T.C.

ANTALYA BILIM UNIVERSITY

INSTITUTE OF POSTGRADUATE EDUCATION

ELECTRICAL AND COMPUTER ENGINEERING

MASTER PROGRAM

UAV-BASED SMART RESCUE SYSTEM UTILIZING A NOVEL WIRELESS COMMUNICATION TECHNIQUE WITH ENHANCED SECURITY AGAINST INTERNAL AND EXTERNAL ATTACKS

DISSERTATION

PREPARED BY:

JOEL PONCHA LEMAYIAN

JANUARY 2021

T.C.

ANTALYA BILIM UNIVERSITY

INSTITUTE OF POSTGRADUATE EDUCATION

ELECTRICAL AND COMPUTER ENGINEERING

MASTER PROGRAM

UAV-BASED SMART RESCUE SYSTEM UTILIZING A NOVEL WIRELESS COMMUNICATION TECHNIQUE WITH ENHANCED SECURITY AGAINST INTERNAL AND EXTERNAL ATTACKS

DISSERTATION

PREPARED BY:

JOEL PONCHA LEMAYIAN

THESIS ADVISOR:

Dr. JEHAD HAMAMREH

JANUARY 2021

APPROVAL/NOTIFICATION FORM

ANTALYA BILIM UNIVERSITY

INSTITUTE OF POST-GRADUATE EDUCATION

Joel Poncha Lemayian, a M.Sc. student of Antalya Bilim University, Institute of Post-Graduate Education, Electrical and Computer Engineering owning student ID 181212001, successfully defended the thesis/dissertation entitled *UAV-based Smart Rescue System Utilizing a Novel Wireless Communication Technique With Enhanced Security Against Internal And External Attacks*, which he prepared after fulfilling the requirements specified in the associated legislation, before the jury whose signatures are below.

Academic title	**Signature**
Thesis Advisor:	_____
Jury Member:	_____
Jury Member:	_____

Date of Submission:06/01/2021.

Date of Defence: 22/01/2021

Director of The Institute: _____

ÖZET

Kentsel nüfustaki mevcut üstel artış nedeniyle çok sayıda sorun yaşanmıştır. Bu tür zorluklar, güvensizlik ve afet yönetimini içerir. Bu sorunlar ve daha fazlası, kentsel gelişmelerdeki kalıcı nüfus artışı nedeniyle gelecekte daha da kötüleşecektir. Bu nedenle, bu tür zorlukları yönetmenin yeni ve verimli yollarının gerçekleştirilmesi çok önemlidir. Drone teknolojisi, esnekliği ve maliyet etkinliği nedeniyle birçok uygulamada kullanılmıştır. Bu tür uygulamalar arasında mal teslimi, veri toplama, gözetim ve izleme bulunur. Bununla birlikte, güvenlik, insansız hava araçlarının daha ileri ve karmaşık uygulamaları için büyük bir endişe ve tökezleyen bir engel olmuştur.

Bu çalışma, yeni bir güvenli iletişim tekniğiyle otonom bir ilk müdahale drone tabanlı (Auto-FRD) akıllı kurtarma sistemi önermektedir. Otomatik FRD paradigması, akıllı bir şehir ortamında kritik durumlara hızlı yanıt vermek için dronları kullanır. Sistem üç ana bölümden oluşur: Sensör sistemi, akıllı dronlar ve komuta merkezi. Dahası, drone ile komuta merkezleri arasındaki yeni güvenli iletişim tekniği, iletilen verilere yardımcı sinyaller ekleyerek güvenliği artırmak için kanalın gürültü ve parazit gibi özelliklerinden yararlanmak üzere tasarlanmıştır.

Auto-FRD sistemi, akıllı sensörlerden bir uyarı sinyali aldıktan sonra dronların otomatik olarak belirli bir konuma konuşlanacağı şekilde tasarlanmıştır. Ayrıca sistem ucuz LoRa teknolojisi kullanılarak uygulanmaktadır. Önerilen paradigmanın verimliliği ve yeniliği matematiksel analiz yoluyla sunulur ve Monte Carlo simülasyonları ile doğrulanır. Sonuçlar, önerilen sistemin büyük ölçüde geleneksel kriz müdahale sistemlerine kıyasla yanıt süresini azaltır. Ayrıca, toplanan veriler araştırmalar sırasında değerlidir.

Keywords: Fiziksel katman güvenliği, Kablosuz iletişim, Nesnelerin interneti, Insansız hava araçları, Akıllı şehir.

ABSTRACT

Numerous problems have been experienced due to the current exponential rise in the urban population. Such challenges include insecurity and disaster management. These problems and more will be exacerbated in the future due to the persistent population increase in urban developments. It is therefore critical that new and efficient ways of managing such challenges are realized. Drone technology has been used in many applications due to its flexibility and cost-effectiveness. Such applications include goods delivery, data collection, surveillance, and tracking. Nevertheless, security has been a major concern and a stumbling block to further and sophisticated applications of drones.

This work proposes an autonomous first response drone-based (Auto-FRD) smart rescue system with a novel secure communication technique. Auto-FRD paradigm uses drones to provide quick response to critical situations in a smart city setting. The system comprises three main sections: Sensor system, intelligent drones, and the command center. Moreover, the novel secure communication technique between the drone and the command centers are designed to utilize the characteristics of the channel such as noise and interference to enhance security by adding auxiliary signals to the transmitted data.

The Auto-FRD system is designed such that the drones automatically deploy to a specific location upon receiving an alert signal from the smart sensors. Moreover, the system is implemented using cheap LoRa technology. The efficiency and novelty of the proposed paradigm is presented via mathematical analysis and validated by Monte Carlo simulations. Results indicate that the proposed system drastically reduces the response time compared to conventional crisis response systems. Also, the data collected is valuable during investigations.

Keywords: Physical layer security, Wireless communications, Internet of things, Unmanned aerial vehicles, Smart city.

DEDICATION

To you, my dearest family:

Dad, Piyiai, baba Taj, mama Liam, mama SimaSwam, Abel, and Osoi, I dedicate this work, this milestone would have never been possible without your unconditional support and sacrifices from each one of you, I am eternally in your debt. And to my very many nephews and nieces I pray that one day you will read this work and may it motivate you to do greater things.

ACKNOWLEDGEMENTS

First, I would like to thank God for the strength, wisdom, and wellness He bestowed upon me to complete this work. Special thanks to my first advisor **Dr. Fadi Alturjman** for his encouragement to undertake this challenge and to my current supervisor **Dr. Jehad Hamamre** for going above and beyond to make me a better researcher and for his valuable support and advice. I would also like to thank the scientific and technological research council of Turkey (TUBITAK) for their support in my research and Antalya Bilim University for giving me the chance to make this achievement possible.

CONTENTS

INSTITUTE OF POSTGRADUATE EDUCATION
ELECTRICAL AND COMPUTER ENGINEERING
MASTERS PROGRAM WITH THESIS

ACADEMIC DECLARATION

I hereby declare that this master's thesis titled *UAV-based Smart Rescue system Utilizing a Novel Wireless Communication Technique With Enhanced Security Against Internal And External Attacks* has been written by myself under the academic rules and ethical conduct of the Antalya Bilim University. I also declare that the work attached to this declaration complies with the university requirements and is my work. I also declare that all materials used in this thesis consist of the mentioned resources in the reference list. I verify all these with my honor.

_____

Joel Poncha Lemayian.(..../..../2021)

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

3GPP: 3rd Generation Partnership Project

AN: Artificial Noise

Auto-FRD: Autonomous First Response Drone

AWGN: Additive White Gaussian Noise

BS: Base Station

BER: Bit Error Rate

BS: Base Station

CCTV: Closed Circuit TV

CSI: Channel State Information

CDMA: Code Division Multiple Access

CD-NOMA: Code-Domain Non-Orthogonal Multiple Access

CP: Cyclic Prefix

ESC: Electronic Speed Controller

FC: Flight controller

LPWAN: Low-Power Wide Area Network

FDMA: Frequency Division Multiple Access

GA: Genetic Algorithm

GPS: Global Positioning System

HD: High Definition

IDE: Integrated Development Environment

IMM: Istanbul Metropolitan Municipality

IoT: Internet of Things

IGMA: Interleave-Grid Multiple Access

IDMA: Interleave Division Multiple Access

ISI: Inter-Symbol Interference

LoRa: Long-Range

LoRaWAN: Long-Range Wide Area Networks

LoS: Line of Sight

MIMO: Multiple Input Multiple Output

mMTC: massive Machine-Type Communication

MISO-NOMA: Multiple-Input Single-Output Non-Orthogonal Multiple Access

MIMO: Multiple Input Multiple Output

MUSA: Multi-User Shared Access

MUST: Multi-User Superposition Technique

NLoS: No Line of Sight

NOMA: Non-Orthogonal Multiple Access

OMA: Orthogonal Multiple Access

OFDMA: Orthogonal Frequency Division Multiple Access

PLS: Physical Layer Security

PD-NOMA: Power-Domain Non-Orthogonal Multiple Access

PAPR: Peak to Average Power Ratio

RFM95: Radio Frequency Modulation 95

ROS: Robot Operating System

RSSI: Received Signal Strength Indicator

RE: Resource Element

RSMA: Resource Spread Multiple Access

SA: Simulated Annealing

SIC: Successive Interference Cancellation

SINR: Signal-to-Interference plus Noise Ratio

SBF: Secrecy Beam-Forming

SS-NOMA: Small Scale Non-Orthogonal Multiple Access

SCMA: Sparse Code Multiple Access

SNR: Signal to Noise Ratio

SISO: Single Input Single Output

TDMA: Time Division Multiple Access

TDD: Time Division Duplex

UAVs: Unmanned Aerial Vehicles

URLLC: Ultra-Reliable Low-Latency Communications

WSMA: Welch-bound Equality Spread Multiple Access

CHAPTER 1

1. INTRODUCTION

Many problems have been experienced due to the current exponential rise in the urban population. Such challenges include insecurity, disaster management, and more. These problems and others will be exacerbated in the future due to the persistent population increase in urban developments. It is therefore critical that new and efficient ways of managing such challenges are realized. Unmanned aerial vehicle (UAV) technology has been used in many applications due to its flexibility and cost-effectiveness. Such applications include goods delivery, data collection, surveillance, and tracking. Nevertheless, security has been a major concern and a stumbling block to further UAV application inventions.

This work proposes an autonomous first response drone-based (Auto-FRD) smart rescue system with a novel secure communication technique. The Auto-FRD paradigm uses drones to provide quick responses to critical situations in a smart city setting. The drone paradigm is composed of three main sections: the command center, the smart drones, and the sensor system. Additionally, the novel secure communication technique between the drone, sensors, and the command centers is designed to utilize the characteristics of the channel such as noise and interference to enhance security by adding auxiliary signals to the transmitted data. Moreover, the Auto-FRD system is implemented using cheap LoRa technology, and optimal base station placement positions are calculated using meta-heuristic algorithms such that the drones are able to provide services over an entire given area with minimal resources. The efficiency and novelty of the proposed paradigm are presented via mathematical analysis and validated by Monte Carlo simulations. Results indicate that the proposed system drastically reduces the response time compared to conventional methods.

This work is composed of three major sections. In the first part, the design of Auto-FRD will be discussed, in the second part, the novel communication technique will be discussed in details, and finally, the optimal placement position of the drone base station

will be determined such that a given area is completely covered while the number of drones and cost are minimized. The main contributions of this work are given below:

1.1 *CONTRIBUTIONS TO LITERATURE*

1. A new emergency drone response system.
2. A cheap alternative emergency response system.
3. A low complexity communication technique suitable for internet of things applications.
4. A novel secure communication system to protect information collected by the drones and secure communications.
5. An optimal drone base station (BS) placement method to minimize cost and maximize coverage.

In the next section, we discuss the design of Auto-FRD.

CHAPTER 2

2. Auto-FRD MODEL FOR CRITICAL SITUATION MANAGEMENT

2.1 *DEMAND FOR DRONES' APPLICATIONS*

Current technology has facilitated the integration of drones in many different application areas. [1]. Commercial companies, such as Amazon prime air, Mercedes, Dominos, and united parcel service (UPS) have realized the benefits of drones and are utilizing them to deliver goods. Special personalized drones used for taking pictures and videos are currently available in the market. UAVs are also used by the military for surveillance and information gathering and even in executing missions. The use of drones has caught the interest of many researchers and academicians mainly because of the many advantages incurred as opposed to using conventional methods. Such advantages include low cost, safety, expandability among others. Researchers are pushing the limits of drone technology to perform new and complex functions aiming at minimizing cost and enhancing efficiency in areas such as communication and security.

