DOI: 10.15849/IJASCA.241130.03

Int. J. Advance Soft Compu. Appl, Vol. 16, No. 3, November2024
Print ISSN: 2710-1274, Online ISSN: 2074-8523
Copyright © Al-Zaytoonah University of Jordan (ZUJ)

Securing UAV Communications with Homomorphic Encryption and Key Regeneration: A Model Checking Approach

Mohammed Y. Alzahrani

Department of Information Technology, Faculty of Computer Science & Information Technology, AlBaha University, AlBaha, Saudi Arabia
e mail:imohduni@gmail.com

Abstract

Unmanned Aerial Vehicles (UAVs) are at the centre of multiple applications across various fields, including delivery, disaster response, and surveillance. However, its use of wireless communications exposes them to security risks such as information distortion and interception. The paper presents a security model based on Homomorphic Encryption (HE) and Key Regeneration (KR) with the incorporation of Model Checking to enhance UAV communication security. Our system employs homomorphic encryption that resolves the data security problem by ensuring data security at the transmission stage, where information is processed at the receiver end without decryption, thus maintaining privacy and the data processing policy at the UAV end. Furthermore, the key regeneration protocol updates the encryption keys regularly, thus reducing the risk denial window and impact in case of key compromise. The security of the protocols is proven through model checking that establishes the system status operation through a systematic study, as per the provided security requirements. The simulation results indicate certain trade-offs in the system with performance degraded in encryption time and computations, unlike the existing system. The system enhancement outweighs the performance, as indicated by the minimized level of threat and integrity violation. Therefore, integrating HE and KR can secure UAV communication in the presence of a smart and capable adversary, making the entire system robust and dependable in the line of operation.

Keywords: *Cybersecurity; Unmanned Aerial Vehicles; Homomorphic Encryption; Model Checking*

1 Introduction

Unmanned aerial vehicles (UAVs), commonly known as Drones, have revolutionized various sectors, from disaster relief to military operations [1]. On the other hand, the priority of the rapid expansion of the UAV sector is the issue of ensuring security, primarily in its functioning. The vulnerability of UAVs to information-technology hacks, which are widely exploited in attacks relying on wireless communication, cannot be disregarded: to eavesdrop, intercept, or modify information [3]. Based on previous studies, researchers proposed a novel security method for UAVs that utilized homomorphic encryption. Is a progressive cryptographic methodology that allows data to

Received 4 July2024; Accepted 8November 2024

be processed without being decrypted. Due to the fact that the data has been encrypted in this context, even if the hackers obtain the data by some means they are unable to decrypt it because they do not have the appropriate keys [4]. Homomorphic encryption involves changing cryptographic keys used for encryption and decryption in an altering manner. If a UAV using this method is continuously changing the keys, it will be tougher to compromise the system even if the attackers get access to a key [5]. Moreover, to demonstrate the application of our proposed method of protecting UAV commination from UAV to the base station we combine and study the homomorphic encryption along with the key-regeneration to produce a secure solver of the UAV commination. Furthermore, the use of a model-checking technique will ensure the safety features of the proposed approach; model-checking is a formal verification methodology that can assess the completeness and safety of a system by systematically comparing its performance to a list of existing desirable criteria.

The main contribution of this study is to develop and test a reliable UAV communication framework that protects data security while reducing computational and performance overhead. In order to enable UAVs to safely process sensitive data, our goal is to create a homomorphic encryption system that is specially suited for them. The model-checking technique will be used to evaluate the security attributes of the proposed system. This strategy will assist us in detecting possible weaknesses and improving the foundation for safe UAV communication. The results obtained from this study will help advance the broad use of UAVs in crucial applications and improve security.

