8-2024

ENHANCING CYBERSECURITY FOR UNMANNED SYSTEMS: A COMPREHENSIVE LITERATURE REVIEW

Jonathan Gabriel Mardoyan
California State University – San Bernardino

ENHANCING CYBERSECURITY FOR UNMANNED SYSTEMS: A COMPREHENSIVE LITERATURE REVIEW

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology:

Cybersecurity

---

by

Jonathan Gabriel Mardoyan

August 2024

ENHANCING CYBERSECURITY FOR UNMANNED SYSTEMS: A COMPREHENSIVE LITERATURE REVIEW

A Project

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Jonathan Gabriel Mardoyan

August 2024

Approved by:

Vincent Nestler PhD, Committee Member, Co-Chair

Conrad Shayo PhD, Committee Member, Co-Chair, & Chair, Information and Decision Sciences Department

ABSTRACT

This culminating experience project addresses the pressing cybersecurity challenges encountered by unmanned autonomous vehicles. The research provides a comprehensive literature review on how hybrid encryption techniques can improve the security of its communication systems. The chosen research questions guiding this study are: (Q1) How can we enhance cybersecurity measures to safeguard the communication and transmission of sensitive data from unmanned systems, thereby preventing unauthorized access by malicious actors? (Q2) How can we ensure the confidentiality and integrity of messages exchanged with unmanned systems to a command-and-control center operating on the tactical edge? (Q3) How can hybrid encryption tackle the consumption problem of substantial processing power required for encrypting and transmitting data in unmanned systems?

The findings are: Q1. hybrid security strategy ensures strong communication integrity and safeguards against malicious interception in operations involving unmanned systems; Q2. lightweight cryptographic algorithms and hybrid encryption methods specifically designed for unmanned systems efficiently protect both the confidentiality and integrity of messages while optimizing computational resources; Q3. when using hybrid encryption, unmanned systems can effectively manage power consumption while

maintaining robust data security protocols. The conclusions are: Q1. combining symmetric encryption for efficient data handling with asymmetric encryption for secure key exchange significantly enhances data confidentiality, integrity, and overall security. Q2. end-to-end encryption, secure key management, and authenticated encryption mechanisms within a hybrid encryption framework reduce risks associated with interception, tampering, and unauthorized access via unmanned systems. Q3. Integrating efficient algorithm selection, optimized key management, resource-aware encryption, and dynamic key generation methods, can address power consumption concerns. Future research directions should include deeper exploration of hybrid encryption practices within unmanned systems to advance understanding in the realm of communication systems for autonomous vehicles.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

Brief Overview

Autonomous unmanned systems have surfaced as essential assets across a vast spectrum of operations. Such operations include unmanned civilian or military air, ground, sea, and space systems. The use of these systems can vary widely between various fields and are used in different areas of industry from civil, commercial, to military operations (Zhou & Gheisari, 2018). Examples range from information gathering, surveillance, to operational uses (Laghari et al., 2023). Through the various functions and utilizations from different industries, the emergence of cybersecurity challenges becomes evident, as an increasing demand for further research is requested to develop proper defense and cybersecurity enhancement technologies (Niyonsaba et al., 2023).

One of the primary security concerns held in the realm of operations for autonomous unmanned systems is the vulnerability of its communication standard (Laghari et al., 2023). This is a substantial issue as communication with control stations, satellites and other intended devices need to remain seamless and secure with its transmissions. Common vulnerabilities found on these systems include but reach far beyond only data breaches; examples for various attacks would be surveillance, control, and other attacks (Döş et al., 2023). When

using traditional communication practices, data is not only susceptible to being intercepted, but can also be tampered with, and/or exploited by malicious actors. This is important to remember, as there is a huge reliance on an unmanned system's wireless communication technologies to be able to receive sensitive data needed for sensor readings, navigational information, and mission-critical commands (Islam et al., 2021). Previous researchers have shed light on the need for robust security to be looked at, by analyzing and discussing trends of known risks and vulnerabilities. As other research has stated, the need for these systems to have a robust and strong encryption mechanism for communications becomes paramount, as assurance of the confidentiality, integrity, and authenticity of transmitted data is heavily relied upon (Tan et al., 2020).

Critical for reducing these risks is the application of a robust encryption mechanism that can protect its confidentiality and integrity for communications against interception and mitigation (Niyonsaba et al., 2023). As traditional methodologies involving symmetric and asymmetric encryption offer viable solutions– each encryption method has its own limitations when applied (Zhang, 2023). For example, symmetric encryption has advantages in its high efficiency and low computational overhead but struggles with challenges when faced with distribution of keys in dynamic constrained and low resource availability environments (Zhang, 2023). On the other hand, asymmetric encryption offers effective key distribution techniques, secure key exchanges, and more robust

security, but oftentimes incurs significant computational overheads as well as impracticality when encrypting large volumes of data (Barker, 2020).

In response to the challenges previously stated, the application of hybrid encryption emerges as a strong candidate by combining strengths from both symmetric and asymmetric encryption techniques (Zhang, 2023). This security approach allows symmetric encryption to be leveraged for its high efficiency regarding data transmission and the security of asymmetric encryption for the secure key exchange process (Barker et al., 2018). Hybrid encryption mitigates known risks to communication vulnerabilities posed by unauthorized threat actors with the addition of strengthening the traditionally used encryption approaches of an unmanned system (Döş et al., 2023). This research endeavors to provide insights into the effectiveness, usage, and practical implications of deploying hybrid encryption solutions in real-world autonomous unmanned systems environments. The focus of this research aims to further investigate the critical role of securing communications by implementing hybrid encryption on autonomous unmanned systems.

Problem Statement

The main objective of this culminating experience project is to address the security challenges associated with insecure communications on autonomous unmanned systems and to provide explanations for questions relating to securing

transmissions with a hybrid security approach. Previous research showed there is a need to study the security challenges associated with insecure communications.