2.2 *EMERGENCY RESPONSE IN A SMART CITY SETTING*

As the population in cities increase, service delivery such as security becomes difficult. Currently, crisis response time is very high, and this is expected to further increase as the cities become more populated. It is therefore critical that new and effective ways are determined to mitigate this problem. Critical situations prompting new emergency response systems include fire accidents, robbery, vehicle accidents, terror attacks, and explosions. This work explores the unique qualities of smart drones and propose a new drone system used to respond to critical situations at minimum time and provide emergency rescue services. The proposed paradigm comprises of smart drones, intelligent sensors, and drone command centers. We will provide a detailed study on drone flight planning, flight path acquisition, and permission to fly authorization. We will discuss about information management both at the drone and command center level. Additionally, a detailed study

and design of the communication system comprising of camera sensors, transmitters, and receivers will also be provided.

The proposed paradigm is different compared to other related works in that, drones are automatically activated by sensors as opposed to human operators. In the event that an accident occurs, people often become very confused and are not able to observe the environment around them. This means that accurate information about the event will be very hard to obtain. Moreover, it takes a response team about 10 to 20 minutes to arrive at the accident scene. CCTV cameras have been used in many incidents to try and determine exactly what happened. Nevertheless, the cameras have many limitations such as dead zones, memory size, weather hazards, cost, and they can easily be damaged or tempered with during the accidents. The proposed system is able to quickly respond to an emergency situation, record the entire incident and even deliver required instruments such as fire extinguishers or first aid items.

Some examples of real-word events where this system could have been used include, the attack that happened in Christchurch New Zealand in March 2019, which left at least 40 people dead. This was the act of a single attacker. Because the police took time to respond, he was able to do more harm. Another example is the attack that happened at Dusit hotel in Nairobi Kenya in January 2019. The police did not respond in time and even after arrival, they could not go into the building immediately to begin rescue operations. The police did not know the location of the attackers, how many they were, or what kind of weapons they had. Therefore, they spent a lot of time trying to design a rescue plan. They relied on CCTV images which took a lot of time to acquire. As a result, the attack left at least 20 people dead. Motivated by these situations and many others, the proposed system will be able to give the police quick and very crucial information that is required to save many lives. Moreover, the drones can be used to distract an attacker and give innocent people time to escape.

Some work analogous to this can be found in literature. The work proposed by [2] is closest to our proposed system. Nevertheless, the paradigm proposed in [2] faces many limitations such as unreliability and false information due to reliance on human deployment. The paradigm proposed in this work is trying to limit human influence and reduce

response time. The drones are activated by distress sensor signals from smart sensors deployed in the city as opposed to people. The drones are activated by sending a global positioning system (GPS) coordinate signals. Once the drones receive this signal they immediately fly to the scene, record and send back live images. When the actual police arrive at the scene, they have access to prior information about the scene.

The information collected by the drones can be used by the police to bring the right people to justice and help prevent wrongful convictions. In Figure 2.1 we observe the use of Auto-FRDs in a smart city paradigm. Drone deployment base stations are places where drones are deployed. In the figure, we can observe that the ideal location for a drone deployment base station is at the top of a tall building (shown by the red arrows). This is so that there will be a good line of sight (LoS), which facilitates strong communication between sensors and drones. Moreover, Figure 2.1 shows two critical situations happening, a car accident and a building on fire. In the figure, we can observe drones hovering above the two critical situations. These drones are sending back live images to the command center and help authorities deal with the situation better.

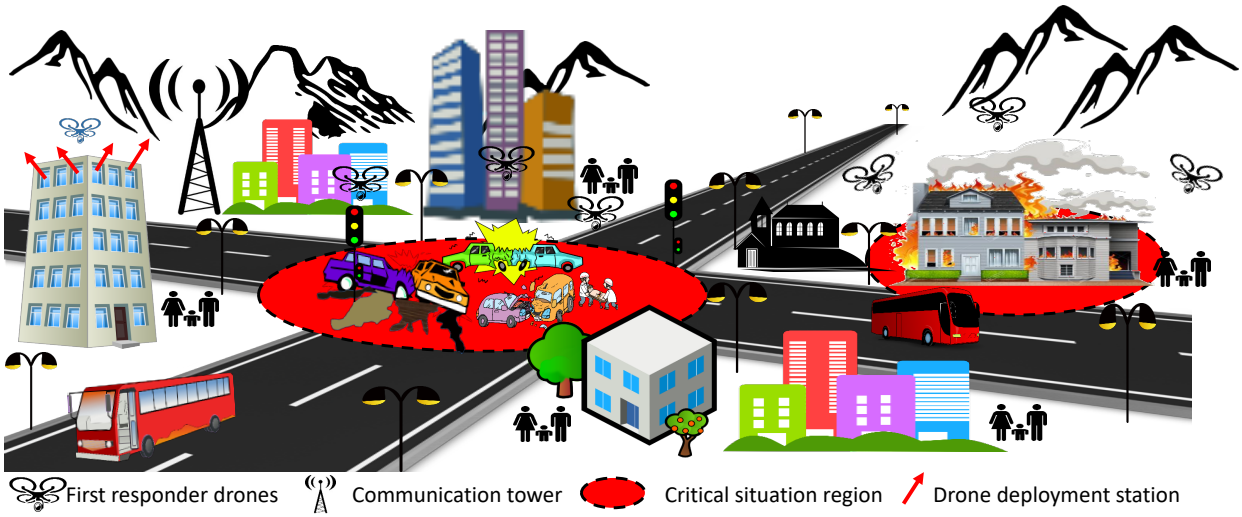

Figure 2.1: Critical situation in a smart city environment.

2.3 *SECTION ORGANISATION*

This section is organized as follows. Section 2.4 talks about related drone applications. Section 2.5 presents the system model and a case study is presented in section 2.6. Section 2.7 highlights the main challenges in implementing this system and section 2.8 provides a section summery.

2.4 *RELATED DRONE APPLICATIONS*

The efficiency of drones in performing multiple tasks have allowed them to be used in executing many tasks with minimum cost and energy. This has attracted many researchers and engineers to employ the use of drones in many different areas. In this section, we highlight drones utilized in rescue missions, emergency cellular coverage, and accident scene mapping.

Drones' compactness and availability have enabled their effective use in searching for survivors in collapsed buildings [3]. Authors in [3] propose a complete architecture for a rescue drone hardware. The rescue team deploy the drone at the scene and use onboard infrared cameras to locate victims. This system is suitable for rescue missions in areas with no GPS accessibility. The proposed system uses, DJI Matrice 100 and hokuyo lidar, as well as Intel RealSense for global and local mapping. According to [3], results show that the proposed system performed better than conventional methods in assisting rescuers to find victims in unknown disaster affected areas.

Additionally, authors in [4] propose a paradigm where drones are deployed to provide 5G cellular coverage to a region requiring emergency cellular coverage. The region could have been affected by a disaster or too much traffic generated by users, resulting to a slow network. The goal of the system proposed in [4] is to determine the minimum number of drones required and their location for a complete coverage of the critical environment with minimum cost. While at the same time maintaining a high data rate and low latency. The authors use meta-heuristic algorithms (Simulating Annealing (SA) and Genetic Algorithm (GA)) to empirically solve the optimization problem. Moreover, authors in [5]

developed a drone system to provide emergency cellular coverage in a densely populated area. Consequently, improving the performance of conventional networks.

According to the European Commission annual report in 2017, forest fires are considered among the top environmental hazards [6]. Authors in [7] propose an emergency support UAV for forest fire surveillance. The system is equipped with thermal sensors, communication modules, and thermal cameras that provide valuable real-time data about the fire to the response team. In addition, the system is implemented using multiple algorithms which automate take-off, landing, path planning, and fire monitoring. The system was simulated by performing several flight tests and the results show great performance in detecting forest fires.

Authors in [8] propose an emergency relief distribution system used after an earthquake. Arman et al. provide a detailed study of the difficulties faced by ground response after an earthquake disaster. As a result, Arman et al. propose the use of drone technology to deliver relief post-earthquake to the affected people. according to [9], this paradigm is not affected by ground transportation constrains and can be used to provide services to inaccessible regions. The results show that the proposed system is very effective when providing emergency relief to affected areas.

Moreover, authors in [10] propose a top-down approach for providing post-earthquake relief using drones to residents of a large metropolitan city. The paradigm focuses on the first 48 hours after an earthquake disaster where the affected people's status and needs are analyzed and then the post-earthquake relief system is designed, and the drones deployed. The drones are deployed and controlled from a ground command center.

The related works discussed above use drones to perform different critical environment operations. The execution of the rescue plan is done when a drone is deployed by a person, or in other cases, the drone is programmed to periodically perform surveillance missions of a specific region. However, our work differs in that the drones do not require any human control to respond to a critical situation and only deploy in case an accident is detected. In many occasions, people cannot be relied to deploy the drones in a timely manner, and periodic deployment of drones is costly, wastes resources, and the drones

can easily miss an accident.

For instance, the work proposed by authors in [11] is limited in a number of ways. First, many people may not have the drone activating-app on their phone, second, their phones may not have power. Third, if someone sends GPS signals using a phone, the done will be sent to their location which may not exactly be the place where the critical situation is happening. Fourth, people may intentionally or accidentally send a false distress signal from their phones. Fifth, because of the critical situation, people may forget or may not be able to send the distress signal. The Auto-FRD system is designed in such a way that in the event of a critical situation, the drones automatically deploy at minimum time to the exact location of the accident.

2.5 *Auto-FRD SYSTEM MODEL*

Fig.2.2 describes the system layout of the drone paradigm. This paradigm is composed of three main parts: the command center, intelligent drones, and smart sensors. The proposed system functions as follows, When the smart sensors located in the streets sense a critical situation such as an explosion or fire, they send GPS signals of the location to the drones. The drones which are constantly on standby automatically fly to this location and send live data to the command center or deliver services. The command center works with the police and can also take control of the drones after arriving at the scene. Each of these sections shall be briefly discussed to provide readers with a clear understanding of this model.

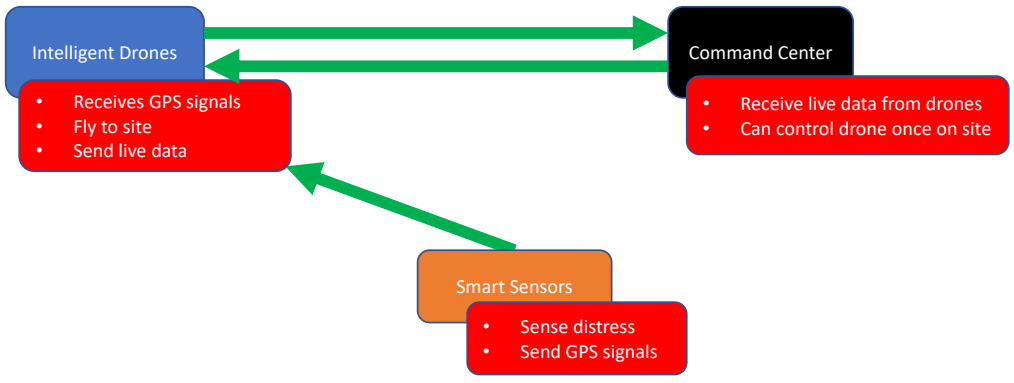

Figure 2.2: System layout of the proposed first response drone-based emergency system.

2.5.1 *Alert signal system*

The Alert signal system comprises of the camera system with the ability to detect a range of critical situations and a signal transmission system used to send an alert message to the drone. In this section, configuration of both parts used in this system shall be discussed.

Sensors and Intelligent camera setup

The intelligent cameras are mounted on locations such streets lights, buildings, and towers as shown in Fig. 2.3 (Currently, there are thousands of cameras around cities, which can easily be integrated with this system).The cameras have a 360 degree vision of the surrounding environment and can accurately detect an accident 3.5km away. The cameras detect the accident and determine the GPS coordinates at the center of the accident. Unusual activity that can be detected by the cameras includes explosions, commotions, fires, and other forms of accidents. The authors in [12] propose an intelligent video-surveillance system with the ability to observe abnormal behavior in crowed areas and set off an alarm system. Additionally, other distress signals can be manually triggered by employees in places such as banks or other business areas in case of an emergency. Fire detectors can also be utilized to deploy drones in case of a fire accident. For example, bush fires can be hard to control. Therefore, Auto-FRDs can be used to get a clear picture of the situation and gather information such as people who need immediate evacuation.

