Protecting Attacks on Unmanned Aerial Vehicles using Homomorphic Encryption

Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 11, No. 1, March 2023, pp. 88~96
ISSN: 2089-3272, DOI: 10.52549/ijeei.v11i1.3932

Protecting Attacks on Unmanned Aerial Vehicles using Homomorphic Encryption

Mohammed Y. Alzahrani[1], Nayeem Ahmad Khan[2*], Lilia Georgieva[3], Alawi M. Bamahdi[4], Omar Ahmed Abdulkader[5], Ahmed H. Alahmadi[6]
[1,2]Department of Computer Sciences and Information Technology, AlBaha University, AlBaha, Saudi Arabia
[3]Department of Computer Science, Heriot-Watt University, Edinburgh, UK
[4]Department of Computer Science, College of Computing (Al Qunfudah), Umm Al-Qura University, Saudi Arabia
[5] Faculty of Computer Studies, Arab Open University, Riyadh, Saudi Arabia
[6]Department of Computer Science and Information, Taibah University, Saudi Arabia.

Article Info

Article history:

Received Jul 4, 2022
Revised Nov 14, 2022
Accepted Dec 5, 2022

Keywords:

Cybersecurity
Unmanned Aerial Vehicles
Homomorphic Encryption
Pallier Cryptosystem
Malware Attacks

ABSTRACT

With the exponential growth in the usage of unmanned aerial vehicles (UAV), often known as drones, for military, civilian, and recreational purposes. Security of internal communication modules and communication to the ground control station is considered the foremost challenge. Hacking into the system and attacking the internal communication devices with malicious code can disaster the vehicle's system. The need for having a secure communication channel between the internal modules of the vehicle and transmission of data to the ground control station is of utmost crucial. Existing mechanisms based on conventional encryption methods are highly suspectable to attacks as their keys can be broken by employing high computing power. Another challenge with these approaches is undesired high-level data communication latency affecting real-time communication. This study implements a homographic encryption-based technique for secure communication. In addition, we also propose a key regeneration algorithm based on pallier homomorphic encryption. Simulations were conducted using OMNET++ and Aerial Vehicle Network Simulator (AVENS). In this study 54 encryption attacks were collected from different sources. Compared to Digital Encryption Standard (DES) and Advanced Digital Encryption (AES), the proposed approach defended all the communication attacks between the UAV and the ground control station.

Corresponding Author:

Dr Nayeem Ahmad Khan,
Faculty of Computer Science & Information Technology,
AlBaha University,
Alaqiq, AlBaha, 65779-7738. Saudi Arabia.
Email: nayeem@bu.edu.sa

1. INTRODUCTION

UAVs are a form of aircraft that does not have a human pilot onboard and operates autonomously. UAVs were most typically connected with the military, which was true for a long time. These aircraft were first utilized as target practice for anti-aircraft missiles, information collecting platforms, and, more controversially, weapons platforms [1]. Recent technological advancements have enabled the creation of a wide range of modern UAVs that may be utilized for various civilian applications, including traffic monitoring, weather updates, agriculture, photography, firefighting, and delivery of items [2]. When it comes to UAV functionality, there are two main modes: flight and navigation mode. UAV needs an energy source to fly, such as a battery or fuel. They are also equipped with rotors, propellers, and a frame. UAV frames are often constructed of lightweight composite materials in order to minimize weight while increasing mobility. UAVs need a

controller, which allows the user to manage the aircraft remotely, including launching, navigating, and landing [3].

Using wireless channels, UAVs interact with one another and with the ground control station, making them susceptible to a variety of attacks. A major problem that needs to be resolved is the security of UAVs while flying. In reality, it is quite simple to initiate attacks against UAVs. Unsophisticated individuals can conduct these UAV attacks at a low cost [4]. Even with just small packs of explosives, commandeered UAVs can be used to disrupt sensitive events, threaten civilian populations and military missions, violate privacy, or supply materials for destructive activities [5]. When the line of sight between a UAV and its ground controller is lost, communications between the two may be carried out through satellite. A UAV transmits data through a satellite back to its ground control station [6]. Smaller UAVs, which are specially used for recreational purposes, do not have any satellite communication but are directly controlled from the ground control station. The flying capabilities of these UAVs are limited only to a few hundred meters. There is a high risk of this communication link being attacked. Some versions, however, are not equipped with encryption features, which is challenging. An attacker may take over the control of the UAV and perform the desired action [7].

Furthermore, their unique configuration, including the open state of the connected sensors, wireless network, and so on, are very vulnerable to technological systems. In recent years, studies have been conducted to investigate cyber security risks to UAVs that are utilized in the military sector [8-11]. However, little research has been conducted to investigate whether extra cyber hazards exist for the usage of commercially accessible UAVs. In addition, most of the security technology and procedures are now being designed without first doing a thorough threat assessment.

