Preprints.org

Article

Not peer-reviewed version

Securing UAV Swarm-Based Smart Metering Infrastructure: A Multi-Phased Approach to Threat Mitigation

Qutaiba Ibrahim * and Mustafa Qassab

Posted Date: 11 March 2025

doi: 10.20944/preprints202503.0821.v1

Keywords: UAV Swarm; smart metering infrastructure; security; IPSec; authentication; confidentiality; integrity; Denial-of-Service; Man-in-the-Middle; threat modeling

Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

Securing UAV Swarm-Based Smart Metering Infrastructure: A Multi-Phased Approach to Threat Mitigation

Qutaiba I. Ali * and Mustafa S. Qassab

University of Mosul/IRAQ

* Correspondence: Qut1974@gmail.com

Abstract: Unmanned Aerial Vehicle (UAV) swarms offer a promising solution for revolutionizing Smart Metering Infrastructure (SMI) by enabling efficient, scalable, and cost-effective data collection. However, the deployment of UAV swarms in critical infrastructure applications raises significant security concerns. This paper presents a comprehensive security model designed to protect a UAV swarm-based SMI against various threats throughout its operational phases. We identify key vulnerabilities and propose a multi-layered security framework that incorporates bidirectional entity authentication, secure communication channels using IPSec (Internet Protocol Security), and proactive measures to mitigate specific attacks, such as denial-of-service and man-in-the-middle attacks. We analyze the effectiveness of our proposed solutions in addressing potential threats during different operational phases: DMC (Data Management Center) interaction, in-flight operations, and data collection. We present a comparative analysis highlighting the advantages of our approach over existing security schemes for UAV swarms. Our findings provide valuable insights into securing UAV swarm-based critical infrastructure and contribute towards building more resilient and trustworthy smart city applications.

Keywords: UAV Swarm; smart metering infrastructure; security; IPSec; authentication; confidentiality; integrity; Denial-of-Service; Man-in-the-Middle; threat modeling

1. Introduction

Rapid urbanization worldwide demands a smart, innovative, and sustainable application of resources, mitigation of environmental impacts, and enhancements in citizen livelihood [1–3]. In this regard, connected with integrated infrastructure and data-driven decision processes, the smart city has emerged as an important development paradigm for cities. While this is a very important basis for a smart city, SMI facilitates smart metering: it effectively provides utilities and consumers with real-time and accurate energy consumption data that empowers these two stakeholders to work together toward better energy use patterns for a more sustainable energy future [4–8]. While SMI might have its potential for transformation, traditional architectures have been highly reliant on manual data collection methods, with human personnel going from door to door or building to building for the collection of data. There are many inherent limitations to this reliance on manual processes [9–13]:

- High Operational Costs: The employment of field personnel in collecting data means higher salary, transportation, and administrative overhead costs. These costs rise even more during the deployment of personnel in difficult geographical terrains or areas that are highly inhabited by people.
- Safety Risks to Personnel: Deployment of human workers in hazardous environments, such as unstable infrastructures, extreme weather conditions, and insecurity is a huge safety risk to personnel. Manual data collection exposes personnel to accidents, injuries, and health hazards.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

- Data inaccuracies and delays: Most data intake mechanisms worked manually are invariably prone to human inaccuracies, further bringing down the accuracy of the consumption readings. Besides that, the time it takes for the actual collection of data manually from a large number of locations inherently makes data availability delayed and limits the real value of real-time monitoring and analysis.
- Recent developments in Unmanned Aerial Vehicle (UAV), or drone, technology have opened exciting vistas in use for transforming many industries and sectors, including urban infrastructure management. Indeed, UAVs inherently offer a very attractive alternative to manual data collection in SMI for several reasons [4,14–18]:
- Agility and Maneuverability: It can navigate through complicated urban environments to reach places where it is hard or dangerous for human personnel. Their agility to move through narrow spaces and to fly at different altitudes favors them as an optimal choice for data acquisition in a wide range of settings.
- Scalability and Cost-Effectiveness: The deployment of a swarm of inter-connected UAVs will have the added advantage of rapid data collection in a very short time from a large number of smart meters deployed within a wide area. Such a scalable solution reduces the time and cost required for manual data gathering considerably.
- Reduced Safety Risks: The use of UAVs in data collection will reduce the need to deploy personnel in hazard-prone environments, and by doing so it reduces accidents, injuries, or health hazards to workers significantly.
- Improved Data Accuracy and Timeliness: Equipped with appropriate sensors, UAVs would be able to download data directly from smart meters with no potential human error from manual entry. Besides, rapid deployment and data transmission by UAVs provide real-time monitoring and analysis in a timely manner.

2. Related Work

Ensuring secure data transmission and system integrity is paramount in UAV-based applications. Researchers have explored various approaches to enhance security within UAV networks. Saini et al. [19] proposed cryptography protocols to safeguard data privacy, minimizing computational overhead to facilitate efficient key establishment between UAVs and other devices. However, their approach's reliance on fixed computational capabilities may limit its applicability in heterogeneous smart city environments with diverse device capabilities.

Authentication mechanisms play a crucial role in verifying the legitimacy of communicating entities within UAV networks. Nguyen et al. [20] developed a message authentication technique based on hash functions, aiming to reduce battery consumption during UAV activation. While their approach addresses authentication, it lacks mechanisms to mitigate denial-of-service attacks, a critical vulnerability in networked systems. Similarly, Zhang et al. [21] designed an authentication scheme for Internet of UAVs (IoUAV) infrastructure, enhancing security but lacking robust mechanisms for detecting and responding to suspicious activities or obstacles.

Ensuring secure communication between UAVs is vital for reliable swarm operation. Khoshafa et al. [22] proposed a two-pronged approach involving safety regulations to detect malicious UAVs and a multi-step negotiation process to establish trusted communication channels. Similarly, Yin et al. [23] introduced a source authentication scheme based on elliptic curve cryptography for secure data exchange in 5G-enabled UAV networks. Lan et al. [24] leveraged blockchain technology to develop an access control system for UAV communication, enhancing security through a multi-stage mutual authentication process and timestamp-based data protection.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

One traditional security model, the IEEE 1609.2 [25], is robust and designed particularly for VANET and uses PKI and digital signatures. However, it shows low efficiency for UAV swarms. Another security scheme is IETF DTLS [26] which aims to enhance the security of datagram-based communication and is suitable for UAVs apart from its computational heaviness. IETF IPsec [27] mainly adds strong network security with good scalability and resistance to DDoS attacks. Table 1 summarizes the key advantages of the proposed model compared to other known models.

Table 1. A comparison of the proposed security model with alternatives.