A reliable and inexpensive communication paradigm is critical to the efficient operation of the Auto-FRD system. Therefore, the system will be implemented using long range (LoRa) communication system, which is enabled by low power-wide area network (LP-WAN). Moreover, an ESP32 board shall be used to interface the GPS module with LoRa and other sensors. The details of these hardware devices used are given below.

Figure 2.3: Surveillance intelligent camera system mounted on the streets.

Alert signal transmission using ESP32-LORA system

LoRa is a long-range wireless communication technology promoted by the LoRa Alliance. It uses radio modulation systems to transmit data. The modulation technique used for communication in LoRa allows for long-range transmission of small data packets. This means low bandwidth consumption. The complexity of a LoRa receiver is also reduced considerably due to the similarity of the offset in time and frequency between the sender and receiver [13]. Moreover, there is minimum interference and low power consumption. These qualities equip LoRa for a plethora of applications in a smart environment setting [14]. In addition, LoRa uses unlicensed frequencies that are freely accessible and can be used by anyone.

LoRa's long-range and low power features make it perfect for battery-operated sensors and low-power applications in the internet of things (IoT), Smart home and Machine-to-machine communication. There are two different topologies for LoRa communication paradigm. Point to point communication and LoRa network (using LoRaWAN for exam-

ple) as seen in Fig. 2.4 and 2.5 respectively.

Figure 2.4: Long range device to device communication.

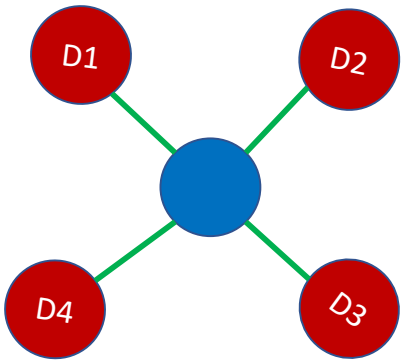

Figure 2.5: Long range wide area network (LoRaWAN) guarantees perfect operation between IoT devices without complex local implementation.

Unlike WiFi or Bluetooth that only support short-distance communication, two LoRa devices with proper antennas can exchange data over a long distance. You can easily configure your ESP32 with a LoRa chip to transmit and receive data reliably at 2-5km in an urban environment and up to 45km diameter in rural areas[14].

This system supports key IoT requirements such as bi-directional communication, mobility and localization of services. LoRaWAN has gained a lot of popularity among researchers and academicians, especially in this age of IoT where billions of things are connected to each other and power consumption becomes a major concern [15]. Table II highlights comparisons between LoRaWAN and other LPWA communication technologies. As can be observed from the table, LoRaWAN is fairly superior in terms of data rate, battery life, interference immunity, and mobility.

Because of the above mentioned reasons, LoRa technology with ES32-RMF95 modules is used to build the communication system between the intelligent sensors deployed in the streets and the standby drones. This link is used to send alert signals. The algorithm used in the transmitter is depicted in algorithm 1. The algorithm shows that the transmitter sends multiple alert GPS coordinate signals when activated. This is to ensure that the

Table 2.1: LoRaWAN and others LPWAN communication technologies

Feature	LoRaWAN	Sigfox	NB-IoT	LTE-M
Modulation	SS Chirp	GFSK/DBPSK	UNB/GFSK/BPSK	OFDMA
Data Rate	290bps –5ookbps	100bps 12/8bytes Max	100bps 12/8bytes Max	200kbps-1Mbps
Link Budget	154 dB	146 dB	151 dB	146 dB
Battery Lifetime	8 - 10 years	7 - 8 years	7 - 8 years	1 -12 years
Power Efficiency	Very High	Very High	Very High	Medium
Security/Authentication	Yes (32 bits)	Yes (16 bits)	No	Yes (32 bits)
Range	2-5 km urban 15 km suburban 45 km rural	23-10 km urban - 30-50 km rural	1.5 km urban - 20-40 km rural	35km – 2G 200km – 3G 200km – 4G
Interference Immunity	Very High	Low	Low	Medium
Scalability	Yes	Yes	Yes	Yes
Mobility/Localization	Yes	No	Limited.No Loc	Only Mobility

packets have a high delivery rate. The communication system was tested by mounting the receiver on high ground and moving the transmitter to different locations as seen in Fig. 2.6.

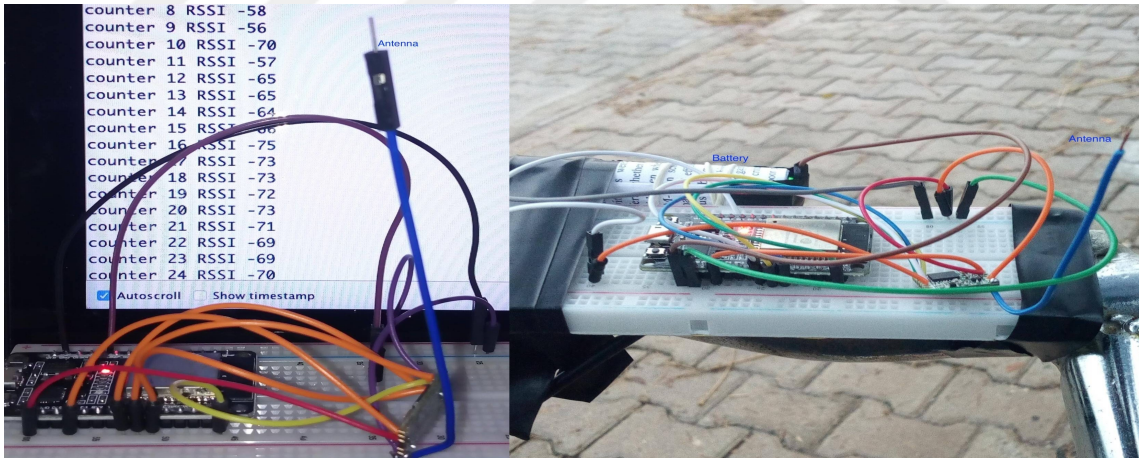

Figure 2.6: Signal receiver (left) depicting the RSSI of the packet and mobile signal transmitter (right) mounted on a bicycle.

Fig. 2.7 shows the different locations where the transmitter was placed. These locations, A through to E, were strategically chosen to measure coverage, as well as RSSI of LoRa on this system under different conditions. Location A has direct LoS, location B has the most dynamic environment due to moving vehicles and location D has the highest

Algorithm 1 GPS Transmitter Pseudo Code

pin declaration: $RXD2, TXD2, ss, rst, di0$;
libraries: $gpd = TinyGPSPlus$;
$counter = 0$;
begin setup
    $Serial.begin(115200)$;
    $Serial2.begin(9600, SERIAL8N1, RXD2, TXD2)$;
    $LoRa.setPins(ss, rst, dio0)$;
    $Initialize\_LoRa\_com\_with\_special\_frq(866E6)$;
    $Declare\_Sync\_word(0-0xFF)$;
end setup
begin loop
while $Serial2.available$ **do**
    $gps = Serial2.read()$;
end while
if $gps.location.isUpdated()$ **then**
    $LoRa.beginPacket()$;
    $LoRa.println(gps.location.lat(), 6)$;
    $LoRa.println(gps.location.lng(), 6)$;
    $LoRa.endPacket()$;
end if
$counter = counter + 1$;
end loop

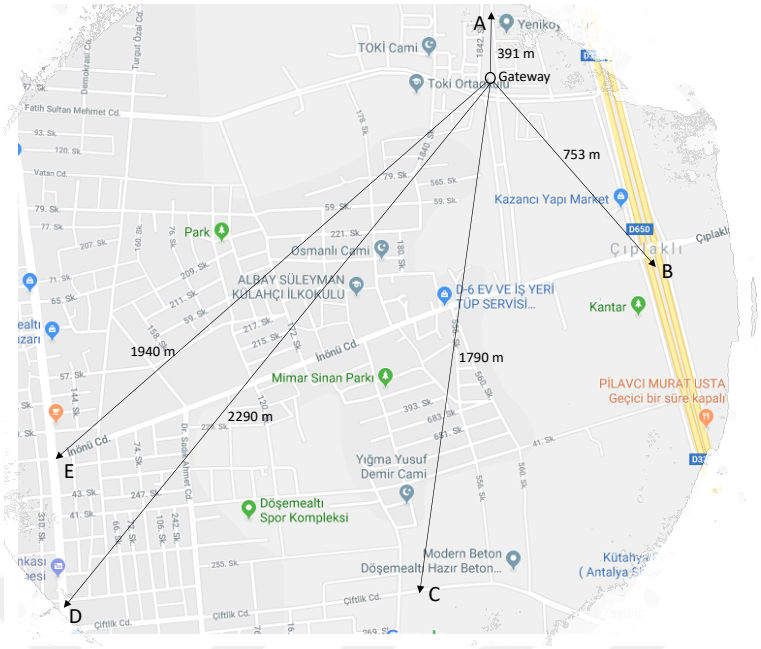

Figure 2.7: Map containing locations used to obtain LoRa RSSI field test data.

interference and distance from the transmitter. RSSI was measured and compared for LoS and NLoS from positions A, C, and E and findings depicted in Fig. 2.8. From the figure, it can be observed that the RSSI for NLoS is weaker than that of LoS. Nevertheless, as the distance increases, the RSSI for both LoS and NLoS converge. Moreover, the rate of received packets was measured from all locations and represented in Fig. 2.9. The figure shows a continued decent in the rate of received packages, with the highest being almost 100% and the lowest 55% at positions A and D respectively. It is determined that communication between the transmitter and receiver in a LoRa system is dependent on the distance and interference encountered by the system. The higher the interference the lower the RSSI. Moreover, the longer the distance, the lower the packet delivery rate.

2.5.2 *Intelligent Drones*

Modern-day technology has allowed for the development of highly intelligent and sophisticated drones. Autonomous drones with the ability to function with minimum human control exist in the market today. For instance, Amazon drones are pre-programmed to fly to the customer and back without human intervention. They are also equipped with

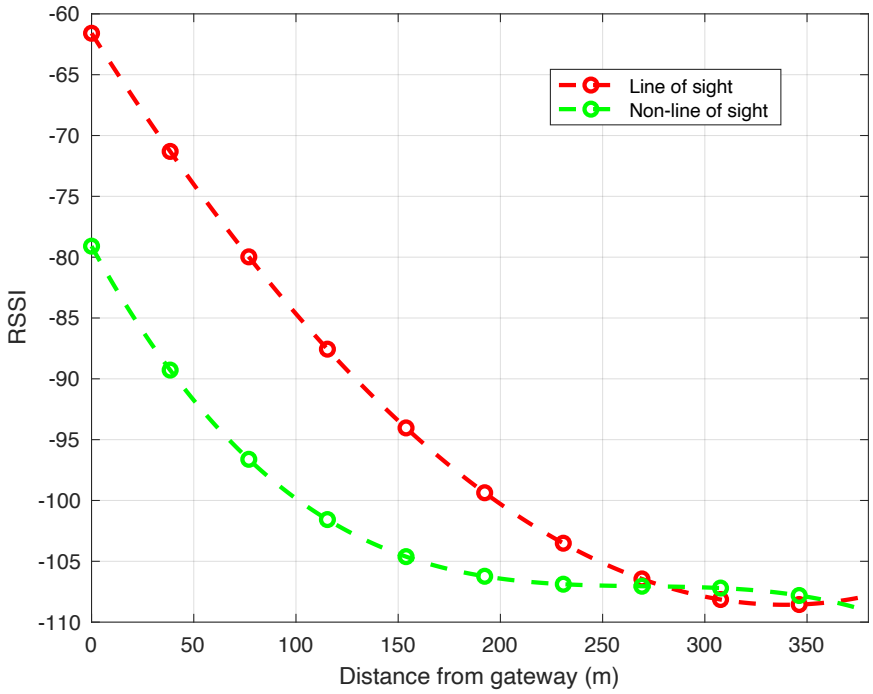

Figure 2.8: RSSI for LoS and NLos as the distance from gateway increases.

anti-collision algorithms, which means that they can avoid colliding with each other or with other objects. Moreover, when the drone loose connection with the control station, they automatically return to a secure location. In this work, the abilities of these intelligent drones are exploited to develop an Auto-FRD system.

Different factors were considered in determining the type of drone to be used in this work. Such aspects include payload, cost, weather, maneuverability, and power consumption. A hexacopter shown in Fig. 2.10 was therefore chosen as a better candidate as it is more stable and can withstand different weather elements compared to other models. Table 2.2 summarises the properties and components of the hexacopter. Components that can be mounted on the drone include optical cameras and high precision sensors (RTK GNSS, accelerator, and gyroscope) for precise data collection (speed, orientation, gravity) as shown in Fig. 2.11. Take-off, path planning and permission to fly procedures will also be discussed in this section.