One solution to securing the communication of UAVs to base stations is to implement encryption. In this study, we employ a homomorphic encryption scheme for safe communication, keeping in view the small nature of the UAVs, which are used for personal purposes. Homomorphic encryption can be used in a distributed fashion as it does not require the decryption of data at any intermediate part, thus wholly reducing the risk of attacks and maintaining confidentiality.

Specifically, the objective of this research study is to find a way to overcome the drawback of traditional cryptographic algorithms. The contribution of this research resides in the implementation of the unique homographic encryption for secure communication UAVs. Compared to other approaches, homomorphic encryption has the benefit of not needing the decryption of the complete message before processing [12]. The data remains encrypted always, thus reducing sensitive information being attacked or compromised. Decryption will be limited to a specified function of the ciphertext, and only that specific information will be sent to the person who has requested the decryption procedure. As a result, it protects the remainder of the data from being compromised. The degree of data security provided by the homomorphic approach makes it appropriate for use in the presence of a hostile environment [13].

Our meticulous experiments reveal much better security and performance when homomorphic encryption is used compared to other types of encryption schemes. Hence, the scheme is suitable for UAVs that are sent to hostile situations and need to transmit pictures, videos, and other updates to a ground control base station.

The rest of the paper is organized as: in section 2, the basic architecture of UAVs is discussed. The related works are discussed in Section 3. Section 4 details the security threats affecting UAV communication. The working of homomorphic encryption is explained in section 5. The proposed approach is presented in Section 6. The experimental setup, simulation, and results are section 7. The conclusion is provided in section 8.

2. ARCHITECTURE OF UAV'S

Non-military UAVs consist of three major modules: the aircraft, ground control base station, and data communication link, as depicted in Figure 1. A summary of the major components of civilian unmanned aerial vehicles is given as following.

2.1. Ground Control Station

A ground control station (GCS) is a system of one or more computers used to control the flight of a UAV. It typically consists of a computer with a graphical user interface, video screen, and keyboard/mouse for controlling the UAV [14].

2.2. Communication Link

The communication link between the ground control station and the UAV is key for successful UAV operations. The ground control station communicates with the UAV and sends commands to it to execute certain tasks. This communication link is usually done through radio waves or satellite data [16]. If there is an issue with the communication link, then the UAV cannot receive commands from the ground control station or send data back. UAV communication types include 3G, 4G, 5G, WiFi, Bluetooth, etc [16].

2.3. Controllers

UAVs have many components that help them fly and stay in the air. The most important ones include body frame, flight controller, GPS, altimeter, rotor, transmitter, battery, receiver, and power distribution panel [17].