Criteria	Proposed System	IEEE 1609.2 [25]	IETF DTLS (RFC 6347) [26]	IETF IPsec (RFC 4301) [27]
Data Encryption	AES-128 (static data), RC4 (streaming data)	AES-128 or equivalent	AES-128 or higher	AES-128 or higher
Authentication Method	Bidirectional Entity Authentication (RSA)	PKI, Digital Certificates	Pre-shared Keys or Certificates	Pre-shared Keys or Certificates
Integrity Mechanism	HMAC-SHA1	Digital Signatures	HMAC with hash	HMAC with hash
Scalability	High (Designed for UAV swarms)	Moderate (Primarily for VANET)	Low to Moderate	High (for scalable networks)
Flexibility	High (Adapts to operational phases of a UAV swarm)	Low to Moderate (For VANET environments)	Moderate (Transport layer security)	High (Supports various network types)
DDoS Resistance	High (Anti-replay mechanisms, Firewall)	Moderate (For VANET resilience)	Moderate	High (Anti-replay protection)

Driven by the potential of UAV swarms to address the limitations of conventional SMI architectures, this paper presents a novel, resilient, and autonomous SMI system that leverages the power of collaborative UAVs. Our primary research objectives are:

1. To design and develop a comprehensive SMI architecture based on a self-organizing UAV swarm for efficient and reliable data collection from smart meters. This architecture encompasses the design of key components (DMC and UAV swarm), communication protocols, and operational phases for seamless data acquisition.
2. While existing research highlights the potential of UAV swarms for smart metering, there is a critical need to address the unique security challenges posed by these interconnected systems. This paper aims to bridge this gap by conducting a comprehensive security analysis of a UAV swarm-based SMI, identifying key threats across different operational phases, and proposing a multi-phased security model to mitigate these vulnerabilities. We will analyze potential attacks targeting the Data Management Center (DMC), individual drones, and communication links, developing tailored security protocols, authentication mechanisms, and countermeasures for each phase. Through rigorous evaluation, we will assess the effectiveness of our proposed solutions in mitigating specific attack types, comparing their strengths and limitations against existing approaches.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

3. System Design and Architecture

3.1. System Overview

The proposed UAV swarm-based SMI system comprises two primary components as shown in Figure 1:

Data Management Center (DMC): Acts as the central command and control hub for the entire system. It is responsible for mission planning, swarm configuration, data processing and analysis, and communication with external systems.

UAV Swarm: Consists of a designated Leader Drone (LD) and multiple Slave Drones (SDs). The LD coordinates the swarm's actions, relays instructions from the DMC to the SDs, aggregates data collected by the SDs, and transmits it back to the DMC. The SDs are responsible for collecting data from individual smart meters using their onboard sensors.

3.2. Data Management Center (DMC)

The DMC serves as the central nervous system of the SMI architecture, responsible for:

1. Mission Planning and Configuration: Human operators interact with the DMC to define mission parameters, such as the target area for data collection, desired swarm formation, data collection frequency, and any specific waypoints or flight paths the swarm should follow.
2. Swarm Configuration and Management: The operator selects the number of SDs to deploy, assigns a specific drone as the LD, and monitors the status of individual drones within the swarm through a user-friendly interface.
3. Data Processing and Analysis: The DMC receives data collected by the UAV swarm, processes it to extract relevant information, performs analysis to identify consumption patterns or anomalies, and generates reports for further action or decision-making.
4. Communication and Interfacing: The DMC establishes communication links with the LD using a reliable wireless communication protocol. It also interfaces with external systems, such as utility company databases or energy management platforms, to share data and facilitate integration with existing infrastructure.

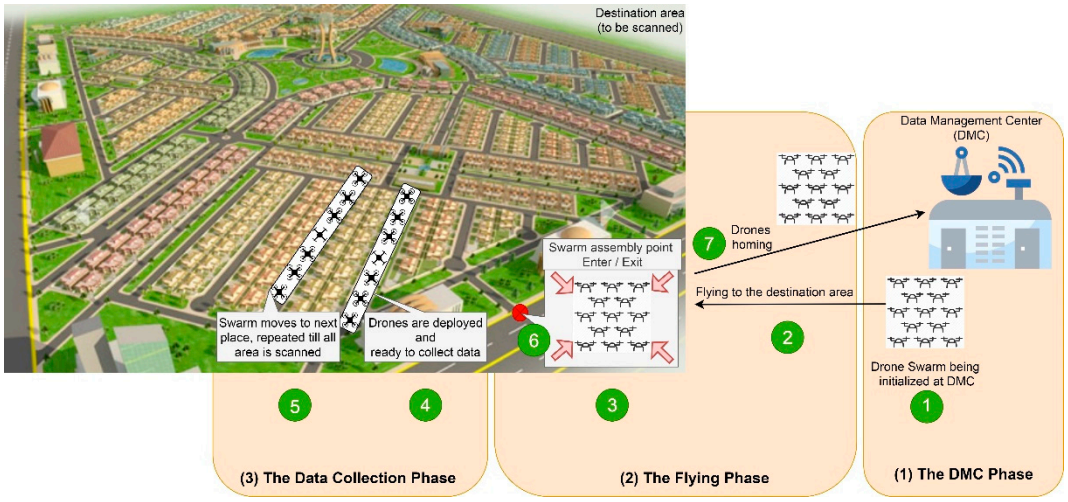

Figure 1. The proposed system procedural diagram.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

3.3. UAV Swarm: Leader Drone (LD) and Slave Drones (SDs)

3.3.1. Leader Drone (LD)

The LD plays a critical role in swarm coordination and communication. It is responsible for:

1. Receiving Mission Instructions: The LD receives detailed mission parameters from the DMC, including GPS waypoints, desired swarm formation, and data collection instructions.
2. Relaying Instructions to SDs: The LD disseminates mission instructions received from the DMC to the SDs, ensuring synchronized swarm movements and task execution.
3. Monitoring Swarm Status: The LD continuously monitors the status of individual SDs, including battery levels, location, and sensor readings. It relays this information back to the DMC for real-time situational awareness.
4. Aggregating Data from SDs: As SDs collect data from smart meters, they transmit it to the LD, which aggregates the data from all SDs and periodically transmits it back to the DMC for processing and analysis.

3.3.2. Slave Drones (SDs)

The SDs are the workhorses of the system, responsible for:

1. Following LD Instructions: SDs receive and execute instructions from the LD, maintaining formation during flight, deploying to specific locations, and initiating data collection sequences.
2. Data Collection from Smart Meters: SDs are equipped with appropriate sensors to collect data from smart meters. This may involve optical character recognition (OCR) to read data from traditional meters or wireless communication protocols to interface with smart meters directly.
3. Transmitting Data to the LD: Once data is collected, SDs transmit it wirelessly to the LD for aggregation and eventual transmission to the DMC.

3.4. Communication Protocols and Data Exchange

Efficient and reliable communication between the DMC, the LD, and the SDs is crucial for successful swarm operation.

- DMC to LD Communication: We propose utilizing a robust wireless communication protocol, such as 4G/LTE or potentially 5G in areas with coverage, for communication between the DMC and the LD. This ensures a stable connection with sufficient bandwidth for transmitting mission data and receiving status updates and aggregated data from the swarm.
- LD to SD Communication: For communication between the LD and SDs, a suitable wireless local area network (WLAN) protocol, such as Wi-Fi or Zigbee, can be employed. These protocols offer high data rates, low latency, and energy efficiency, essential for maintaining swarm coordination and exchanging data effectively.

3.5. Operational Phases

The operational cycle of the proposed UAV swarm-based SMI system can be broken down into three distinct phases, see Figure 2:

3.5.1. DMC Phase (Initialization and Configuration)

1. Swarm Power-Up: The operator powers up the required number of SDs and the designated LD.
2. Connection Establishment: The LD establishes a secure connection with the DMC, and the SDs connect to the LD, forming the swarm network.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

3. Mission Information Upload: The operator defines mission parameters (e.g., target GPS coordinates, swarm formation, data collection frequency) through the DMC interface. The DMC transmits this information to the LD.
4. SD Configuration: The LD receives the mission information and configures each SD with its specific role and tasks for the mission.

3.5.2. Flying Phase (Transit and Formation)

1. Swarm Launch: Upon receiving the launch command from the DMC, the LD initiates takeoff, followed by the SDs.
2. Formation Establishment: The LD guides the SDs to form the pre-defined swarm formation (e.g., linear, grid) while navigating towards the target area.
3. Waypoint Navigation: The LD, following the designated flight path and waypoints, leads the swarm to the target location for data collection. The SDs maintain their relative positions within the formation throughout the flight.