The project will seek to answer the following questions:

1. How can we enhance the security measures to safeguard the communication and transmission of sensitive data from unmanned systems, thereby preventing interception or unauthorized access by malicious actors? (Döş et al., 2023)
2. How can we ensure the confidentiality and integrity of messages exchanged with unmanned systems to a command-and-control center operating on the tactical edge? (Shafik et al., 2023)
3. How can hybrid encryption tackle the consumption problem of substantial processing power required for encrypting and transmitting data in unmanned systems? (Laghari et al., 2023)

This culminating experience project is structured and organized as follows: Chapter 1 introduces the culminating project, chapter 2 provides a literature review, chapter 3 covers the research methods used to answer the research questions, chapter 4 is analysis and findings, and chapter 5 is a discussion of the results, conclusions, and recommendations for future research.

CHAPTER TWO

LITERATURE REVIEW

A few academic studies have researched the importance of cybersecurity practices being implemented on unmanned systems; Döş et al. (2023), Rani et al. (2016), Sanghavi & Kaur (2023), Niyonsaba et al. (2023), Tan et al. (2020), Mohsan et al. (2023), Aissaoui en et al. (2023). This literature review outlines the origins of the three research questions, derived from the suggested areas for further study.

Question 1: How can we enhance the security measures to safeguard the communication and transmission of sensitive data from unmanned systems, thereby preventing interception or unauthorized access by malicious actors? (Döş et al., 2023)

With unmanned systems renowned for their practical use in real-world scenarios, several academic studies have highlighted the lack of cybersecurity practices in communications and transmissions of sensitive data from these systems. Notable studies by Tan et al. (2020), Rani et al. (2016), Sanghavi & Kaur (2023), Mohsan et al. (2023), Shafik et al. (2023), and Niyonsaba et al. (2023) underscore this issue. The researchers often discuss the lack of

cybersecurity practices for these systems, emphasizing the potential for exploitation due to these vulnerabilities through communications via threat actors. For example, in an article by Rani et al. (2016), the author mentions the wide range of tasks unmanned systems can perform, the severe consequences of these systems being hacked, and potential ways to protect them from such attacks. To further solidify this point, the authors conducted a controlled experiment in which a drone was hacked using different widely available open-source tools with the point to showcase the extreme lack of security against cyber threats. Subsequently, the authors demonstrated the extreme lack of security against cyber threats. This experiment reinforced the need for robust security measures by showing the ease of exploitation of unmanned systems. The authors recommended stronger encryption and put more emphasis on protection of communications through unmanned systems (Rani et al.,2016).

Similarly, the article by Tan et al. (2020) presents a comprehensive security analysis for unmanned systems across different layers–physical, communication, and application–addressing the wide range of attack types and countermeasures within a two-dimensional security model. This model follows by identifying and discussing the existing security challenges in unmanned system security, to set the stage for future research directions in this area. The discussion goes into depth describing how this model can be used to analyze technical attacks and potential threats across various unmanned system platforms. This includes but is not limited to, the broad application of this model

within different fields such as military, medical, commercial, and agriculture, with their associated risks in mind. The authors conclude their discussions on future challenges by mentioning future research directions regarding secure privacy and data protection.

In the article by Sanghavi & Kaur (2023), the authors propose a comprehensive study to enhance the overall security posture of unmanned systems in the various fields. They examine cybersecurity threats in communications with unmanned systems, detailing the components, vulnerabilities, and strategies to defend against different types of attacks. A proposed roadmap focuses on identifying and mitigating potential cyber risks, conducted on unmanned system security. Furthermore, highlighting the susceptibility of these systems with examples of different cyber-attacks, that can ultimately lead toward data theft, hijacking, and lastly incapacitation of the system. To circumvent the exploitation of these risks, hardening strategies are discussed to fortify the systems against attackers, mentioning the use of more robust encryption protocols as one solution to communication and sensor-based GPS, which are primary targets for attacks.

As the importance of securing communication channels is highly discussed, this point later in the discussion alludes to the general overarching problem of needing to improve cybersecurity practices to prevent recurrent attacks (such as eavesdropping, hijacking, and jamming). In support of this, the previously mentioned article by Mohsan et al. (2023), explicitly addresses the

significant concerns of security issues related to unmanned systems by also highlighting the susceptibility of drones to cyber-attacks (examples including hijacking, denial-of-service attacks, and GPS spoofing). The author acknowledges the current lack of robust countermeasures to prevent such security breaches, stressing the need for further research and development in unmanned system security to mitigate these vulnerabilities. Areas of further research recommended by Moshan et al. suggest more power efficient and secure algorithms to be used for encryption processes. As this was made a point for further research, my studies will explore stronger more power efficient method of encryption for unmanned systems.

Laghari et al. (2023) emphasizes the rising level of security attacks and the high risks of transmitting sensitive data open to potential threats. The author suggests for future research that these areas should be investigated; stronger encryption, implementation of intrusion detection systems (IDSs), and defense against DoS attacks, as areas of further studies. As the focus of my study is on securing communications, with stronger encryption being mentioned, Laghari et al. (2023) highlights the effectiveness this can have in the case of securing information and how better regulation over proper communication security would ultimately protect the privacy for these systems. Mentioned are the various attacks that have similarly been discussed by the previous authors, such as GPS spoofing, communication jamming, and man-in-the-middle attacks, and highlight the need for better communication security regulations. This is further supported

by Mekdad et al. (2023), as the author's article surveys the security and privacy issues of unmanned systems, classifying them into hardware, software, and communication levels. They discuss the lack of protection against various attacks due to manufacturers prioritizing efficiency over security. The authors conclude with stressing the importance of collaboration between military and commercial sectors to develop security frameworks for communications with unmanned system communications.