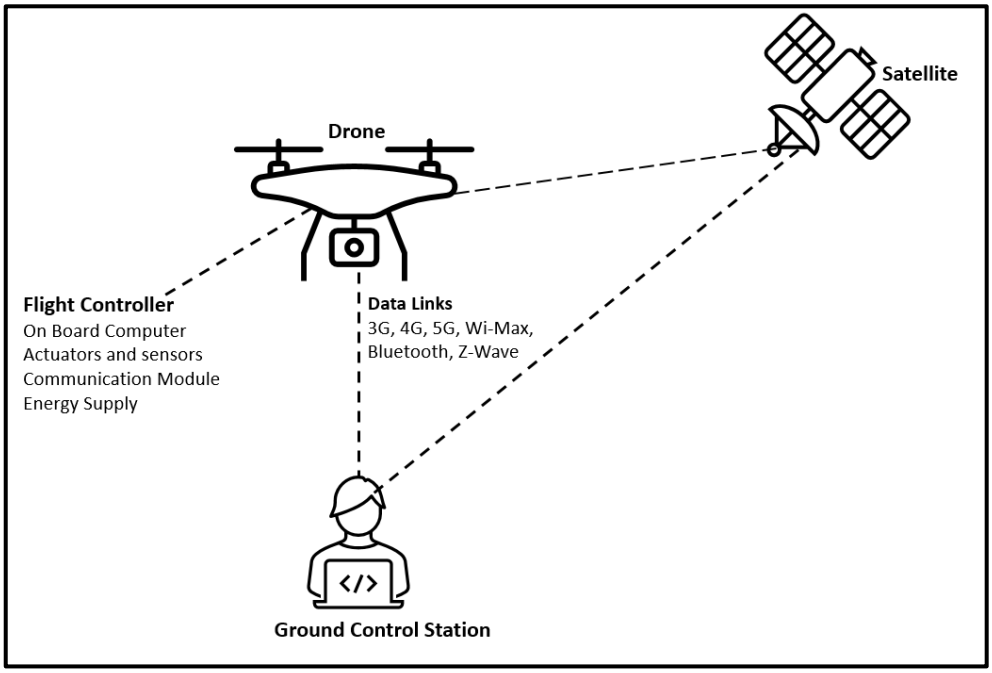

Figure 1. Architecture of a UAV

3. RELATED WORK

Several authors have contributed to the effort of ensuring the safety of the ground-based station and UAV. A study by [18] concluded that not only the lost cost UAV's but UAV's employed on monitoring the critical infrastructure and operations such as by security forces are also vulnerable to attacks. The authors simulated a Man-in the middle injection attack on the control command to compromise the UAV. A study by [19] illustrates that different vulnerabilities are exploited on UAV's and subsequently the need for a new method to prevent intrusions. A hacking procedure has been performed on commercially available UAVs, and its severe results on UAV's are also presented. A study by [20] reveals that UAVs with more than 60GHZ, which are high band frequency, perform better in detecting invasion attacks than a low-frequency UAV with 2.5GHz-5GHz. A study by [21] investigates that a crucial threat, a Jelly fish attack over MASNETS in sync, affects the UAV. A multicast relay protocol has been developed to prevent such attacks. MASNETS a collection of mobile nodes that may operate as both routers and hosts in an ad hoc wireless network and that can dynamically self-organize in a wireless network without the need for any pre-existing infrastructure[22]. Cryptography has also been used for information security in UAVs. According to the authors [23], the identity-based authentication strategy should be used to secure the UAV-aided HetNet; nevertheless, the decryption procedure and communication overheads are the key downsides of this approach. As mentioned by [24], authentication and security for partitioned data kept on UAVs and shared between a UAV and the ground station may be assured via the use of the encryption key negotiation mechanism. Nevertheless, the drawback of such a mechanism is that the UAVs incur a non-negligible time cost to perform a new negotiation implicating in a significant increase of latency and potentially affecting their required precision. Additionally, there are several apparent security flaws, such as communication via an unencrypted wireless network and the widespread use of the User Datagram Protocol (UDP). UDP is prone to packet loss and some of the lowest-grade encryption algorithms, one being a symmetric key algorithm called RC4. Researchers [25] assert that the inclusion of a link encryption layer over wireless communication eliminates the majority of security concerns. Taking into consideration the growing number of UAVs, a successful GSM-based Passive Coherent Location (PCL) system for the detection of tiny unmanned aerial vehicles (UAVs) has been presented [26]. The system is based on the integration of information from many base stations. The PCL system employs the concept of Area Surveillance that is based on the estimation of mobile users' trajectories. When it comes to big aircraft, there is a fully defined and well-understood regulatory system in place [27]. However, regulatory arrangements

for tiny civil UAVs are very unpredictable and unreliable when it comes to addressing security issues such as behavioral and data privacy [28]. Users need assurances that their private data is protected and secure when using such devices [29].

Data encryption plays an important role in data and privacy protection and is an excellent way to maintain data confidentiality, integrity, and availability. It is also one of the most critical preconditions for information security and confidentiality of data. It provides strong protection against unauthorized access to information, and in some cases, it may be protected from damage or accidental destruction [30]. Some new encryption approaches, like Homomorphic encryption, remove the drawbacks of traditional encryption schemes [31]. Homomorphic encryption supports both data confidentiality and data integrity, but also has some unique features that are limited to the scenarios that require tamper-resistance. In this paper, we will use Homomorphic encryption as a tamper-tolerant encryption scheme. Homomorphic Encryption fulfills that role by preventing data communication from getting attacked from a UAV to a base station and vice versa.

4. SECURITY THREATS AFFECTING UAV COMMUNICATION

Eliminating vulnerabilities is an endless game against one's adversaries in an environment of continual and fast technological development. It is, therefore, necessary that these vulnerabilities are always under watch and constantly hunted down by the security community. The financial and political benefits will continually motivate adversaries, while the personal benefits are a means of furthering technical and offensive capabilities through an unsupervised environment [32]. Common types of UAVs attacks are Spoofing, Denial of Service, and Packet Attacks.

4.1 Spoofing:

Spoofing is a term that refers to a collection of threats that circumvent authentication procedures, allowing an attacker to pose as someone when they are not. Spoofers take over a UAVs communication connection by sending a counterfeit signal that the UAV interprets as genuine due to its resemblance to the original signal. When an attacker has established a valid connection, spoofing may allow the perpetrator to intercept and manipulate almost any function on the UAV [33].

4.2 Denial of Service Attack

DOS (Denial of Service) is a well-known and recognized kind of cyber-attack in the cyber world, and it is being exploited for jamming UAV communication. When it is done through a variety of different sources, it is referred to as DDOS (Distributed Denial of Service). The interception of UAV remote controls is yet another real threat. DDOS attacks on UAVs can have a number of unexpected consequences [34].

