Republic of Iraq
Ministry of Higher Education
and Scientific Research
University of Diyala
College of Science

Security Of The Drone Communication

A Thesis

Submitted to the Computer Science Department \College of Science \University of Diyala
In a Partial Fulfillment of the Requirements for The Degree of Master of Science in Computer

By
Hani Merdas Ismail

Supervised By

Prof. Dr. ziyad Tariq Mustafa

2021 A.D.		1442 A.H.

بسم الله الرحمن الرحيم

يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ
دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ ◌ۚ(11)

صدق الله العظيـم

سورة المجادلة (11)

Acknowledgments

First of all, Praise is to Allah, Lord of the worlds, for a blessing that helped me in achieving this research until the end of it, I would like to express my thanks and gratitude to my supervisor ***Prof. Dr. Ziyad Tariq Mustafa*** *for supervising this research and for the bounty, patience and continued guidance throughout the work.*

My thanks to all academics and administrative staff at the Department of computer science.

Hani Merdas

Dedication.

I would like to dedicate this Work To:

The soul of both my father and my brother, and also dedicate to The rest of my family

Hani Merdas

Abstract

Nowadays, drones (unmanned aerial vehicles (UAV)) are used in a variety of fields, including military, civilian and humanitarian purposes, including drug delivery and other environmental monitoring, particularly in circumstances where human intervention may pose risks such as epidemics. Therefore, the protecting of drone communications from piracy, spoofing, and other security threats is considered important.

This thesis proposes securing drone communications using lightweight encryption algorithms. The proposed secured drone communications include three stages. The first stage is the Preparation stage, which includes the key generation process using a one-dimensional Chebyshev chaotic map, which results in a unique and random key for each session. The second stage in the proposed system is encryption/decryption using lightweight algorithms (block cipher algorithm (Hight) and cipher stream chacha20). The last stage in the proposed system is the authentication stage to check the authentication of the drone before receiving massege.

The Results of the proposed system are done on two different types of data (colored image and text) with different sizes. Based on error sensitivity metrics the block cipher HIGHT algorithm on ciphering colored images and text achieves better results than Chacha 20 algorithm. In terms of speed, the chacha20 algorithm is faster in execution time than the lightweight HIGHT algorithm in ciphering for both colored images and text.

List of contents

List of Tables

List of Figures

List Of Algorithms

□ □

Abbreviations

AD	Average difference
1D	One-Dimensional
ACK	Acknowledgment
AES	Advanced Encryption Standard
BANs	Body Area Networks
eCLSC TKEM	Efficient Certificate Less Sign-Encryption Tag Key Encapsulation Mechanism
GCS	Ground Control Station
GE	Gate Equivalents
GPS	Global Position System
IOD	Internet Of Drones
IoT	Internet Of Things
ISM	Industrial, Scientific And Medical Applications Of Radio Frequency Energy
LUT	Look-Up Table
MANETs	Mobile Ad Hoc Networks
MAV	Micro Air Vehicle
MD	Maximum Difference
MSE	Mean Square Error1
NAE	Normalized Absolute Error
NCC	Normalized Cross-Correlation
NIST	National Institute Of Standards And Technology
NIST	National Institute Of Standards And Technology
OTP	One-Time Password
PAN	Personal Area Network
PSNR	Peak Signal To Noise Ratio
Q.R	Quarter-Round
RFID	Radio Frequency Identification
□□	Structural Content
SNR	Signal To Noise Ratio
TLS	Transport Layer Security
TTP	Trusted Third Party Number
UAS	Unmanned Aircraft System
UAV	Unmanned Air Vehicle

UDDI	Universal Description Discovery and Integration
UQI	Universal Quality Index
VANETs	Vehicular Ad Hoc Networks
WSA	Web Services architecture
WSNs	Wireless Sensor Networks
XML	Extensible Markup Language
AD	Average Diffrence

CHAPTER ONE

□

INTRODUCTION

CHAPTER One

□□tr□□□ct□□□

□□□□□tr□□□ct□□□

Over recent years, drones are increasingly being used not only for military tasks only, but also for civilian tasks too, such as environment and traffic monitoring, delivery services, and aerial surveys. Also, some research projects have adopted drones as mobile collectors for monitoring applications based on wireless sensor networks (WSNs). For example, on-ground sensors can be deployed in farms to monitor the conditions of soil, and drones can periodically collect information from these sensors and perform in-network processing of this information [1].