As commercial use is primarily discussed by the previous authors, the article from Mohsan et al. (2023) discusses the emergence of unmanned systems in similar contributions to society– by mentioning uses in leisure, economic, military, and academic purposes as well. In this article, the susceptibility of these systems to vulnerabilities is mentioned as the authors talk about the ways unmanned systems in these different environments are susceptible to being exploited by common attacks. The range of exploitation is given as examples of the following: interception, hijacking, DoS attacks, and spoofing. With that being said, the authors raise the concern of there not being enough involvement promoting the importance of security on these unmanned systems in response to these kinds of attacks– which ultimately raises concerns as unmanned systems are expanding into many different areas.

Throughout these discussions, all authors consistently emphasize the importance of enhancing security practices for unmanned systems, addressing data security and privacy assurance in communications. This is made a point as

similar problems between the contributing authors arise, having to do with data security and privacy assurance for communications (Islam et al. 2021). The questions that I've produced are a result of these areas recommended by numerous authors for further study.

Question 2: How can we ensure the confidentiality and integrity of messages exchanged with unmanned systems to a command-and-control center operating on the tactical edge? (Shafik et al., 2023)

With unmanned systems playing a crucial role in mission-critical operations, several academic studies have emphasized the importance of ensuring the confidentiality and integrity of messages exchanged with command-and-control centers operating on the tactical edge. Notable studies by Döş et al. (2023), Niyonsaba et al. (2023), Zhang (2023), Mekdad et al. (2023), and Aissaoui et al. (2023) underscore this issue.

The article by Niyonsaba et al (2023), explores foundational cybersecurity principles to build more robust security enhancements for unmanned systems. They highlight the CIA triad (Confidentiality, Integrity, and Availability) as essential for strengthening security across physical, application, and communication layers. Enforcing these three principles can strengthen security especially when applied amongst the three critical attack layers: physical, application, and communication (Niyonsaba et al., 2023).

The CIA triad serves as a foundation for conceptualizing cybersecurity practices; (Shafik et al., 2023) however, there is no standardized framework for applying secure safeguards across its three layers within unmanned systems (Döş et al., 2023). With no standards being set forth, security on unmanned systems isn't generally enforced due to the varying difference and requirements needed from one system to the other (Mohsan et al., 2023). As a result, this creates inconsistency for implementing security standards, although they may not be universally applicable.

In the article by Niyonsaba et al. (2023), the paper further surveys cybersecurity in unmanned systems, by proposing an analysis of cyber-attacks and examining defense techniques with confidentiality, integrity, and availability in mind. They emphasize the rising cyber-attack risks associated with the increasing use of drones, which threaten operations and sensitive data. The risks mentioned include data theft, loss of drones, and disruption of performance. The existence of communication risks highlights the urgency of implementing enhanced security measures, as exploitation/manipulation of data jeopardizes both confidentiality and integrity, resulting in significant consequences. Advanced defense techniques are suggested by the author and looked at to enhance unmanned systems security, some of which include introducing concepts such as machine learning, while others aim to improve existing system operations such as the improvement of cryptographic techniques in wireless communications.

Reviewing these studies highlights the recurring concern for ensuring data security and privacy. With the general highlighted point being the lack of cybersecurity on unmanned systems, while following the CIA triad, analysis of possible beneficial encryption methods can be looked at for improvement with data communications. The literature consistently points to the lack of cybersecurity in unmanned systems and suggests hybrid encryption technologies as a potential solution for addressing confidentiality and integrity issues (Zhang, 2023; Döş et al., 2023; Mekdad et al., 2023).

In the article by Zhang (2023), the author discusses a hybrid security approach tailored for encrypting communications. This approach combines symmetric and asymmetric encryption to leverage the efficiency of symmetric encryption for large data volumes and the security of asymmetric encryption for key protection. Hybrid encryption effectively addresses the vulnerabilities of each method, enhancing information transmission precision and protecting user data. In doing so, it effectively addresses the vulnerabilities inherent in each encryption method and takes advantage of the benefits. The author further emphasizes that employing hybrid encryption algorithms in the physical layer software control notably enhances the precision of information transmission while proficiently averting the loss of critical user data. Highlighting the pivotal role of hybrid encryption technology in cyber security, ensuring communication security and protecting the interests of both communicating parties by mitigating the limitations of standalone symmetric and asymmetric encryption algorithms. In

further studies, the author proposes the application of hybrid encryption in different possible applications including security with software

In the article by Döş et al. (2023), the authors discuss a hybrid security approach for unmanned systems that integrates software, physical, and communication security elements. The author underscores the importance of integrating cybersecurity measures, hardware features, and electronic warfare elements to create a collegial relationship. This approach aims to improve operational effectiveness by addressing system vulnerabilities and threats across multiple fronts, including cyber-attacks, electronic jammers, and unauthorized data access.

The article by Aissaoui et al. (2023), examines the integration of hybrid encryption to enhance secure communications in unmanned systems. The study underscores the importance of hybrid encryption, particularly within the Transport Layer Security (TLS) protocol, facilitating authenticated key exchange over a public communication channel using algorithms such as the Elliptic Curve Diffie-Hellman (ECDHE). Furthermore, the study emphasizes the necessity for a comprehensive security architecture that incorporates hybrid encryption, especially in the context of unmanned system traffic management, for the significance of confidentiality and integrity in communications with external systems. Highlighting the crucial role of hybrid encryption in establishing a secure communication channel.

The literature discussed in this question examines the critical challenges and solutions related to ensuring the confidentiality and integrity of communications between unmanned systems and command-and-control centers operating in tactical environments. It highlights the absence of robust security standards and explores the vulnerabilities and threats associated with insecure communications and data compromise.