2 Related Work

One of the major breakthroughs in cryptographic technology is homomorphic encryption which is especially relevant in the context of improving communication security in different technological fields, including Unmanned Aerial Vehicles. Specifically, this method is aimed at enabling secure multiparty computation, meaning processing encrypted data without decrypting it, which ensures that the confidentiality and integrity of information are maintained while in transit between UAVs and the corresponding ground stations [6]. This capacity is vital to ensure operational security in constant exchange-sensitive information environments. Furthermore, employing key generation algorithms based on the concept of homomorphic encryption adds an additional security layer [7]. Essentially, re-introducing encryption keys on a regular basis shortens the time frame during which the system is vulnerable to breaches, thereby ensuring greater overall safety of communication. The flexibility of this method goes beyond UAVs and can be used in other areas, such as personalized recommendation systems and medicine, where data is sensitive and privacy is paramount [8]. Moreover, the flexibility of this method resulted in it being incorporated into a blockchain-based federated learning system that allows for private and secure multiparty using machine learning [9]. Moreover, as an essential element of the Internet of Things, fully homomorphic encryption with optimal key generation is essential to ensure interconnected devices' safety and communication [10]. Additionally, this method is already in application in UAV systems since using homomorphic encryption for secure communication and employing key regeneration algorithms has proved to be successful [11]. This is especially relevant as UAVs become widely used in commercial delivery and military surveillance. In general, this method is especially pertinent to the Next-Generation Communication systems that often involve multiple networks and communicating entities. Aspects such as maintaining the safe transmission of the model updates and ensuring the channel's robustness are instrumental to the systems that depend on real-time data exchange and transformation [12]. Indeed, it can be concluded that homomorphic encryption is not only defending the data in transit but also preserving the privacy of the information, which is crucial for the well-being of the operational process. By introducing key regeneration algorithms and allowing for secure computations among multiple parties, this approach presents a complete framework for protecting the UAV's communication. Overall, the massive incorporation of a new degree of encryption in the UAVs exemplifies a new form of cyber-attack protection. Therefore, such methodologies will prepare the UAVs for new vulnerabilities by staying ahead of emerging threats. As widely adopted in other fields, homomorphic encryption can be viewed as a central method for protecting future communication facilities [6,7,11]. A study conducted by [13] employed a statistical model checking in to evaluate the signal strength and availability of a communication device in the presence of single event upsets.

3 Understanding UAV Communication Systems

Efficient UAV operations and communication are very crucial ranging from survey and surveillance to search and rescue [14]. UAV communications systems send commands to the UAV, allowing the UAV crew to access essential telemetry data. Data communication is vital to UAV operations as it uses different data types, sensor readings, images, video, and mission data. Thus, as part of these two forms of broad connectivity, the UAV systems require an uplink and downlink in relation to every system. An uplink from a ground station or an operator control station to the UAV sends commands, waypoints, and mission specifications. In contrast, the downlink allows the transmission of mission-critical information from the UAV to the ground station, including telemetry data, real-time video transmission, sensor measurements, and other data, including range, accessible frequency bands, and relevant mission requirements, plus a few modifications [15].

The most widely used method for UAV navigation is still radio-frequency (RF) navigation. It uses different frequency bands to create and establish communications networks, including Wi-Fi, specific UAV frequencies, and even cellular networks. Satellite networks are used to configure BLOS (Beyond Line-of-Sight) communications lines in conditions types requiring remote or activities in remote locations possible. However, UAV navigation systems have some challenges, including uninterrupted communication and reliability [16, 17].

4 Attack scenario on UAVs

An attack on UAVs involves intentional activities intended to jeopardize their security, performance, or integrity. Such actions may have a number of motives, such as espionage, terrorism, data theft, operation disruption, or even targeted attacks against certain people or organizations. Fig 1 depicts some of the common attacks on UAVs.

