Jurnal Mantik, 7 (4) (2024), ISSN 2685-4236 (Online)

Published by:Institute of Computer Science (IOCS)

Jurnal Mantik

Journal homepage: www.iocscience.org/ejournal/index.php/mantik

Designing an adaptive modular management system for data security in Multi-UAV by using a Pattern Language Approach

Gregorius Airlangga
Information System, Atma Jaya Catholic University of Indonesia, Jakarta, Indonesia

A R T I C L E I N F O

Article history:

Received Nov 24, 2023
Revised Jan 16, 2024
Accepted Feb 15, 2024

Keywords:

Adaptive Modular;
Data Security;
Software Architecture;
Software Pattern;
UAV.

ABSTRACT

In the rapidly evolving landscape of Unmanned Aerial Vehicle (UAV) technology, the dynamic and unpredictable nature of operational environments presents substantial challenges for data security systems. This research introduces a novel software pattern design tailored for enhancing data security in online UAV operations within such environments. Inspired by the principles of the Pattern Language of Program Community (PLOP), this study proposes a comprehensive design pattern focused on modularity, adaptability, and scalability. The proposed design intricately combines various software patterns, forming a unified framework that addresses key aspects of UAV data security operations, including real-time adaptability, environmental responsiveness, and efficient resource management. The architecture of this framework integrates behavioral, structural, and creational patterns, meticulously selected to bolster the UAVs' decision-making capabilities, data handling, and dynamic adaptation in response to changing environmental and operational conditions. Theoretical analysis and conceptual evaluations underpin this research, favoring a detailed theoretical exploration over empirical experimentation. This approach allows for an in-depth examination of the design's potential and applicability in the context of UAV data security. The research contributes to the UAV field by offering a structured and standardized methodology, laying a robust theoretical foundation for future empirical studies and practical implementations. The goal is to significantly enhance the security, efficiency, and safety of UAV operations in dynamic and challenging environments, setting a new benchmark for data security solutions in the realm of UAV technology.

Corresponding Author:

Gregorius Airlangga,
Information System,
Atma Jaya Catholic University of Indonesia,
Jl. Jenderal Sudirman No. 51, Jakarta,10220, Indonesia.
Email: gregorius.airlangga@atmajaya.ac.id

1. INTRODUCTION

The accelerated integration of Unmanned Aerial Vehicles (UAVs) across diverse sectors such as military surveillance, environmental monitoring, and disaster response presents a critical need for robust data security systems (N. Mohamed J. Al-Jaroodi & Mohammed,

2020; S. A. H. Mohsan N. Q. H. Othman & Khan, 2023; Shakhatreh et al., 2019). Traditional security approaches, while offering foundational protection, often lack the necessary dynamism to adapt to the complex, changing operational landscapes of UAVs (S. A. H. Mohsan M. A. Khan & Alsharif, 2022; S. A. H. Mohsan N. Q. H. Othman & Khan, 2023; Shakeri et al., 2019). This paper introduces an innovative solution, the Adaptive Modular Management System, utilizing a pattern language approach to address these emerging challenges in multi-UAV data security.

The deployment of UAVs in critical operations has amplified concerns regarding the security of data being collected and transmitted. Current research, as outlined by (N. Neshenko E. Bou-Harb & Ghani, 2019) primarily revolves around static security models, which, although secure, offer limited flexibility against the backdrop of ever-evolving threat scenarios. The work from (Thibbotuwawa Bocewicz & Nielsen, 2019) further highlights the shortcomings of these models in adapting to variable operational environments typical of UAV missions. These models, rooted in traditional security paradigms, fall short in addressing the nuanced requirements of modern UAV operations, as indicated by (Goldfarb & Lindsay, 2022; Hassler & Baysal-Gurel, 2019; R. Zhang L. Cao & Shu, 2023).

A significant gap identified in the current research, as per (et al., 2019; K.-Y. Tsao T. Girdler & Vassilakis, 2022) is the lack of comprehensive security solutions that cater specifically to the unique attributes of multi-UAV systems, notably their mobility, autonomy, and varying operational contexts. Existing approaches often do not integrate diverse security aspects, from encryption methodologies to anomaly detection mechanisms, into a cohesive, dynamic system (Elsayed & Zulkernine, 2020; M. F. Khan & Abaoud, 2023; Pal & Jadidi, 2021). This highlights the pressing need for an overarching, adaptable security framework that can efficiently manage the complexities inherent to UAV data security. The trend towards dynamic security models, as explored by (N. S. Labib M. R. Brust & Bouvry, 2021; Oubbati, Atiquzzaman, Ahanger, & Ibrahim, 2020; Wang, Yang, Vo, & Nguyen, 2022), represents a significant shift in UAV data security.

The incorporation of a pattern language approach, though relatively nascent in this field, offers a promising avenue for crafting flexible and modular security solutions. This approach, as discussed by (Allioui & Mourdi, 2023; Fuertes, Pérez, & Meza, 2023), is particularly suited for integrating various security components into a unified system that can adapt to the multifaceted challenges of UAV operations. Our research proposes the Adaptive Modular Management System, a cutting-edge solution designed to fortify data security in multi-UAV systems. Drawing from the insights of (Bagaa, Taleb, Bernabe, & Skarmeta, 2020; Rahouti et al., 2022; Restuccia, Meza, & Kastner, 2021), this system is predicated on a pattern language framework, allowing for the dynamic reconfiguration of security modules in response to changing threats and operational demands. This system's inherent flexibility and adaptability are key to enhancing the resilience and operational efficacy of UAVs in diverse security scenarios. The remaining tructure of the paper can be detailed in four sections. In literature survey, we critically examine existing literature in UAV data security. It discusses the evolution from traditional static security systems to more adaptive models, evaluating the contributions and limitations of various methodologies, with references to the work of (Yang, Manias, & Shami, 2021). Then, in the next section we introduce the pattern template, which is the concept and methodology of pattern language in the design of security systems. This section, drawing on the research of (Shaukat, Luo, Varadharajan, Hameed, & Xu, 2020; Yang et al., 2021) explain the structure, components, and relevance of pattern language in crafting adaptable UAV security solutions.