4.3 Packet Attack

Packets are collections of digital data that are transferred in a certain sequence over a period of time. When sending a data packet that is much larger than the receiver's capacity, it is possible to generate an overload on the system [35]. A packet injection attack refers to an attack in which an intruder intercepts data packets and injects malicious packets into the network – which the compromised receiver receives, processes, and forges an appropriate response [36]. This attack can be used in order to disrupt the network or destroy sensitive information. Usually, hackers rely on packet injection to make the target host send traffic back towards the attacker in order to mask their true identity. The UAVs' wireless communication transmits out beacon frames that can be captured. They contain information such as the MAC addresses of the UAV and the remote-control device that is operating the UAV, and the wireless network channel that the UAV is using to communicate [37].

5. HOMOMORPHIC ENCRYPTION

The studies conducted for security in cyber-physical systems differ based on the application domain in which the system is used [38]. Due to the physically dispersed nature of cyber-physical systems, the connectivity and communication latency must be kept to a minimum. UAVs are often resource-restricted in terms of computing, communication, energy, and storage. As a result, security solutions for UAV data transfer must be resilient, fast, and able to meet the demands of real-time operations. At the same time, it must be as light as possible without compromising on performance [39]. In addition, the integrity of communications in UAV-based security applications also needs to be protected, given the critical nature of their application domain. This paper proposes a homomorphic-based encryption approach to achieve high security in UAV communication without compromising its efficiency.

Homomorphic encryption, which is a public-key cryptosystem, offers the user the possibility of computing an operation on the ciphertexts of two or more encrypted files without decrypting these ciphertexts

[40]. The principal use of homomorphic encryption is to preserve and maintain the privacy of data and information outsourced for storage and processing [42]. The ability to process data without decrypting it allows commercially accessible cloud services to preserve a greater degree of data privacy than is otherwise possible. Although perfect homomorphic encryption has been proven to be practical, fast and efficient systems are being used in sectors ranging from medicine to retail [42].

There are three types of homomorphic encryption: partial, somewhat, and full form of homomorphic encryption [43]. In order to keep sensitive data safe, partial homomorphic encryption restricts the number of mathematical functions that may be performed on encrypted data [44]. Common allowed operations include addition, XOR, and multiplication. Options include symmetric encryption as in RSA and AES. Some commonly used partial homomorphic encryption, Unpadded RSA, ElGamal, Goldwasser–Micali, Benaloh, Paillier [45].

Somewhat homomorphic encryption allows for just a limited number of operations to be executed at a time, with each operation only being performed once [46]. This means that the encrypted content can be converted into a form where some operations can occur. However, it does not mean that every operation is possible. Indeed, a very limited range of arithmetic operations is allowed for encrypted data. The operation of multiplication can be performed on encrypted data, but it cannot be performed multiple times. Fully homomorphic encryption is the global standard of homomorphic encryption since it keeps data secure while still making it accessible to authorized users. Fully homomorphic encryption allows treating ciphertext like plaintext in the sense that both can be processed with the same algorithms [47]. The algorithm used for homomorphic encryption divides plaintext into very small parts and makes them unreadable during the encryption. Among the most significant contributions of this study is the proposal and implementation of Paillier homomorphic encryption for data protection, which is being examined for the first time and represents a novel technique.

The Paillier homomorphic encryption has shown to be useful in a number of crucial areas, including electronic voting and electronic financial transactions [48]. Moreover, it has been shown that the Paillier homomorphic cryptosystem provides a useful stepping stone for other cryptography applications. The Paillier cryptosystem is a probabilistic method that relies on asymmetric and public-key cryptography to achieve its goals of security. It was originally proposed in 1999 by Pascal Paillier [49]. Such a system can be used to encrypt arbitrary messages, but its primary use case is for key-agreement protocols. The implementation of the Paillier homomorphic cryptosystem requires both a scheme for probabilistic encryption and a scheme for probabilistic decryption, such as a Paillier cryptosystem that uses the RSA probabilistic encryption scheme and the Paillier probabilistic decryption scheme. The primary use case of the Paillier cryptosystem is for key-agreement protocols, which are used in a number of cryptographic primitives like pseudorandom generators and Diffie–Hellman. A probabilistic encryption scheme is an algorithm that takes as input a key and the encryption of some message and then outputs another encryption of the same message but with less randomness. The implementation of the Paillier homomorphic cryptosystem requires both a scheme for probabilistic encryption and a scheme for probabilistic decryption. There are many uses for the Pallier homomorphic cryptosystem, including the ability to leverage this cryptography application in other areas.
Definition: an encryption scheme is considered homomorphic,

$$iff: from\ Enc(a)\ and\ Enc(b)\ it\ is\ possible\ to\ computer\ Enc(f(a,b))$$

Where, $f = +, X, \oplus\ and\ without\ using\ private\ key.$

6. PROPOSED APPROACH

We propose an extra key generation encryption technique in conjunction with the Paillier Cryptosystem in order to prevent cipher data from being attacked, as shown in Figure 2. In the homomorphic encryption technique, data was encrypted using the private key, while the public key was stored on the client's side only for security reasons. Our algorithm then puts that data through the additional key encryption algorithm a second time, resulting in the generation of random key cipher data each time. If an attacker has the first key, an additional key will be required to decode it using two distinct keys. If an attacker obtains the plaintext once, he will not be able to get the plaintext of every message sent between the source and the destination. As a result, this system offers more security than the old method. In order to decrypt the algorithm, it will require the knowledge of both keys. The proposed algorithm based on the pallier cryptosystem is given in Table 1.