3.5.3. Data Collection Phase (Deployment and Sensing)

1. Target Area Arrival: The LD, upon reaching the designated target area, signals the SDs to prepare for deployment.
2. SD Deployment: The SDs autonomously deploy to their assigned locations within the target area, following a pre-defined deployment strategy to ensure efficient coverage of smart meters.
3. Data Acquisition: SDs activate their onboard sensors and collect data from the designated smart meters. The data collected may include energy consumption readings, voltage levels, and other relevant parameters.
4. Data Transmission to LD: Each SD transmits its collected data wirelessly to the LD for aggregation.
5. LD Aggregation and Transmission to DMC: The LD aggregates the data received from all SDs and periodically transmits it back to the DMC using the established long-range communication link.
6. Mission Completion and Return: Upon receiving confirmation from the DMC that sufficient data has been collected, the LD initiates the swarm's return to the launch site, maintaining formation throughout the flight back.

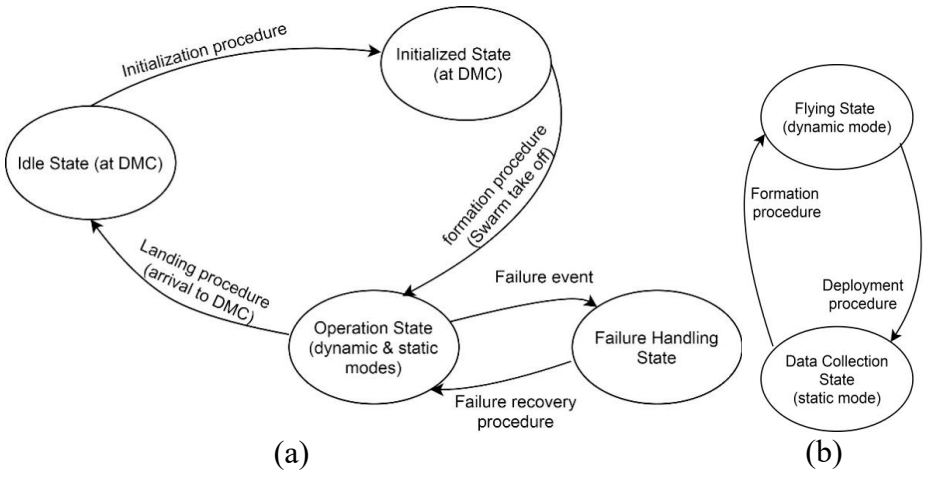

Figure 2. Main system state diagrams: (a) System overview (b) Operational modes.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

4. Ensuring System Reliability: Robust Failure Handling

Real-world deployments of UAV swarms are susceptible to various uncertainties, including drone malfunctions, communication interruptions, and unpredictable environmental conditions. To ensure system reliability and mission success even in the presence of such challenges, we have incorporated robust failure-handling mechanisms into our design, see Figure 3:

4.1. Leader Drone (LD) Failure Handling

LD failure poses a significant risk to mission success as it acts as the central coordinator of the swarm. To address this, we implement a multi-layered approach:

1. Backup LD Designation: During the initialization phase, the operator designates a specific SD as the backup LD. This backup LD possesses all the capabilities of the primary LD and remains on standby throughout the mission.
2. Hard Handover (Immediate LD Failure): In the event of a sudden and unexpected LD failure (e.g., collision, loss of communication), the backup LD immediately takes over the leadership role. It assumes responsibility for swarm coordination, data aggregation, and communication with the DMC, ensuring minimal disruption to the mission.
3. Soft Handover (Predicted LD Failure): To further enhance resilience, we introduce a novel failure prediction mechanism. The LD continuously monitors its onboard sensors (e.g., battery level, temperature) and can predict potential failures in advance. If the LD anticipates a failure, it initiates a soft handover process, transferring leadership to the designated backup LD before the failure occurs. This proactive approach allows for a smoother transition and potentially extends the operational life of the failing LD by allowing it to enter a power-saving mode.

4.2. Slave Drone (SD) Failure Handling

While SD failures are less critical compared to LD failures, they can still impact overall mission efficiency. To address SD malfunctions, we implement:

1. Dynamic Task Reallocation: If an SD fails or becomes unresponsive, the LD dynamically reassigns its tasks to other available SDs within the swarm. This ensures that all designated smart meters are covered, maintaining data collection continuity.
2. Failure Isolation: The LD isolates the failed SD from the swarm network to prevent potential communication interference or disruption to other operational drones.
3. Optional Return to Base: Depending on the severity of the failure and mission parameters, the LD can instruct the failed SD to return to the base station autonomously for maintenance or replacement.

4.3. Environmental Disturbance Mitigation

Operating in real-world urban environments exposes the UAV swarm to various environmental disturbances, such as wind gusts and obstacles. To mitigate the impact of such disturbances:

- Robust Formation Control Algorithm: The swarm utilizes a robust formation control algorithm that considers environmental factors and adjusts drone positions and movements dynamically to maintain formation integrity and prevent collisions.
- Onboard Sensors for Obstacle Avoidance: Each drone is equipped with onboard sensors (e.g., cameras, ultrasonic sensors) to detect and avoid obstacles autonomously, ensuring safe navigation through complex urban environments.