On the next section, we detail the design and operational mechanics of the Adaptive Modular Management System. This section, inspired by (Ming et al., 2023; Romeh & Mirjalili, 2023) elucidate how the proposed pattern specifically addresses the multifaceted challenges inherent in multi-UAV systems. On the last section, we provide a summation of key research findings, discusses the implications of the Adaptive Modular Management

System in the broader context of UAV data security, and outlines potential avenues for future research. This study aims to contribute significantly to the field of UAV data security by presenting a novel, adaptable solution in the form of the Adaptive Modular Management System. By navigating through the complexities and evolving requirements of multi-UAV operations, this approach promises to usher in a new era of resilient, efficient, and adaptable security frameworks, ensuring the safe and effective deployment of UAVs across various domains.

As UAV applications expanded, the limitations of traditional, static security models in UAV systems became increasingly apparent. Research conducted by (Adriaensen, Decré, & Pintelon, 2019; Rugo, Ardagna, & Ioini, 2022) indicated that these models were ill-equipped to cope with the dynamic and variable nature of UAV operational environments. The work from (Huda & Moh, 2022; Okoye, Collins, & Mbah, 2023) further emphasized the need for more flexible and adaptive security frameworks, capable of responding to evolving threat landscapes and operational requirements in real-time. In response to these challenges, the focus of UAV security research shifted towards dynamic and adaptive security models. The work of (A. Khan, Gupta, & Gupta, 2022) proposed the development of security systems capable of real-time adaptation to emerging threats, a significant departure from the static models previously employed. This approach marked a pivotal moment in UAV data security, emphasizing the need for systems that could rapidly adjust their defense mechanisms in response to new information and changing conditions.

The concept of modular security design gained prominence as researchers sought solutions offering greater customization and scalability. The work from (Kotraski, Piljek, Pranjić, Carlo Giorgio Grlj, & Josip Kasać, 2021) introduced the idea of developing security solutions for UAVs using modular components, allowing systems to be tailored to specific operational needs. This modular approach to security design marked a significant step towards developing UAV security systems that were not only robust but also flexible and scalable. Despite advancements in modular and adaptive security systems, the application of software pattern language principles in UAV security remained largely unexplored. Software pattern languages, commonly used in software engineering, provide a structured approach to solving design problems through reusable and adaptable patterns. As explored by (Bakirtzis et al., 2022), these principles offer a methodical framework for designing complex systems with an emphasis on adaptability, reusability, and scalability - key attributes for effective UAV data security systems.

Our research addresses this gap by integrating the principles of software pattern language into the design of an Adaptive Modular Management System for UAV data security. Building on this foundation, our study extends the application of software pattern language into UAV data security, proposing the Adaptive Modular Management System as a novel solution. This system is designed to dynamically configure security modules in response to changing operational contexts and threats, effectively addressing the unique challenges inherent in multi-UAV systems. Our research not only contributes a new perspective to UAV data security but also sets a precedent for the application of software pattern language in this domain.

2. RESEARCH METHOD

The concept of pattern language first emerged in architecture during the 1970s. Christopher Alexander was pivotal in this development, creating a system that effectively organizes and connects design patterns to address complex architectural challenges (Angel & Salingaros, 2022). This groundbreaking approach soon found relevance in software engineering, mirroring benefits such as the promotion of reusable solutions, enhanced cohesiveness, modular construction, and increased adaptability (Mo et al., 2023).Distinct features define pattern language. Primarily, it facilitates the linking of individual design patterns, underscoring their interrelationships and offering guidance for their application

and amalgamation (Axelsson, 2022). This interlinking allows for a systematic and coherent implementation of these patterns. Significantly, pattern language is often customized to specific problem domains or systems, offering a systematic methodology for addressing a range of design issues within those domains (Buckley & Fernandez, 2023). Pattern language also encourages iterative development, allowing software developers to continuously refine their designs as they gain a more profound understanding of the problem domain and its needs (Alami & Krancher, 2022).

In the realm of software engineering, pattern language brings multiple advantages. It provides comprehensive, structured solutions for recurrent software design challenges, covering a wider range of issues in a specific domain compared to individual design patterns (Arnold, 2022). It advocates for modular design, leading to a division of systems into smaller, more manageable units, thus enhancing system maintenance, understanding, modification, and expansion (Waseeb & Vranić, 2023). Another key benefit is the extensibility it offers. Systems built on established pattern languages can more readily adapt to evolving requirements and new functionalities, securing their long-term functionality and progression (Zimmermann, Stocker, Lubke, Zdun, & Pautasso, 2022). Pattern language also plays a crucial role in improving communication among developers by establishing a common terminological framework, thus facilitating effective collaboration and knowledge sharing (Romero & Fernandez, 2023). The Pattern Template proposed in (Thapa, Fernandez, Cardei, & Larrondo-Petrie, 2023) outlines a structured approach for defining and interpreting a design pattern, each aspect of which is thoroughly delineated.

3. RESULTS AND DISCUSSIONS

3.1. Intent

The intent of this pattern is to guarantee data protection in multi-UAV systems through the implementation of flexible security measures and modular design approaches. Such a strategy ensures versatility and the ability to adapt in various operational environments.

3.2. Example

Consider a scenario where a group of UAVs is deployed to oversee forest fire surveillance over an extensive geographical region. This operation may involve several UAVs, each outfitted with diverse sensors to detect temperature fluctuations, observe fire progression, and monitor wildlife movements for safety. Upon deployment, these UAVs begin collecting and transmitting significant volumes of crucial data. Each UAV gathers sensor data, relaying it to a central control center and possibly to other UAVs too. This data encompasses details about the fire's expansion, current environmental conditions, and other essential factors. The collected information is crucial for informed decision-making, response coordination, and, if needed, evacuation planning.