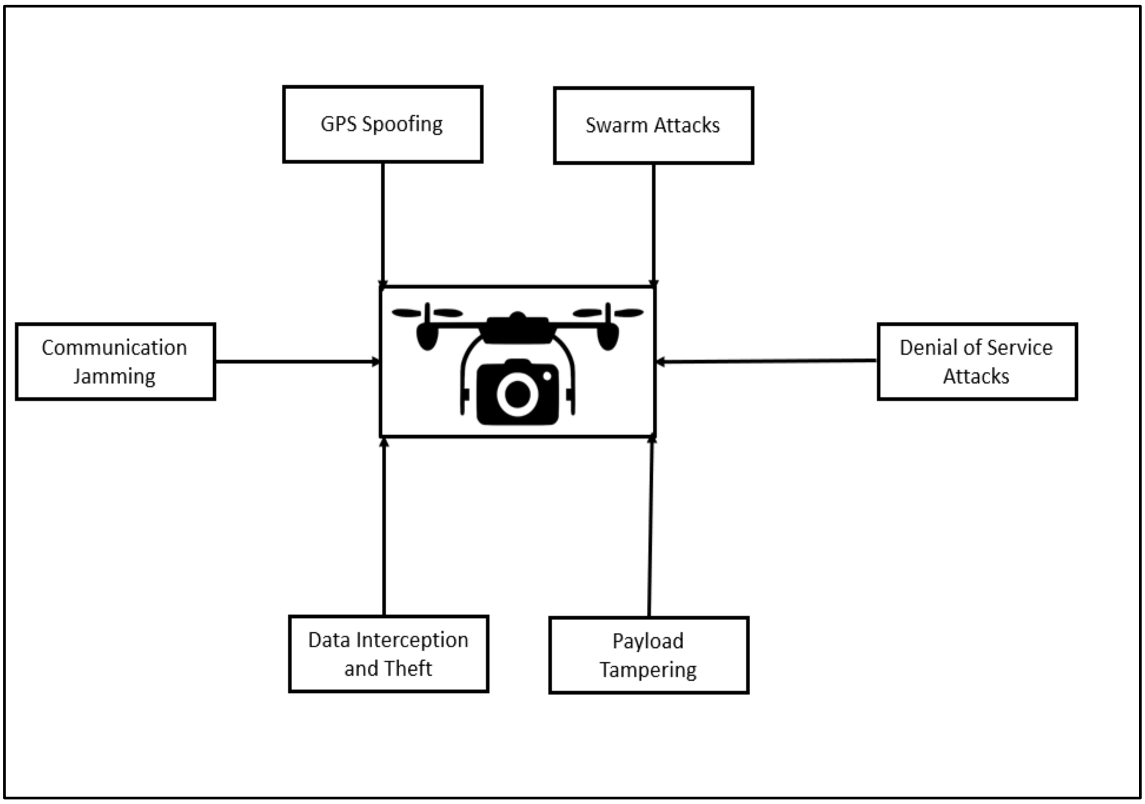

Figure 1: Types of Attacks on UAV’s

4.1 GPS Spoofing

The primary goal of GPS spoofing on UAVs is to trick a GPS receiver by transmitting fake signals. A GPS signal generated by a fake GPS simulator can transmit GPS signals in order to perform spoofing attacks on UAVs. Thus, An anti-spoofing approach is necessary to guarantee UAVs' operational security [18].

4.2 Swarm Attack

Swarm attacks on UAVs are described as a series of coordinated and synchronized attacks by a number of UAVs working together. The swarm attacks multiple UAVs working together and can target a single object or location, overwhelming the defence of a target or causing disruption [19]. The swarm attacks on UAVs have been considered a major concern due to the nightmare of destruction they could cause and the difficulty of combating them. These UAVs operate with exceptional precision and adaptability due to advanced communication and artificial intelligence algorithms, making them a major threat in various areas. Infrastructure and public safety face this new threat, while the military area is concerned about new intelligence collection or attack methods. In addition, the potential for the use of swarm UAVs in an emergency response, such as a search and rescue mission, is still being investigated [20].

4.3 Denial of Service Attacks

A Denial of Service Attack (DoS) attack against a drone would involve sending overwhelming traffic through the wireless link, completely disconnecting the communication from the ground control station to the UAV [21]. If successful, the attack leaves the drone unable to receive any commands or transmit any data to the vicinity of the ground control station. This leads not only to the disruption of the vehicle’s regular operation but also to a security threat since it allows the attacker to get control over the compromised drone.

4.5 Payload Tampering

Payload tampering is another threat that results from unauthorized physical access to a UAV. This involves the threat of making unauthorized adjustments to the data or the devices that a UAV is transporting [22]. Depending on the payload and functions involved, payload tampering may be highly disastrous. While a UAV can be used to carry a camera, sensor, packages, and medical supplies, among other things, there is a potential reason for attackers to compromise the integrity of the payload. Data tampering may involve the use of a weaponized payload to mislead the recipients after the assailants alter the data collected or transmitted by the drone. Hardware tampering can also entail physical adjustments of the UAV's components involving the assailants tampering with the UAV's devices or integration of new malevolent devices. The same case applies to software tampering, which may also involve the installation of malware and harmful software into the UAV system to gain unauthorized access or disrupt the UAV. Interception and replacement, which include substitution, as the attackers intercept the UAV and vitiate the genuine payload with a counterfeit product. The activities may result in the loss of highly sensitive information, dissemination of banned materials, illegal spying, and the eventual destruction of the UAV. Authorization of physical and digital tamper-proof support is required to reduce the threat [23].

4.6 Data Interception and Theft

Data interception and theft on UAVs refer to the unauthorized access and extraction of records collected, transmitted, or stored by UAVs during operations. Interception entirely involves malicious actors that access the record when UAVs communicate to intercept records, including video feeds and sensor logs. Record theft involves extracting valuable data from the records stored in the UAV. Encryption, secure authentication, software updates, and physical security, as well as intrusion detection systems, would help protect against these attacks [24]. Access controls would be required in conjunction with the above measures but would be just as crucial in providing data integrity and confidentiality when operating UAVs. This measure would ensure that only those authorized have the required permissions to access and alter the data collected. With regular audits and monitoring of the data access logs, any unauthorized attempts or breaches could be easily tracked down and remedied [25].