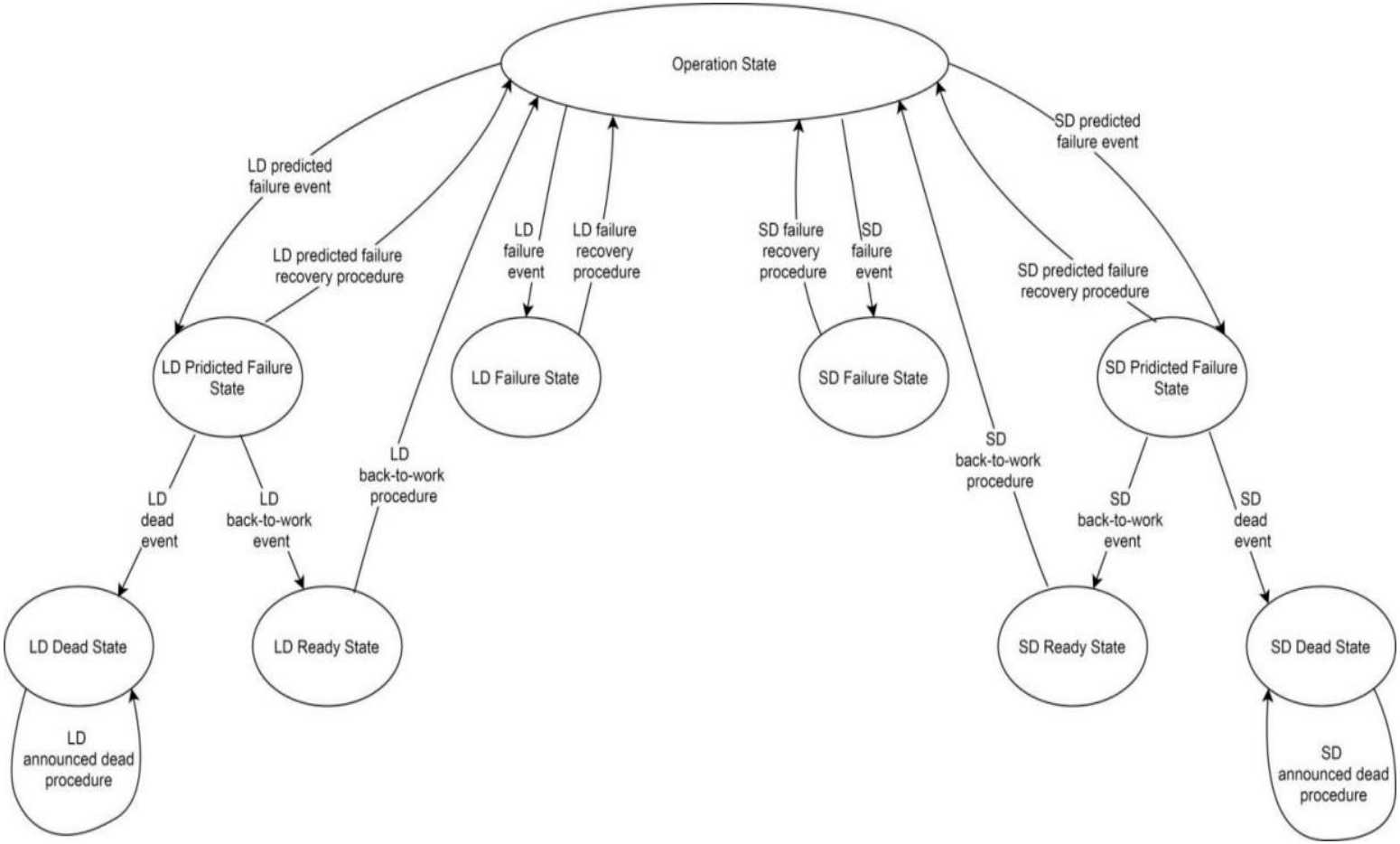

Figure 3. Failure Handling Diagram.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025

doi:10.20944/preprints202503.0821.v1

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

5. The Proposed System Security Model

The primary objective in developing an autonomous system is to collaborate with humans and assist them in various tasks. These tasks could be the ones that require operation in challenging and life-threatening situations such as Search and Rescue Missions (SARs). However, inappropriate implementation or malicious intention could lead to disasters [28]. For a swarm of UAVs, some core operations are required for a successful mission accomplishment which could include; flight control, flight routing, obstacle avoidance, self-protection, and regulation conformation for airspace usage, concerning physical integrity and cybersecurity [29]. Additionally, incorporating an anomaly detection framework by utilizing machine learning models could be referred to as high-level design. This involves detecting unusual behavior, identifying outliers, and discriminating any intruder nodes that may join the formation.

5.1. Swarm Mission Roadmap and Phases

Generally, the swarm operational procedure involves three main phases, see Figure 4.

1. **The DMC Phase:** Includes swarm member selection and initialization before launching the operation (pre-operation procedure) as well as swarm member inspection after returning from a mission (post-operation procedure).
2. **The Flying Phase:** Comprises the swarm flight from the DMC to the destination area and vice versa, the moving from one place to another within the destination area, and the formation/deployment procedures.
3. **The Data Collection Phase:** In this phase, data is collected as the drones stay stationary with no mobility, either hovering or landing.

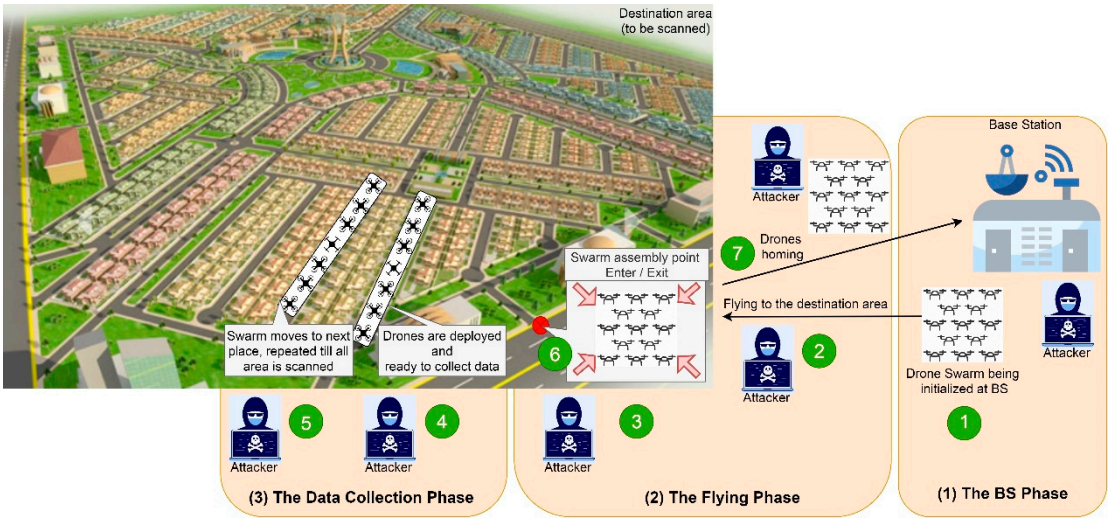

Figure 4. Mission procedural phases and attack possibility.

From the above scenario, 3 main phases of the swarm mission could be highlighted and the threats/attacks could be in any phase of the operation. The security requirements, thus, differ for each phase according to the swarm behavior and certain threats could be expected at each stage of the mission.

In the coming subsections and for each operational procedure phase, the threat model, network security model, and security solution analysis for the proposed UAV swarm-based smart metering infrastructure will be discussed in detail.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

5.2. Security Analysis and Countermeasures

Compromising a group of UAVs is done for malicious purposes, especially when they act as a Self-Organizing Network (SON) [30]. Thus, it is required to detect attacks and prevent them from damaging the system [31]. Therefore, the threat model, network security model, and security solution assessment will be carried out for each operational phase to give an overview of the security possible attacks and mitigations for the whole swarm operation.

The threat modeling procedure consists of several stages; starting with identifying and understanding the possible threats to a specific system, following that countermeasures must be defined to mitigate the threats. This procedure assists in the process of evaluating security risks and countermeasures as the system is susceptible to attacks. Expecting possible threats is a challenging task. Analyzing every single part of the system for various security aspects by following the Confidentiality, Integrity, Availability (CIA) model provides the basis for researchers to identify certain attacks [32].

To immunize the proposed SMI, we will suggest a security model for both the DMC and the drones to protect them against different internal and external threats. The main goal is to protect message transactions as well as their functionality and accessibility.

The proposed network security model should respond to several objectives; it must guarantee that the exchanged data is correct and undiscoverable, i.e. authenticity, integrity, and privacy of data, and the source is legitimate, i.e. source authentication, further, the system must be reliable and available. The suggested security solutions are analyzed to verify their addressing capability of the expected threats.

The focus of this work will be on the network layer level and the goal is securing message transactions, where related common threats and attacks will be highlighted, then available well-known solutions will be suggested and analyzed for each operational phase.

5.3. The Threat Model

In this section, we are concentrating on attacks perpetrated against the UAV and the DMC server as essential elements in the proposed SMI. Security threats against a UAV can take multiple forms and originate from various sources. When investigating potential attacks, UAVs are vulnerable to a broad range of attacks that vary in their nature, goals, and destructive effects [33]. We have made a survey on the possible attacks against drone swarm and the results are abstracted in Table 2.

Table 2. The possible attacks against the proposed system.