However, this data, crucial for forest fire management, might also attract ill-intentioned entities. Hostile parties could seek to access this data for their gain or disrupt operations by tampering with the data or UAV systems. For example, they could engage in GPS spoofing attacks, disrupting the UAVs' navigational systems, causing them to veer off course or even collide. They might also intercept data transmission to access crucial fire information unlawfully. In extreme cases, a Denial of Service (DoS) attack on the central command center could be executed, halting the entire operation. In such scenarios, the Adaptive Modular Management pattern becomes crucial. This pattern is designed to maintain data integrity, confidentiality, and availability by enabling the flexible, dynamic configuration of security modules based on the operational context and identified threats.

3.3. Context

Multi-UAV systems are utilized in a range of scenarios and settings, each presenting distinct operational demands and obstacles. These systems, comprising multiple

autonomous or semi-autonomous drones, serve in various capacities such as environmental surveillance, disaster response, search and rescue missions, agricultural assessments, infrastructure inspections, and beyond. In all these use cases, the UAVs collect and process an extensive amount of information through their onboard sensors. This data is often shared between the UAVs and a central control center, aiding in decision making and action coordination. For example, in search and rescue missions, the UAVs' data about terrain, weather, and potential survivor sightings can significantly support the rescue operations.

Nevertheless, the data gathered and transmitted in these scenarios can be extremely sensitive. In military surveillance, for example, the data may include critical details like troop movements or strategic locations, posing a severe risk if compromised. In infrastructure inspections, the data might expose vulnerabilities in essential systems, attractive targets for malicious entities. Additionally, the environments in which multi-UAV systems operate can be dynamic and sometimes hostile. The UAVs may need to function under challenging conditions such as poor connectivity, extreme weather, or threats of cyber-attacks and electronic warfare.

3.4. Problem

Securing data in multi-UAV systems is fraught with numerous challenges, detailed as follows:

1. Ensuring Data Integrity: It's vital that data gathered and circulated by UAVs remains unaltered during transmission and storage. There's a persistent threat of data corruption, whether due to system malfunctions or deliberate sabotage. Adversaries may seek to manipulate the data, distorting its accuracy to disrupt system functionality.
2. Maintaining Data Confidentiality: Given the often-sensitive nature of data in UAV operations, it becomes a target for espionage and other malicious endeavors. There's a risk of data interception during transmission or unauthorized access to stored data, making it critical to restrict data access to only authorized users.
3. Guaranteeing Data Availability: Timely data access is essential in multi-UAV systems for coordinated actions and informed decision-making. Denial-of-service attacks, aimed at overwhelming or interrupting the system, can render data inaccessible at crucial moments, potentially leading to severe consequences.

3.5. Solution

The Adaptive Modular Management pattern provides a tailored solution for addressing the data security challenges in multi-UAV systems. Central to this approach is its emphasis on flexibility and adaptability, achieved by dynamically adjusting security modules based on the current operational scenario and evolving threat landscape.

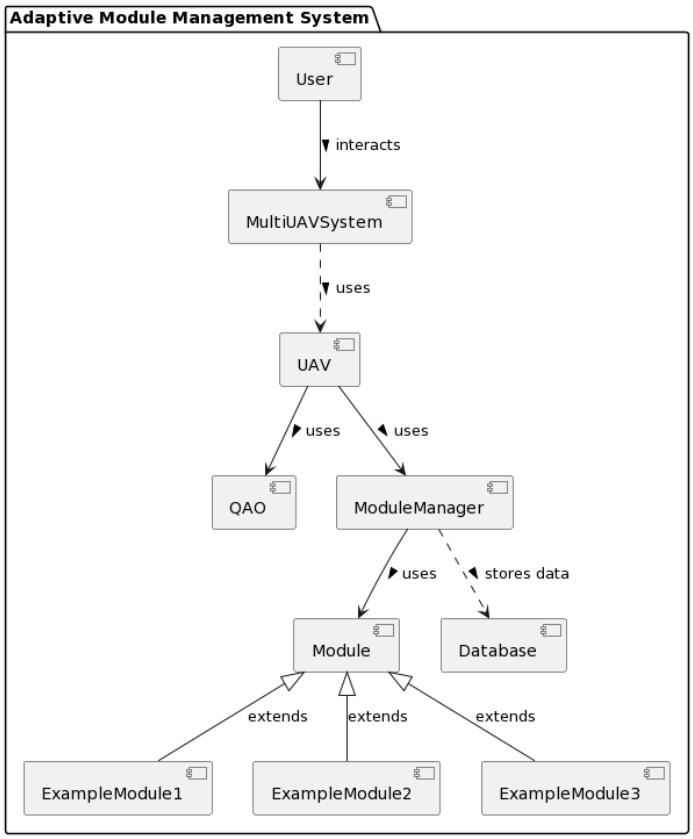

Figure 1. Adaptive Modular Management System

3.6. Structure

The Adaptive Modular Management pattern, designed for multi-UAV systems, comprises several key components: Module, QAO (Quality Attribute Optimization), ModuleManager, UAV (Unmanned Aerial Vehicle), and MultiUAVSystem. To elucidate the architecture of this pattern, we provide sequence and class diagrams. The class diagram details the structure of the Adaptive Module Management pattern within the code. It gives an intricate view of the various classes, their roles, and how they interact within the system. The UAV class symbolizes an individual UAV and acts as the system's core unit. Each UAV is equipped with a QAO instance and a ModuleManager instance. The QAO class is critical for decision-making, analyzing module performance metrics, setting priorities, and flagging problems.

It employs methods like set_initial_configurations_and_priorities() and update_configurations_and_priorities() for optimizing module configurations using exponential smoothing based on problem flags.