Drones are a kind of tool that can control the flight without the pilot's operation, and it is gradually popularizing people's life. With the continuous expansion of its market scale, the key technology of drones has become the focus of scientific researchers. In the course of the flight, drones usually need a wireless network to control their network. The information collected during flight needs to be transmitted back, which also needs the support of the network. When the information transmitted is confidential, the security performance of the network will be important [2].

When the line of sight between the drone and its ground controller is broken, communications between them can be carried out via satellite. Unfortunately, some implementations are not equipped with encryption functions. As a result, the control function could be taken over by an adversary. Incidentally, in 2009 a terrorist group was found to have captured an unencrypted unmanned aerial vehicle video feed using sky grabber [3].

Due to different methods and objects of attacks, the consequences are also different. Some attacks aim to steal information through security holes of communication links while others aim to spoof sensors, such as GPS spoofing[4].

The technological advancement enables easy manipulations via smart-phones to fly mini-drones instead of using remote controllers. The use of drones is not limited to commercial and personal aims. Law enforcement and border control surveillance teams are using drones. In case of natural disasters, search and rescue teams employ them to gather information or to drop essential supplies. On the other hand, the reliance on wireless communications makes drones vulnerable to various attacks. These attacks can have drastic effects, including commercial and non-commercial losses. In this context, there is a lack of proper understanding of how hackers perform their attacks and hijack a drone, to intercept it or even crash it. Drones can also be compromised for malicious purposes. Hence, there is a need to detect them and prevent them from causing any damage[5].

In this thesis, the security of the drone communication network is introduced for surmounting the challenging information leakage problem due to potential eavesdropping. This work aims to design an authentication system model between the drone and ground station and make a secure channel to exchange data using lightweight algorithms.

[illegible]

The following are some studies and works that are associated with the suggested work in this thesis:

1. [illegible] designed a security protocol for an unmanned aircraft system (UAS) that prevents breaches in the confidentiality and integrity of the UAS with minimal computation overhead. This research did successfully implement a low-cost encryption mechanism to the UAS. This work was regarded as an easy cryptographic break, but under the assumption of a short flight time, the key is not feasibly breakable. This research ensured the security of the system, with a proper key transmission, a unique key would be generated for each direction of communication. They used the RC5 lightweight encryption algorithm for encryption, decryption and used a unique key would be generated for each direction of communication. the research did successfully implement a low-cost encryption mechanism to the UAS.

2. [illegible] proposed an efficient certificate-less sign-encryption tag key encapsulation mechanism (eCLSC TKEM). The eCLSC-TKEM reduced the time required to establish a shared key between a drone and a smart object by minimizing the computational overhead at the smart object. Also, their protocol improved the drone's efficiency by utilizing dual channels which allows many smart objects to concurrently execute eCLSC-TKEM. They evaluated their protocol on commercially available devices, namely(AR. Drone2.0 and TelosB), by using a parking management testbed. The experimental results showed that the proposed protocol was much more efficient than other protocols in time of

computation where (eCLSC-TKEM 9.25 s),(CLSC-TKEM 13.37s),(Sun's CL-AKA 15.10s)and (Yang's CL-AKA 32.84s).

3. **□ar□□□ □□ □□□□t □a □□□□□□□□□□□□**.carried out a software security analysis of the MAVLink protocol, which was expected to become a worldwide standard within the drone code project. More specifically, they investigated potential design or implementation protocol flaws using fuzzing techniques. The goal was to inject invalid or semi-invalid data to produce an unexpected software behavior. They formulated three different research questions: (i) How can software security flaws be identified in the MAVLink framework? (ii) What are the consequences of exploiting these security flaws? and (iii) Could countermeasures be provided to mitigate such issues?. They used the drone simulator the ArduCopter for testing, Resulting from the listed test cases, they were able to identify a few security flaws. Particularly, from the sixth test case, where the payload increased randomly, the fuzzing script was able to crash the virtual drone. The error caused by the fuzzing script can be the floating-point exception aborting and the operation aborted (core dumped).then they were able to identify a few security flaws. Particularly, from the sixth test case, where the payload was increased randomly, the fuzzing script was able to crash the virtual drone. To investigate the cause of the exceptions they used the gdb debugger and the core dump of the memory when the kernel crash occurred. From an analysis, they identified that errors correspond to three specific functions. The next step of the work is to complete the entire range of the test cases aiming to gain more results identifying error flaws of the MAVLink software implementation. However, they had to stress that fuzzing all possible test cases is a resource-demanding operation. For instance, there is a limitation concerning memory usage. They looked to

further improve the fuzzing scripts aiming to make the fuzzing operations more memory efficient.

