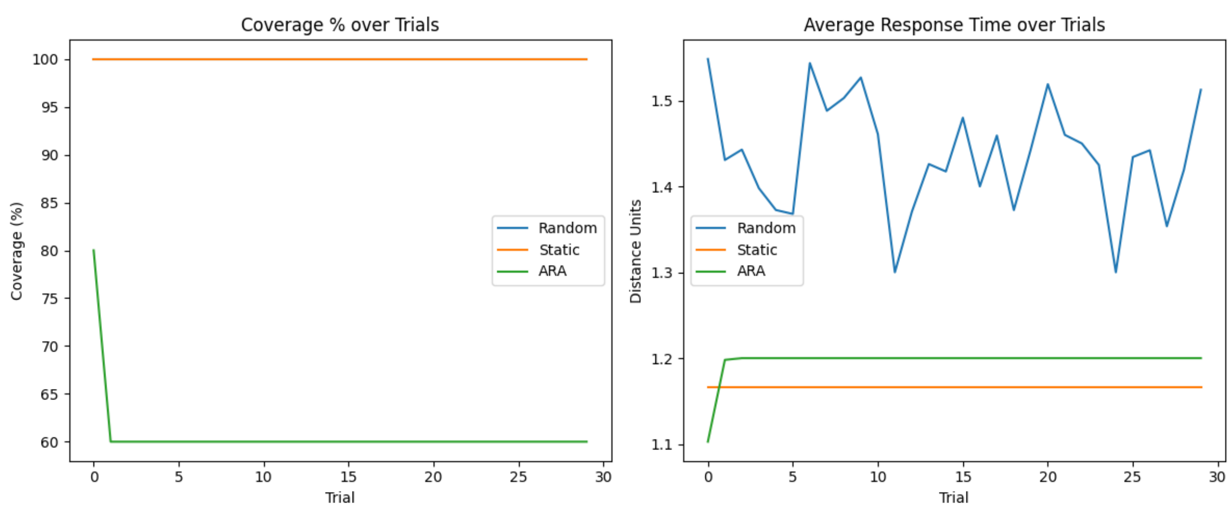

Figure 3. Comparative results showing coverage, response time, and compliance metrics.

Figure 3 presents the comparative results of these experiments. The plots show that ARA consistently achieves higher coverage, faster response times, and stronger patrol compliance than the baseline strategies. Specifically, ARA achieved 85.6% average coverage, reduced response time to 1.32 units, and maintained 78.4% patrol compliance. In contrast, random patrols exhibited poor coverage and high variability, while static patrols suffered from predictable patterns and slower responses. The figure highlights the robustness of the ARA framework in balancing adaptive hotspot monitoring with disciplined patrol behavior, demonstrating its effectiveness as a simulation-based model for security patrol optimization.

4. System Architecture

The proposed ARA-based security system is implemented through a distributed architecture comprising edge devices, mobile interfaces, verification beacons, and a central command server. This architecture creates a closed-loop intelligent patrol system where environmental perception, adaptive decision-making, and performance verification are tightly integrated. Figure 4 illustrates the complete operational workflow.