Attack Type	Description
ID Spoofing	Pretending to be the real drone, is achieved by compromising the communication link and obtaining the ID of a certain UAV.
Eavesdropping Attacks	To improve communication performance, most UAVs avoid encrypting wireless communication hence allowing them to eavesdrop on transferred data, e.g. sensor and GPS data.
DoS and DDoS Attacks	Flooding the drone's network card with random invaluable traffic by sending excessive requests which overloads its resources and disrupts its availability.
Man-in-the-Middle Attacks	One of the popular attacks is done by controlling the communication link and modifying packets maliciously.
Replay Attacks	After a successful eavesdropping attack, it replays valid data to the drone to enforce it to receive repeated data without the ability to separate legitimate requests from malicious ones.
Forgery Attacks	Compromising drone communication link integrity by sending a forged request to unauthenticated drones.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

5.4. The Network Security Model

The different transactions among the DMC server and the LD as well as between the LD and the rest of the swarm are vulnerable to several types of attacks and care should be taken to secure the messages and their origins. We suggest these methods to ensure message transaction security:

1. Bidirectional entity authentication between the DMC server and the LD and also between the LD and other SDs.
2. All the transferred packets, i.e. the transactions among swarm nodes and the DMC, are encrypted and sent along with their Hash-based Message Authentication (HMAC) to achieve message confidentiality, integrity, and authentication. The Internet Protocol Security (IPSec), explained in detail in the coming sub-section, is adopted for this purpose.
3. Implementing a suitable firewall solution.

Within the IPv6 environment, each UAV has it is own ID that is hardware built-in and stored as default settings besides a public-private key pair assigned for each drone. The combination of these three secrets (the IPv6 address, the default factory setting ID, and the private key) could be used to identify a UAV in the swarm, i.e. entity authentication.

Symmetric keys, e.g. Advanced Encryption Standard (AES) in our case, are adopted mainly for message encryption because the method of public-key encryption requires more resources, time, and processing capabilities to perform the needed calculations, therefore, we suggest using it only in the procedures that demand short packets, i.e. key distribution, thus, we recommend using AES for other encryption purposes. However, different sets, or pairs, of AES keys are required for encrypting the data packets in various sessions. Table 3 summarizes the required encryption keys, their purpose, and source-destination pairs. Furthermore, having similar UAVs in a swarm, as in the case of the proposed system, could increase the security as if they are identical in shape, size, and color, it becomes challenging for the adversary to identify the backbone UAV [28], i.e. the LD.

Table 3. The required key groups.

Key Name	Purpose	Nodes
AES key group 1 (multiple key pairs each for a UAV)*	To encrypt the intra-swarm reports and commands and also for bidirectional entity authentication.	SD - LD
AES key 2 (one key pair)*	To encrypt the inter-swarm reports and commands and also for bidirectional entity authentication.	LD - DMC
Public-Private key group 1 (one pair for each network node)	Key management.	SD - LD LD - DMC
RC4 stream ciphering*	To encrypt streamed data (if any)	SD - LD LD - DMC

* These keys are renewed during operation.

5.4.1. Bidirectional Entity Authentication

Before accepting any connection, the DMC server, the LD, or the SD, i.e. any network node, should verify the identity of the other system node. This can be done in various ways, and we suggest adopting the challenge-response procedure as shown in Figure 5.

The challenge consists of the UAV ID and its IPv6 address which are both encrypted using the receiver's public key and then sent by the sender node. The recipient node decrypts the packet, authenticates the sender, and then sends a response back to the sender node, the response contains the receiver's ID with its IPv6 address and both are encrypted by the sender's public key. Similarly,

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

the sender decrypts the response and authenticates the receiver. We called this procedure a bidirectional authentication as it confirms the node identity for both peers.

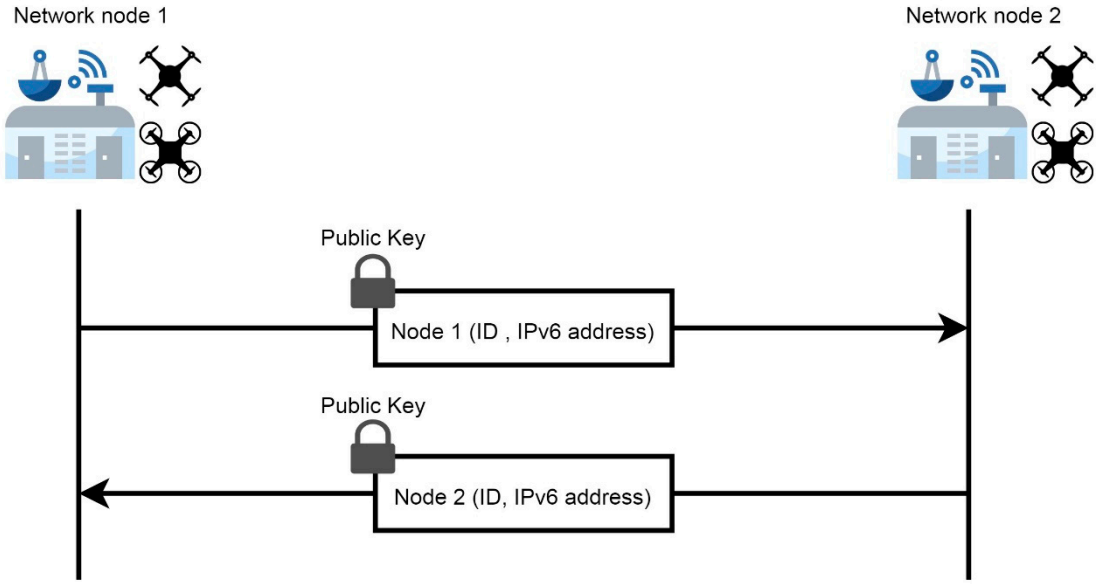

Figure 5. The adopted bidirectional entity authentication technique.

This procedure proves the node's identity in many aspects:

1. The challenge/response messages are encrypted using the other end's public key, so no node can decrypt the message unless it has the associated private key.
2. When decrypting the message, the node ID is considered another identity proof of the sender.
3. Also, the sender has a unique IPv6 address which can be extracted when decrypting the message, and it also proves the identity of the sender.
4. The procedure is bidirectional and the same procedure is repeated for the other node. Additionally, when the receiver accepts the challenge and replies with a response, this is another proof of its identity.

5.4.2. Bidirectional Message Confidentiality, Integrity, and Authentication

By adopting IPv6 in the suggested system, it allows the system to have more efficient security by customizing the available Internet Protocol Security (IPSec) features to suit our proposed UAV swarm approach, this is done in all operational phases, as follows:

1. IPSec Mode: This is considered to work in the tunneling mode for all the system connections acting as a Virtual Private Network (VPN) between each pair of nodes. The reason behind this is not to only encrypt the IPSec header and payload for a packet but also to allow the IPv6 header to be encrypted as well, which provides a better information-hiding for security purposes. In tunnel mode, the (inner) IP header carries the ultimate addresses for the source and destination, whereas an (outer) IP header may contain specific IP addresses, e.g. addresses of security gateways.
2. IPSec Type: The Encapsulating Security Payload (ESP) protocol type of IPSec is selected to provide security features that are implemented in all communicating peers, thus, protecting the whole session. ESP provides many services including; data confidentiality, data origin authentication and message integrity, anti-replay service, and Key management.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

3. Data Confidentiality: This could be provided by using 128-bit AES keys, as mentioned earlier, as a block cipher. However, if the system application contains data streaming as in the proposed SMI system, e.g. video call, then a stream ciphering should be used to provide data encryption, refer to Table 3. We suggest using the 128-bit Rivest Cipher 4 (RC4) algorithm as a lightweight and fast stream ciphering approach that offers a reasonable level of confidentiality to encrypt the transmitted streaming packets among system nodes.
4. Data Origin Authentication and Message Integrity: This could be achieved by using a Hashed Message Authentication Code using HMAC-SHA1 where the combination of the message and the AES key is hashed and yields the intermediate Message Authentication Code (MAC) that is hashed again with the same key to generate the HMAC. Finally, before data transmission, the resulting HMAC is appended to the encrypted message.
5. Anti-replay Service: This is an IPSec built-in feature and could be enabled which adds an IPSec sequence number to differentiate messages and prevent anti-replay attacks.
6. Key Management: This is provided in IPSec through the Internet Key Exchange (IKE) protocol. We suggest using one pair of public-private keys for each network node, see Table 3, IKE version 2 (IKEv2) is the version of choice as it supports mobility, maintains the form of IKEv1, and designs the connection process more simply and quickly [34]. IKEv2 uses several cryptographic algorithms to deliver its function, including four transform types; encryption algorithm, integrity algorithm, Diffie-Helman Groups, and pseudorandom functions [35].
7. Renewing Cipher Keys: This could be achieved by assigning SAs a certain lifetime for the specified set of keys.