4.7 Communication Jamming

Communication jamming on the UAV purposely interrupts the Wi-Fi signals used in the UAV's communication, disconnecting the UAV and the operator or other devices. This causes the loss of management control, failure of data accessibility, delay in operations, and possible safety hazards [26]. However, the UAVs have superior techniques to mitigate the communication jamming menace. The UAVs are developed with advanced protocols, encryptions, and frequency hopping, thus ensuring that they operate safely and powerfully despite the interference. For instance, the UAVs might have frequency agility to allow them to interchange from one frequency to another to prevent jamming seemingly. This preserves the other UAV's communication, providing that the jamming cannot stop nomadic interference. It also encompasses the usage of multiple antennas or satellite data exchange to act as a contingency to maintain the communication line in the case of jamming [27].

5. Homomorphic encryption

After Rivest, Shamir, and Adleman presented RSA, homomorphic encryption was first used in 1978 [28], with the full guarantee that only the holder of the private keys can decrypt the message and access and use the content. Homomorphic encryption features enable the manipulation of encrypted data using arithmetic operations [29]. The use of homomorphic encryption algorithms offers a quick and effective means to ensure a certain amount of anonymity. The method encrypts the data before sending it to the other party. The disadvantage of block ciphers, which were created using AES encryption algorithms, is that they can only permit data manipulation after first decrypting the ciphertext. Thus, we must make sure we employ the proper encryption techniques. This problem was solved by public key encryption systems, which use asymmetric keys for encryption and decryption. They make it so that anyone with a public key can encrypt a message, but only the rightful owner or recipient with the required private keys can decrypt it. Homomorphic encryption can provide a foolproof security mechanism for drone communication to ground stations and third parties without compromising data privacy [30].

6. Role of Formal Method and Model Checking in protecting UAV communication

Besides, the increasing use of UAVs has highlighted the inherent need for a secure, resilient, and reliable protocol stack for communication systems. They are one of the key targets for adversaries, including interception and disruption of data and unlawful access that establishes separate encrypted channels for management and data exchange. The introduction of formal methods such as model checking against those attacks is the most effective and efficient in light of increasing confidence in security and reliability [31].

The term "formal methods" is a collection of mathematically grounded approaches used to contract, design, and verify software and hardware [32]. While formal techniques in the field of UAV communication do serve a purpose, their systemic approach holds the complicated relations between UAV and control stations, which is the core to clear everything. The diversity of potential states and environmental conditions that UAVs may face are other methods that minimize the damages caused by human error. Formal technique comes with the advantages of the systems synthesizing of being made abstract through modeling using mathematical models. This kind of standoff allows the timely recognition and obviation of any potential security concerns and weaknesses in the systems while the software is still being developed.

The essence of formal methods is devoted to automation of the model checking that theoretically provided that the system model is provided and the temporal logic specification exists [33]. Such systems present a timely example of UAVs, which require flawless information security since their mission depends on that information. Model-checking tools may have the ability to simulate all possible conditions of the communication protocol and independent states, each of which eludes the scenario of security breaks or communication failures [34]. One such case is model checking, which may flag up the intrusion and attack possibilities where an unauthorized person can interfere and tamper communications, preventing the intended attack vectors in advance.

The strength of formal methods and model checking in achieving safety for UAV communication is mainly highlighted by incorporating those with cybersecurity measures. Special verification, such as formal one, can also aid by ensuring that encryption protocols are correctly developed and hence have no immunity against any known encryption attacks. Not only that, but also this method can verify the precision of intrusion detection systems for UAV communication networks that are used to monitor them for malicious behaviors and filter out such points where such systems are both exhaustive in their threat detection capability. Also, in a sense, the nature of UAV operations and the evolving world around them call for adaptive communication at all times, ensuring that security and reliability are maintained. Formal methods help to develop adaptive protocols based on a virtual assessment of relevant environmental and operation conditions that can be further put into model-checking analysis. Therefore, in order to be able to function reliably both in usual and challenging conditions, the communication systems of a UAV as well as ground control station, should be able to withstand both environmental and adversarial scenarios, which could be accomplished through careful design by the UAV developers.

The development of communication software for UAVs using formal methodologies and model verification techniques can also be integrated with robust tools that assure dependable and accessible design in these systems. This technique involves creating a solid fundamental structure for identifying and eliminating every possible type of vulnerability. Therefore, there are no exposed issues in the UAV communication, so no issues were caused by the multiple possible hazards they would encounter during mission operations. Given the trend of malicious setting up clones of UAVs in many contexts, it is evident that pursuing model checking and formal approaches is adequately critical to ensuring safety in the UAV communication system. Research and development on formal techniques are of significant importance as they are recognized for developing safety measures to install in UAVs.