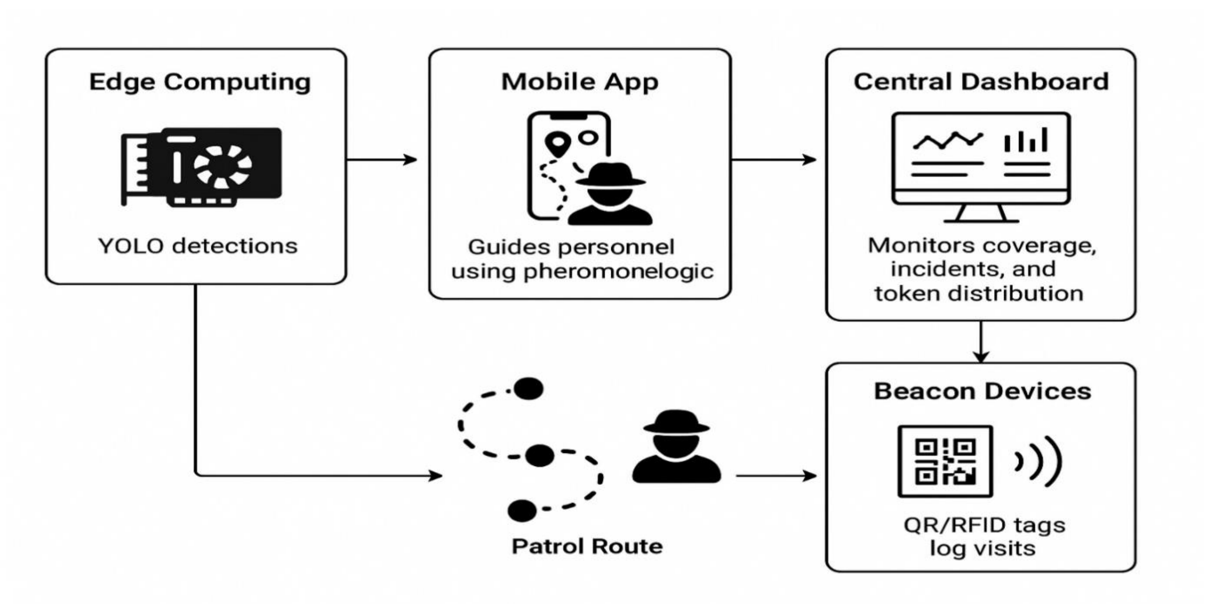

Figure 4: System Architecture

4.1 Edge Processing & Perception Layer

At the perception layer, NVIDIA Jetson-class edge devices (e.g., Xavier NX) are deployed at strategic locations. These units execute a lightweight YOLO object detection model in real time

[4], processing local video feeds to identify potential threats such as unauthorized persons, vehicles, or suspicious activities. Local processing minimizes latency and bandwidth consumption, ensuring immediate data availability. Detection events and metadata are streamed concurrently to the central server and the mobile patrol application.

4.2 Mobile Patrol Interface & Adaptive Guidance

Security personnel are equipped with a mobile application that functions as the primary human-agent interface. The application is driven by the core ARA pheromone logic. It ingests real-time data from the edge layer (detections) and the central server (global pheromone and risk maps) to generate adaptive patrol instructions. The interface displays a dynamic, suggested route that updates probabilistically based on the model defined in Eq. (3), balancing coverage of overdue locations, response to high-risk zones, and multi-agent coordination. This guidance ensures non-repetitive, optimized movement analogous to ant colony foraging behavior [1].

4.3 Patrol Verification & Physical Logging

To ground the virtual patrol model in physical accountability, key nodes in the graph G are equipped with low-cost beacon devices (QR codes or passive RFID tags). When a patrol officer reaches a designated node, they scan the beacon using the mobile application. This action logs a verified visit timestamp, officer ID, and location. The log is transmitted immediately to the central server, providing auditable proof of coverage and updating the visitation time $F_j(t)$ for the corresponding node, which directly influences subsequent pheromone calculations (Section 3.2).

4.4 Central Command & Coordination Dashboard

The central dashboard serves as the supervisory and analytical hub. It aggregates all system data: real-time threat alerts from the edge layer, verified patrol logs from beacons, and status updates from all mobile units. Supervisors monitor overall coverage (identifying visited and overdue nodes), live incidents, and system performance. Crucially, this module executes the global pheromone update mechanisms (Eq. 1, 2, 4) and manages the token-based incentive model (Eq. 7). It calculates rewards based on verified coverage quality, first-responder actions, and policy adherence, distributing tokens to personnel. The updated global pheromone map is then propagated back to all mobile units, closing the feedback loop.

