Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Deploying Drones for Smart Surveillance: an Efficient and Adaptive Monitoring Solution

Tahar ALLAOUI[1], Mustapha BOUAKKAZ[2]
[1]*Computer science and mathematics Laboratory, LIM. Computer science department, University of Amar Thelidji, Laghouat, Algeria,* t.allaoui@lagh-univ.dz
[2]*Computer science and mathematics Laboratory, LIM. Computer science department, University of Amar Thelidji, Laghouat, Algeria,*

ARTICLE INFO

Received: 29 Dec 2024

Revised: 15 Feb 2025

Accepted: 24 Feb 2025

ABSTRACT

The growing need for real-time and adaptable surveillance solutions has prompted the investigation of cutting-edge technologies within security and monitoring frameworks. This paper introduces an innovative surveillance approach that utilizes drones to improve situational awareness and operational efficiency across various domains, including public safety, border security, and environmental monitoring. The proposed system integrates autonomous drones equipped with sophisticated imaging capabilities, data processing techniques, and machine learning algorithms, facilitating real-time monitoring, threat identification, and comprehensive data analysis. Notable features of this system include autonomous path planning, the ability to adapt to changing environmental conditions, and effective communication with ground control stations. By merging drone technology with AI-enhanced analytics, this approach provides a scalable and cost-efficient surveillance solution that minimizes the need for human intervention while enhancing accuracy and response times.

In this paper, we detail the design, implementation, and performance assessment of our system, underscoring its potential to transform conventional surveillance practices.

Keywords: Smart Surveillance. Drones. Mobility. GM. RWP. Clustering.

1. INTRODUCTION

The integration of drone technology into urban surveillance systems represents a transformative shift in how cities manage security and monitoring. As urban environments evolve into smart cities, the demand for efficient, real-time surveillance solutions has intensified, prompting researchers and practitioners to explore the capabilities of drones in enhancing situational awareness and operational efficiency. Drones, equipped with advanced imaging technologies and data processing capabilities are increasingly being deployed for a variety of applications, including public safety, environmental monitoring, and law enforcement [1]. Recent studies highlight the multifaceted benefits of employing drones in smart city infrastructures. For instance, drones can autonomously monitor large gatherings, providing law enforcement with critical situational insights that enhance public safety [2]. Moreover, the application of machine learning algorithms in drone operations has been shown to improve threat identification and response times, making these systems not only more effective but also more adaptable to changing conditions airspace [3]. This adaptability is crucial in urban settings, where dynamic environments necessitate a flexible approach to surveillance. However, the proliferation of drone technology also raises significant concerns regarding cybersecurity and privacy. As drones become integral to smart city operations, ensuring the security of drone networks is paramount. Research has focused on developing robust cybersecurity measures, including machine learning approaches for detecting cyber-attacks and frameworks for intrusion detection within drone networks [4] . Addressing these challenges is essential for fostering public trust and ensuring the safe deployment of drones in urban areas. In summary, the convergence of drone technology with advanced analytics and machine learning presents a promising avenue for enhancing urban surveillance systems. This paper aims to explore the design, implementation, and performance assessment of innovative drone surveillance solutions, emphasizing their potential to revolutionize conventional practices while addressing the critical issues of security and privacy in smart city contexts.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

2. RELATED WORKS

In the rapidly advancing field of drone surveillance, numerous studies have emerged that explore various applications, methodologies, and technological innovations. To provide a clearer understanding of the existing literature, we propose a new classification of previous works into five distinct categories: Agricultural Monitoring and Management, Smart City Surveillance and Security, Advanced Technologies and Frameworks, Cybersecurity and Privacy in Drone Networks, and Event Monitoring and Law Enforcement. This classification not only highlights the diverse applications of drone technology but also identifies key areas for further exploration.

1. Agricultural Monitoring and Management Drones: have increasingly been utilized in agriculture for monitoring and managing crops effectively. Studies such as [1] and [5] focus on the application of drone surveillance for advanced agricultural monitoring, employing techniques like convolutional neural networks for disease assessment and efficient monitoring. These works demonstrate the potential of drones to revolutionize agricultural practices through improved monitoring and data collection.

2. Smart City Surveillance and Security: The integration of drones into smart city infrastructures has been a significant area of research. Provide a systematic review of the involvement of surveillance drones in smart cities, exploring their applications and benefits for urban management [6]. Furthermore, the study by Akram et al. in [2] introduces a secure and lightweight drone-access protocol aimed at enhancing smart city surveillance, addressing security and privacy concerns associated with UAV operations. These contributions highlight the critical role of drones in enhancing urban security and monitoring capabilities.