Additionally, to defend against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, the DMC can block traffic from the UDP port of origin (port 1900) among inbound traffic [36]. The proposed security model for the SMI system is shown in Figure 6.

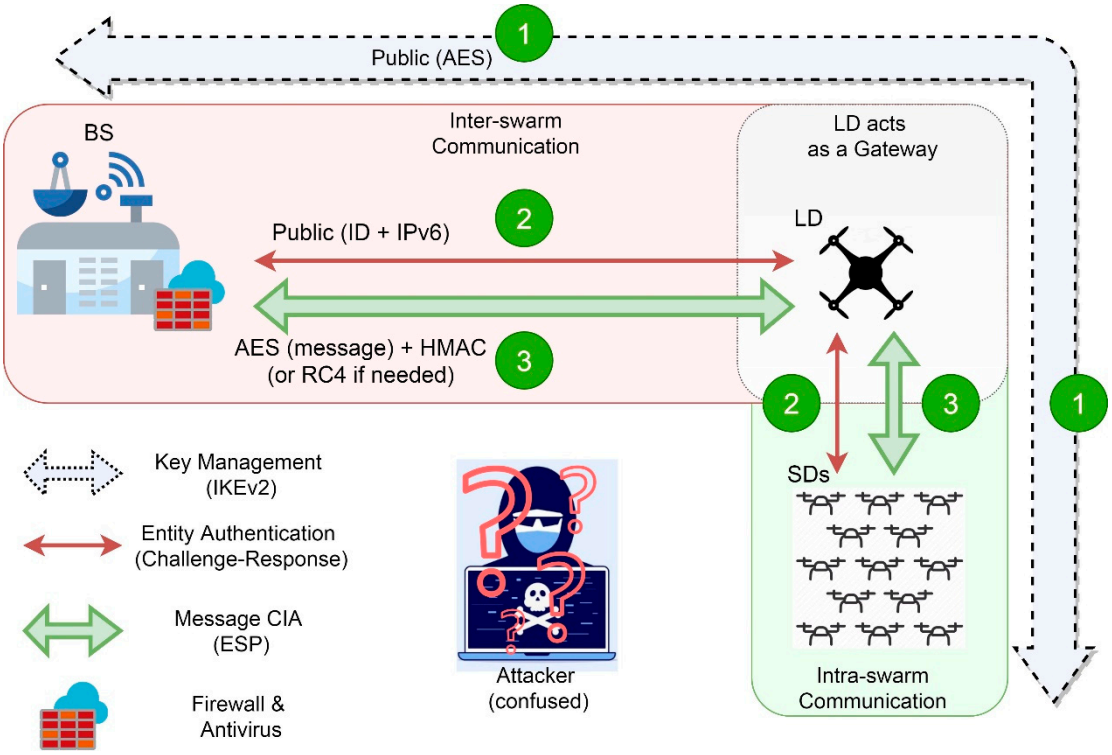

Figure 6. The suggested security model.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

5.4.3. The System Phases and Specific Security Procedures

Now, all the proposed security solutions are applicable the all three operational phases. Nevertheless, each phase has a unique nature and requires a special security procedure along with the common security model for the whole swarm. The distinct security procedures for each phase are discussed in the coming sub-sections.

1. **The DMC Phase:**

This is the phase where the drone swarm is in the DMC either before the mission is conducted or after mission completion. In each case, a strict security policy should be followed to protect message and data transactions. All the aforementioned security practices are common for all operational phases. However, in addition to that, for the DMC phase two procedures will be carried out depending on the operation status as explained:

- **Pre-operation Launch:** In this scenario, the drone swarm operator performs an identity check for system nodes before authentication, then configures the SAD for each network node so it will have the required sets of keys, i.e. AES key pair and RC4 (if any), that might be renewed during the mission for each phase and also while swarm repositioning when collecting readings in the field. After that, the mission information file, which contains all required information for the mission completion such as a list of GPS coordinates as waypoints, is encrypted and uploaded to the LD, which in turn sends the required information to each swarm member.
- **Post-operation Completion:** After drone swarm homing and landing in the DMC, an identity inspection for each UAV is done to ensure that neither a legitimate UAV nor a malicious UAV has joined the swarm. Also, all stored readings are uploaded to the server and all security keys are erased from the SAD.

2. **The Flying Phase**

This phase is the only phase that has mobility among operational phases, where UAVs fly from one point to another in formation. Drones either travel between the DMC and the destination area or from one location to another within the testing field. Due to the continuing mobility of the swarm in this phase, the possibility of a malicious UAV joining the swarm as well as creating forged messages is high. Therefore, special practices are suggested to prevent the possible occurrence of such attacks which are:

- **Renewing Cipher Keys:** The AES and RC4 keys should be renewed, i.e. calling for a new key set from the SAD, before each flight.
- **Periodic Entity Authentication:** Entity check should be performed periodically using the suggested entity authentication mechanism, refer to Figure 6, during the flight.

3. **The Data Collection Phase:**

UAVs in this phase collect readings, either stationary (hovering) or landing. These messages exchanged in this phase are more critical as the swarm might collect sensitive data that should be well-protected and secured. This phase is normally the longest phase where sensitive data might be collected and transmitted to the DMC either in real-time or periodically as mission reports, the possibility of intercepting the exchanged data is high, e.g. eavesdropping and man-in-the-middle attacks, hence, special practices are suggested to prevent the possible occurrence of such attacks which are:

- **Renewing Cipher Keys:** The AES and RC4 keys should be renewed periodically, i.e. retrieving a new key set from the SAD, after each landing.
- **Periodic Entity Authentication:** This procedure should be carried out before transferring any sensitive data using the suggested entity authentication approach, refer to Figure 6.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

5.4.4. The Security Solutions Assessment

After mentioning the possible attacks that could be performed on our proposed system along with the network security model that explains in detail the adopted security protocols and features, now we can analyze and assess the proposed countermeasures against possible threats. Table 4 shows the possible attacks and adopted countermeasures against these attacks.

Table 4. Possible attacks and adopted security countermeasures.