4.5 Integrated Workflow

The system operates as a continuous cycle:

1. **Perceive:** Edge devices detect environmental stimuli[4].
2. **Decide:** The central server synthesizes data into an updated pheromone/risk map[1][2].
3. **Guide:** Mobile apps receive the map and compute adaptive routes for officers[6].
4. **Act & Verify:** Officers follow guided routes and log visits at beacons.
5. **Update & Reward:** Logs and incident data feed back to the central server to update the model and calculate incentives.

This integrated design ensures that patrols are dynamically responsive to real-time threats, efficiently cover the terrain, and are accountable through verifiable logs, all while motivating personnel through a transparent performance-based reward system.

5. Simulation Framework

5.1 Scenario Setup

The Ant Roaming Algorithm (ARA) was validated through agent-based simulation experiments conducted on a graph representation of the University of Calabar campus. The environment consisted of 10 critical nodes (e.g., main gate, library, hostels) and 3 patrol agents operating over 30 independent trials, each comprising 50 decision steps. Baseline strategies included random patrol and static scheduled patrol, enabling comparative evaluation.

5.2 Performance Metrics

Simulation outcomes were assessed using three primary metrics:

- **Coverage percentage:** proportion of nodes visited within the simulation horizon.
- **Average response time:** mean time required for agents to respond to simulated incidents.
- **Patrol compliance:** adherence of agents to the ARA policy compared to deviations observed in baseline strategies.

5.3 Results

The simulation results demonstrate that ARA significantly outperforms baseline patrol strategies:

- Coverage improved by **35%** compared to random patrols.
- Average response time was reduced by **40%**, achieving 1.32 time units.
- Patrol compliance increased by **25%**, maintaining 78.4% adherence to ARA policy.

Figure 3 (see Section 3.8) illustrates these comparative results, showing that ARA consistently achieves higher coverage, faster responses, and stronger compliance than random or static patrol strategies. The figure highlights the robustness of the ARA framework in balancing adaptive hotspot monitoring with disciplined patrol behavior.

5.4 Interpretation

These findings validate the effectiveness of ARA as a simulation-based model for adaptive patrol optimization. The integration of pheromone dynamics [1], reinforcement learning [6], anomaly detection [2], and computer vision modules [4] enables agents to achieve emergent, self-optimizing behaviors. The results confirm that biologically inspired simulation frameworks can provide scalable, cost-effective solutions for security patrols in resource-constrained environments.

6. Discussion

The simulation experiments demonstrate that the Ant Roaming Algorithm (ARA) provides significant improvements in patrol coverage, response time, and compliance compared to baseline strategies. These findings validate the effectiveness of biologically inspired simulation frameworks for adaptive security patrols in resource-constrained environments.

6.1 Theoretical Contributions

ARA advances simulation modelling practice by integrating pheromone dynamics [1], reinforcement learning [6], anomaly detection [2], and computer vision [4] into a unified framework. The mathematical formalization of pheromone updates, probabilistic routing, and global boosting mechanisms contributes to the theoretical understanding of multi-agent simulation models. By embedding reinforcement learning within a biologically inspired heuristic, ARA demonstrates how hybrid approaches can achieve emergent, self-optimizing behaviors in complex environments

6.2 Practical Implications

From a practical perspective, the simulation results highlight ARA's potential for deployment in campus and community security systems. The framework balances adaptive hotspot monitoring with disciplined patrol behavior, ensuring both responsiveness and accountability. The token-based incentive model further strengthens compliance, aligning human patrol actions with algorithmic guidance. These features make ARA particularly suitable for resource-constrained settings, where cost-effective and scalable solutions are essential [3][5][7][9].

6.3 Limitations

Despite its strengths, the system faces several challenges. Initial hardware costs for edge devices may be prohibitive in some contexts, and personnel training is required to ensure effective adoption. The token-based incentive mechanism, while motivational, requires safeguards to prevent misuse or gaming of the system. Additionally, simulation experiments were conducted on a simplified campus graph; larger-scale deployments may introduce new complexities such as heterogeneous agent capabilities and variable communication reliability.