When a drone located at base station at position (x_0, y_0) receives an alert signal at point (x_e, y_e) which is the location of an emergency, the first thing the drone does is to request permission to fly by sending locations coordinates (x_0, y_0) and (x_e, y_e) to the traffic control

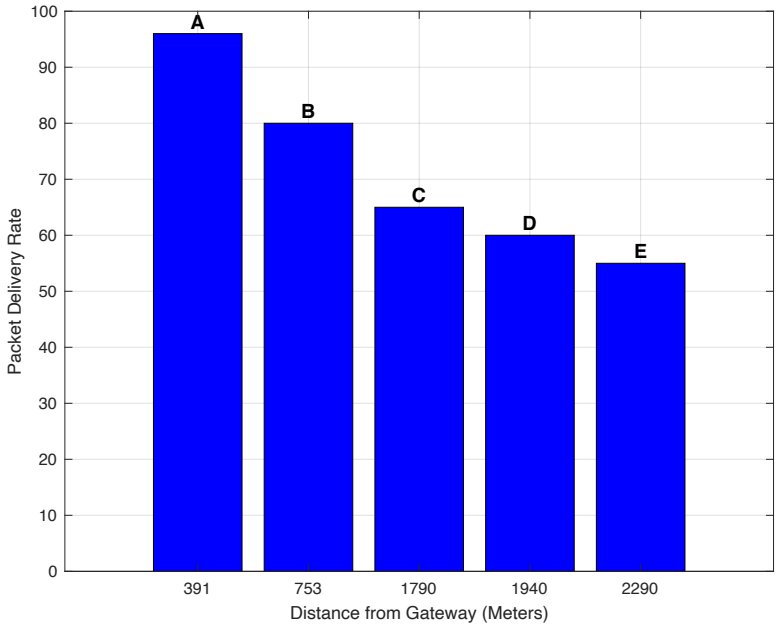

Figure 2.9: The rate of packet delivery as distance between gateway and transmitter increases as well as obstacles.

Table 2.2: Drone properties

Properties and components	Quantity
Take-off mass	8.2 kg
Flying top speed	32 m/s
Endurance	18 mins
flight controller	PixHawk 2 Cube
Dimensions	1250 mm 1250 mm 730 mm

center. After the permission to fly is granted, the drone then takes off to a safe altitude h allowed by the city's drone flying regulations.

From point o = (x_0, y_0, h_o) the path finding algorithm finds the path with the lowest probability of collision to $p_e = (x_e, y_e, h_e)$. The algorithm considers three potential paths used by the drone to arrive at the final destination. From Fig. 2.12, the drone can use path $o - p_e$, $o - o_l - p_e$, or $o - o_r - p_e$.

First, the path finding algorithm calculates a safety coefficient k_{o-pe} of path $o - p_e$. Then, locations o_l and o_r are calculated depending on the location of the accident, by

Figure 2.10: Auto-FRD model.

considering the furthest points with no obstacles from (x_0, y_0, h_o), and the algorithm also allocates a safety coefficient k_{o-ol} and k_{o-or} which determines if the drone will choose point o_l or o_r. The algorithm then calculates the safety coefficient from the chosen point to (x_e, y_e, h_e).

Finally, the algorithm determines the path to be used by the drone by choosing the path with the highest safety coefficient. Algorithm 2 shows the route generating algorithm described above.

2.5.3 *Command Center*

A graphical user interface (GUI) is developed at the command station to allow personnel to control and monitor drone activity while at the scene (see the GUI model in Fig. 2.13). The GUI is divided into two main sections. The first section is used to establish a connection between the on-board computer and the base while the second is used to visualize the on-board sensor readings. The second part is further divided into the following sections:

- Optical sensors: This section displays the live video signal from the HD camera on the drone.
- Autopilot information: This section displays all the information about the drone

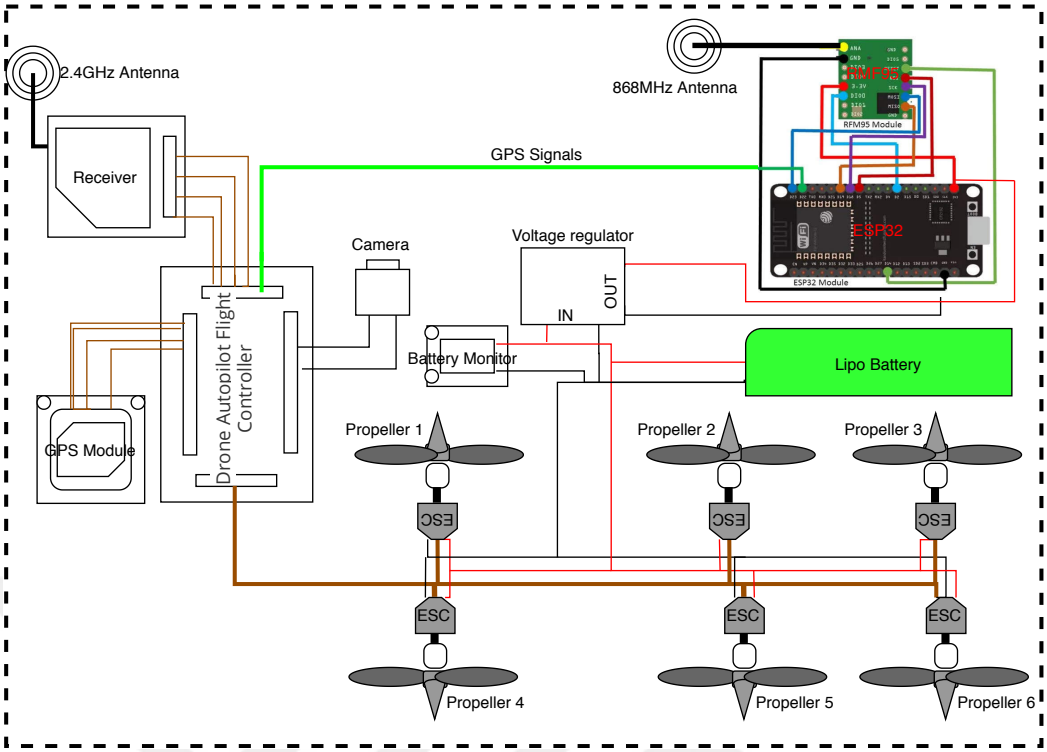

Figure 2.11: Proposed drone paradigm incorporating the GPS receiver for Auto-FRDs.

from the autopilot. Such information include drone speed, altitude, battery life, and other information about the status of the flight.

- Drone position on map: This section shows the location of the drone as well as the path of the drone on a satellite mode map.

As noted by authors in [16], human labor is still required despite the high level of programming in autonomous smart drones. People are required to monitor the flight path of the drones as well as maintain the drones. In this system, the command centers are used for this purpose. Moreover, when the drones arrive at the critical environment scene, they send live signals to the station. The command centers can therefore, collaborate with the police to provide urgent and valuable information about the scene.

2.6 *Auto-FRD CASE STUDY*

The Auto-FRD system is designed to automatically provide fast services to people in need. Therefore, the time used by the proposed system to provide the emergency service

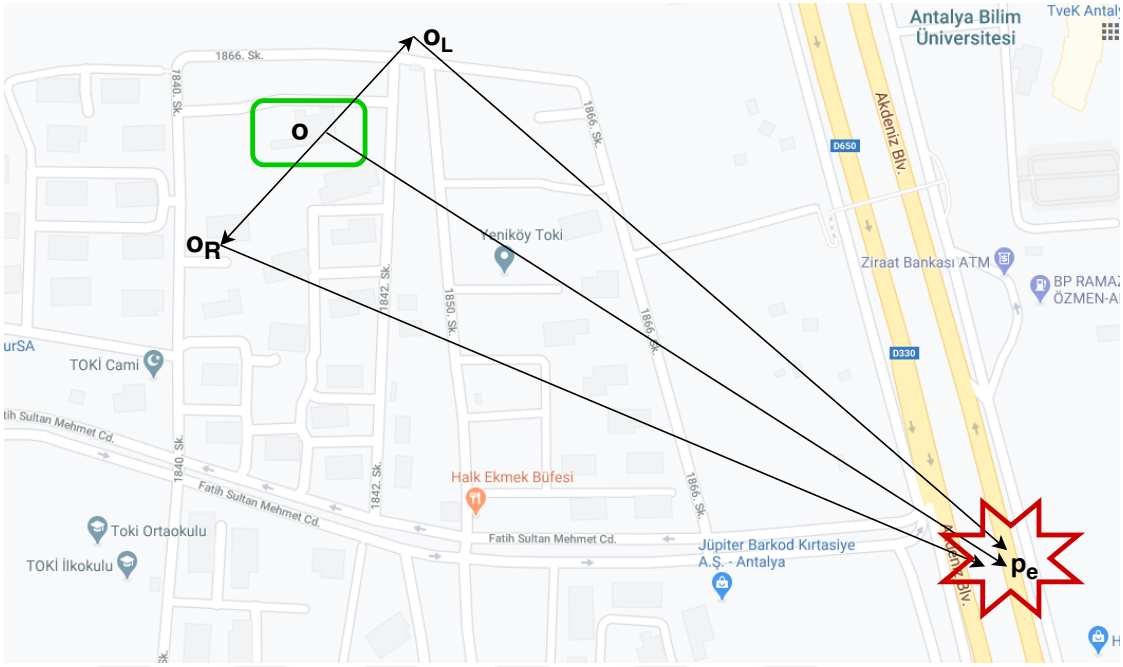

Figure 2.12: Map containing locations used to obtain LoRa RSSI field test data.

must be compared against conventional methods. The speed of a smart drone is mostly dependent on variables such as wind speed and direction, and payload of the drone. In this work, the top speed archived by the designed drone is approximately 32 m/s.

Therefore, for a distress signal 5 km away from the drone deployment base station, the Auto-FRD would take less than 3 minutes to get to the scene. On the other hand, the time used by the police to respond to a distress call is affected by many variables. The day of the week is one variable that affects police response time. The authors in [17] claim that the police workload is higher on Friday and Saturday than any other day of the week. Therefore, they take a longer time to respond to distress calls. Moreover, the time of the day (night-time or day-time), location of the incident (characteristics of the neighborhood), and the type of the incident are also other factors affecting police response time. According to a study done by [17] on the response time by police to a burglary in progress in Texas USA, about 75% of the calls were responded to in less than 5 minutes. Wheres, almost 5% took more than 10 minutes. In this section, a case study of implementing the proposed model in one of the most crowded city in the world, Istanbul in Turkey was done.

Algorithm 2 Route Generating Algorithm.

Inputs: $Drone\_initial\_location, o = (x_0, y_0, h_o)$,
$emergency\_location, p_e = (x_e, y_e, h_e)$
Outputs: $Route\_from\_o\_to\_p_e, rt_f = (x_i, y_i, h_i)$
Define variables: $Safety\_coefficient : k_{o-p}, k_{o-ol}, k_{o-or}$,
$Best\_safety\_coefficient : k_{fin}, Via, location\_o_{RL}, Routs : rt_1, rt_2$
begin setup
    $p_e \leftarrow senceEmergencyLocation()$
    $h \leftarrow setAltitude()$
    $k_{o-p} \leftarrow calculateKop()$
    $k_{o-ol} \leftarrow calculateKool()$
    $k_{o-or} \leftarrow calculateKoor()$
    $k_{fin} \leftarrow calculateKfin(k_{o-p}, k_{o-ol}, k_{o-or})$
    if $k_{fin} == k_{o-p}$ **then**
        $rt_f \leftarrow createFinalRoute(o, p_e)$
    else
        $o_{RL} \leftarrow setViaLocation(k_{fin})$
        $rt_1 \leftarrow createViaRoute(o, o_{RL})$
        $rt_2 \leftarrow createViaRoute(o_{RL}, p_e)$
        $rt_f \leftarrow createFinalViaRoute(rt_1, rt_2)$
    end if
end setup.