Question 3: How can hybrid encryption tackle the consumption problem of substantial processing power required for encrypting and transmitting data in unmanned systems? (Laghari et al., 2023)

The literature discussed in this question delves into the challenge of high-power consumption associated with encrypting and transmitting data in unmanned systems, exploring various themes concerning the optimization of computational resources through hybrid encryption methodologies. Notable studies by Shafik et al. (2023), Aissaoui et al. (2023), Laghari et al. (2023).

The article by Shafik et al. (2023) discusses the significance of system security and integrity amidst the rapid advancements in unmanned vehicle technology. The article highlights the vulnerabilities these systems face due to their limited computing resources and the wide range of evolving threats and techniques they must contend with.

Aissaoui et al. (2023) delves into the integration of hybrid encryption to enhance secure communications in unmanned systems. The authors discuss how hybrid encryption can mitigate computational and bandwidth limitations inherent in these systems. By combining symmetric and asymmetric encryption, hybrid methods leverage the strengths of both approaches—ensuring efficient data handling and secure key exchanges without overwhelming the system's computational resources.

Laghari et al. (2023) review the constraints of using lightweight operations in unmanned systems, particularly focusing on the trade-offs between performance parameters, mission requirements, strategic credibility, and the limitations of onboard power availability with communication capabilities. The authors address the challenges of balancing power for communications during missions against the power requirements for data transmission. They also discuss various attacks, such as GPS spoofing, communication jamming, and man-in-the-middle attacks, which underscore the need for robust encryption solutions.

Overall, these articles collectively highlight that while unmanned systems face significant constraints in terms of computational power and energy resources, hybrid encryption emerges as a promising solution. By optimizing encryption processes, hybrid methods can ensure secure data transmission while conserving critical system resources, thereby maintaining the operational efficiency of unmanned systems.

CHAPTER THREE

RESEARCH METHODS

This study explores hypothetical scenarios within unmanned systems, as several researchers (Aissaoui et al., 2023; Yaacoub, 2024; Alzahrani, 2023; Tan et al., 2020; Moshan et al., 2023) have highlighted the need for future research in enhancing security, particularly the development of more efficient and secure encryption methods. While significant research has been conducted on enhancing the security of unmanned systems through various encryption methods, the specific hypothetical implementation of hybrid encryption as proposed in this study has not been previously explored. This approach allows for a deeper understanding of the complex issues involved, paving the way for more effective solutions.

Table #1. Database Search and Relevant Articles Selected

Database Searched	**Search Words**	**Number of Relevant Articles found**	**Number of Articles Selected**	**Article Authors**
doi	Unmanned systems security	12	2	Tan et al. (2020), Mohsan et al. (2023),
doi	Hybrid encryption	4	1	Zhang (2023)

doi	Unmanned systems encryption	8	3	Mekdad et al. (2023), Laghari et al. (2023), Niyonsaba et al. (2023)
doi	Hybrid encryption on unmanned systems	3	2	Döş et al. (2023), Aissaoui en et al. (2023)
doi	Cybersecurity on unmanned systems	7	3	Rani et al. (2016), Sanghavi & Kaur (2023), Niyonsaba et al. (2023)
ieeexplore	Unmanned systems	9	3	Zhou & Gheisari (2018), Afghah et al. (2019), Islam et al. (2021

Question 1: How can we enhance the security measures to safeguard the communication and transmission of sensitive data from unmanned systems, thereby preventing interception or unauthorized access by malicious actors? (Döş et al., 2023)

To answer this question, utilizing various types of research methods will help in guiding and exploring the topic of securing communications and preventing unauthorized access via unmanned systems. As the article by Aissaoui en et al. (2023) provides the first discussion on implementing hybrid encryption via unmanned systems, a thorough research review is essential to identify current strategies, challenges, and gaps unique to cybersecurity in unmanned systems with conducted research (Mekdad et al., 2023). With this, the

examination of research conducted, provided by various research articles in different areas, helps with providing invaluable insights from different authors about vulnerabilities and weaknesses within existing security frameworks. While finding research studies of the specific implementation of hybrid encryption in the manner I propose has not been previously explored. One article involves an experiment conducted by Alzahrani et al. (2023) that examines the effectiveness of homomorphic encryption in a simulated environment with unmanned systems. This experiment uses the Aerial Vehicle Network Simulator (AVENS) on OMNET++ (an event simulation software) to evaluate the overall impact of applying this encryption method and its ability to protect data transmissions from various attacks. This helps to give a more general analysis of common issues relayed between unmanned systems to see an overall trend with the analysis of past incidents.

Moreover, researching technical assessments involving penetration testing and vulnerability analyses are crucial. This will aid in identifying trends for potential weaknesses in communication protocols, encryption methods, and system configurations between different authors. The weaknesses highlighted and pointed out by the authors offer opportunities to evaluate the effectiveness of various security measures in assessing and mitigating exploits found from common cyberattacks. The various articles will be part of the literature review where other scholars address how we can enhance security measures to

safeguard the communication and transmission of sensitive data from unmanned systems and then identifying areas for further study.

This is significant because in such discussions, policy analysis becomes challenging as there are no secure and established standards in place, given the absence of a centralized security framework for these systems. However, researching the different applications of security via commercial partners, government agencies, and academia, help to gather intelligence and resource-sharing between various studies, thus enabling a broad understanding of potential cybersecurity techniques that can be applied to most unmanned systems. The integration of multiple research methods enables a comprehensive analysis, leading to conclusive findings.