7. Proposed approach

In this paper, we introduce a new method to improve the security of UAV communications using a combination of Homomorphic Encryption and a dynamic Key Regeneration approach as validated by Model Checking from state-machine models. Our method is intended to address the twofold task of privacy and integrity of data, as well as the flexibility of usage for UAV operations in highly dynamic operating environments. The security mode proposes a central capability in which Homomorphic Encryption is adopted. This is a form of encryption that allows computations to be conducted on ciphertexts. Ultimately, this generates an encrypted result whose decryption is similar to the result of operations on the plaintext. This is useful in UAV communications because it can help to conduct secure computations on the encrypted data. This ultimately ensures that the data privacy is maintained while not compromising the utility of the services. For instance, Homomorphic Encryption can empower the ground station to conduct critical decisions even as the data analysis is made with the telemetry data from UAV being encrypted. This implies that the data would not be decrypted, and the risks of data exposure are therefore minimized.

Model Checking will generate all the possible states of the UAV communication system, and all possible attack vectors will be used on these states. This way, it highlights all the situations in which the security properties can be infringed. Model Checking will also validate the soundness of the key regeneration algorithm, ensuring that key transitions are secure and consistent, and the regeneration process does not introduce new vulnerabilities. Additionally, it will confirm that the system is robust to certain types of attacks, such as man-in-the-middle (MitM), replay, and cryptographic attacks, demonstrating that the integrated HE and KR model can counter a wide range of adversarial behaviour.

In order to test the proposed HE and KR framework following Model Checking to both its performance and security efficacy, the system would be run in a simulated UAV communication system where the outputs will be measured through various metrics. These metrics include the encryption and decryption time, KR regeneration time, and the reduced throughput in communication to determine the viability of the framework. The system's security efficacy will be tested on the basis of data confidentiality and integrity against a number of simulated attacks.

Mathematical Model:

The mathematical model designed to integrate Homomorphic Encryption with key regeneration for ensuring secure UAV communication defines the different key elements and integrates them into the model. The concise structure of the described model way how the encoding procedure, the process of decryption, the generation of keys, and the verification of the security properties through the model checking is represented as:

$(pk, sk) \leftharpoonup KeyGen(\leftthreetimes)$ // Key Generation (1)

$$KeyGen(\leftthreetimes): \begin{cases} pk \in K & (public\ key\ for\ encryption) \\ sk \in K & (private\ key\ for\ encryption) \end{cases} \quad (2)$$

$c \leftharpoonup Enc_{pk}(m)$ // Encryption (3)

$Enc_{pk}(m) = c \in C$ (4)

$m \leftharpoonup Dec_{sk}(c)$ // Decryption (5)

$Dec_{sk}(c) = m \in P$ (6)

$for\ m_1, m_2 \in P$: *// Homomorphic Operation* (7)

$c_1 = Enc_{pk}(m_1), c_2 = Enc_{pk}(m_2)$ (8)

$Dec_{sk}(c_1 \oplus c_2) = m_1 \oplus m_2$ (9)

$\Phi_{conf} = \forall_s \in S, \forall_s \in Actions: HasAcess\ (a, s) \Rightarrow IsAuthorised(a, s)$ (10)

// Confidentiality

$\Phi_{int} = \forall_s \in S, \forall_s \in Actions\ \forall d \in Data$ (11)

$Modifies(a, d, s) \Rightarrow IsLegitimateChange(a, d, s)$ *// Integrity* (12)

$\mathit{\Phi}_{int} = \forall_s \in S, \exists\ s' \in S: CanAccess\ (s) \Rightarrow CanAccess(s')$ *// Availability* (13)

Using the properties of Linear Temporal Logic (LTL) and Computational Logic (CTL)

AG(Φ_{int}) //CTL for Integrity (14)

G(Φ_{conf}) // LTL for Confidentiality (15)

F(Φ_{avail}) // LTL for Availability (16)

$\tau: S \times S \rightarrow \{true, false\}$ // state transition function (17)

$\forall_s \in S, \exists\, s_0 \in S: \tau(s_0, s) \wedge (\Phi_{conf} \wedge \Phi_{int} \wedge \Phi_{avail}$ (18)

// verification of all potential states

ModelCheck (S, τ, Φ)={if $\forall_s \in S, \exists\, s_0 \in S$) ∈ S (19)

Evaluate (τ, Φ,s_0, s) = true (PASS) or Fail (20)