Attack Type	Against	Flaws	Suggested Defense
ID spoofing	UAV, server	Pretending to be a legitimate node.	The use of suitable entity authentication methods.
Eavesdropping attacks	Communication link	Data disclosure, including telemetry, feeds, and DMC commands.	Adopting authenticated encryption.
DoS and DDoS attacks	Communication link	Compromising the availability of certain services	Using a firewall to block incoming traffic from the UDP port of origin (port 1900).
Man-in-the-Middle attacks	Communication link	Controlling the communication channel and modifying the packets maliciously.	Encrypting control commands. Implementing solutions to authenticate UAVs.
Replay attacks	UAV, server	Node confusion so it cannot separate legitimate requests from malicious ones.	Secure communication scheme establishment. The use of authentication mechanisms. The use of IPSec sequence number.
Forgery attacks	Communication link	Compromising UAV's communication integrity by sending a forged request to unauthenticated UAVs.	Encryption and integrity of control commands. Implementing techniques to authenticate UAVs

6. Performance and Overhead Analysis

The proposed security mechanism for the UAV swarm-based SMI, as its equivalents, produces some performance overhead. Therefore, to quantify and analyze this overhead, a general mathematical model that considers both computational and communicational overhead and how they impact swarm duration [37–43] is introduced in this section.

6.1. Model Derivation

1. **Computational Overhead (Time):** The total time of cryptographic operations (O_c) can be calculated by multiplying the time per operation (t_c), the frequency of operations (f_c), and the total mission time (T_mission) as shown:

$$O_c = t_c * f_c * T_{mission} \quad \text{.....(Eq1)}$$

2. **Communication Overhead (Time):** Likewise, the time spent on security-related communication (O_comm) can be found by multiplying the time per message transmission (t_comm), the frequency of transmissions (f_comm), and the mission time as given:

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

O_comm = t_comm * f_comm * T_mission ……..(Eq2)

3. **Total Time Overhead:** Summing the computational and communication overheads yields the total time overhead (O_total) as illustrated:

O_total = O_c + O_comm ……..(Eq3)

4. **Computational Overhead (Energy):** Similar to the time overhead, the energy consumed by cryptographic operations (E_comp) is calculated using energy per operation (E_c) instead of time as shown:

E_comp = E_c * f_c * T_mission ……(Eq4)

5. **Communication Overhead (Energy):** Similarly, the energy consumed by communication (E_comm_total) is calculated using energy per message (E_comm) as shown:

E_comm_total = E_comm * f_comm * T_mission ……(Eq5)

6. **Total Energy Overhead:** The sum of computational and communication energy expenditures gives the total energy overhead (E_total) as given:

E_total = E_comp + E_comm_total ……...…….(Eq6)

7. **Feasible Mission Time:** The feasible mission time (T_feasible) is calculated by dividing the battery capacity (B) by the total power consumption (base power (P_base) added to the average power overhead) as shown:

T_feasible = B / (P_base + (E_total / T_mission)) ……(Eq7)

8. **Swarm Impact (Communication):** The communication overhead is affected by the swarm size (n). To model the increased communication burden as the swarm grows, a scaling factor (α) that represents the proportion of communication overhead related to the number of other UAV groups is introduced. We assume the leader drone (LD) handles aggregation efficiently, thereby inter-UAV communication is not directly proportional to n.

O_comm_swarm = O_comm * (1 + α(n-1)) ……(Eq8)

6.2. The Proposed Scenario Settings and Results

The roles of each member in the UAV-based swarm could vary according to the application assigned to the group. However, to give approximate figures indicating the performance of the swarm, the following assumptions are made, see Table 5.

Table 5. Parameter Settings and Values.

Parameter	Description	Value
t_c	Cryptographic operation time (ms)	AES-128: 2, SHA-256: 1, Auth: 5
t_comm	Message transmission time (ms)	0.04
E_c	Energy per cryptographic operation (mJ)	AES-128: 0.1, SHA-256: 0.05, Auth: 0.25
E_comm	Energy per message transmission (mJ)	0.01
B	Battery capacity (mJ)	6000
P_base	Base power consumption (mW)	500
α	Swarm scaling factor	0.1
T_mission	Desired mission time (s)	3600
f_c	Frequency of crypto operations (1/s)	1/300 (every 5 min)
f_comm	Frequency of transmissions (1/s)	1/300 (every 5 min)

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

By utilizing the aforementioned equations (Eq1 to Eq8) and substituting the values given in Table 5, approximate figures of computational, communicational, and total overhead could be calculated as shown in Table 6.

Table 6. Performance Metrics for Different Scenarios.

Scenario	O_total (s)	E_total (mJ)	T_feasible (s)
Baseline (n=5,α=0.1)	1.2336	12.24	3599.83
Larger Swarm (n=25,α=0.1)	1.2816	12.24	3599.82
Higher Comm Frequency (fcomm=1/60)	2.0160	18.36	3599.69
Larger Swarm (n=50,α=0.1)	1.5616	12.24	3599.80
Extreme Swarm (n=100,α=0.1)	1.8816	12.24	3599.77
Increased Scaling (n=50,α=0.2)	1.8320	12.24	3599.78
High Scaling (n=50,α=0.5)	3.0240	12.24	3599.66
High Scaling (n=100,α=0.5)	4.6080	12.24	3599.54

The results point out the robustness of the proposed security model under varying conditions. The approach can effectively handle the scalability to larger swarms and greater communication needs, reducing overheads and minimizing impact on energy consumption and mission duration alike. This reflects the system's suitability for deployment in real-world UAV swarm scenarios.

7. Conclusions

This paper demonstrates the necessity of a comprehensive security framework for a mobile Smart Metering Infrastructure (SMI) based on UAV swarms, highlighting potential threats to various operational phases. The proposed framework enhances the overall reliability and trustworthiness of UAV warms by integrating IPsec-based communication and bidirectional entity authentication. Infrastructure resiliency is protected by addressing proactive countermeasures for well-known attacks, i.e. denial-of-service (DoS), man-in-the-middle, and replay attacks. The work is compared against traditional alternatives to illustrate its key strengths including adaptability and effectiveness. Future work could address and mitigate the security-related computational overhead, developing lightweight cryptographic solutions, and suggesting real-time anomaly detection mechanisms. As a critical smart city application solution, UAV swarms could be enabled to their full potential by adopting these advancements that ensure security and privacy in dynamic environments.

Competing Interest declaration: there are no Competing Interests.

References

1. K. C. Aleksander, "Military use of unmanned aerial vehicles–a historical study," *Safety & Defense,* vol. 4, pp. 17-21, 2018.
2. J. Kim, S. Kim, C. Ju, and H. I. Son, "Unmanned aerial vehicles in agriculture: A review of perspective of platform, control, and applications," *Ieee Access,* vol. 7, pp. 105100-105115, 2019.
3. M. Lyu, Y. Zhao, C. Huang, and H. Huang, "Unmanned aerial vehicles for search and rescue: A survey," *Remote Sensing,* vol. 15, p. 3266, 2023.
4. M. S. Qassab and Q. I. Ali, "A UAV-based portable health clinic system for coronavirus hotspot areas," *Healthcare Technology Letters,* vol. 9, pp. 77-90, 2022.
5. K. Peng, J. Du, F. Lu, Q. Sun, Y. Dong, P. Zhou, *et al.*, "A hybrid genetic algorithm on routing and scheduling for vehicle-assisted multi-drone parcel delivery," *IEEE Access,* vol. 7, pp. 49191-49200, 2019.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