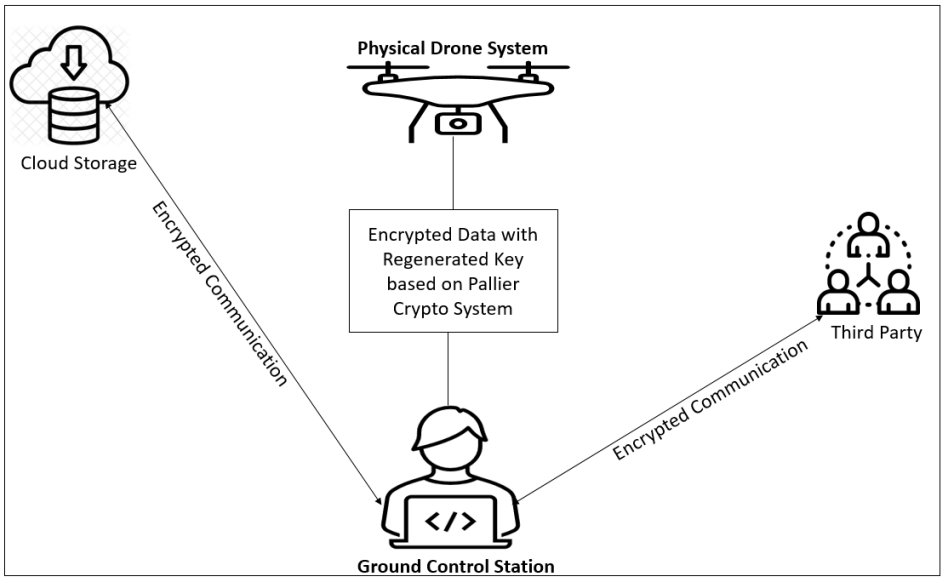

Figure 2. Proposed Approach

Table 1. Proposed extra key generation algorithm based on Paillier Cryptosystem

Key Generation	1. Take two large prime numbers p and q, randomly, Confirm that gcd $(pq,(p-1)(q-1)$ *is* 1. if not start again 2. Compute $n-pq$. 3. Define function $L(x)=\frac{z-1}{n}$ 4. Computer λ as $lcm(p-1,q-1)$ 5. Pick a random integer g in the set $\mathbb{Z}_n^*$ 6. Calculate $\mu=(L(g^{\lambda} mod\ n^2))^{-1}$ 7. The public key is (n,g) for encryption 8. The Private key is λ for decryption
Encryption	1. Let m be a message to be encrypted where $0 \le m \le n$ 2. Select random r where $0<r<n$ 3. Computer ciphertext as: $c=g^m.r^n mod\ n^2$
Extra Key Generation	1. Again, compute private and public key (R_{sk},R_{pk}) 2. Re-Encrypt ciphertext produced by Pailler algorithm and send public key R_{pk} to receiver.
Decryption	1. Let c be the ciphertext to decrypt, where $c \in \mathbb{Z}_{n2}$ 2. Compute the plain message as: $m=L(c^{\lambda}, mod\ n^2.\mu\ mod\ n$

7. EXPERIMENTAL SETUP AND RESULTS

The experimental simulations were conducted using hardware Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz, 2901 Mhz, 2 Core(s), 4 Logical Processor(s), 8GB RAM and having high end NVIDIA GEFORCE DTX-950M. The whole experiment was simulated using OMNET++. OMNET++ is a general-purpose discrete event simulation software package developed in 1997 by the OMNET++ Alliance [50]. The software is designed to simulate large-scale networks of heterogeneous elements, such as communication networks, computer networks, and power grids. OMNET++ provides a set of modeling primitives that allow users to build models of real-world networks. It also provides a rich library of standard models that can be used as-is or starting point for building custom models. The Models are specified using an intuitive graphical language (Pajek) and can be run in either batch mode or interactively. It is a modular and extensible tool that can be used in various fields of study. OMNET++ includes various tools for network analysis, from the simplest to the most complex.