The given equations define a formal verification procedure and a cryptography system. Equations (1) and (2) describe the KeyGen procedure, which creates a private key sk for decryption and a public key pk for encryption, respectively. Equation (3) illustrates how encryption works. Using the public key, plaintext m is encrypted to create a ciphertext c, which is then verified by equation (4). Equation (5) describes the decryption process, which involves utilizing the private key to decrypt the ciphertext and recover the original message, which is then verified by equation (6). The homomorphic features introduced by equations (7) to (9) enable the direct manipulation of encrypted values. Specifically, the combination of their respective plaintexts m1 and m2 is the result of decrypting combined ciphertexts c1 and c2. Equations (10) through (16) guarantee the confidentiality, integrity, and availability of the system by applying the concepts of Computational Tree Logic (CTL) and Linear Temporal Logic (LTL). Last but not least, equations (17) through (20) outline a state transition function and model checking to confirm that all possible system states adhere to the specified security criteria.

8. Experimental Setup and Results

Our research on securing UAV communications uses a variety of advanced simulation and cryptographic tools, specifically selected for their unique features and abilities to address multiple aspects of UAV communication security. In particular, we rely on NS-3 as our main simulation platform, employed for detailed network simulations relevant to UAV communication networks and the testing of homomorphic encryption methods. While we use it to be able to predict network performance under various conditions required for proper protocol evaluation, we also leverage this ability to assess the ability of individual network nodes to terminate human-based traffic analysis or intercept individual packets based on behavioral signatures. We also use Microsoft SEAL to deploy homomorphic encryption schemes to ensure operations data privacy. Crypto++ Library was incorporated for providing the numerous standard and advanced cryptographic functions required to establish a baseline comparison and to execute our novel key regeneration ideas. This integrated library is adopted to ensure that the security solutions we propose are compliant with the most recent cryptographic standards. In this study UPPAL was used which serves as our model checking tools, and UPPAAL is especially beneficial for systems with timed automatons, as precise timing constraints are necessary when working with such systems-based applications.

We have constructed an experimental environment for securing UAV communication. A simulation was built to emulate actual UAV network topography the UAV nodes, ground stations, and possible adversary entities. The simulation permits us to examine the performance of our security mechanisms in a practical setting. Standard UAV communication protocols have been altered to incorporate Homomorphic Encryption and Key Regeneration mechanisms to assure they are wholly compatible with cutting-edge security upgrades. The varying potential adversary performance, including eavesdropping, data tampering, and replay attacks, will also be integrated to assess the performance of our method. This all-inclusive setup allows for the realistic deployment and complete testing of our security updates within a well-controlled but challenging environment. The experimental results obtained are summarised in Table 1.

Table 1: Experimental Results

Metric	Baseline	HE+KR	Improvement (%)
Encryption Time (ms)	50	70	-40%
Decryption Time (ms)	50	70	-40%
Key Regeneration Time (ms)	N/A	30	NA
Data Throughput (Mbps)	100	80	-20%
Computational Overhead (CPU %)	10%	15%	+50%
Memory Usage (MB)	100	150	+50%
Security Breach Instances	5	1	-80%
Data Integrity Violations	3	0	-100%

The integration of Homomorphic Encryption and Key Regeneration into UAV communication protocols results in several performance trade-offs while vastly improving security metrics. The 40% increase in encryption and decryption time with the HE+KR implementation, compared to the baseline configuration, is an indicator of a higher computational load required, which is feasible due to the complexity of homomorphic encryption processes. While this decrease in performance can potentially interfere with the real-time requirements of communication, it is necessary to trade for higher data security during the transmission process. The introduction of key regeneration with 30ms overhead not present in the baseline configuration is necessary for proper security in dynamic communication, as it minimizes the time of threat instance exposure for a single key. The 20% decrease in data throughput compared to the baseline configuration also signifies HE+KR's inefficiency in transmission rates; again, it is likely due to the additional data processing required from encryption and key regeneration. Additionally, the increase in CPU usage and memory usage by 50% each shows that the HE+KR solution is quite resource intensive and calls for updated hardware tools that can absorb additional computational and storage necessities, which might add to the overall cost and energy consumption of UAV operations. Most critical improvements that indicate the effectiveness of the HE+KR approach are observed from the metrics of security and data integrity, with the first showing an 80% decrease and the latter dropping to zero errors. The total absence of data integrity violations especially exemplifies the strength of the system against any unsanctioned data changes, which are a common concern given the sensitivity of UAV applications. While still representing a negative impact on performance metrics like failure times or data integrity, gains in security dimensions overshadow these downsides. Such trade-offs are common for scenarios where secure communication is highly important, such as security or critical infrastructure monitoring, so further improvements in homomorphic encryption algorithms and key regeneration processes need to be improved for future use. This includes optimizing current solutions to be less obstructive toward performance indicators or enriching the computational power of systems to mitigate the negative impacts better.