Question 2: How can we ensure the confidentiality and integrity of messages exchanged with unmanned systems to a command-and-control center operating on the tactical edge? (Shafik et al., 2023)

To answer this question, examined research will be conducted to explore potential solutions for ensuring the confidentiality and integrity of messages exchanged with unmanned systems operating on the tactical edge. While following previous analysis methods from question one, similar research methods will be applied to answering question two. Additionally, conducting a research analysis of various encryption techniques, such as hybrid encryption,

homomorphic encryption, or quantum encryption, can be explored to fulfill the need for securing the confidentiality of messages exchanged between unmanned systems and the command-and-control center in our specific created use case scenario. As authors have stressed the need to improve security through communications, a comprehensive literature review with hybrid encryption applications is conducted to assess vulnerabilities and effectiveness in ensuring the confidentiality and integrity of exchanged messages on unmanned systems. This will involve investigating existing secure communication protocols such as transport layer security (TLS) with established communication channels between unmanned systems and command-and-control centers. Within these communication channels, analyzing the message flows between unmanned systems and command-and-control centers will assist with identifying potential security vulnerabilities. By employing a combination of these research methods, a robust cybersecurity framework can be established to guarantee the confidentiality and integrity of messages exchanged between unmanned systems and the command-and-control center operating on the tactical edge.

Question 3: How can hybrid encryption tackle the consumption problem of substantial processing power required for encrypting and transmitting data in unmanned systems? (Laghari et al., 2023)

Likewise, to the first and second question, a variety of research methods will be employed. Similarly, following the process of conducting a literature review on hybrid encryption techniques and their application in unmanned systems will assist in providing insights through both theoretical foundations and practical implementations. Doing this and analyzing existing real-world examples where hybrid encryption has been employed in unmanned systems will help to assess results in reducing processing power consumption while ensuring data security. The examination of a real-world simulation by Yaacoub et al. (2024) will be explored, where the authors test the process of utilizing multiple iterations of hybrid encryption processing. This study employs MATLAB to evaluate the computational effort and time required for encryption in unmanned systems during autonomous deliveries. Designing and conducting virtual experiments additionally can allow for the evaluation of hybrid encryption algorithms' performance in unmanned systems across various scenarios, this will allow for the analysis of measuring processing power consumption and data encryption/transmission efficiency. By integrating these research methods, a comprehensive understanding of how hybrid encryption can address the consumption problem of substantial processing power in unmanned systems, as discussed by Aissaoui et al. (2023), can be achieved.

CHAPTER FOUR

DATA ANALYSIS AND FINDINGS

This chapter describes the data analysis and provides the findings to the previously asked questions. The data analyzed in this chapter consists of a collection of published articles and documents discussing cybersecurity and encryption in unmanned systems. This study provides a comprehensive literature review of the application of hybrid encryption mechanisms specifically designed to meet the distinct needs and limitations of unmanned systems. The primary aim of this chapter is to provide an explanation to the three research questions:

Question 1: How can we enhance the security measures to safeguard the communication and transmission of sensitive data from unmanned systems, thereby preventing interception or unauthorized access by malicious actors? (Döş et al., 2023)

The use of hybrid encryption presents an effective security approach to enhancing communications and transmissions of sensitive data and effectively preventing malicious actors from interception or unauthorized access via unmanned systems. (Zhang, 2023). In providing a secure means of communication for transmissions from an unmanned system, it is crucial to use a

versatile solution that is both secure and lightweight. (Mohsan et al., 2023) Hybrid encryption would meet this purpose by combining the strengths of both symmetric and asymmetric encryption to cater to the security needs of unmanned systems. (Aissaoui et al., 2023)

Symmetric encryption plays a pivotal role as the primary encryption method for user-requested data in unmanned systems. (Niyonsaba et al., 2023) Leveraging the use of symmetric encryption algorithms in constrained parameters for unmanned systems offers speed and efficiency, making them ideal for handling and encrypting bulk data without significantly increasing file sizes. (Zhang, 2023) Being well-suited for scenarios involving large volumes of data, the use of symmetric encryption algorithms ensures minimal time and power consumption upon request. (Niyonsaba et al., 2023) This approach enables the system to promptly generate symmetric encryption for requested data upon contact, securely encapsulating the data into a secure optimal file size that is to be expected in transmissions. (Aissaoui et al., 2023) The key advantage of symmetric encryption in this case is to act as the first layer of encryption, while simultaneously capsizing the data load for transmission to meet an unmanned system's low demand for processing power, where managing large data volumes efficiently and quickly is critical. (Aissaoui et al., 2023) This is important as to recognize the crucial importance of unmanned system capabilities prior to deployment, this method ensures operational stability without the need for significant adjustments during active service. This simplicity and efficiency make

symmetric encryption a preferred choice for extensive data handling, including unmanned systems, where managing large data volumes efficiently is crucial. (Niyonsaba et al., 2023)

Hybrid encryption algorithms seamlessly merge the efficiency of symmetric encryption with the secure key exchange capabilities of asymmetric encryption. (Zhang, 2023) Asymmetric encryption follows as the session key is used for the communication session and an added second layer of protection. Even before deployment, this communication session is pre-established between the unmanned system and command-and-control center. In this streamlined process, asymmetric encryption keys are generated beforehand, and the corresponding keys are allocated to the designated parties. This strategic approach enables a secure key exchange, where the public key can be freely distributed for decryption by its intended recipients, while the private key remains securely stored on the Trusted Platform Module of the unmanned system. (Döş et al., 2023) Here, the sender (unmanned system) holds the public key for encrypting the communication session, while the receiver (command-and-control center) possesses the private key for decrypting the encrypted session upon retrieval.

This personalized key allocation ensures robust integrity and confidentiality throughout the communication process. (Zhang, 2023) Moreover, data encryption involves using a symmetric key, further encrypted with the recipient's public key. This dual-layer encryption ensures that only the recipient's

private key can decrypt the symmetric key, fortifying both the key exchange process and the data itself. (Aissaoui et al., 2023) This makes it so that potential hijacking attempts are thwarted, preventing threat actors from deciphering captured payloads without the requisite private key.