3. Advanced Technologies and Frameworks: Recent advancements in technology have led to the development of innovative frameworks for drone surveillance. In [7] a study is presented on dynamic monitoring and tracking using intelligent image analysis, showcasing the capabilities of drones in real-time surveillance applications. Similarly, in [8] an IoT-enabled deep learning framework for multiple object detection in remote sensing images was proposed, illustrating how drones can be integrated with advanced technologies for enhanced monitoring. These studies underline the importance of leveraging cutting-edge technologies to improve the effectiveness of drone surveillance systems.

4. Cybersecurity and Privacy in Drone Networks: As drone technology becomes more prevalent, ensuring the security and privacy of drone networks is paramount. Baig et al. in [3] explore machine learning approaches for detecting cyber-attacks on drones, emphasizing the need for robust cybersecurity measures in smart city airspace. Additionally, the work in [4] focuses on developing a smart cybersecurity framework for intrusion detection in the Internet of Drones, highlighting the challenges and solutions related to privacy and security in drone operations. These contributions are essential for safeguarding drone networks against potential threats.

5. Event Monitoring and Law Enforcement: Drones have proven to be valuable tools for monitoring large events and supporting law enforcement efforts. In [9], Royo et al. discuss the enhancement of drones for law enforcement and capacity monitoring at large events, proposing methodologies that integrate deep learning algorithms into drone operations. Furthermore, the studies by [10] and [11] addresse surveillance routing with a minimum number of drones, providing insights into optimizing drone deployment for effective monitoring. These studies illustrate the practical applications of drones in maintaining public safety and managing large gatherings. In summary, this proposed classification of the existing literature provides a structured framework for understanding the diverse applications and challenges of drone surveillance.

This paper aims to build upon these foundational studies by proposing a novel surveillance method that leverages autonomous drones equipped with advanced imaging and machine learning algorithms to enhance situational awareness and operational efficiency.

3. BASIC IDEA

In our method, we are going to use the clustering method, which consists of grouping similar objects, the clustering permits to devide the network into groups, so the mouvement will be reduced. Several types of clustering exist, and for our algorithm, we have chosen a very well known type, which is hierarchical clustering (top-down), which consists

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

of grouping drones into different levels. The number of levels in our method is fixed at three (03). The area to be monitored will be devided into 4 zones, in each zone a number of UAVs carry out the monitoring operation, and they are considered to be the lowest level. Each zone is assigned to a leader who collects all the information from the monitoring UAVs, and the four leader UAVs, which represent the second level, send the information to a Master UAV, which represents the highest level of monitoring.

3.1 Determining the tasks of each level

The first level (the highest level) contains a single drone called the Master, which has the following tasks:

- Divide the entire area to be monitored into four (04) sub-areas, then sends the second level drones, which are four (04) of the above sub-areas, the points (x_i,y_i).
- Sent to the four (04) drones the number of third-level drones belonging to them (i.e. the number of drones in each sub-area doing the surveillance).
- Collecting data from the four second-level drones.

The second level contains four (04) drones, each drone is the leader of its sub-area, each of these four (04) drones is responsible for :

- The leader receives the coordinates (x_i,y_i), so it also receives the number of drones carrying out the surveillance and which belong to it (these parameters are sent by the master),
- Send the points (x_i, y_i) for each surveillance drone on the third level,
- Data collection from the third-level drones that belong to it,
- Follow a strategy in the event of difficulties linked to low batteries or unforeseen breakdowns. The aim of this last task is to ensure the continuity of the surveillance mission.

The third level (low level) contains the drones that monitor the sub-zones. The surveillance drone must inform the leader if there are any changes, as well as if the battery level is low.

For choosing the Master and leaders are chosen by convention the master at index 0 (Host[0]) and the leaders from index 1 to 4 (Host[1..4]).

3.2 Assigning UAVs to zones

The principle of assigning UAVs to sub-areas is to assign UAVs, which have a successive identification number to different sub-areas. In other words, at each iteration the current UAV is included in a different sub-area to the previous one, and this process is repeated until the number of UAVs is equal to zero (0).

3.3 Choosing a mobility model

The third phase consists of choosing a mobility model to ensure complete coverage of the zone. This phase can be considered to be the improvement phase of the Gauss Markov (GM) and Random Way Point (RWP) mobility models. In the latter two models, the drone moves throughout the zone, which means that the amount of energy consumed is significant.