Istanbul is the fifth largest Megacity in the world [18]. Spanning over two continents (Europe and Asia), the city holds a population of over 15 million people [18]. As a result, the city is facing problems such as traffic congestion, insecurity, and insufficient fire station to meet the needs of its residents. According to the Istanbul fire department, there are about 70 fire stations currently operating in the city. The stations range from small outposts known as squads, to big main fire centers [19]. Each station covers an area of about $80km^2$. Many fire stations have been developed by the Istanbul metropolitan municipality (IMM) in an effort to provide emergency service to the large population of

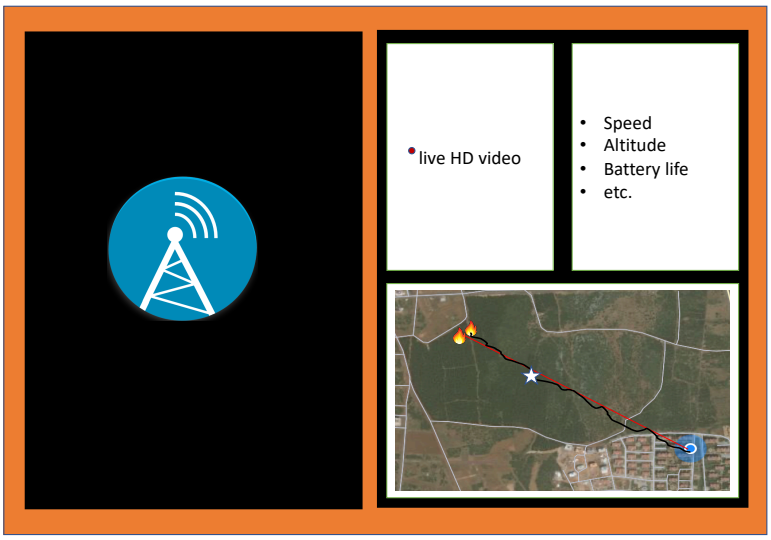

Figure 2.13: GUI to control and observe the drone while in the field.

the city [19]. The average response time is calculated using the equation below.

$$\tau = d/u + x + \delta_t(\mu_t, \alpha_t) + y + \delta_r(\mu_r, \alpha_r), \tag{2.1}$$

where, d is the distance between the fire station and the emergency location, u is the speed of the vehicle. x and y are the average delay caused by the traffic and fire fighters respectively. δ_t is the variation delay caused by road traffic as well as the delay due to the location of the fire accident (Such as narrow pathways). δ_r is the variation delay caused by the personnel when getting ready. δ_t and δ_r are uniform distribution with mean μ and variance α, this is because the exact delay caused by the two events is not constant but varies with $\pm\alpha$. μ_t and α_t are determined by the traffic delay during peak and off-peak hours in the city, while μ_r and α_r are determined by how ready the firefighter personnel are during the emergency call. Using the proposed drone system, δ_t is the effect of air resistance and wind on the drone and δ_r is the time taken to send and receive the permission to fly request.

The average speed of an emergency vehicle is dependent on many factors such as the condition of the road and the driver. In this study, it is assumed that these factors cause negligible delay and that the fire truck is able to maintain an average speed of 17m/s which is the common speed maintained by firetrucks during an emergency [9]. Equation (2.1) is used to compute and compare the emergency response time of both the Auto-FRD system and using the fire truck. Fig. 2.14 depicts the performance of the fire department in

Istanbul compared to the proposed Auto-FRD system. As it can be observed, the proposed system performs better by having a lower response time. In addition, since drones cover a large area in a very short time, only a few base stations are required to cover the city as opposed to having many fire stations and personnel, and hence save money.

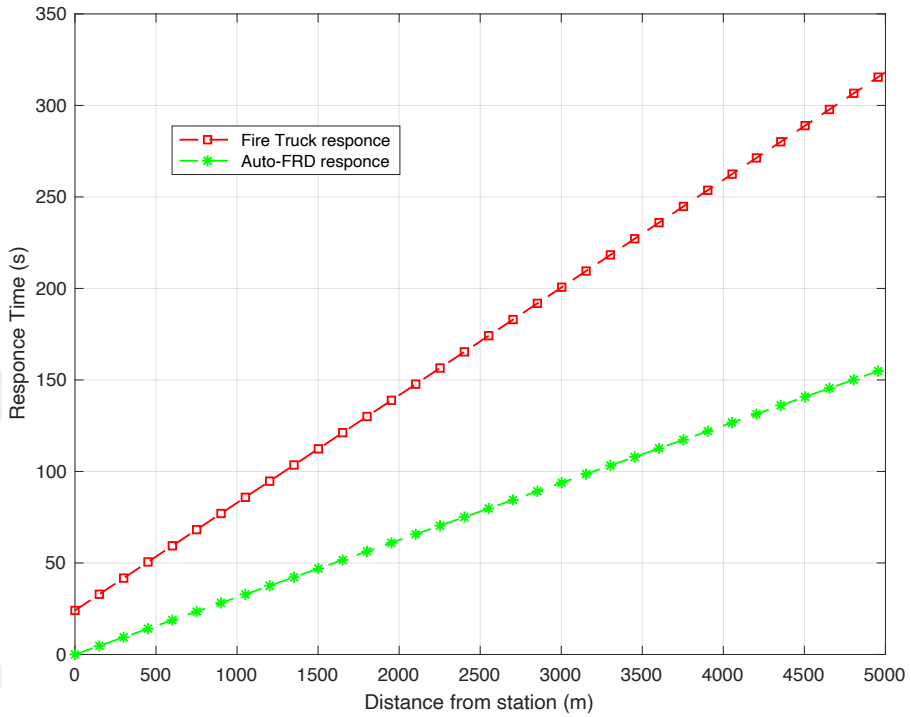

Figure 2.14: Performance of the proposed Auto-FRD system Vs Istanbul Fire Department

Table 2.3 compares the performance metrics of the proposed system with conventional police response system and related drone paradigms like these covered in the related work section (referred here as other drone paradigm). The metrics considered included the monthly cost of implementing and maintaining the system. There are two methods used by the police to reduce response time to a critical situation [20]. The first method is hiring one additional response officer (M1) and the second is the relocation of response stations (M2). From the table, it can be observed that the Auto-FRD system is cheaper compared to other drone response paradigms such as those proposed in [11], [21], and [22], as well as the police emergency response system. The response time is the average time taken for a response service to arrive at the emergency scene.

On average, the police take 4 minutes to respond to an emergency with a 2.66-minute standard deviation [17]. Most other emergency response drones paradigms require people

to deploy them. Therefore, their response time is greater than the proposed Auto-FRD system but less than the conventional police methods. Reliability metric measures if the system delivers when called upon. Police response systems are limited by many factors such as traffic jam, police ethics (ie. some police may choose to ignore an emergency call), and availability of personnel, hence they may not always deliver. On the other hand, systems that use drones are more reliable as they have fewer limitations and are more likely to respond. Complexity is the amount of effort needed to request an emergency service. For the police system, a person is required to make a phone call and request a service. For other drone systems, a person is required to press an alarm signal[11]. However, in the proposed Auto-FRD system, people are not required to do anything, and hence it has the lowest complexity compared to other systems.

Table 2.3: Performance metrics of the proposed system compared to other emergency situation response systems.

Measurement Metric	Auto-FRD System	Police System	Other drone systems (eg. [13])
Cost	$\approx 300.00\$$	M1 $\approx 5082\$$ M2 $\approx 41,078.44\$$	$\approx 8,870.00\$$
Response Time (s)	≈ 180	≈ 525	180¡time¡525
Reliability	High	Medium	High
Complexity	Low	Medium	High
False alarm Rate	Low	High	Medium
Accuracy of information obtained	High	Medium	High
Volume of Information obtained	High	Low	Medium
Automation	Fully	None	Semi

False alarm rate is the measure of false requests for an emergency. As noted by [23], the emergency police response unit receives a high number of false calls which cost time, money and put lives in danger. These calls are deliberately made with criminal motives such as crime concealment, revenge, or terror. Other drone systems where people press emergency signals can be used in the same way as making a false emergency call to

the police, moreover, one must acquire the application to send the signal in addition to having a phone. On the other hand, Since the proposed system uses smart sensors to send a distress signal, the rate of error observation is low compared to the other methods. Nevertheless, If the sensors are not trained well to identify emergency situations, a false signal may be sent. However, this mistake can easily be rectified by using well-trained sensors.

The accuracy of information obtained measures how well the data obtained can reflect the exact emergency situation. Using drones provide video and picture evidence, as opposed to obtaining a descriptive account of the situation by the witnesses which is what happens in many police response systems. Volume of information obtained measures the amount of information collected about the critical event. This is greatly affected by the response time because the lower the response time, the more an emergency can be observed and obtain accurate and more data. The automation metric shows the response system's human dependence. Most police response systems have limited or no automation. Also, many emergency drone systems require some form of human interaction before they are deployed. However, the proposed Auto-FRD system is fully automated during an emergency response situation. According to the performance metrics considered in Table 2.3, the proposed paradigm is better than other emergency response systems.

2.7 *SECTION SUMMERY*

This section showed that using Autonomous First Response Drones-based smart rescue system for critical situation management is a novel idea that can be used to save many lives by significantly reducing emergency response time. In addition, the paradigm is inexpensive and reliable compared to conventional response-time-reduction methods. One of the major concerns consumers have when considering using intelligent drones and intelligent systems in general is security. Therefore, in the next section, we develop a secure communication technique which will guarantee zero information leakage. The technique will be used for secure communication between the Auto-FRD system components.

CHAPTER 3

3. A NOVEL NON-ORTHOGONAL COMMUNICATION TECHNIQUE WITH ENHANCED SECURITY FOR UAVs

In this section, an advanced novel small-scale non-orthogonal communication technique utilizing physical layer security (PLS) for enhanced security and reliability for Auto-FRD communication is proposed. This work is motivated by current challenges faced by conventional non-orthogonal multiple access (NOMA) techniques, for instance, the recent exclusion of power-domain NOMA (PD-NOMA) from 3GPP release 17 due to its performance degradation resulting from channel estimation errors and the utilization of successive interference cancellation (SIC) algorithms at the receiver. The proposed model uses the wireless channel characteristics to eliminate user interference as well as completely degrade the received signal at the eavesdropper's terminal. More specifically, auxiliary signals are precisely designed and superimposed on top of user signals from a dual-transmitter system to provide perfect secrecy against external and internal eavesdroppers, while providing low complexity at the receiver. The efficiency and novelty of the proposed system are presented via mathematical analysis and validated by Monte Carlo simulations. Results obtained indicate that the proposed model achieves less complex, secure, and more efficient communication, suitable for low power consumption and limited processing applications.

3.1 *SECTION INTRODUCTION*

Internet of things (IoT) is a network of millions of interconnected wireless devices accessible through the internet [24]. The idea of IoT was made possible by advanced wireless communication technology (5G and beyond). This is due to the many advantages such as increased data rate, reduced delay, and enhanced cellular coverage in the communication technologies over preceding technologies [25]. These advantages will have a huge impact on future service delivery. Some areas influenced by IoT are smart drones, autonomous driving, healthcare, entertainments, industrial appliances, smart cities, smart

energy grids, sports, and remote surgery [26]. Therefore, countries around the world are employing IoT technologies to combat challenges such as traffic congestion, insecurity, and infrastructure management caused by overpopulation. The information shared by these devices is sensitive, hence, it is critical that the communication system used by IoT devices is secure in order to protect confidential information and operations [24].

Due to its unique properties, non-orthogonal multiple access (NOMA) communication technique has received tremendous attention in the current 5G and future 6G technologies [1]. These properties include high spectral efficiency, low latency, improved coverage, and massive connectivity [1]. Nevertheless, NOMA has various security limitations that must be addressed. Firstly, an external eavesdropper can intercept messages between multiple NOMA users using the same resources simultaneously. Secondly, independent communication between legitimate NOMA users must be secured to prevent internal eavesdropping. Moreover, according to [2], power-domain NOMA is no longer considered as a work item in the 3rd generation partnership project (3GPP) and was excluded in release 17 due to numerous performance degradation issues. For example, it is common knowledge that power-domain NOMA systems utilising successive interference cancellation (SIC) achieves higher connectivity and throughput than orthogonal multiple access (OMA) schemes [27], however, power-sharing among multiple NOMA users causes the degradation of signal-to-interference-plus-noise ratio (SINR) for each user.

Cryptography and physical layer security (PLS) techniques are the two main security techniques used in current communication systems [1] [28] [29] such as NOMA. Nevertheless, according to [1], cryptographic methods are not enough to provide the required security in future communication paradigms due to the following reasons. Firstly, future networks will be made up of decentralized and diverse systems. Therefore, key sharing and management will be an extremely tedious and costly task. Secondly, future communication paradigms will include new technologies such as massive machine-type communications (mMTC) and ultra-reliable low-latency communications (URLLC). These systems are designed for low-power consumption and delay-sensitive applications. Therefore, application of cryptography-based methods on future communication systems will not be feasible. Thirdly, future communication paradigms will be applied to many different areas with varied levels of security. However, according to [30], encryption-based

techniques can only provide binary-level security. Additionally, the emergence of quantum computing and supercomputers makes cryptography more vulnerable, as a security breach is just a matter of time [14].