4. **□□s□a□□□ □□□□□t□a□□□□□□□□□□**proposed some methods/actions that can be implemented to increase the communication security of drones. Drones were vulnerable to GPS spoofing, therefore there was a need for developing anti-spoofing and anti-jamming receivers. While there had been a lot of promising work and methods proposed for the detection and avoidance of civilian GPS anti-spoofing and anti-jamming in the literature. Those methods could be broadly classified into cryptographic (spread spectrum, dual receiver correlation), and non-cryptographic (antenna array). However, these methods were either difficult to implement or require costly hardware. Therefore, they proposed some simpler software-based techniques for spoof detection. For example, checking latency: the movement speed can be validated for a change in location in just a brief instant and the Checking GPS Sub-frame Data. The changes of coordinates can be recorded and validated given the time it takes to change the coordinates, and they planned to analyze the P4P drone communication signals using the SDR equipment, such as HackRF and BladeRF, and live video transmission.

5. **□□r□st□a□□□□□□s□□□□t□a□□□□□□□□□□□□□** examined and analyzed a standard UAV communication and control protocol (i.e., the DSM protocol family). They discussed common approaches for attacks, minor observations, and associated

security vulnerabilities of this protocol. Since the number of commercially available communication components is small, these findings can easily be ported to other protocols such as (HOTT, S-FHSS, FrSky, and others) by using brute force attack to the message of the radio chip used (*CYRF6936*) and the DSMX protocol are and they got measurement results of the practical implementation of the attack. when Receive transfer packet a 10848878 µs (≈10 s), when Brute force CRC seed 623649 µs (≈0.6 s)and the overall 11645488 µs (≈11 s). They recommended using the longest possible secret (at least 6 bytes). This makes a brute force attack considerably more difficult and ensures stronger authentication of the legitimate owner. Finally, they recommended using cryptographic methods. These should be publicly known and acknowledged. It should be noted that hardware resources are limited and that response times must have adhered to.

6. **Azza Allouch, et. al. (2019) [9]**discussed the security vulnerabilities of the MAVLink protocol and propose MAVSec, a security-integrated mechanism for MAVLink that leverages the use of encryption algorithms to ensure the protection of exchanged MAVLink messages between UAVs and GCSs. To validate MAVSec, they implemented it in Ardupilot and evaluated the performance of different encryption algorithms (i.e. AES-CBC, AES-CTR, RC4, and ChaCha20) in terms of memory usage and CPU consumption. The experimental results show that ChaCha20 has a better performance and is more efficient than other encryption algorithms. Integrating ChaCha20 into MAVLink can guarantee its messages confidentiality, without affecting its performance, while occupying less memory and CPU consumption, thus, preserving memory and saving the battery for the resource-constrained drone.

7.

1.□ □□o□le□ □tate□e□t

Drones are also the world's first use and they reach many fields of military and civil life. However, these drones remain a threat because of their communications potential interceptions Additionally, it is possible that to identify the sender and recipient of drone communications. Therefore, the problem of securing drone communications and ensuring the reliability of the identity of the sender and recipient is the problem of this thesis.

1.□A□□ □o□□he□□□

The propose secure communication of drone aims to Increase the security of information transmission through drone communications with ground control stations using Hight block cipher lightweight algorithm, and Chacha 20 stream cipher lightweight algorithm. Also proposing an authentication method between the ground station and drone using proposed hash chacha20 lightweight algorithm key management.

1.□ □o□t□□□ut□o□

The main contribution of this thesis is to secure the data payload of the MAV link protocol based on the Hight and Chacha 20 algorithms. and the addition of an authentication method by using the proposed hash chacha20 lightweight key management between the grand station and drone. This new contribution will provide secure communication channels for the transmission of data between the grand station and drone.

1.□ □he□□□ □utl□□e

In addition to this chapter this thesis includes four chapters as follows:

□ha□te□2: "□heo□et□cal □ac□□□ou□□".

This chapter describes the lightweight algorithm.

□ha□te□□: "□□o□o□e□ □□□te□".

This chapter describes the details of the proposed system.

□ha□te□□: "□e□ult□a□□ □e□t□".

This chapter shows the results of the proposed system.

□ha□te□□□□□o□clu□o□□a□□ □u□□e□t□o□ □o□□utu□e □ o□□□.

In this chapter, conclusions and recommendations for future works are presented.