While significant research has been conducted on enhancing the security of unmanned systems through various encryption methods, the specific implementation of hybrid encryption combining both asymmetric and symmetric encryption techniques in the manner I propose has not been previously explored. Existing experiments, such as the one by Alzahrani et al. (2023), have primarily focused on homomorphic encryption or other individual encryption methods. However, they have not addressed the unique combination of hybrid encryption that leverages the strengths of both asymmetric and symmetric encryption methods to optimize security and performance in unmanned systems. My approach aims to fill this gap by introducing a novel hybrid encryption framework tailored to the specific requirements and constraints of unmanned systems, ensuring enhanced protection of sensitive data transmissions against interception and unauthorized access.

By leveraging the efficient data transmission and processing swiftness of symmetric encryption, along with the secure key exchange and authentication of asymmetric encryption, this approach guarantees robust communication integrity and prevents malicious actors from interception of the transmitted data. (Zhang, 2023)

Hybrid encryption leverages Transport Layer Security (TLS) as a crucial component of their encryption mechanisms, using its capability to integrate various cryptographic techniques, including both symmetric and asymmetric encryption methods to fortify security. (Aissaoui. 2023) In the scenario for an unmanned system, TLS facilitates the negotiation of a session key between a client and server using asymmetric encryption within the handshake process. Subsequently, symmetric encryption is employed for the bulk of data transmission due to its efficiency. (Zhang, 2023) TLS, renowned as a standard protocol for securing network communications, seamlessly integrates into the application of hybrid security techniques to ensure the confidentiality, integrity, and authenticity of data transmissions. (Aissaoui et al., 2023) Its use is justified by its robust authenticated key exchange mechanisms, included in techniques like Diffie-Hellman Ephemeral (DHE), Elliptic Curve Diffie-Hellman Ephemeral (ECDHE), and RSA. This highlights the adaptability of the protocol and underscores the significance of selecting an appropriate algorithm to streamline workload via key exchange mechanisms. The key exchange process involves symmetric and asymmetric encryption methods to securely transmit keys between parties, ensuring that only the intended recipient can decrypt the transmitted data. (Zhang, 2023) The symmetric keys in this case will be ephemeral, as they can be ever changing due to the circumstance of only the asymmetric keys having to be static, for successful retrieval of requested data. (Aissaoui et al., 2023) The key distribution process entails bundling the

ephemeral session key, encrypted data derived from that ephemeral key, and wrapping them together under the pre-established public key for transmission as a single payload. (Zhang, 2023) This payload is transmitted and only the recipient that possesses the corresponding private key can decrypt the payload and obtain the ephemeral key to retrieve the requested data. Thus, implementing a robust authentication mechanism to prevent interception and unauthorized access by malicious threat actors.

Question 2: How can we ensure the confidentiality and integrity of messages exchanged with unmanned systems to a command-and-control center operating on the tactical edge? (Shafik et al., 2023)

Ensuring the confidentiality and integrity of messages exchanged with unmanned systems to a command-and-control center operating on the tactical edge requires robust encryption techniques. Given the dynamic and potentially hostile environments in which unmanned systems operate, employing advanced encryption mechanisms becomes significant when sustaining secure communications (Rani et al., 2016). In achieving this goal, several key factors are important to address for implementing robust encryption in unmanned systems; end-to-end encryption, secure key management, and authenticated encryption.

To achieve this objective, deploying customized lightweight cryptographic algorithms, coupled with hybrid encryption tailored for unmanned systems, can

effectively safeguard message confidentiality and integrity while efficiently managing the system's limited computational resources. (Aissaoui et al., 2023) Despite their unmatched efficiency and versatility, unmanned systems face significant security risks due to vulnerabilities in data transmission. (Mekdad et al., 2023) It's essential to prioritize the secure retrieval process of data in transit to maintain the security of end-to-end encryption when implementing this encryption approach. The hybrid encryption process should incorporate asymmetric encryption to safeguard data integrity along the entire transmission path, extending from the established communication channel between unmanned systems and the command-and-control center. (Mekdad et al., 2023) This tunnel created between the unmanned system and command-and-control center drastically mitigates the threat of interception or unauthorized access by malicious entities, guaranteeing that intercepted data remains unintelligible. (Laghari et al., 2023) Furthermore, the integrity of the data remains uncompromised, as this end-to-end encryption prevents unauthorized access to the content of messages exchanged with the unmanned system. This approach ensures confidentiality and integrity by restricting decryption and requesting data access solely to authorized users. (Rani et al., 2016)

Regarding key management with authorized users, implementing robust practices on unmanned systems prior to deployment is crucial to securely generate, distribute, and store encryption keys. (Zhang, 2023) Initially, establishing a secure channel for key exchange between the command-and-

control center and unmanned systems is paramount, achieved through asymmetric encryption techniques like RSA or Elliptic Curve Cryptography (ECC). (Zhang, 2023) Before deployment, the command-and-control center generates a key pair and shares its public key with unmanned systems for encryption, stored on a trusted platform module. Adhering to secure asymmetric algorithms meeting NIST standards or regulatory frameworks is essential. (Aissaoui et al., 2023) As this encryption pertains to data transmission, it forms the protective shell for incoming payloads. Ensuring proper key assignment before deployment and managing access to private keys from the command-and-control center is crucial. (Zhang, 2023) For symmetric encryption, unmanned systems dynamically generate new keys for each data request, updating keys regularly to maintain confidentiality and integrity. (Aissaoui et al., 2023) The process involves generating a new key upon request, encrypting the data, packaging the public key with the encrypted data, and encrypting it with the session key as a single payload. During this, symmetric keys are not stored on the system and are disposed of after each use, making it one-time use per request.