Our approach is to reduce the mobility of each drone by using the notion of clustering, where the drone's mobility is proportional to the amount of energy it consumes. In other words, if we reduce the mobility of each drone, this will be followed by a reduction in the energy consumed.

4. SIMULATION AND RESULTS

The aim of this simulation is to choose the most appropriate mobility model for our surveillance algorithm. Clearly, the mobility model chosen must be the one that minimises energy consumption.

4.1 Mobility models in comparison

1. Random Way Point (RWP);

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

2. Gauss Markov (GM);
3. Clustering RWP (CRWP) : this is an improvement of the original method where we use the clustering;
4. GM clustering (CGM) : this is an improvement of the original method where we use the clustering.

4.2 Simulation Scenarios

In our study, we focus on the average-consumed energy (ACE). In order to define the best mobility methode we will change the mobility models in each scenario.

Scenario 1:

In this scenario, we want to compare the RWP mobility model and our monitoring method using CRWP, in order to observe the ACE as a function of the variation in the number of nodes, and to determine the best method between these two.

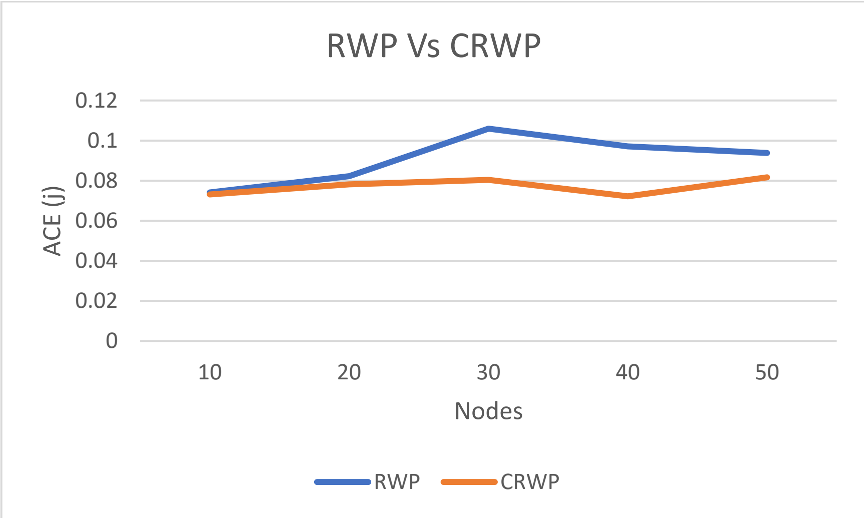

Figure 1. Comparison between RWP and CRWP

From the comparative graph showing the ACE as a function of node density in Figure 1, it can be seen that the RWP model consumed the highest value of ACE, which reached (0.105934433 J) when using (30) nodes. On the other hand, the most optimal value of ACE was achieved by CRWP, which is equal to (0.072172225 J) when using (40) nodes. the ACE of CRWP is better than the ACE of RWP in all cases where the number of nodes varies.

In conclusion, in this scenario, our method using Clustering RWP (CRWP) is better than RWP in terms of energy consumed during node variation.

Scenario 2:

We want to compare the GM mobility model and the CGM method, in order to observe the ACE as a function of the variation in the number of nodes, and to determine the best method between these two.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

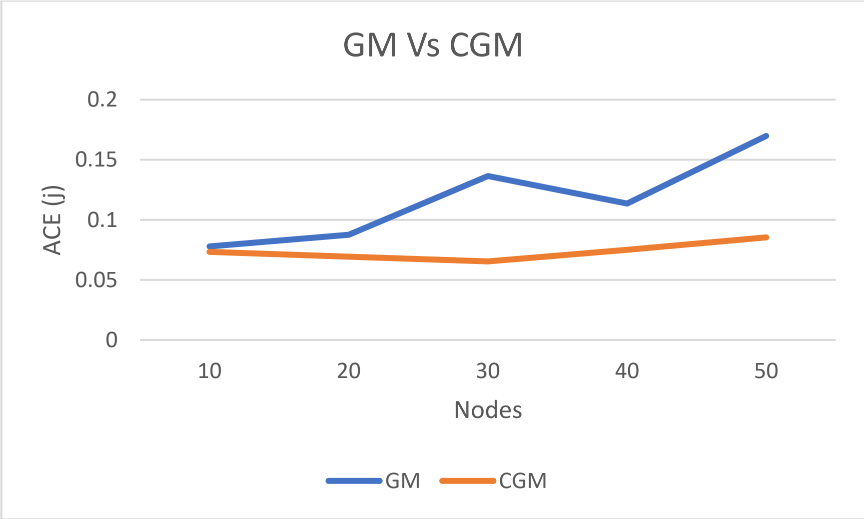

Figure 2. Comparison between GM and CGM

From the comparative graph representing the ACE as a function of node density in Figure 2, we can see that the GM model consumed the highest value of ACE, which reached (0.16981282 J) when using (50) nodes. On the other hand, the most optimal value of ACE was achieved by the CGM model, which equalled (0.065382833 J) when using (30) nodes. Also, the ACE of CGM is better than the ACE of GM in all cases where the number of nodes varies. So, in this scenario the CGM model is better than GM in terms of energy consumed during node variation.