In addition to this we used AVENS - Aerial Vehicle Network Simulator [51]. The goal of AVENS is to provide a framework for mobile ad hoc network analysis in which unmanned aerial vehicles (UAVs) serve as mobile nodes that share a wireless channel for exchanging messages. When managing the aerial vehicles, a flight simulator is used along with a network simulator for getting network metrics such as transmission rate, throughput, RSSI (Received Signal Strength Indication), package loss, number of retransmissions, and so on. The parameters for the scenarios are all flexible. In other words, one can easily draw any topology by using our flight and network simulators, specifying the number of UAVs, their distances from each other, their locations such as flight altitude velocity. It is designed to be used in various fields, such as the development of UAVs, validation of UAV designs, and testing of new configurations. AVENS supports several different platforms and allows for easy customization of the simulation environment. It allows for the creation of

scenarios that simulate a user-defined UAV, environment, and threats and allows for the simulation of UAV sensors and control devices without worrying about the details of physics or platform support. Since the simulator is much more practical and convenient than owning an actual UAV, it was decided to use the simulator. It was ideal to use the simulator because it will allow the team to practice and even modify the setting of the UAV with ease and convenience. The setting, features, behavior, and function of the commonly used drone" Lifoto Drone Strobe" was mimicked in the simulator.

In this study, our focus was on three types of attacks: Spoofing, Denial of Service, and Packet attack, as discussed in section 3. The attack signatures were collected from different open-source databases used to attack different encryption schemes. Our collected set of attacks includes DDOS attacks, packet attacks, and snooping attacks. Our collected set of 54 attacks includes DDOS attacks, packet attacks, and Spoofing attacks. We mainly concern ourselves with these attacks because they are the most common in cyberspace. The performance of the proposed approach compared to other approaches such as DES and AES was based on the number of attacks successful, key size, memory usage, and computation time. The results obtained are given in Table 2. An attack was considered successful even if one of the message packets was affected.

Table 2. Simulation Results

Encryption Scheme	Attacks Prevented	Attacks Successful	Key Size (Bits)	Message Size (KB)	Memory Usage (KB)	Computational Time (MS)
DES	48	6	142	1,164	7346	195
AES	51	3	132	2396	12439	253
Proposed Approach	54	0	448	2236	27567	1567

The experimental results show that the proposed approach was able to defend all of the 54 attacks. In comparison, as DES encryption scheme was able to defend 48, and the AES encryption scheme was able to defend against 51 attacks. The proposed approach utilized more memory usage and computational time resources than DES and AES. The number of attacks prevented using DES was 48, while AES and the proposed approach performed better and prevented 51 and 54 attacks, respectively. The key size used was 448 bits, while DES and AES are comparatively lower, with 142 bits and 132 bits, respectively. The proposed approach's memory consumption and computational time were 27567 KB and 1567ms, while DES and AES requires memory usage of 7346KB and 12439 KB and computational time of 195ms and 253ms, respectively. Keeping in view of the currently available computing power and memory, this is very negligible. Experimental results show that the proposed approach, which is based on the pallier cryptosystem, can be easily implemented to prevent UAV communication from getting attacked despite the size of the UAV. The proposed crypto scheme has been evaluated through simulation, and experimental results show that the proposed scheme is efficient in providing defense against a UAV cyber-attack. It can also be easily implemented into commercial off-the-shelf hardware components.

9. CONCLUSION

A homomorphic-based encryption scheme was proposed in this study to protect UAV communication from being attacked in the event that an adversary eavesdrops on communications between the base station and the UAV and impersonates them by sending fake commands to affect the current communication or even take control of the UAV. Pallier Homomorphic encryption was used to encrypt the message, which is a strong candidate for enhancing the security of communication in different scenarios. We also proposed a key regeneration algorithm based on pallier homomorphic encryption. The efficiency of the proposed approach was evaluated using a customized simulation framework, which was then compared to conventional methods. The experimental results show that the proposed scheme is suitable for securing communication between UAVs and ground control stations.

REFRENCES

[1] Gupta SG, Ghonge D, Jawandhiya PM. Review of unmanned aircraft system (UAS). International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume. 2013;2.

[2] Hiebert B, Nouvet E, Jeyabalan V, Donelle L. The application of drones in healthcare and health-related services in north america: A scoping review. Drones. 2020 Sep;4(3):30.

[3] Tomic T, Schmid K, Lutz P, Domel A, Kassecker M, Mair E, Grixa IL, Ruess F, Suppa M, Burschka D. Toward a fully autonomous UAV: Research platform for indoor and outdoor urban search and rescue. IEEE robotics & automation magazine. 2012 Aug 29;19(3):46-56.