6. W. Chen, J. Liu, H. Guo, and N. Kato, "Toward robust and intelligent drone swarm: Challenges and future directions," *IEEE Network,* vol. 34, pp. 278-283, 2020.
7. G. Skorobogatov, C. Barrado, and E. Salamí, "Multiple UAV systems: A survey," *Unmanned Systems,* vol. 8, pp. 149-169, 2020.
8. S.-J. Chung, A. A. Paranjape, P. Dames, S. Shen, and V. Kumar, "A survey on aerial swarm robotics," *IEEE Transactions on Robotics,* vol. 34, pp. 837-855, 2018.
9. C. W. Reynolds, "Flocks, herds and schools: A distributed behavioral model," in *Proceedings of the 14th annual conference on Computer graphics and interactive techniques*, 1987, pp. 25-34.
10. H. T. Do, H. T. Hua, M. T. Nguyen, C. V. Nguyen, H. T. Nguyen, H. T. Nguyen, *et al.*, "Formation control algorithms for multiple-uavs: a comprehensive survey," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems,* vol. 8, pp. e3-e3, 2021.
11. Q. Ouyang, Z. Wu, Y. Cong, and Z. Wang, "Formation control of unmanned aerial vehicle swarms: A comprehensive review," *Asian Journal of Control,* vol. 25, pp. 570-593, 2023.
12. K.-K. Oh, M.-C. Park, and H.-S. Ahn, "A survey of multi-agent formation control," *Automatica,* vol. 53, pp. 424-440, 2015.
13. Y. Liu, J. Liu, Z. He, Z. Li, Q. Zhang, and Z. Ding, "A survey of multi-agent systems on distributed formation control," *Unmanned Systems,* pp. 1-14, 2023.
14. F. Saffre, H. Hildmann, and H. Karvonen, "The design challenges of drone swarm control," in *International conference on human-computer interaction*, 2021, pp. 408-426.
15. O. I. Abiodun, A. Jantan, A. E. Omolara, K. V. Dada, N. A. Mohamed, and H. Arshad, "State-of-the-art in artificial neural network applications: A survey," *Heliyon,* vol. 4, 2018.
16. V. François-Lavet, P. Henderson, R. Islam, M. G. Bellemare, and J. Pineau, "An introduction to deep reinforcement learning," *Foundations and Trends® in Machine Learning,* vol. 11, pp. 219-354, 2018.
17. S. L. Qaddoori and Q. I. Ali, "An efficient security model for industrial internet of things (IIoT) system based on machine learning principles," *Al-Rafidain Engineering Journal (AREJ),* vol. 28, pp. 329-340, 2023.
18. M. H. Khoshafa, T. M. Ngatched, Y. Gadallah, and M. H. Ahmed, "Securing LPWANs: A Reconfigurable Intelligent Surface (RIS) Assisted UAV Approach," *IEEE Wireless Communications Letters,* 2023.
19. H. K. Saini and K. Jain, "Heuristics to Secure IoT-Based Edge-Driven UAV," in *Multidisciplinary Approaches to Sustainable Human Development*, ed: IGI Global, 2023, pp. 283-301.
20. S. Q. Nguyen, A.-T. Le, C.-B. Le, P. T. Tin, and Y.-H. Kim, "Exploiting user clustering and fixed power allocation for multi-antenna UAV-assisted IoT systems," *Sensors,* vol. 23, p. 5537, 2023.
21. Y. Zhang, L. Meng, M. Zhang, and W. Meng, "A secure and lightweight batch authentication scheme for Internet of Drones environment," *Vehicular Communications,* vol. 44, p. 100680, 2023.
22. A. Aljumah, "UAV-Based Secure Data Communication: Multilevel Authentication Perspective," *Sensors,* vol. 24, p. 996, 2024.
23. Z. Yin, N. Cheng, Y. Song, Y. Hui, Y. Li, T. H. Luan, *et al.*, "UAV-assisted secure uplink communications in satellite-supported IoT: Secrecy fairness approach," *IEEE Internet of Things Journal,* 2023.
24. J. Wang, Z. Jiao, J. Chen, X. Hou, T. Yang, and D. Lan, "Blockchain-aided secure access control for UAV computing networks," *IEEE Transactions on Network Science and Engineering,* 2023.
25. I. Committee, "IEEE standard for wireless access in vehicular environments-security services for applications and management messages," *IEEE Vehicular Technology Society,* vol. 1609, 2013.
26. E. Rescorla and N. Modadugu, "Datagram transport layer security version 1.2," 2070-1721, 2012.
27. S. Kent and K. Seo, "Security architecture for the internet protocol," 2070-1721, 2005.
28. Y. Mekdad, A. Aris, L. Babun, A. E. Fergougui, M. Conti, R. Lazzeretti, *et al.*, "A Survey on Security and Privacy Issues of UAVs," *arXiv preprint arXiv:2109.14442,* 2021.
29. R. N. Akram, K. Markantonakis, K. Mayes, O. Habachi, D. Sauveron, A. Steyven, *et al.*, "Security, privacy and safety evaluation of dynamic and static fleets of drones," in *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, 2017, pp. 1-12.
30. Q. Ibrahim and M. Qassab, "Theory, Concepts and Future of Self Organizing Networks (SON)," *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science),* vol. 15, pp. 904-928, 2022.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 March 2025 doi:10.20944/preprints202503.0821.v1

31. V. A. Dovgal and D. V. Dovgal, "Security analysis of a swarm of drones resisting attacks by intruders," in *Distance educational technologies: proceedings of the 5th Intern. scient. and pract. conf. Simferopol*, 2020, pp. 372-377.
32. F. Jahan, W. Sun, Q. Niyaz, and M. Alam, "Security modeling of autonomous systems: a survey," *ACM Computing Surveys (CSUR)*, vol. 52, pp. 1-34, 2019.
33. Q. I. Ali, "Towards Secure & Green Advanced Metering Infrastructure (AMI)," *International Journal of Applied Science and Engineering*, vol. 14, pp. 147-169, 2017.
34. D. H. Lee and J. G. Kim, "IKEv2 authentication exchange model and performance analysis in mobile IPv6 networks," *Personal and ubiquitous computing*, vol. 18, pp. 493-501, 2014.
35. S. Praptodiyono, M. I. Santoso, T. Firmansyah, A. Abdurrazaq, I. H. Hasbullah, and A. Osman, "Enhancing IPsec performance in mobile IPv6 using elliptic curve cryptography," in *2019 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2019, pp. 186-191.
36. Y.-j. Lee, H.-s. Chae, and K.-w. Lee, "Countermeasures against large-scale reflection DDoS attacks using exploit IoT devices," *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, vol. 62, pp. 127-136, 2021.
37. Y. Su, H. Zhou, Y. Deng, and M. Dohler, "Energy-efficient cellular-connected UAV swarm control optimization," *IEEE Transactions on Wireless Communications*, 2023.
38. K. Han, E. Al Nuaimi, S. Al Blooshi, R. Psiakis, and C. Y. Yeun, "Scalable Authenticated Communication in Drone Swarm Environment," *Journal of Internet Technology*, vol. 25, pp. 255-265, 2024.
39. Q. I. Ali ,"Design and implementation of an embedded intrusion detection system for wireless applications." *IET Information Security*, 6(3), 171-182. , 2012, DOI: 10.1049/iet-ifs.2011.0152.
40. M.H., Q. I. Ali, Internet of Autonomous Vehicles Communication Infrastructure: A Short Review, n(2023), 24 (3),DOI: 10.29354/diag/168310
41. Q. I. Ali (2016). "Securing solar energy-harvesting road-side unit using an embedded cooperative-hybrid intrusion detection system." *IET Information Security*, 10(6), 386-402. DOI: 10.1049/iet-ifs.2015.0180.
42. Q. I. Ali, "An efficient simulation methodology of networked industrial devices," in *Proc. 5th Int. Multi-Conference on Systems, Signals and Devices*, 2008, pp. 1-6.
43. Q. I. Ali, "Security issues of solar energy harvesting road side unit (RSU)," *Iraqi Journal for Electrical & Electronic Engineering*, vol. 11, no. 1, 2015.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.