On the other hand, PLS can explore the properties of the channel such as noise, channel randomness, and interference to utterly degrade the received signal at the illegitimate user's terminal [30], hence achieving key-less secure transmission by signal design and signal processing techniques. In PLS, properly designed artificial noise (AN) is superimposed on legitimate users' signal and hence eliminating the need for private key production and management, moreover, it facilitates flexible transmission through the design of adaptive communication protocol [24, 31]. According to [30], PLS is a promising solution to the security threats faced by 5G and future 6G network devices.

There are numerous advantages of using PLS over conventional cryptography methods [30]. Firstly, PLS can utilize a commonly used channel between legitimate users to disrupt the received signal at the eavesdropper's antenna. Hence eliminating the need to share and manage keys. Secondly, most PLS design techniques require simple signal processing methods. This is beneficial to services with limited processing and low power requirements [1]. Finally, according to [32], channel-dependent resource allocation and link adaptation schemes in PLS can be employed to design adaptive security models that are dependent on specific occurrences.

Numerous works in literature have proposed enhancing NOMA security using PLS designs and overcome NOMA security limitations. Authors in [33] propose a PLS design in cognitive radio inspired NOMA network with multiple primary and secondary users. The scheme pairs primary and secondary users according to their channel gain and then power-domain NOMA is used to transmit the signal. According to the authors, secrecy levels can be improved by pairing the primary users with the best channel gains or by reducing the number of secondary users. Additionally, authors in [34] propose a new secrecy beam-forming (SBF) scheme by exploiting the use of artificial noise to protect confidential information of two NOMA users. The paradigm is designed for multiple-input single-output non-orthogonal multiple access (MISO-NOMA) systems such that only the eavesdropper's signal gets degraded. However, the proposed power-domain schemes still

sufferers from SINR degradation.

Also, authors in [2] propose Waveform-Domain NOMA. The paradigm proposes the utilization of multiple waveforms in the same resource element (RE), where relevant waveforms are assigned to each user and then decoded at the receiver side. The drawback to this system is that it contains additional processing at the receiver. Which increases power consumption as well as complexity.

A reliable communication system for future wireless communication is expected to be safe and secure from all kinds of threats. There are two types of eavesdroppers that a communication paradigm must be secured against, external and internal eavesdroppers. An internal eavesdropper is a legitimate user who illegally acquires information from other users, while an external eavesdropper is not in the authorised users' set. Moreover, an eavesdropper can be passive or active [1]. An active eavesdropper is one who has the channel state information (CSI) available at the receiver, while a passive eavesdropper does not have the CSI available at the receiver. Internal eavesdroppers are generally active while external are passive.

Based on the aforementioned discussion, the need for a new and robust NOMA technique utilizing PLS for enhanced security is recognised. This work proposes small-scale NOMA (SS-NOMA) paradigm, where, auxiliary signal superposition using time diversity is used to enhance communication security and reliability of future low-complexity, massive machine type communication. The main objectives and contribution of the proposed SS-NOMA design utilizing PLS are listed below.

3.1.1 *Novelty and contributions of the proposed algorithm*

The novelty and contributions of the proposed SS-NOMA paradigm are to develop a NOMA scheme with:

1. Low-power consumption.
2. PLS design against internal eavesdroppers

3. PLS design against external eavesdroppers.

4. Two rounds auxiliary-signal-base transmission for two users, which is more complex for eavesdropper decode private information compared to a single user.

5. Low complexity. Conventional NOMA systems use interference cancellation algorithms [1] such as successive interference cancellation (SIC) at the legitimate user's receiver to cancel the interference. However, the proposed algorithm uses specially designed auxiliary signals to automatically cancel the interference. Hence simplifying transmission complexity.

6. Minimum computation. The channel matrices are diagonal, therefore, the inverse operation is simple. Consequently, the auxiliary signal matrices can be designed by simple computation.

7. No power dependent communication for near and far NOMA users.

The remainder of this work is organised as follows: Section II provides a review on NOMA. Section III discusses the overall system model of the proposed system. The algorithm is discussed in detail in section IV. Section V talks about performance analysis. Section VI highlights the simulation results, and finally, the conclusion is presented in section VII.

3.2 *A NOMA REVIEW*

The evolution of multiple access schemes over the last few decades can clearly be observed as 1G, 2G, 3G, and 4G [35]. The respective corresponding multiple access technologies are frequency division multiple access (FDMA), time division multiple access (TDMA), code division multiple access (CDMA), and orthogonal frequency division multiple access (OFDMA) [36]. These multiple access communication technologies were designed for orthogonal multiple access (OMA) where wireless resources are orthogonally allocated to multiple users in time, frequency, and code domain, hence known as OMA communication techniques. Nevertheless, OMA is faced with a number of problems as enumerated below [35].

1. The number of supported users is limited to the number of available orthogonal resources.

2. Despite the different domain techniques (frequency, time, and code), the orthogonality is almost always destroyed by the effects of channel variations. Therefore, orthogonality restoration measures are implemented at the receiver leading to high complexity.

Hence, the challenge for OMA to support massive connectivity, which is a key requirement for 6G technologies persists. Additionally, OMA is unable to meet other critical requirements such as very high spectral efficiency and low latency [13]. NOMA was developed as a technique with the ability to support more users than available orthogonal resources and solve the problems of OMA. The novelty in the design of NOMA is to support non-orthogonal resource allocation but at the expense of increasing the complexity at the receiver where the non-orthogonal user's signal is decoded.

A major milestone was achieved with NOMA technique when 3GPP LTE release 13 approved study item of downlink multi-user superposition technique (MUST) in an effort to standardize NOMA [27]. The main objectives of MUST according to [37][38][39][40][41][42][43] was:

1. To identify possible enhancements accomplished by downlink multiuser communication schemes in a single cell.

2. Investigate potential system-level gain and possible trade-offs between complexity and performance under real-world deployment conditions and traffic models.

3. Identify required standard changes needed to assist user equipment to cancel or suppress cell-to-cell interference.

The study item concluded that NOMA can increase system capacity and enhance user experience, where it is high performing during peak traffic load in the network, compared to sub-band scheduling case, it is more beneficial in user perceived throughput

for wideband scheduling, and also more beneficial in user perceived throughput for cell-edge UEs compared to other UEs [27]. Additionally, LTE Release 14 has released a new work item of downlink MUST for LTE, with a central objective of developing necessary infrastructure to allow LTE to perform cell-to-cell multiuser superposition transmission for the physical downlink shared channel [42]. Moreover, multiple NOMA schemes have been investigated in literature[35][44][45], including power-domain NOMA (PD-NOMA) [46], sparse code multiple access (SCMA) [47], pattern division multiple access (PDMA) [48], resource spread multiple access (RSMA) [49], multi-user shared access (MUSA) [50], interleave-grid multiple access (IGMA) [51], Welch-bound equality spread multiple access (WSMA) [52], and interleave division multiple access (IDMA) [53].

The NOMA schemes mentioned above follow the superposition principle and can generally be placed under PD-NOMA or code-domain NOMA (CD-NOMA). However, since NOMA principle allows multiple user signals to be superimposed on the same resources, this leads to interference and security issues. In the subsequent sections, a novel NOMA inspired communication technique is modeled, the technique utilizes characteristics of the channel to provide perfect security to users as well as cancel interference without any additional processing at the receiver.

3.3 *PROPOSED COMMUNICATION SYSTEM MODEL*

This communication technique can be modeled to serve any number of users. However, the scheme discussed in this work is designed for two users for simplicity purposes, where the system is composed of a dual-transmit antenna and two single-antenna legitimate users. The legitimate transmit antennas are trying to communicate with the users in the presence of a single-antenna eavesdropper as shown in Fig. 3.1. In addition, it is assumed that the transmitter has no knowledge of the passive eavesdropper's channel. In the figure, the channel is indicated by $\mathbf{H_{km}}$. Where $\mathbf{H_{km}}$ is the diagonal channel frequency response of user k during transmission round m. The channels between $antenna-1$ and $antenna-2$ and all the users are assumed to be known at the transmitter and are taken to be slowly varying multi-path Rayleigh fading with the exponentially decaying channel.

Moreover, we employ channel sounding techniques to derive the channel from the transmitter to the receiver. The technique enables the reproduction of the channel using the receiver to transmitter channel in a time division duplexing (TDD) system. The proposed paradigm utilizes dual antennas for transmission, and the transmission is done in rounds. During each round, only one antenna is active, while the other is inactive. The active legitimate antenna wants to communicate to a particular user such that neither the external passive eavesdropper nor the internal active eavesdropper (other user) can decode the information.

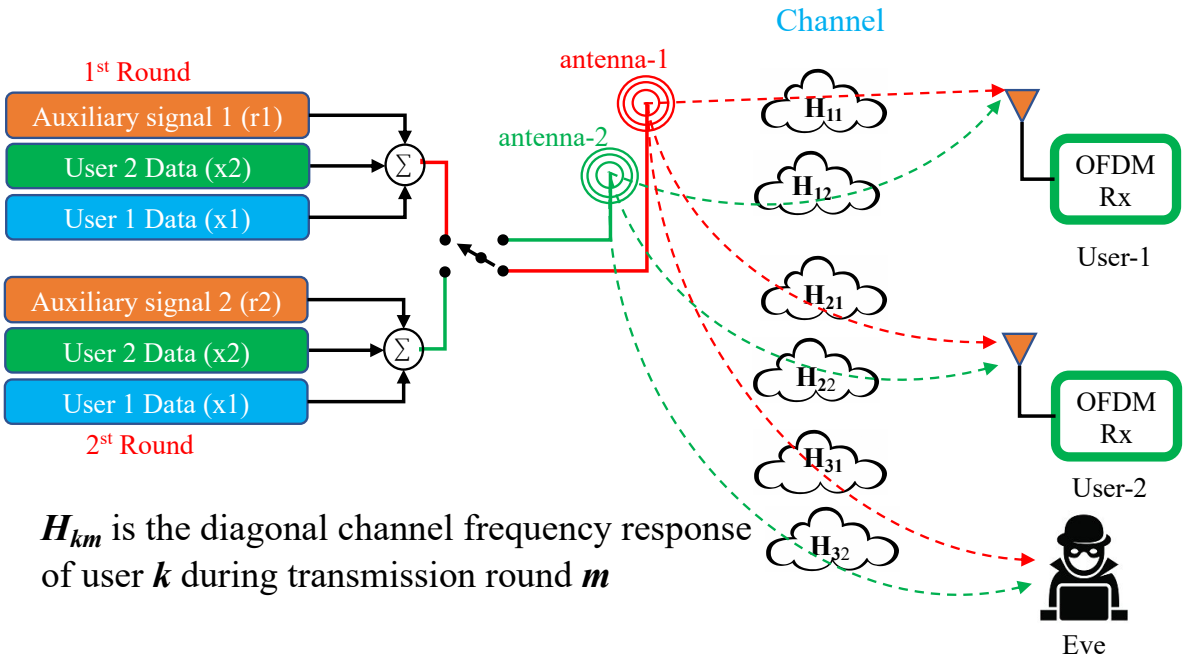

Figure 3.1: Novel small scale NOMA multiple input single output OFDM detailed model.

3.4 *PROPOSED ALGORITHMS*

In this section, we focus on developing the proposed algorithm and justifying the calculations.

3.4.1 *NOMA with auxiliary signal superposition*

This work explores the use of auxiliary signals that are superimposed on user signals to enhance the security and reliability of future applications with limited processing abilities at the receiver [26]. The system is designed such that there are two transmissions from two different antennas. However, only one antenna is active during each transmission round. A superimposed auxiliary signal is calculated and added to the sum of the users' signal during each transmission round. The down-link transmission from two different antennas is to ensure different channels. Consequently enabling the design of the auxiliary signals to guarantee secure and reliable communication against internal and external eavesdroppers. Moreover, communicating with two users during each transmission round make it very complex for the eavesdropper to decode the transmitted information. This is because the designed auxiliary signal is a function of both users' channel. Compared to a single user system, a two-user system will provide perfect secrecy against eavesdroppers while making it easy for legitimate users to decode their respective signals.