[4] Hartmann K, Steup C. The vulnerability of UAVs to cyber attacks-An approach to the risk assessment. In2013 5th international conference on cyber conflict (CYCON 2013) 2013 Jun 4 (pp. 1-23). IEEE.
[5] Snead J, Seibler JM, Inserra D. Establishing a legal framework for counter-drone technologies. Heritage Foundation; 2018 Apr 16.
[6] Zeng Y, Wu Q, Zhang R. Accessing from the sky: A tutorial on UAV communications for 5G and beyond. Proceedings of the IEEE. 2019 Dec 2;107(12):2327-75.
[7] Vergouw B, Nagel H, Bondt G, Custers B. Drone technology: Types, payloads, applications, frequency spectrum issues and future developments. InThe future of drone use 2016 (pp. 21-45). TMC Asser Press, The Hague.
[8] Yağdereli E, Gemci C, Aktaş AZ. A study on cyber-security of autonomous and unmanned vehicles. The Journal of Defense Modeling and Simulation. 2015 Oct;12(4):369-81.
[9] Khan N, Abdullah J, Khan AS. Defending malicious script attacks using machine learning classifiers. Wireless Communications and Mobile Computing. 2017 Feb 7;2017.
[10] Alqarni AA, Alsharif N, Khan NA, Georgieva L, Pardade E, Alzahrani MY. MNN-XSS: Modular neural network based approach for XSS attack detection. Computers, Materials and Continua. 2022;70(2):4075-85.
[11] Rugo A, Ardagna CA, Ioini NE. A Security Review in the UAVNet Era: Threats, Countermeasures, and Gap Analysis. ACM Computing Surveys (CSUR). 2022 Jan 17;55(1):1-35.
[12] Yousuf H, Lahzi M, Salloum SA, Shaalan K. Systematic review on fully homomorphic encryption scheme and its application. Recent Advances in Intelligent Systems and Smart Applications. 2021:537-51.
[13] Brakerski Z, Döttling N, Garg S, Malavolta G. Candidate iO from homomorphic encryption schemes. InAnnual International Conference on the Theory and Applications of Cryptographic Techniques 2020 May 10 (pp. 79-109). Springer, Cham.
[14] Alladi T, Bansal G, Chamola V, Guizani M. Secauthuav: A novel authentication scheme for uav-ground station and uav-uav communication. IEEE Transactions on Vehicular Technology. 2020 Oct 22;69(12):15068-77.
[15] Chaari L, Chahbani S, Rezgui J. Mav-dtls toward security enhancement of the uav-gcs communication. In2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall) 2020 Nov (pp. 1-5). IEEE.
[16] Islam N, Rashid MM, Pasandideh F, Ray B, Moore S, Kadel R. A review of applications and communication technologies for internet of things (Iot) and unmanned aerial vehicle (uav) based sustainable smart farming. Sustainability. 2021 Jan;13(4):1821.
[17] Chamola V, Kotesh P, Agarwal A, Gupta N, Guizani M. A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. Ad hoc networks. 2021 Feb 1;111:102324.
[18] Lakew Yihunie F, Singh AK, Bhatia S. Assessing and exploiting security vulnerabilities of unmanned aerial vehicles. InSmart systems and IoT: innovations in computing 2020 (pp. 701-710). Springer, Singapore.
[19] Fotohi R. Securing of Unmanned Aerial Systems (UAS) against security threats using human immune system. Reliability Engineering & System Safety. 2020 Jan 1;193:106675.
[20] Zhao N, Yang X, Ren A, Zhang Z, Zhao W, Hu F, Rehman MU, Abbas H, Abolhasan M. Antenna and propagation considerations for amateur uav monitoring. IEEE Access. 2018 May 18;6:28001-7.
[21] Thomas A, Sharma VK, Singhal G. Secure link establishment method to prevent jelly fish attack in MANET. In2015 International Conference on Computational Intelligence and Communication Networks (CICN) 2015 Dec 12 (pp. 1153-1158). IEEE.
[22] Jebaseelan VG, Srinivasan A. ArcRectZone: A Lightweight Curved Rectangle Vector Based Secure Routing for Mobile Ad-Hoc Sensor Network. International Journal of Intelligent Engineering and Systems. 2017;10(6):116-24.
[23] Li Y, Cai L. UAV-assisted dynamic coverage in a heterogeneous cellular system. IEEE Network. 2017 Jul 28;31(4):56-61.
[24] Steinmann JA, Babiceanu RF, Seker R. Uas security: Encryption key negotiation for partitioned data. In2016 Integrated Communications Navigation and Surveillance (ICNS) 2016 Apr 19 (pp. 1E4-1). IEEE.
[25] Samland F, Fruth J, Hildebrandt M, Hoppe T, Dittmann J. AR. Drone: security threat analysis and exemplary attack to track persons. InIntelligent Robots and Computer Vision XXIX: Algorithms and Techniques 2012 Jan 23 (Vol. 8301, p. 83010G). International Society for Optics and Photonics.
[26] Płotka M, Malanowski M, Samczyński P, Kulpa K, Abratkiewicz K. Passive bistatic radar based on VHF DVB-T signal. In2020 IEEE International Radar Conference (RADAR) 2020 Apr 28 (pp. 596-600). IEEE.
[27] Al-Turjman F, Abujubbeh M, Malekloo A, Mostarda L. UAVs assessment in software-defined IoT networks: An overview. Computer Communications. 2020 Jan 15;150:519-36.
[28] Casagrande G, Gusto DD. Concepts and Issues. InSmall Flying Drones 2018 (pp. 13-45). Springer, Cham.
[29] Lin C, He D, Kumar N, Choo KK, Vinel A, Huang X. Security and privacy for the internet of drones: Challenges and solutions. IEEE Communications Magazine. 2018 Jan 12;56(1):64-9.
[30] Viji D, Saravanan K, Hemavathi D. A journey on privacy protection strategies in big data. In2017 international conference on intelligent computing and control systems (ICICCS) 2017 Jun 15 (pp. 1344-1347). IEEE.