Table 2: Extended Experimental Results Including Formal Methods and Model Checking

Metric	**Baseline**	**HE+KR Approach**	**Improvement (%)**
Encryption Time (ms)	50	70	-40%
Decryption Time (ms)	50	70	-40%
Key Regeneration Time (ms)	N/A	30	NA
Data Throughput (Mbps)	100	80	-20%
Computational Overhead (CPU %)	10%	15%	+50%
Memory Usage (MB)	100	150	+50%
Security Breach Instances	5	1	-80%
Data Integrity Violations	3	0	-100%
Model Checking Time (s)	200	300	-50%
Number of Properties Verified	10	15	+50%
Vulnerabilities Identified	2	5	+150%

Further, the experiments were extended while model checking, number of properties and vulnerabilities identified were added as a metric. Since model checking takes longer, it verifies more properties and identifies no vulnerabilities. The number of proactive mitigation strategies has also improved by 150%, which makes the system more resilient. Thus, even though the HE+KR approach comes with performance implications, the security benefits more than justify these trade-offs. Moreover, more work should be done on optimizing the encryption and key regeneration to do better performance-wise.

9. Conclusion

Our experimental results demonstrate that although the integration of HE and KR imposes additional computational overhead, including longer encryption/decryption times, additional CPU and memory consumption, the disadvantages are wellcompensated by massive gains in security measures. This observation is evidenced by the reduction of security breaches instances by 80% and the elimination of data integrity violations. The latter metrics are particularly paramount for sensitive UAV applications, where security breaches may entail dramatic repercussions. Additionally, model checking proved itself as a powerful, tool for rigorously verifying the proposed approach's security properties. The process ensured that all potential vulnerabilities were identified and addressed in the design phase before being deployed. The results were entirely aligned with the effectiveness of the security strengthening methods, which were confirmed whilst the simulated attack vectors, specifically, man-in-the-middle and replay attack. Future research in this direction will focus on developing more efficient homomorphic encryption and key regeneration algorithms to make the two impediments, mentioned above, more pathological. Alternatively, one can speculate the enhancement of computational resources of UAV systems to enable more sufficient capacity for balancing security and performance. Ultimately, this study contributes to UAV's broader application horizon by promoting secure communication approaches that guarantee better protection against complex cybersecurity threats, and therefore, increase the reliance on UAV operations.

References

[1] Mohsan, S. A., Khan, M. A., Noor, F., Ullah, I., & Alsharif, M. H. (2022). Towards the unmanned aerial vehicles (UAVs): A comprehensive review. *Drones, 6*(6), 147.

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

[3] 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), 1-35.

[4] 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, 11*(1), 88-96.

[5] Kilat, V. S., Khan, A. S., James, E., & Khan, N. A. (2023). Recapitulation of survey on taxonomy: Security unmanned aerial vehicles networks. *Journal of Computing and Social Informatics, 2*(1), 21-31.

[6] Wang, Y., Su, Z., Ni, J., Zhang, N., & Shen, X. (2021). Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions. *IEEE Communications Surveys & Tutorials, 24*(1), 160-209.

[7] Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S. (2022). A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing. *International Journal of Intelligent Networks, 3*, 16-30.

[8] Hadi, H. J., Cao, Y., Nisa, K. U., Jamil, A. M., & Ni, Q. (2023). A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. *Journal of Network and Computer Applications, 213*, 103607.

[9] Feng, C., Liu, B., Yu, K., Goudos, S. K., & Wan, S. (2021). Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs. *IEEE Transactions on Industrial Informatics, 18*(5), 3582-3592.

[10] Albakri, A., Alshahrani, R., Alharbi, F., & Ahamed, S. B. (2023). Fully homomorphic encryption with optimal key generation secure group communication in Internet of Things environment. *Applied Sciences, 13*(10), 6055.

[11] Yan, X., Zhou, G., Huang, Y., Meng, W., Nguyen, A. T., & Huang, H. (2024). Secure estimation using partially homomorphic encryption for unmanned aerial systems in the presence of eavesdroppers. *IEEE Transactions on Intelligent Vehicles*.

[12] Sarfraz, M., Sohail, M. F., Alam, S., JavvadurRehman, M., Ghauri, S. A., Rabie, K., Abbas, H., & Ansari, S. (2022). Capacity optimization of next-generation UAV communication involving non-orthogonal multiple access. *Drones, 6*(9), 234.