Once the determination of the secure key management process is made, using additional methods such as Authenticated Encryption (AE) in symmetric encryption enhances data confidentiality and integrity involving counter models such as GCM (Galois/Counter Mode) or CCM (Counter with CBC-MAC). (Aissaoui et al., 2023) These methods use a counter mode, which generates a

unique value for each block of plaintext, preventing identical blocks from producing the same ciphertext. By incorporating AE, methods like GCM and CCM protect against tampering or unauthorized access by verifying the integrity of the ciphertext. (Aissaoui et al., 2023) Additionally, to secure message integrity, employing cryptographic hash functions or Message Authentication Codes (MACs) along with the encrypted messages can enhance message integrity with an additional layer of verification. Overall, employing authenticated encryption methods with cryptographic hash functions or MACs can significantly bolster the security of transmitted data.

Together, these measures can guarantee the confidentiality and integrity of communications for unmanned systems, thereby mitigating the risks associated with interception, tampering, or unauthorized access to sensitive information.

Question 3: How can hybrid encryption tackle the consumption problem of substantial processing power required for encrypting and transmitting data in unmanned systems? (Laghari et al., 2023)

Hybrid encryption addresses the consumption problem of substantial processing power required for encryption and the transmission of data in unmanned systems. (Aissaoui et al., 2023) As power consumption is critical in unmanned systems, it directly impacts the system's duration of functionality and

operational capabilities within active missions. (Laghari et al., 2023) Especially since these systems rely on battery power for energy purposes and require efficient energy management to extend operational periods. (Mohsan et al., 2023) The substantial energy consumption during data transmission in unmanned systems emphasizes the urgent requirement for energy-efficient communication solutions tailored to unmanned operations. (Islam et al., 2021) Employing different strategies including efficient algorithm selection, optimized key management, resource-aware encryption, and dynamic key generation methods can contribute to establishing robust encryption protocols while mitigating power consumption concerns.

To fulfill the requirements of efficient algorithm selection, hybrid encryption enables symmetric and asymmetric encryption. (Zhang, 2023) While symmetric encryption excels in speed and efficiency for handling large volumes of data, asymmetric encryption is employed for secure key exchange, despite being less frequent but computationally intensive. (Zhang, 2023) This aspect, as previously discussed in question one, has addressed the efficiency aspects of symmetric and asymmetric encryption.

To fulfill the demands of resource-aware encryption, tailored lightweight cryptographic algorithms for unmanned systems can be optimized to ensure secure encryption while efficiently managing limited computational resources, thus optimizing energy consumption. (Aissaoui et al., 2023) Emphasizing lightweight cryptography is pivotal due to its reduced computational complexity

and memory usage, directly translating to lower power consumption. This makes cryptographic measures accessible to devices with stringent power constraints. Hybrid encryption can be tailored to meet the specific needs of unmanned systems without overwhelming their capabilities. (Zhang, 2023) Different symmetric encryption algorithms can be applied on a case-by-case basis, allowing for scalability. (Yaacoub et al., 2024)

One instance of this was in the research conducted by Yaacoub et al. (2024), the focus was on testing multiple iterations using MATLAB to determine the time required for the encryption process. Yaacoub et al. (2024) conducted a test of 1,000 iterations to estimate the time required for encryption using AES. The unmanned systems in this case were simulated to act as autonomous delivery drones. The study found that the processing for key generation and encryption does not pose a computational burden on the system. Depending on the symmetric algorithm used, the encryption process can be scaled to match the system's power requirements. Yaacoub et al. (2024) also noted that the decryption process takes longer than encryption; however, this is not an issue since decryption does not occur on the unmanned system. Additionally, the adoption of lightweight cryptographic algorithms enhances security in constrained unmanned system environments by facilitating efficient and secure communication without straining the system's limited resources (Aissaoui et al., 2023). Notably, the Chacha20 algorithm emerges as a preferred lightweight symmetric encryption choice for IoT, including unmanned systems, owing to its

superior performance compared to AES in terms of energy cost, time efficiency, and memory usage. (Aissaoui et al., 2023) This makes it notably more efficient for applications where power consumption is a critical concern.

To fulfill the necessity of dynamic key generation, systems can dynamically produce new encryption keys, diminishing the risk of compromise and upholding data security while mitigating the computational load. (Aissaoui et al., 2023) As previously addressed in question two, this involves generating ephemeral keys upon request.

By employing these hybrid encryption strategies, unmanned systems can effectively manage the consumption problem of substantial processing power required for encrypting and transmitting data, maintaining security while optimizing resource utilization. (Aissaoui et al., 2023)

CHAPTER FIVE

DISCUSSION, CONCLUSION, AND RECOMMENDATIONS FOR FURTHER RESEARCH

This last chapter will discuss the analysis's findings, provide a conclusion, and areas for further study for each of the three questions.

Question 1: How can we enhance the security measures to safeguard the communication and transmission of sensitive data from unmanned systems, thereby preventing interception or unauthorized access by malicious actors?

In conclusion, the comprehensive literature review conducted in this study has addressed the critical question of enhancing security measures to protect the communication and transmission of sensitive data from unmanned systems against interception or unauthorized access by malicious actors. Through comprehensive exploration, it has been demonstrated that hybrid encryption stands out as a viable solution to this challenge. (Zhang, 2023) The utilization of symmetric encryption ensures efficiency in handling bulk data, while asymmetric encryption facilitates secure key exchange, enhancing overall security. This method not only strengthens the confidentiality and integrity of data but also reduces the chances of interception or unauthorized access. Moving forward, the adoption of hybrid encryption in unmanned systems can significantly strengthen

security protocols, ensuring the protection of sensitive information in dynamic and potentially hostile environments. Further research into the optimization and implementation of hybrid encryption techniques tailored specifically for unmanned systems would be valuable for advancing the field of secure communication in autonomous platforms.