[31] Gahi Y, Guennoun M, El-Khatib K. A secure database system using homomorphic encryption schemes. arXiv preprint arXiv:1512.03498. 2015 Dec 11.
[32] Cronin AK. Why drones fail: when tactics drive strategy. Foreign Aff.. 2013;92:44.
[33] Kerns AJ, Shepard DP, Bhatti JA, Humphreys TE. Unmanned aircraft capture and control via GPS spoofing. Journal of Field Robotics. 2014 Jul;31(4):617-36.
[34] Chen J, Feng Z, Wen JY, Liu B, Sha L. A container-based DoS attack-resilient control framework for real-time UAV systems. In2019 Design, Automation & Test in Europe Conference & Exhibition (DATE) 2019 Mar 25 (pp. 1222-1227). IEEE.
[35] Garg S, Aujla GS, Kumar N, Batra S. Tree-based attack–defense model for risk assessment in multi-UAV networks. IEEE Consumer Electronics Magazine. 2019 Oct 31;8(6):35-41.
[36] Khan N, Abdullah J, Khan AS. A dynamic method of detecting malicious scripts using classifiers. Advanced Science Letters. 2017 Jun 1;23(6):5352-5.
[37] Pan M, Chen C, Yin X, Huang Z. UAVs-aided emergency environmental monitoring in infrastructure-less areas: LoRa mesh networking approach. IEEE Internet of Things Journal. 2021 Jul 8.
[38] Schmittner C, Ma Z, Schoitsch E, Gruber T. A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems. InProceedings of the 1st ACM Workshop on Cyber-Physical System Security 2015 Apr 14 (pp. 69-80).
[39] Liu CH, Chen Z, Tang J, Xu J, Piao C. Energy-efficient UAV control for effective and fair communication coverage: A deep reinforcement learning approach. IEEE Journal on Selected Areas in Communications. 2018 Aug 10;36(9):2059-70.
[40] Benzekki K, El Fergougui A, Elbelrhiti EA. A secure cloud computing architecture using homomorphic encryption. International Journal of Advanced Computer Science and Applications. 2016 Feb 1;7(2):293-8.
[41] Mittal D, Kaur D, Aggarwal A. Secure data mining in cloud using homomorphic encryption. In2014 IEEE international conference on cloud computing in emerging markets (CCEM) 2014 Oct 15 (pp. 1-7). IEEE.
[42] Bocu R, Costache C. A homomorphic encryption-based system for securely managing personal health metrics data. IBM Journal of Research and Development. 2018 Jan 25;62(1):1-.
[43] Acar A, Aksu H, Uluagac AS, Conti M. A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys (Csur). 2018 Jul 25;51(4):1-35.
[44] Bos JW, Lauter K, Naehrig M. Private predictive analysis on encrypted medical data. Journal of biomedical informatics. 2014 Aug 1;50:234-43.
[45] Cominetti EL, Simplicio MA. Fast additive partially homomorphic encryption from the approximate common divisor problem. IEEE Transactions on Information Forensics and Security. 2020 Apr 6;15:2988-98.
[46] Fan J, Vercauteren F. Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive. 2012.
[47] Armknecht F, Boyd C, Carr C, Gjøsteen K, Jäschke A, Reuter CA, Strand M. A guide to fully homomorphic encryption. Cryptology ePrint Archive. 2015.
[48] Sharma T. E-voting using homomorphic encryption scheme. International Journal of Computer Applications. 2016 May;141(13):14-6.
[49] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. InInternational conference on the theory and applications of cryptographic techniques 1999 May 2 (pp. 223-238). Springer, Berlin, Heidelberg.
[50] OMNeT++ Discrete Event Simulator, Available online: https://omnetpp.org/
[51] AVENS, Aerial Vehicle Network Simulator, Available online: https://omnetpp.org/download-items/AVENS.html