The design of the proposed algorithm is as follows: A dual multi-carrier OFDM system with two transmit antennas is used, as shown in Fig. 3.2. Moreover, two single-antenna users and a passive eavesdropper are included in the system. The transmission process consists of two transmission rounds, where only one antenna is active during each transmission round as it can be observed from Fig. 3.1 (i.e, in round 1 $antenna-1$ is active $antenna-2$ is inactive, in round 2 $antenna-2$ is active $antenna-1$ is inactive). Furthermore, it is assumed that both transmission rounds are within the coherence time of the channel. The frequency response of each OFDM symbol for user-1 and user- 2 at $antenna-1$ and $antenna-2$ can be represented as $\mathbf{x_1} = [x_0, x_1, ..., x_{N_f-1}]$ and $\mathbf{x_2} = [x_0, x_1, ..., x_{N_f-1}]$ respectively. Where N_f is the total number of modulated symbols in one OFDM block, and both $\mathbf{x_1}$ and $\mathbf{x_1} \in C^{[N_f \times 1]}$.

Afterward, $\mathbf{x_1}$ and $\mathbf{x_2}$ are converted from serial to parallel and then their sum is added to the designed auxiliary matrix before transmission. The design steps of the auxiliary matrices for the proposed model are outlined in the subsequent discussion.

The signal from the first antenna after superposition to user-1 and user-2 is given as:

$$\mathbf{u_1} = \mathbf{x_1} + \mathbf{x_2} + \mathbf{r_1}. \tag{3.1}$$

Similarly, the signal from the second antenna is given as:

$$\mathbf{u_2} = \mathbf{x_1} + \mathbf{x_2} + \mathbf{r_2}, \tag{3.2}$$

where, $\mathbf{x_1}$ and $\mathbf{x_2}$ are the vector data in frequency domain for user-1 and user-2 respectively. Moreover, $\mathbf{r_1}$ and $\mathbf{r_2}$ are the auxiliary matrices expressly designed using the legitimate users' channel. $\mathbf{r_1}$ and $\mathbf{r_2}$ will make sure that the signal received by user-1 and user-2 is secure from internal and external eavesdropping. In the following subsections, we will explain the details of the received signal at user-1, user-2, and eavesdropper. Afterward, we will explain the design of the auxiliary signals.

Received signal at User-1

The received signal in the frequency domain at user-1 during round-1 using $antenna-1$ can be given as:

$$\mathbf{y_{11}} = \mathbf{H_{11}u_1} + \mathbf{z_{11}}, \tag{3.3}$$

where $\mathbf{H_{11}}$ is the frequency response of the channel and $\mathbf{z_{11}}$ is the additive white gaussian noise (AWGN) between user-1 and $antenna-1$ during round-1. Similarly, the received signal at user-1 during round-2 using $antenna-2$ is given as:

$$\mathbf{y_{12}} = \mathbf{H_{12}u_2} + \mathbf{z_{12}}, \tag{3.4}$$

where $\mathbf{H_{12}}$ is the frequency response of the channel, and $\mathbf{z_{12}}$ is the AWGN between user-1 and $antenna-2$ during round-2. The combined received signal using maximum ratio combining (MRC) from round-1 and round-2 at user-1 can be written as:

$$\hat{\mathbf{y}}_1 = \mathbf{H_{11}^H y_{11}} + \mathbf{H_{12}^H y_{12}}, \tag{3.5}$$

where $\mathbf{y_{11}}$ is the received signals at user-1 during round-1 through $antenna-1$ and $\mathbf{y_{12}}$ is the received signals at user-1 round-2 through antenna-2. $(\cdot)^H$ denotes the Hermitian

transposition. After substituting the values of $\mathbf{y_{11}}$ and $\mathbf{y_{12}}$ in (3.5), the combined signal is written as follows:

$$\hat{\mathbf{y}}_\mathbf{1} = |\mathbf{H_{11}}|^2\mathbf{u_1} + \mathbf{H_{11}^H}\mathbf{z_{11}} + |\mathbf{H_{12}}|^2\mathbf{u_2} + \mathbf{H_{12}^H}\mathbf{z_{12}}, \tag{3.6}$$

where $\mathbf{u_1}$ and $\mathbf{u_2}$ are the superimposed transmitted signals during the first and second round. After substituting the values of $\mathbf{u_1}$ and $\mathbf{u_2}$ in (3.6), the combined signal is:

$$\hat{\mathbf{y}}_\mathbf{1} = |\mathbf{H_{11}}|^2(\mathbf{x_1} + \mathbf{x_2} + \mathbf{r_1}) + \mathbf{H_{11}^H}\mathbf{z_{11}} + |\mathbf{H_{12}}|^2(\mathbf{x_1} + \mathbf{x_2} + \mathbf{r_2}) + \mathbf{H_{12}^H}\mathbf{z_{12}}. \tag{3.7}$$

Rearranging (3.7) and collecting like terms gives us:

$$\begin{aligned}\hat{\mathbf{y}}_\mathbf{1} = {} & (|\mathbf{H_{11}}|^2 + |\mathbf{H_{12}}|^2)\mathbf{x_1} + (|\mathbf{H_{11}}|^2 + |\mathbf{H_{12}}|^2)\mathbf{x_2} + |\mathbf{H_{11}}|^2\mathbf{r_1} + |\mathbf{H_{12}}|^2\mathbf{r_2} + \\ & \mathbf{H_{11}^H}\mathbf{z_{11}} + \mathbf{H_{12}^H}\mathbf{z_{12}}.\end{aligned} \tag{3.8}$$

The first term in (3.8) is the desired term with respect to user-1, while the remaining terms are undesired. The added auxiliary signals will ensure that the undesired terms, as well as the channel effects, are removed and canceled at user-1.

Received signal at User-2

Similar to user-1, the received signal in the frequency domain at user-2 during round-1 using $antenna - 1$ is given as:

$$\mathbf{y_{21}} = \mathbf{H_{21}}\mathbf{u_1} + \mathbf{z_{21}}, \tag{3.9}$$

where $\mathbf{H_{21}}$ is the frequency response of the channel and $\mathbf{z_{21}}$ is the AWGN between user-2 and $antenna - 1$ during round-1. Likewise, the received signal at user-2 during round-2 using $antenna - 2$ is given as:

$$\mathbf{y_{22}} = \mathbf{H_{22}}\mathbf{u_2} + \mathbf{z_{22}}, \tag{3.10}$$

where $\mathbf{H_{22}}$ is the frequency response of the channel, and $\mathbf{z_{22}}$ is the AWGN between user-2 and $antenna - 2$ during round-2. The combined received signal by using MRC from round-1 and round-2 at user-2 is:

$$\hat{\mathbf{y}}_\mathbf{2} = \mathbf{H_{21}^H}\mathbf{y_{21}} + \mathbf{H_{22}^H}\mathbf{y_{22}}, \tag{3.11}$$

where $\mathbf{y_{21}}$ is the received signal at user-2 during round-1 from $antenna-1$ and $\mathbf{y_{22}}$ is the received signal at user-2 during round-2 from antenna-2. After substituting the values of $\mathbf{y_{21}}$ and $\mathbf{y_{22}}$ into (3.11), the combined signal is presented as follows:

$$\hat{\mathbf{y}}_2 = |\mathbf{H_{21}}|^2\mathbf{u_1} + \mathbf{H_{21}^H z_{21}} + |\mathbf{H_{22}}|^2\mathbf{u_2} + \mathbf{H_{22}^H z_{22}}, \tag{3.12}$$

where $\mathbf{u_1}$ and $\mathbf{u_2}$ are the superimposed transmitted signals during the first and second round. Substituting the values of $\mathbf{u_1}$ and $\mathbf{u_2}$ into (3.12) results in the combined signal shown below.

$$\hat{\mathbf{y}}_2 = |\mathbf{H_{21}}|^2(\mathbf{x_1}+\mathbf{x_2}+\mathbf{r_1}) + \mathbf{H_{21}^H z_{21}} + |\mathbf{H_{22}}|^2(\mathbf{x_1}+\mathbf{x_2}+\mathbf{r_2}) + \mathbf{H_{22}^H z_{22}}. \tag{3.13}$$

Rearranging (3.13) and collecting like terms gives us:

$$\hat{\mathbf{y}}_2 = (|\mathbf{H_{21}}|^2 + |\mathbf{H_{22}}|^2)\mathbf{x_1} + (|\mathbf{H_{21}}|^2 + |\mathbf{H_{22}}|^2)\mathbf{x_2} + |\mathbf{H_{21}}|^2\mathbf{r_1} + |\mathbf{H_{22}}|^2\mathbf{r_2} + \mathbf{H_{21}^H z_{21}} + \mathbf{H_{22}^H z_{22}}, \tag{3.14}$$

The second term in (3.14) is the desired term with respect to user-2 while the remaining terms are undesired. Likewise, the added auxiliary signals will make sure that the undesired terms, as well as the channel effects, are removed and canceled at user-2.

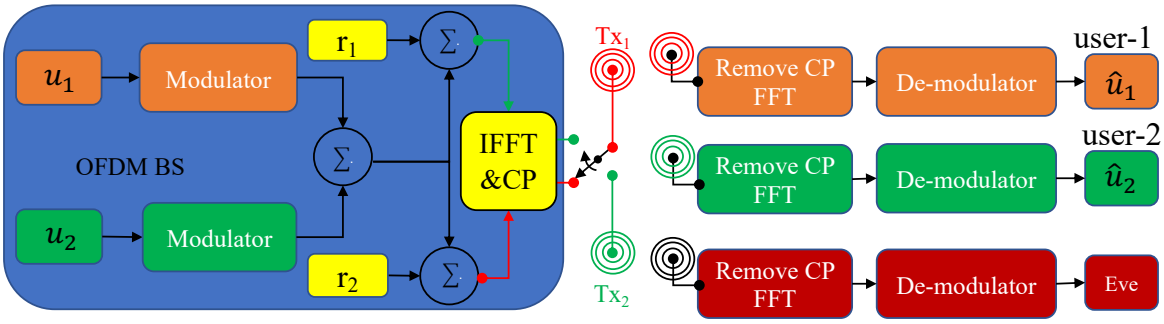

Figure 3.2: Dual multi-carrier OFDM system with two transmit antenna.

Received signal at Eavesdropper

For the case of the eavesdropper (Eve), the combined received signal from round-1 and round-2 is:

$$\hat{\mathbf{y}}_3 = \mathbf{H_{31}^H y_{31}} + \mathbf{H_{32}^H y_{32}}, \tag{3.15}$$

where $\mathbf{y_{31}} = \mathbf{H_{31}u_1} + \mathbf{z_{31}}$ and $\mathbf{y_{32}} = \mathbf{H_{32}u_2} + \mathbf{z_{32}}$ are the received signal at the eavesdropper during round-1 and round-2 from $antenna-1$ and antenna-2, respectively, where $\mathbf{H_{31}}$ and $\mathbf{z_{31}}$ are the frequency response of the channel and AWGN between the eavesdropper and $antenna-1$ during round-1 while $\mathbf{H_{32}}$ and $\mathbf{z_{32}}$ are the frequency response of the channel and AWGN between the eavesdropper and $antenna-2$ during round-2. Substituting the values of $\mathbf{y_{31}}$ and $\mathbf{y_{32}}$ into (3.15) results in the following equation:

$$\hat{\mathbf{y}}_3 = |\mathbf{H_{31}}|^2\mathbf{u_1} + \mathbf{H_{31}^H z_{31}} + |\mathbf{H_{32}}|^2\mathbf{u_2} + \mathbf{H_{32}^H z_{32}}, \tag{3.16}$$

where $\mathbf{u_1}$ and $\mathbf{u_2}$ are the superimposed transmitted signals during the first and second round. After substituting the values of $\mathbf{u_1}$ and $\mathbf{u_2}$ into (3.16) we get:

$$\hat{\mathbf{y}}_3 = |\mathbf{H_{31}}|^2(\mathbf{x_1} + \mathbf{x_2} + \mathbf{r_1}) + \mathbf{H_{31}^H z_{31}} + |\mathbf{H_{32}}|^2(\mathbf{x_1} + \mathbf{x_2} + \mathbf{r_2}) + \mathbf{H_{32}^H z_{32}}. \tag{3.17}$$

Rearranging (3.17) and collecting like terms gives us:

$$\hat{\mathbf{y}}_3 = (|\mathbf{H_{31}}|^2 + |\mathbf{H_{32}}|^2)\mathbf{x_1} + (|\mathbf{H_{31}}|^2 + |\mathbf{H_{32}}|^2)\mathbf{x_2} + |\mathbf{H_{31}}|^2\mathbf{r_1} + |\mathbf{H_{32}}|^2\mathbf{r_2} + \mathbf{H_{31}^H z_{31}} + \mathbf{H_{32}^H z_{32}}. \tag{3.18}$$

The eavesdropper will try to get information from both user-1 and user-2. Therefore, for Eve, both terms of equation (3.18) are desirable. However, as shown in (3.18) it is extremely difficult for Eve to cancel the interference it gets from users' signals as well as that coming from auxiliary signals. Therefore, it is impossible for Eve to decode the signal for user-1 or user-2. The derivation of the values of the auxiliary signals, $\mathbf{r_1}$ and $\mathbf{r_2}$, is explained in the subsequent section.