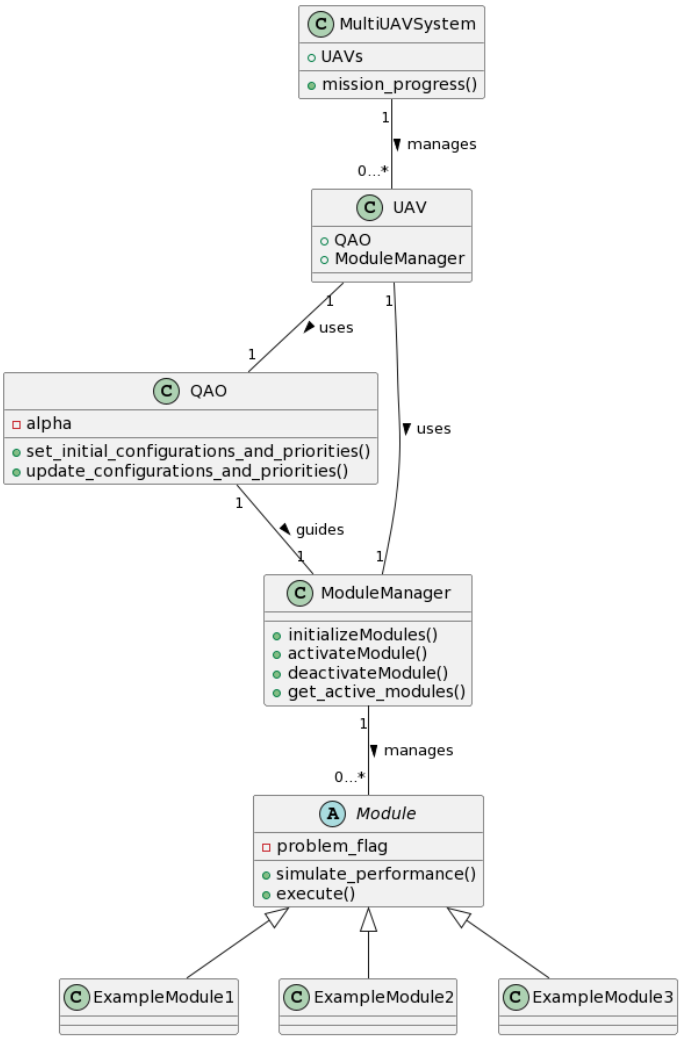

Figure 2. Class Diagram of Adaptive Modular Pattern

The ModuleManager class is pivotal in overseeing the lifecycle of the Module instances and their subclasses. It initializes modules and manages their activation or deactivation according to the QAO class's decisions. Its get_active_modules() method helps identify which modules are in use, ensuring the UAV functions correctly during its mission. The Module class serves as a base for various module types, such as ExampleModule1, ExampleModule2, and ExampleModule3. These subclasses implement specific behaviors through methods like simulate_performance() and execute(), allowing them to simulate performance, execute tasks, and spot potential issues. They each have a problem_flag attribute to signal any issues to the QAO class.

The MultiUAVSystem class manages a group of UAVs, orchestrating their collective mission progress. It coordinates UAV actions using the mission_progress() method, relying on QAO and ModuleManager to manage modules effectively. This class also enables UAVs to exchange performance data and issues, enhancing the system's adaptability. The relationships among these classes are essential for the Adaptive Module Management pattern's functionality. The UAV class relies on the QAO for optimization and the ModuleManager for module handling. This interplay allows the system to adjust to varying conditions and optimize module performance.In real-time operations, the QAO updates module configurations and priorities based on performance metrics and problem instances.

Its alpha parameter influences the exponential smoothing of these metrics, balancing recent and historical data. The ModuleManager adjusts modules as directed by the QAO. UAVs within the system share their performance and problem data, facilitating adaptive management across the network.