[13] Abdelhamid, M., Atallah, A., Ammar, M., & Mohamed, O. A. (2021). Reliability analysis of autonomous UAV communication using statistical model checking. In *2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS)* (pp. 340-343). IEEE.

[14] Lyu, M., Zhao, Y., Huang, C., & Huang, H. (2023). Unmanned aerial vehicles for search and rescue: A survey. *Remote Sensing, 15*(13), 3266.

[15] Hua, M., Yang, L., Wu, Q., & Swindlehurst, A. L. (2020). 3D UAV trajectory and communication design for simultaneous uplink and downlink transmission. *IEEE Transactions on Communications, 68*(9), 5908-5923.

[16] Khalifeh, A., Mazunga, F., Nechibvute, A., & Nyambo, B. M. (2022). Microcontroller unit-based wireless sensor network nodes: A review. *Sensors, 22*(22), 8937.

[17] Rupar, M. A., Larsen, E., Saglam, H. B., Savin, J. A., Peltotalo, S., & Gurdil, B. (2022). Scenarios for BLOS connectivity. *Procedia Computer Science, 205*, 198-207.

[18] Dang, Y., Benzaïd, C., Yang, B., Taleb, T., & Shen, Y. (2022). Deep-ensemble-learning-based GPS spoofing detection for cellular-connected UAVs. *IEEE Internet of Things Journal, 9*(24), 25068-25085.

[19] He, D., Yang, G., Li, H., Chan, S., Cheng, Y., & Guizani, N. (2020). An effective countermeasure against UAV swarm attack. *IEEE Network, 35*(1), 380-385.

[20] Zhou, Y., Rao, B., & Wang, W. (2020). UAV swarm intelligence: Recent advances and future trends. *IEEE Access, 8*, 183856-183878.

[21] de Carvalho Bertoli, G., Pereira, L. A., & Saotome, O. (2021). Classification of denial of service attacks on Wi-Fi-based unmanned aerial vehicle. In *2021 10th Latin-American Symposium on Dependable Computing (LADC)* (pp. 1-6). IEEE.

[22] Jacobsen, R. H., & Marandi, A. (2021). Security threats analysis of the unmanned aerial vehicle system. In *MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM)* (pp. 316-322). IEEE.

[23] Chamola, V., Kotesh, P., Agarwal, A., Gupta, N., & Guizani, M. (2021). A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. *Ad Hoc Networks, 111*, 102324.

[24] Vajravelu, A., Ashok Kumar, N., Sarkar, S., & Degadwala, S. (2023). Security threats of unmanned aerial vehicles. In *Wireless Networks: Cyber Security Threats and Countermeasures* (pp. 133-164). Cham: Springer International Publishing.

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

[26] Wu, Y., Guan, X., Yang, W., & Wu, Q. (2021). UAV swarm communication under malicious jamming: Joint trajectory and clustering design. *IEEE Wireless Communications Letters, 10*(10), 2264-2268.

[27] Yang, B., Taleb, T., Fan, Y., & Shen, S. (2021). Mode selection and cooperative jamming for covert communication in D2D underlaid UAV networks. *IEEE Network, 35*(2), 104-111.

[28] Kiratsata, H. J., & Panchal, M. (2021). A comparative analysis of machine learning models developed from homomorphic encryption based RSA and Paillier algorithm. In *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1458-1465). IEEE.

[29] Iezzi, M. (2020). Practical privacy-preserving data science with homomorphic encryption: An overview. In *2020 IEEE International Conference on Big Data (Big Data)* (pp. 3979-3988). IEEE.

[30] Yang, W., Wang, S., Cui, H., Tang, Z., & Li, Y. (2023). A review of homomorphic encryption for privacy-preserving biometrics. *Sensors, 23*(7), 3566.

[31] Toman, Z. H., Hamel, L., Toman, S. H., Graiet, M., & Valadares, D. C. (2024). Formal verification for security and attacks in IoT physical layer. *Journal of Reliable Intelligent Environments, 10*(1), 73-91.

[32] Luckcuck, M. (2023). Using formal methods for autonomous systems: Five recipes for formal verification. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 237*(2), 278-292.

[33] Gruber, J., Humml, M., Schröder, L., & Freiling, F. C. (2023). Formal verification of necessary and sufficient evidence in forensic event reconstruction. In *Proceedings of Digital Forensics Research Conference Europe (DFRWS EU).*

[34] Gao, H., Dai, B., Miao, H., Yang, X., & Barroso, R. J. (2023). A novel gapg approach to automatic property generation for formal verification: The gan perspective. *ACM Transactions on Multimedia Computing, Communications and Applications, 19*(1), 1-22.