Scenario 3:

We want to compare the CGM method and the CRWP method, in order to observe the ACE as a function of the variation in the number of nodes, and to determine the best method between these two.

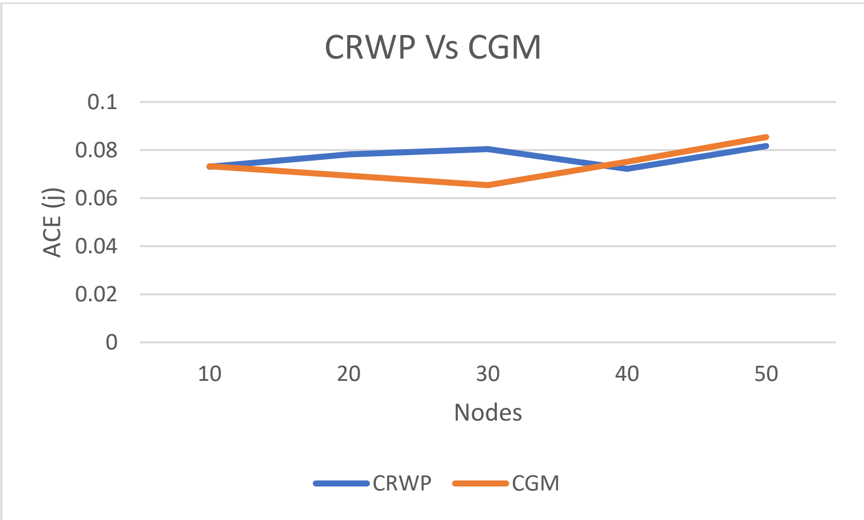

Figure 3. Comparison between CRWP and CGM

From the comparative graph representing the ACE as a function of node density in Figure 3, we can see that the CGM model consumed the highest value of ACE, which reached (0.08537488 J) when using (50) nodes. Also, the most optimal value of ACE was achieved by the CGM model, which equalled (0.065382833 J) when using (30) nodes. We notice that the values of both curves fluctuate up to 30 nodes, which means that the CRWP model is better than the CGM model.

Now, we will study the influence of the area surface on the different mobility methods, so in the rest of the scenarios, the number of drones equals 50 and we will change the area surface.

Scenario 4:

We will compare the CGM and CRWP models, and observe the ACE as a function of the area monitored. The table below shows the obtained results after simulating this scenario.

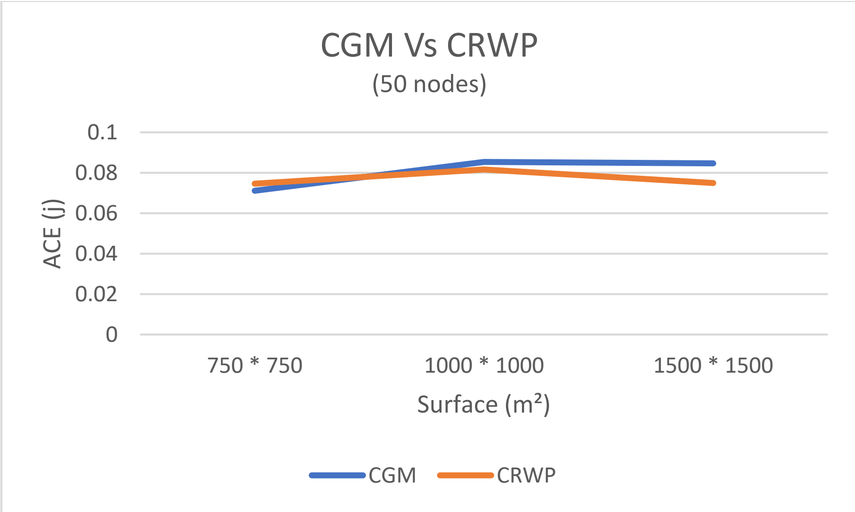

Figure 4. Influence of the surface on the mobility modals (CRWP vs CGM)

It can be seen from the comparative graph above in Figure 4, which represents the ACE as a function of the variation in surface area, that the CGM model consumed the highest value of ACE, which reached (0.08537488 J) when monitoring an area of (1000m * 1000m). Also, the most optimal ACE value was obtained by the same model (Clustering GM), which reached (0.07112186 J) when monitoring an area of (750m * 750m). In the various remaining values in the comparative graph above, the two curves (CGM and CRWP) converge, except in the last case, when monitoring an area of (1500m * 1500m), the ACE of CRWP is better than the ACE of GM.