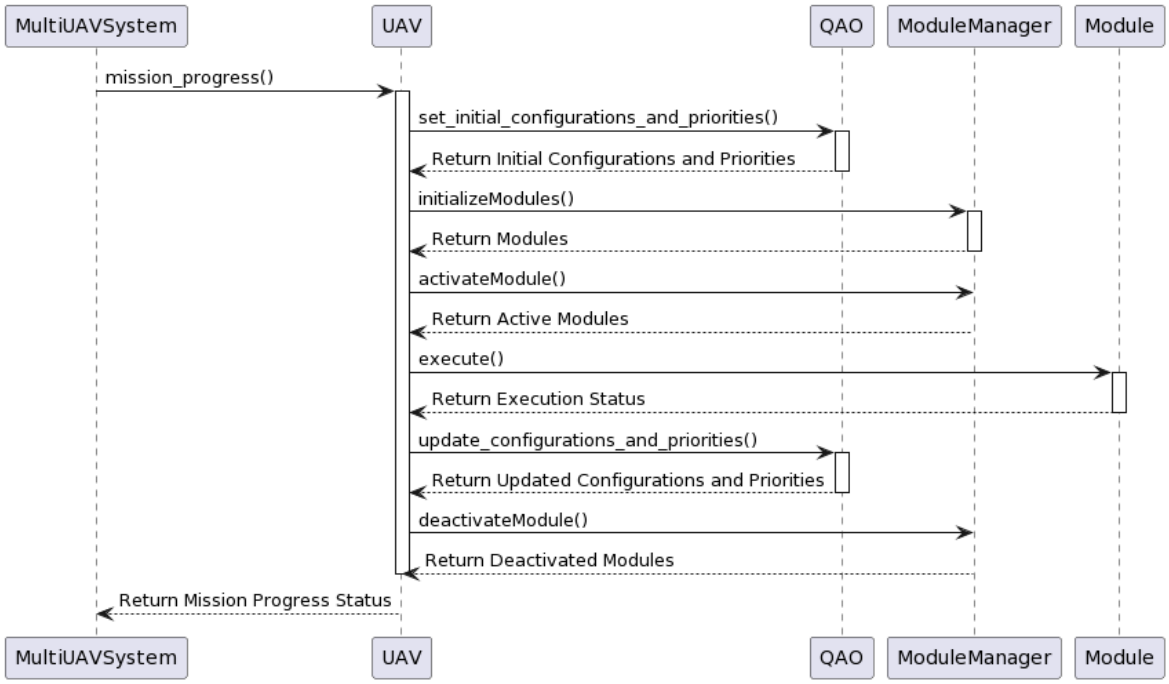

Figure 3. Sequence Diagram of Adaptive Modular Pattern

The sequence diagram illustrates the dynamic interactions in the Adaptive Module Management pattern, emphasizing module monitoring, adaptation, and execution during missions. The process starts with the UAV sourcing performance data and problem reports from the QAO. The QAO gathers and processes this data from each module, recalculates performance averages, and revises priorities to adapt effectively to current conditions. Following priority updates, the QAO revises module configurations, which the Module Manager then uses to activate or deactivate modules as necessary. This flexible approach allows the system to efficiently allocate resources and prioritize tasks. The UAV, informed of active modules, executes each in sequence, ensuring task completion in a prioritized manner. Additionally, UAVs may share their performance and problem data with other UAVs, enhancing coordination and overall system adaptability. The sequence diagram captures the dynamic processes integral to the Adaptive Module Management pattern, showcasing how it enables a multi-UAV system to adapt to mission changes and optimize resource use.

3.7. Dynamics

At the commencement of its operations, the "UAV" actor initiates the "Initialize Configurations and Priorities" use case. This stage involves setting the initial configurations and priorities for the UAV's modules, considering any pre-established parameters or settings. This step creates a foundational operational state for the modules and sets the stage for quality attribute optimization. Following this, the "UAV" undertakes the "Initialize Modules" task. Here, the UAV, through its Module Manager component, readies each module for subsequent use, equipping them for potential activation or deactivation. The subsequent step involves the "Activate Module" use case, where the UAV activates

necessary modules. This activation is pivotal, enabling the system to carry out specific functionalities associated with each module.

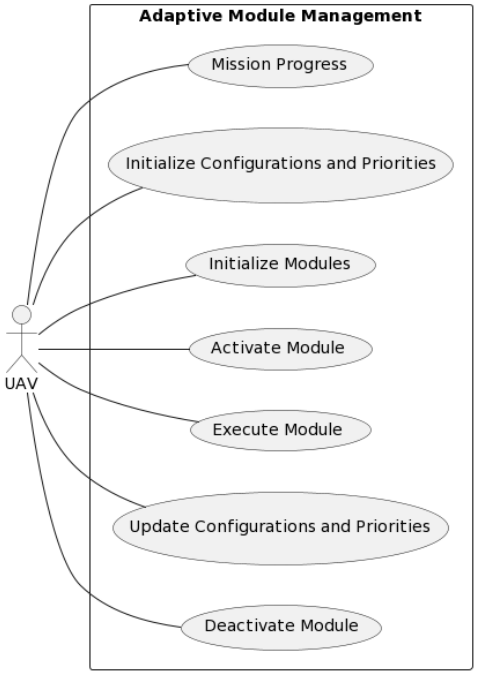

Figure 4. Use Case Diagram of Adaptive Modular Pattern

After activating the required modules, the "UAV" actor progresses to the "Execute Module" use case. During this phase, the UAV operates the active modules, each performing its designated functions, which might range from gathering data to executing complex computations. Post execution, the UAV engages in "Update Configurations and Priorities." In this phase, the QAO component comes into action, adjusting the modules' configurations and priorities based on performance data and any identified problems. This adjustment aims to enhance system performance and adapt to any emerging challenges.

3.8. Implementation

The deployment of the adaptive modular management pattern in multi-UAV systems necessitates a methodical approach, considering various elements of the system and its operational context. Here are some key guidelines:

1. Comprehending System Requirements: The initial step is to thoroughly understand the unique requirements and constraints of the multi-UAV system. This includes identifying the nature of data handled by UAVs, its sensitivity level, the specific operational environment, potential security threats, and other unique operational needs. This comprehension is vital for designing and implementing the adaptive security modules effectively.
2. Developing Security Modules: At the heart of the adaptive modular management pattern are the security modules. These modules, which encompass data encryption, access control, and intrusion detection functions, must be designed to be both adaptable and efficient. Adaptability allows for responsiveness to varying conditions, while efficiency ensures minimal impact on system performance and energy use.
3. Implementing the QAO Component: The Quality Attribute Optimization (QAO) component is integral to the system. It evaluates module performance and issues influencing the management of these modules. This component facilitates informed

decision-making regarding the activation or deactivation of security modules, based on performance metrics and the prevailing security landscape.

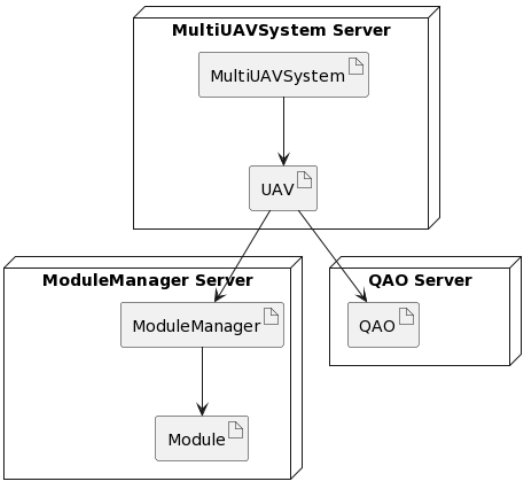

Figure 5. UAV Deployment Diagram

3.9. Known Uses

The Adaptive Modular Management pattern for data security (Bouhamed, Bouachir, Aloqaily, & Ridhawi, 2021; Kumar & Jain, 2021), with its focus on adaptable and modular security measures, has been successfully implemented in various sectors utilizing multi-UAV systems, underscoring its practicality and value:

1. Military Surveillance: In military contexts, where UAVs are crucial for reconnaissance, the sensitive data acquired necessitates stringent security. The adaptive nature of this pattern, capable of responding to fluctuating threat levels and operational needs, aligns well with the often volatile and unpredictable military environments(Hildmann & Kovacs, 2019).
2. Border Control Operations: UAVs play a growing role in border surveillance, tasked with monitoring and securing national frontiers. In such applications, the Adaptive Modular Management pattern ensures the protection of critical data, such as imagery and locational details, from unauthorized access or manipulation. This is vital for upholding the integrity and security of national border operations(Bassoli, Sacchi, Granelli, & Ashkenazi, 2019).
3. Disaster Response and Management: In the realm of disaster management, where multi-UAV systems are employed for damage evaluation, search and rescue, and coordination of relief efforts, the security of sensitive data is paramount. This pattern has been utilized in these scenarios to guarantee the data's security, integrity, and accessibility, even amidst challenging and rapidly evolving situations (A. Khan et al., 2022).
4. Various Multi-UAV Applications: Beyond these specific domains, the Adaptive Modular Management pattern has demonstrated its effectiveness in a range of other multi-UAV operations. These include environmental monitoring, infrastructure examination, and agricultural surveys. In each of these applications, the pattern has proven its efficacy in safeguarding against data breaches and maintaining data integrity and availability (Yaacoub, Noura, Salman, & Chehab, 2020).

3.10. Consequences

Adopting the Adaptive Modular Management pattern in multi-UAV systems for data security offers several benefits but also presents certain challenges that need to be managed:

1. Enhanced Data Security: The foremost benefit of this pattern lies in its substantial improvement of data security. Through its adaptive security measures and modular framework, it effectively safeguards sensitive data and upholds the integrity of the system. This contributes to a reduced likelihood of data breaches and unauthorized information access.
2. Adaptability: The pattern's adaptable nature allows the system to adapt promptly and efficiently to evolving threat landscapes and operational requirements, enabling rapid responses to emerging threats or changes in the environment.
3. Counteracting GPS Spoofing: GPS spoofing poses a major risk to UAV systems. The pattern bolsters the system's resilience to such threats by identifying them and shifting to alternative navigation systems as necessary, thereby mitigating the impact of GPS spoofing on the system's operations.

3.11. Related Patterns

Within the framework of the Adaptive Modular Management pattern for ensuring data security in multi-UAV systems, various auxiliary patterns serve as integral components of the larger system. These complementary patterns encompass distinct adaptive security mechanisms within the overarching structure.

1. Anomaly Detection Patterns: These patterns play a key role in recognizing abnormal or suspicious activities in the system. They can be applied to different facets of the multi-UAV system, such as communication behaviors, UAV operational patterns, and data transfers. Detection of anomalies prompts the system to initiate suitable security responses, which may include heightened encryption, restricted data sharing, or notifications to system operators (Yaacoub et al., 2020).
2. Encryption Patterns: Vital for maintaining the confidentiality and integrity of transmitted data in the system, encryption patterns vary in method and security level, depending on the data type and required protection degree. The overarching management pattern's adaptive quality enables the flexible selection and modification of encryption techniques, tailored to current security threats and system needs(Tan, Wang, Liu, & Zhang, 2020).
3. Access Control Patterns: These patterns focus on guaranteeing that only verified entities have access to the UAVs' collected and shared data. Access control may be determined by several criteria, including the accessing entity's role, the data's sensitivity, and the prevailing operational circumstances. The adaptive modular management pattern is capable of modifying access control strategies in response to shifts in either system dynamics or the threat environment(M. Mahdi Azari, Giovanni Geraci, Adrian Garcia-Rodriguez, 2020).

These associated patterns are not isolated entities but rather critical elements of the comprehensive adaptive modular management pattern. They function collaboratively, each enhancing the other, to forge a flexible and robust data security framework for multi-UAV systems. Their capacity for adaptive adjustment in the face of changing operational scenarios and evolving threats significantly bolsters the system’s resilience against a wide range of security challenges.

4. CONCLUSION

Our investigation into the current state of UAV data security revealed a pivotal shift towards more dynamic and adaptive security approaches. The integration of modular designs in security systems has emerged as a promising development, offering customizable and scalable solutions. However, the application of software pattern language principles in the realm of UAV data security remains an underexplored area. This gap presented a unique opportunity for innovation, leading to the development of our proposed Adaptive Modular Management System Design. This design, grounded in the principles of software pattern language, represents a novel approach in UAV data security. By

combining the adaptability, flexibility, and modular construction inherent in pattern languages with the practical requirements of UAV operations, our system offers a comprehensive, scalable, and dynamic solution to data security challenges. The Adaptive Modular Management System is designed to dynamically configure security modules in response to changing operational contexts and emerging threats, thereby enhancing the resilience and efficacy of UAVs in diverse security scenarios. Therefore, our research contributes an advancement in the field of UAV data security. By bridging the gap between traditional security models and the dynamic needs of modern UAV operations, the Adaptive Modular Management System sets a new benchmark in the domain. This innovative approach not only addresses the current challenges in UAV data security but also paves the way for future research and development in this rapidly evolving field.

REFERENCES

Adriaensen, Decré, & Pintelon. (2019). Can Complexity-Thinking Methods Contribute to Improving Occupational Safety in Industry 4.0? A Review of Safety Analysis Methods and Their Concepts. *Safety*, *5*(4), 65. https://doi.org/10.3390/safety5040065

Alami, A., & Krancher, O. (2022). How Scrum adds value to achieving software quality? *Empirical Software Engineering*, *27*(7), 165. https://doi.org/10.1007/s10664-022-10208-4

Allioui, H., & Mourdi, Y. (2023). Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey. *Sensors*, *23*(19), 8015. https://doi.org/10.3390/s23198015

Angel, S., & Salingaros, N. A. (2022). Christopher Alexander's Architectural Insights and Limitations. *New Design Ideas*, *6*(3), 386–401. https://doi.org/N/A

Arnold, I. (2022). *Enterprise Architecture Function: A Pattern Language for Planning, Design and Execution*. https://doi.org/N/A