Question 2: How can we ensure the confidentiality and integrity of messages exchanged with unmanned systems to a command-and-control center operating on the tactical edge?

In conclusion, safeguarding the confidentiality and integrity of messages exchanged between unmanned systems and command-and-control centers operating on the tactical edge is paramount to ensuring the security and effectiveness of mission-critical operations. Through an exploration of end-to-end encryption, secure key management, and authenticated encryption mechanisms, it becomes evident that an all-around approach is necessary to address the complex security challenges inherent in such communications. Fundamentally, the combination of end-to-end encryption, robust key management, and authenticated encryption within a hybrid encryption framework provides a comprehensive remedy to aid in safeguarding communications between unmanned systems and command-and-control centers operating at the tactical edge. Within my research, embracing these methodologies enable organizations

to alleviate threats stemming from interception, tampering, and unauthorized access, thus guaranteeing the confidentiality and integrity of critical data exchanges crucial for operations in ever-changing environments.

Question 3: How can hybrid encryption tackle the consumption problem of substantial processing power required for encrypting and transmitting data in unmanned systems? (Laghari et al., 2023)

The utilization of hybrid encryption presents a promising solution to address the challenge of managing the substantial processing power demands inherent in encrypting and transmitting data within unmanned systems. By employing a varied approach utilizing efficient algorithm selection, optimized key management, resource-aware encryption, and dynamic key generation methods, organizations can establish strong encryption protocols while effectively mitigating concerns related to power consumption. This comprehensive strategy not only enhances the security of data transmissions but also ensures the efficient utilization of computational resources, thereby facilitating the operations of unmanned systems in various environments. As technology continues to evolve, further research and development in hybrid encryption methodologies hold the potential to unlock new avenues for optimizing power consumption while maintaining robust security measures in unmanned systems.

REFERENCES

Afghah, F., Razi, A., Chakareski, J., & Ashdown, J. (2019). Wildfire Monitoring in Remote Areas using Autonomous Unmanned Aerial Vehicles. IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 835–840. https://doi.org/10.1109/INFCOMW.2019.8845309

Aissaoui, R., Deneuville, J.-C., Guerber, C., & Pirovano, A. (2023). A survey on cryptographic methods to secure communications for UAV traffic management. Vehicular Communications, 44, 100661.

Alzahrani, M. Y., Khan, N. A., Georgieva, L., Bamahdi, A. M., Abdulkader, O. A., & Alahmadi, A. H. (2023). Protecting Attacks on Unmanned Aerial Vehicles using Homomorphic Encryption. Indonesian Journal of Electrical Engineering and Informatics (IJEEI), 11(1), 88–96. https://doi.org/10.52549/ijeei.v11i1.3932

Döş, O., Karakoca, Y. E., Camadan, E., & Baykali, F. (2023). Hybrid cyber security of unmanned aerial vehicles. International Journal of Applied Methods in Electronics and Computers, 4.

https://doi.org/10.58190/ijamec.2023.65

Islam, N., Rashid, M.M., Pasandideh, F., Ray, B., Moore, S., & Kadel, R. (2021). A Review of Applications and Communication Technologies for Internet of Things (IoT) and Unmanned Aerial Vehicle (UAV) based Sustainable Smart Farming. Sustainability, 13(1821). https://doi.org/10.3390/su13041821

Laghari, A. A., Jumani, A. K., Laghari, R. A., & Nawaz, H. (2023). Unmanned aerial vehicles: A review. Cognitive Robotics, 3(1), 8-22.

Mekdad, Y., Aris, A., Babun, L., Fergougui, A., Conti, M., Lazzeretti, R., & Uluagac, A. S. (2023). A survey on security and privacy issues of UAVs. Computer Networks, 224(109626).

Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., & Khan, M. A. (2023). Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. Intelligent Service Robotics. https://doi.org/10.1007/s11370-022-00452-4

Niyonsaba, S., & Konate, K. (2023). A survey on cybersecurity in unmanned aerial vehicles: Cyberattacks, defense techniques, and future research

directions. International Journal of Computer Networks and Applications (IJCNA), 10(5), September-October. https://doi.org/10.22247/ijcna2023223417.

Rani, C., Modares, H., Sriram, R., Mikulski, D., & Lewis, F. (Year). Security of unmanned aerial vehicle systems against cyber-physical attacks. Journal of Defense Modeling and Simulation: Applications, Methodology, Technology. https://doi.org/10.11771548512915617252.

Sanghavi, P., & Kaur, H.. (2023). A Comprehensive Study on Cyber Security in Unmanned Aerial Vehicles. https://ieeexplore.ieee.org/document/10112549/;jsessionid=3941A71065F42C278A996E1ACDBC8EFDonid=3941A71065F42C278A996E1ACDBC8EFD

Shafik,W.,Mojtaba Matinkhah,S. & Shokoor,F.(2023).Cybersecurity in Unmanned Aerial Vehicles: a Review. International Journal on Smart Sensing and Intelligent Systems,16(1) -. https://doi.org/10.2478/ijssis-2023-0012

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

Yaacoub, E., Abualsaud, K., & Mahmoud, M. (2024). Hybrid Encryption for Securing and Tracking Goods Delivery by Multipurpose Unmanned Aerial Vehicles in Rural Areas Using Cipher Block Chaining and Physical Layer Security. Drones, 8(3), 111. https://doi.org/10.3390/drones8030111

Zhang, J. (2023). Application of hybrid encryption algorithm in physical layer software control. Results in Physics, 51, 106665.

Zhou, S., & Gheisari, M. (2018). Unmanned aerial system applications in construction: A systematic review. Construction Innovation, 18(4), 453–468. https://doi.org/10.1108/CI-02-2018-0010