From all the simulation scenarios, we can say that CRWP is the best mobility method that ensures the optimal ACE for our monitoring algorithm.

5. CONCLUSION

In conclusion, the integration of drone technology into urban surveillance systems marks a significant advancement in the pursuit of efficient and adaptive monitoring solutions within smart cities. Our study indicates that drones equipped with advanced imaging capabilities and can enhance situational awareness and operational efficiency across various domains, including public safety, environmental monitoring, and law enforcement. The ability of drones to autonomously monitor large events and adapt to dynamic environments underscores their potential to transform conventional surveillance practices, providing timely and accurate data that can inform decision-making processes. Moreover, the incorporation of cutting-edge technologies, such as IoT frameworks and intelligent image analysis, further amplifies the effectiveness of drone surveillance systems. These innovations facilitate real-time monitoring and threat identification, enabling a proactive approach to urban management. However, the deployment of drones in urban settings also necessitates a robust focus on cybersecurity and privacy concerns. As drone technology becomes more prevalent, ensuring the security of drone networks is critical to maintaining public trust and safeguarding sensitive information.

REFRENCES

[1] Gao, J., Bambrah, C. K., Parihar, N., Kshirsagar, S., Mallarapu, S., Yu, H. & Yang, Y. (2023). Building Smart Surveillance Solutions for Livestock Farms.

Journal of Information Systems Engineering and Management
2025, 10(61s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[2] Akram, M. W., Bashir, A. K., Shamshad, S., Saleem, M. A., AlZubi, A. A., Chaudhry, S. A., ... & Zikria, Y. B. (2021). A secure and lightweight drones-access protocol for smart city surveillance. IEEE Transactions on Intelligent Transportation Systems, 23(10), 19634-19643.

[3] Baig, Z., Syed, N., & Mohammad, N. (2022). Securing the smart city airspace: Drone cyber attack detection through machine learning. Future Internet, 14(7), 205.

[4] Ashraf, S. N., Manickam, S., Zia, S. S., Abro, A. A., Obaidat, M., Uddin, M. & Alsaqour, R. (2023). IoT empowered smart cybersecurity framework for intrusion detection in internet of drones. *Scientific Reports*, *13*(1), 18422.

[5] Maulana, R., Wibowo, U., Wiyono, D. S., & Ardian, D. (2023). Efficiency of Using Drones and Boats in Monitoring the Security of the Pang Pang Bay Water Aerodrome Area. *Sinergi International Journal of Logistics*, *1*(3), 96-107.

[6] Gohari, A., Ahmad, A. B., Rahim, R. B. A., Supa'at, A. S. M., Abd Razak, S., & Gismalla, M. S. M. (2022). Involvement of surveillance drones in smart cities: A systematic review. *IEEE Access*, *10*, 56611-56628.

[7] Yao, C. B., Kao, C. Y., & Lin, J. T. (2023). Drone for Dynamic Monitoring and Tracking with Intelligent Image Analysis. *Intelligent Automation & Soft Computing*, *36*(2).

[8] Ahmed, I., Ahmad, M., Chehri, A., Hassan, M. M., & Jeon, G. (2022). IoT enabled deep learning based framework for multiple object detection in remote sensing images. *Remote Sensing*, *14*(16), 4107.

[9] Royo, P., Asenjo, À., Trujillo, J., Çetin, E., & Barrado, C. (2022). Enhancing drones for law enforcement and capacity monitoring at open large events. *Drones*, *6*(11), 359.

[10] Mori, K., Nishira, M., Nishikawa, H., & Tomiyama, H. (2023, November). Surveillance Routing with a Minimum Number of Drones. In *2023 Eleventh International Symposium on Computing and Networking Workshops (CANDARW)* (pp. 366-367). IEEE.

[11] Crupi, L., Butera, L., Ferrante, A., & Palossi, D. (2024, April). A Deep Learning-based Pest Insect Monitoring System for Ultra-low Power Pocket-sized Drones. In *2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT)* (pp. 323-330). IEEE.