Axelsson, J. (2022). Systems-of-Systems Design Patterns: A Systematic Literature Review and Synthesis. *2022 17th Annual System of Systems Engineering Conference (SOSE)*, 171–176. https://doi.org/10.1109/SOSE55472.2022.9812681

Bagaa, M., Taleb, T., Bernabe, J. B., & Skarmeta, A. (2020). A Machine Learning Security Framework for IoT Systems. *IEEE Access*, *8*, 114066–114077. https://doi.org/10.1109/ACCESS.2020.2996214

Bakirtzis, G., Sherburne, T., Adams, S., Horowitz, B. M., Beling, P. A., & Fleming, C. H. (2022). An ontological metamodel for cyber-physical system safety, security, and resilience coengineering. *Software and Systems Modeling*, *21*(1), 113–137. https://doi.org/10.1007/s10270-021-00892-z

Bassoli, R., Sacchi, C., Granelli, F., & Ashkenazi, I. (2019). A Virtualized Border Control System based on UAVs: Design and Energy Efficiency Considerations. *2019 IEEE Aerospace Conference*, 1–11. https://doi.org/10.1109/AERO.2019.8742142

Bouhamed, O., Bouachir, O., Aloqaily, M., & Ridhawi, I. A. (2021). Lightweight IDS For UAV Networks: A Periodic Deep Reinforcement Learning-based Approach. *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 1032–1037. https://doi.org/N/A

Buckley, I., & Fernandez, E. B. (2023). Dependability Patterns: A Survey. *Computers*, *12*(10), 214. https://doi.org/10.3390/computers12100214

Elsayed, M. A., & Zulkernine, M. (2020). PredictDeep: Security Analytics as a Service for Anomaly Detection and Prediction. *IEEE Access*, *8*, 45184–45197. https://doi.org/10.1109/ACCESS.2020.2977325

et al., A. F. (2019). Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges. *IEEE Communications Surveys & Tutorials*, *21*(4), 3417–3442. https://doi.org/10.1109/COMST.2019.2906228

Fuertes, A. B., Pérez, M., & Meza, J. (2023). Transpiler-Based Architecture Design Model for Back-End Layers in Software Development. *Applied Sciences*, *13*(20), 11371. https://doi.org/10.3390/app132011371

Goldfarb, A., & Lindsay, J. R. (2022). Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War. *International Security*, *46*(3), 7–50.

Hassler, S. C., & Baysal-Gurel, F. (2019). Unmanned Aircraft System (UAS) Technology and Applications in Agriculture. *Agronomy*, *9*(10), 618. https://doi.org/10.3390/agronomy9100618

Hildmann, H., & Kovacs, E. (2019). Review: Using Unmanned Aerial Vehicles (UAVs) as Mobile Sensing

Platforms (MSPs) for Disaster Response, Civil Security and Public Safety. *Drones*, *3*(3), 59. https://doi.org/10.3390/drones3030059

Huda, S. M. A., & Moh, S. (2022). Survey on computation offloading in UAV-Enabled mobile edge computing. *Journal of Network and Computer Applications*, *201*, 103341. https://doi.org/N/A

K.-Y. Tsao T. Girdler, & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, *133*, 102894.

Khan, A., Gupta, S., & Gupta, S. K. (2022). Emerging UAV technology for disaster detection, mitigation, response, and preparedness. *Journal of Field Robotics*, *39*(6), 905–955. https://doi.org/N/A

Khan, M. F., & Abaoud, M. (2023). Blockchain-Integrated Security for Real-Time Patient Monitoring in the Internet of Medical Things Using Federated Learning. *IEEE Access*, *11*, 117826–117850. https://doi.org/10.1109/ACCESS.2023.3326155

Kotraski, D., Piljek, P., Pranjić, M., Carlo Giorgio Grlj, & Josip Kasać. (2021). A Modular Multirotor Unmanned Aerial Vehicle Design Approach for Development of an Engineering Education Platform. *Sensors*, *21*(8), 2737. https://doi.org/10.3390/s21082737

Kumar, A., & Jain, S. (2021). Drone-Based Monitoring and Redirecting System. In R. Krishnamurthi, A. Nayyar, & A. E. Hassanien (Eds.), *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead* (pp. 163–183). https://doi.org/10.1007/978-3-030-63339-4_6

M. Mahdi Azari, Giovanni Geraci, Adrian Garcia-Rodriguez, S. P. (2020). UAV-to-UAV Communications in Cellular Networks. *IEEE Transactions on Wireless Communications*, *19*(9), 6130–6144. https://doi.org/10.1109/TWC.2020.3000303

Ming, R., Jiang, R., Luo, H., Lai, T., Guo, E., & Zhou, Z. (2023). Comparative Analysis of Different UAV Swarm Control Methods on Unmanned Farms. *Agronomy*, *13*(10), 2499. https://doi.org/10.3390/agronomy13102499

Mo, F., Querejeta, M. U., Hellewell, J., Rehman, H. U., Rezabal, M. I., Chaplin, J. C., … Ratchev, S. (2023). PLC orchestration automation to enhance human–machine integration in adaptive manufacturing systems. *Journal of Manufacturing Systems*, *71*, 172–187. https://doi.org/10.1016/j.jmsy.2023.07.015

N. Mohamed J. Al-Jaroodi, I. J. A. I., & Mohammed, F. (2020). Unmanned aerial vehicles applications in future smart cities. *Technological Forecasting and Social Change*, *153*. https://doi.org/10.1016/j.techfore.2020.119293

N. Neshenko E. Bou-Harb, J. C. G. K., & Ghani, N. (2019). Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. *IEEE Communications Surveys & Tutorials*, *21*(3), 2702–2733. https://doi.org/10.1109/COMST.2019.2910750