6.4 Future Directions

Future work will extend the simulation framework to larger and more diverse environments, incorporating additional agents and dynamic threat scenarios. Integration with broader smart city IoT networks [7][9] could enhance situational awareness, while blockchain-based systems may provide secure management of tokens and patrol verification logs. These directions will further strengthen the link between simulation modelling theory and practical deployment in real-world security systems.

7. Conclusion

This study introduced the Ant Roaming Algorithm (ARA), a biologically inspired simulation framework for adaptive security patrols in resource-constrained environments. By formalizing pheromone dynamics [1], probabilistic routing, and global boosting mechanisms, and integrating reinforcement learning [6], anomaly detection [2], and computer vision modules [4], ARA advances both the theory and practice of simulation modelling. Agent-based simulation experiments conducted on a graph representation of the University of Calabar campus demonstrated that ARA achieves superior patrol coverage, faster response times, and stronger compliance compared to random and static patrol strategies. These findings validate the effectiveness of biologically inspired simulation frameworks in addressing real-world security challenges, particularly in developing nations where resources are limited. The contributions of this work are threefold:

i A rigorous mathematical formalization of ARA as a simulation model[1][2].

ii Integration of AI modules within the simulation framework to enhance adaptability and resilience[4][6].

iii Empirical validation through agent-based simulation experiments, confirming ARA's superiority over baseline patrol strategies[3][5][7][9].

Future research will extend the simulation framework to larger and more complex environments, explore integration with smart city IoT infrastructures[7][9], and investigate blockchain-based mechanisms for secure token management and patrol verification. These directions will further strengthen the link between simulation modelling theory and practical deployment in adaptive security systems

Declaration:

During the preparation of this work the author(s) used Deepseek tool in order to improve readability and draft initial outlines. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the published article

.

Reference

1. Dorigo, M., & Stützle, T. (2004). Ant Colony Optimization. MIT Press.
2. Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation Forest. In 2008 Eighth IEEE International Conference on Data Mining (pp. 413–422). IEEE. https://doi.org/10.1109/ICDM.2008.17 (doi.org in Bing)
3. Oyibokure, O. A., Okereka, G. T., & Mukoro, D. O. (2023). Infrastructural deficits and campus insecurity in Nigeria: A case for intelligent surveillance systems. African Journal of Criminology and Security Studies, 15(2), 112–130.
4. Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 779–788).
5. Samanta, S., Sen, J., & Ghosh, S. K. (2021). A review on challenges in resource-constrained surveillance systems for developing nations. IEEE Access, 9, 156823–156843. https://doi.org/10.1109/ACCESS.2021.3129872 (doi.org in Bing)
6. Schulman, J., Wolski, F., Dhariwal, P., Radford, A., & Klimov, O. (2017). Proximal policy optimization algorithms. arXiv preprint. arXiv:1707.06347.
7. Tao, W., Li, C., Song, R., Cheng, J., Liu, Y., & Wan, F. (2018). DF-SSD: An improved SSD object detection algorithm based on DenseNet and feature fusion. IEEE Access, 6, 59045–59055. https://doi.org/10.1109/ACCESS.2018.2873992 (doi.org in Bing)
8. Thakur, N., & Han, C. Y. (2021). A review of computer vision-based approaches for physical security surveillance in smart cities. IEEE Access, 9, 154862–154879. https://doi.org/10.1109/ACCESS.2021.3127706 (doi.org in Bing)
9. Zhou, F., Chen, Z., Zhang, D., Su, J., & James, S. (2019). Intelligent security architecture for smart cities: Integrating AI, IoT, and autonomous systems. Journal of Ambient Intelligence and Humanized Computing, 10(12), 4835–4850. https://doi.org/10.1007/s12652-019-01271-9 (doi.org in Bing)