N. S. Labib M. R. Brust, G. D., & Bouvry, P. (2021). The Rise of Drones in Internet of Things: A Survey on the Evolution, Prospects and Challenges of Unmanned Aerial Vehicles. *IEEE Access*, *9*, 115466–115487. https://doi.org/10.1109/ACCESS.2021.3104963

Okoye, C., Collins, O. C., & Mbah, G. C. E. (2023). Mathematical approach to the analysis of terrorism dynamics. In J. T. Omenma, I. E. Onyishi, & A.-M. Okolie (Eds.), *Ten Years of Boko Haram in Nigeria: The Dynamics and Counterinsurgency Challenges* (pp. 95–106). https://doi.org/N/A

Oubbati, O. S., Atiquzzaman, M., Ahanger, T. A., & Ibrahim, A. (2020). Softwarization of UAV Networks: A Survey of Applications and Future Trends. *IEEE Access*, *8*, 98073–98125. https://doi.org/10.1109/ACCESS.2020.2994494

Pal, S., & Jadidi, Z. (2021). Analysis of Security Issues and Countermeasures for the Industrial Internet of Things. *Applied Sciences*, *11*(20), 9393. https://doi.org/10.3390/app11209393

R. Zhang L. Cao, Y. L. R. G. J. L., & Shu, P. (2023). Decoding Spontaneous Informal Spaces in Old Residential Communities: A Drone and Space Syntax Perspective. *ISPRS International Journal of Geo-Information*, *12*(11), 452. https://doi.org/10.3390/ijgi12110452

Rahouti, M., Xiong, K., Xin, Y., Jagatheesaperumal, S. K., Ayyash, M., & Shaheed, M. (2022). SDN Security Review: Threat Taxonomy, Implications, and Open Challenges. *IEEE Access*, *10*, 45820–45854. https://doi.org/10.1109/ACCESS.2022.3168972

Restuccia, F., Meza, A., & Kastner, R. (2021). Aker: A Design and Verification Framework for Safe and Secure SoC Access Control. *2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, 1–9. https://doi.org/10.1109/ICCAD51958.2021.9643538

Romeh, A. El, & Mirjalili, S. (2023). Theoretical Framework and Practical Considerations for Achieving

Superior Multi-Robot Exploration: Hybrid Cheetah Optimization with Intelligent Initial Configurations. *Mathematics*, *11*(20), 4239. https://doi.org/10.3390/math11204239

Romero, V. M., & Fernandez, E. B. (2023). Towards a Reference Architecture for Cargo Ports. *Future Internet*, *15*(4), Art. no. 139. https://doi.org/10.3390/fi15040139

Rugo, A., Ardagna, C. A., & Ioini, N. E. (2022). A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis. *ACM Computing Surveys (CSUR)*, *55*(1), 21. https://doi.org/N/A

S. A. H. Mohsan M. A. Khan, F. N. I. U., & Alsharif, M. H. (2022). Towards the Unmanned Aerial Vehicles (UAVs): A Comprehensive Review. *Drones*, *6*(6), 147. https://doi.org/10.3390/drones6060147

S. A. H. Mohsan N. Q. H. Othman, Y. L. M. H. A., & Khan, M. A. (2023). Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends. *Intelligent Service Robotics*, *16*(1), 109–137.

Shakeri, R., Al-Garadi, M. A., Badawy, A., Mohamed, A., Khattab, T., Al-Ali, A. K., … Guizani, M. (2019). Design Challenges of Multi-UAV Systems in Cyber-Physical Applications: A Comprehensive Survey and Future Directions. *IEEE Communications Surveys and Tutorials*, *21*(4), 3340–3385. https://doi.org/10.1109/COMST.2019.2924143

Shakhatreh, H., Sawalmeh, A. H., Al-Fuqaha, A., Dou, Z., Almaita, E., Khalil, I., … Guizani, M. (2019). Unmanned Aerial Vehicles (UAVs): A Survey on Civil Applications and Key Research Challenges. *IEEE Access*, *7*, 48572–48634. https://doi.org/10.1109/ACCESS.2019.2909530

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access*, *8*, 222310–222354. https://doi.org/10.1109/ACCESS.2020.3041951

Tan, Y., Wang, J., Liu, J., & Zhang, Y. (2020). Unmanned Systems Security: Models, Challenges, and Future Directions. *IEEE Network*, *34*(4), 291–297. https://doi.org/10.1109/MNET.001.1900546

Thapa, B., Fernandez, E. B., Cardei, I., & Larrondo-Petrie, M. M. (2023). Abstract Entity Patterns for Sensors and Actuators. *Computers*, *12*, Art. no. 93. https://doi.org/N/A

Thibbotuwawa Bocewicz, Z., & Nielsen. (2019). A Solution Approach for UAV Fleet Mission Planning in Changing Weather Conditions. *Applied Sciences*, *9*(19), 3972. https://doi.org/10.3390/app9193972

Wang, C.-N., Yang, F.-C., Vo, N. T. M., & Nguyen, V. T. T. (2022). Wireless Communications for Data Security: Efficiency Assessment of Cybersecurity Industry—A Promising Application for UAVs. *Drones*, *6*(11), 363. https://doi.org/10.3390/drones6110363

Waseeb, S., & Vranić, V. (2023). Toward Organizational Pattern Ontology. *Proc. of the 27th European Conference on Pattern Languages of Programs (EuroPLop '22)*, Art. no. 20. https://doi.org/10.1145/3551902.3551983

Yaacoub, J.-P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, *11*. https://doi.org/10.1016/j.iot.2020.100218

Yang, L., Manias, D. M., & Shami, A. (2021). PWPAE: An Ensemble Framework for Concept Drift Adaptation in IoT Data Streams. *2021 IEEE Global Communications Conference (GLOBECOM)*, 1–6. https://doi.org/10.1109/GLOBECOM46510.2021.9685338

Zimmermann, O., Stocker, M., Lubke, D., Zdun, U., & Pautasso, C. (2022). *Patterns for API Design: Simplifying Integration with Loosely Coupled Message Exchanges*.