Designing the superimposed auxiliary signals for the proposed algorithm

In this section, we will design the auxiliary signals $\mathbf{r_1}$ and $\mathbf{r_2}$ such that the combined signal sent during round-1 and round-2 is received at the intended user with no extra computations at the receiver while providing meaningful and reliable information as well as protecting the user from internal and external eavesdroppers.

Auxiliary signals $\mathbf{r_1}$ and $\mathbf{r_2}$ are designed as follows: As illustrated in (3.8), the first term is the desired term for user-1. Therefore, the auxiliary signals $\mathbf{r_1}$ and $\mathbf{r_2}$ will be designed such that the effect of the channels on user-1 is removed as well as the interference

by user-2 on user-1. Hence, the second, third, and fourth term in (3.8) should be equated to zero as follows:

$$(|\mathbf{H_{11}}|^2 + |\mathbf{H_{12}}|^2)\mathbf{x_2} + |\mathbf{H_{11}}|^2\mathbf{r_1} + |\mathbf{H_{12}}|^2\mathbf{r_2} = 0. \tag{3.19}$$

Similarly, looking at (3.14), the second term of (3.14) is the desired term for user-2. Therefore, the auxiliary signals $\mathbf{r_1}$ and $\mathbf{r_2}$ will be designed such that the effect of the channels on user-2 is removed as well as the interference by user-1 on user-2. Hence, the first, third, and fourth term in (3.14) should be equal to zero and can be shown as:

$$(|\mathbf{H_{21}}|^2 + |\mathbf{H_{22}}|^2)\mathbf{x_1} + |\mathbf{H_{21}}|^2\mathbf{r_1} + |\mathbf{H_{22}}|^2\mathbf{r_2} = 0. \tag{3.20}$$

Equations(3.19) and (3.20) can jointly be solved to determine the values of auxiliary signals $\mathbf{r_1}$ and $\mathbf{r_2}$ as follows:

$$\mathbf{r_2} = \frac{(|\mathbf{H_{11}}|^2(|\mathbf{H_{21}}|^2 + |\mathbf{H_{22}}|^2)\mathbf{x_1} - |\mathbf{H_{21}}|^2(|\mathbf{H_{11}}|^2 + |\mathbf{H_{12}}|^2)\mathbf{x_2}}{|\mathbf{H_{12}}|^2|\mathbf{H_{21}}|^2 - |\mathbf{H_{11}}|^2|\mathbf{H_{22}}|^2}, \tag{3.21}$$

$$\mathbf{r_1} = \frac{-(|\mathbf{H_{21}}|^2 + |\mathbf{H_{22}}|^2)\mathbf{x_1} - |\mathbf{H_{22}}|^2\mathbf{r_2}}{|\mathbf{H_{21}}|^2}. \tag{3.22}$$

Using the auxiliary signals, $\mathbf{r_1}$ and $\mathbf{r_2}$ shown in (3.21) and (3.22), signals for user-1 and user-2 during round-1 and round-2 are send from the transmitters as shown in Fig. 3.1. The auxiliary signals will guarantee complete secrecy against internal and external eavesdroppers.

3.5 *ALGORITHM'S PERFORMANCE ANALYSIS APPROACH*

In this section, we will outline the approach used to analyse the performance of the system. We will start by discussing performance at the two legitimate users' terminals (User-1 and User-2), then discuss the performance at the eavesdropper's terminal.

3.5.1 *Legitimate users (User-1,User-2)*

In order to conduct a performance analysis on the legitimate users, we will use numerical data fitting methods, similar to that used in [26]. To determine the BER at each

legitimate user's terminal, we must calculate the instantaneous signal-to-noise ratio γ_b at each user's node. The auxiliary signals $\mathbf{r_1}$ and $\mathbf{r_2}$ depicted in (3.21) and (3.22) respectively are designed to protect each user from inter-user interference as well as from the effects of the channel. According to [26], the distribution of the power of sub-channels corresponding to the received signal for each user must be determined so that γ_b can be calculated using numerical data fitting method. Fig. 3.3 shows the power distribution of sub-channels corresponding to the received signal at the legitimate user. As it can be observed, the fitted distribution follows Weibull distribution with scale and shape parameters of $\omega = 1.53$ and $\mu = 2.08$ respectively.

Analytical data fitting method proposed in [26] is used to compute the theoretical BER of the proposed NOMA schemes. The statistics of the effective instantaneous signal-to-noise ratio (SNR), γ_b is first calculated for the legitimate user utilizing each scheme. The probability density function for the effective instantaneous SNR is calculated as:

$$P_{\gamma b}(\gamma_b) \approx \left(\frac{1}{\omega}\right)^{\mu} \frac{1}{\Gamma(\mu)} \frac{\Omega^{\frac{3}{2}}\sqrt{\gamma_b}}{\hat{\gamma}_b^{\frac{3}{2}}} exp\left(-\frac{1}{\omega}\frac{\omega\gamma_b}{\hat{\gamma}_b}\right), \tag{3.23}$$

where Ω, $\hat{\gamma}_b$, and $\Gamma(\mu)$ are the mean squire of the sub-channels, average SNR, and the gamma function respectively. $P_{\gamma b}(\gamma_b)$ can then be used to calculate the BER.

$$BER_b = \frac{1}{2}\int_0^{\infty} erfc(\sqrt{\gamma_b}) P_{\gamma_b}(\gamma_b) d\gamma_b. \tag{3.24}$$

After substituting $P_{\gamma b}(\gamma_b)$ in (3.24) with (3.23) we get the equation below:

$$BER_b = \frac{1}{2}\int_0^{\infty} erfc(\sqrt{\gamma_b}) \left(\frac{1}{\omega}\right)^{\mu} \frac{1}{\Gamma(\mu)} \frac{\Omega^{\frac{3}{2}}\sqrt{\gamma_b}}{\hat{\gamma}_b^{\frac{3}{2}}} exp\left(-\frac{1}{\omega}\frac{\omega\gamma_b}{\hat{\gamma}_b}\right) d\gamma_b. \tag{3.25}$$

According to [47] when (3.25) is simplified we get the equation below:

$$BER_b \approx \frac{\left(\frac{1}{\omega}\right)^{\mu} \frac{1}{\Gamma(\mu)} \frac{\Omega^{\frac{3}{2}}}{\hat{\gamma}_b^{\frac{3}{2}}}}{2\sqrt{\pi}} \left(\frac{arctan\left(\sqrt{\frac{1}{\omega}\frac{\omega}{\hat{\gamma}_b}}\right)}{2\frac{1}{\omega}\frac{\omega}{\hat{\gamma}_b}^{3/2}} - \frac{1}{2\frac{1}{\omega}\frac{\omega}{\hat{\gamma}_b}\left(1+\frac{1}{\omega}\frac{\Omega}{\hat{\gamma}_b}\right)}\right), \tag{3.26}$$

where, $arctan(\cdot)$ denotes the inverse tangent.

3.5.2 *Eavesdropper (Eve)*

Analysing the case for the eavesdropper, from equation (3.18) we observe that the eavesdropper is interested in information from both user-1 and user-2. The signal to

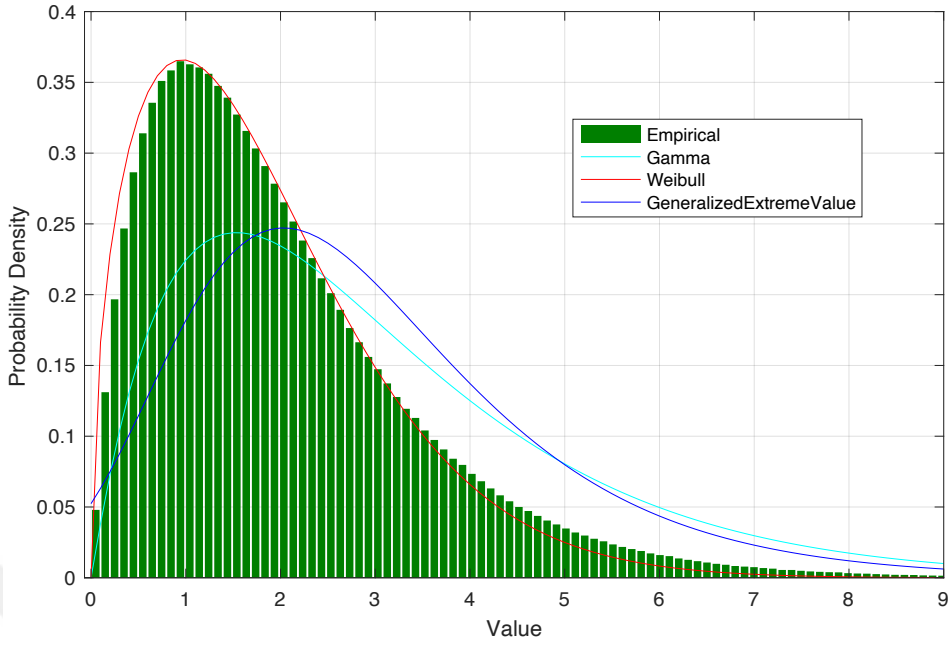

Figure 3.3: Power distribution of sub-channels corresponding to the received signal at legitimate user (Bob)

interference at the eavesdropper's terminal for listening to the signal deliberated for user-1 is given as:

$$SINR_{e1} = \frac{(|\mathbf{H_{31}}|^2 + |\mathbf{H_{32}}|^2)|\mathbf{x_1}|^2}{(|\mathbf{H_{31}}|^2 + |\mathbf{H_{32}}|^2)|\mathbf{x_2}|^2 + |\mathbf{H_{31}}|^2\mathbf{r_1} + |\mathbf{H_{32}}|^2\mathbf{r_2} + \sigma_{\mathbf{31}}^{\mathbf{2}} + \sigma_{\mathbf{32}}^{\mathbf{2}}}, \tag{3.27}$$

where $\sigma_{\mathbf{31}}^{\mathbf{2}}$ is the variance of channel noise corresponding to $\mathbf{H_{31}^H z_{31}}$ and $\sigma_{\mathbf{32}}^{\mathbf{2}}$ is the variance of channel noise corresponding to $\mathbf{H_{32}^H z_{32}}$. Likewise, The relevant signal to interference at the eavesdropper's terminal for listening to the signal intended for user-2 is given as:

$$SINR_{e2} = \frac{(|\mathbf{H_{31}}|^2 + |\mathbf{H_{32}}|^2)|\mathbf{x_2}|^2}{(|\mathbf{H_{31}}|^2 + |\mathbf{H_{32}}|^2)|\mathbf{x_1}|^2 + |\mathbf{H_{31}}|^2\mathbf{r_1} + |\mathbf{H_{32}}|^2\mathbf{r_2} + \sigma_{\mathbf{31}}^{\mathbf{2}} + \sigma_{\mathbf{32}}^{\mathbf{2}}}. \tag{3.28}$$

Analysing (3.27) and (3.28), we observe that there is tremendous inter-user interference depicted by the interference at the denominator of the equations. Additionally, $\mathbf{H_{11}}, \mathbf{H_{12}}, \mathbf{H_{21}}$ and $\mathbf{H_{22}}$ which are functions of $\mathbf{r_1}$ and $\mathbf{r_2}$ at the denominator are unknown to the eavesdropper. Consequently, this leads to severe degradation at the eavesdropper while trying to decode secured information intended for both user-1 and user-2.

3.6 *SIMULATION RESULTS*

In this section, we analyse the simulation results of the proposed algorithm using bit error rate (BER), throughput, and packet error rate as performance metrics. The parameters used in this work are depicted in the table below.

Table 3.1: Proposed algorithm system parameters

Channel	Multipath Rayleigh Fading Channel
Channel Length	9
Cyclic Prefix (CP)	9
FFT Size	64
Modulation Type	BPSK

The designed system uses OFDM transmitters Tx_1 and Tx_2 with 64 sub-carries for each user as shown in Fig. 3.2. In addition, a cyclic prefix (CP) of length 9 is used to prevent inter-symbol interference (ISI). The channel between the transmitters Tx_1 and Tx_2, and receivers, user-1, user-2, and Eve, is assumed to be multi-path Rayleigh fading channel with equal number of taps $(L = 9)$ as shown in table 3.1.

Fig. 3.4 depicts the BER verses SNR graph for users utilizing the proposed algorithm, single input single output (SISO), and dual single input single output (SISO-dual) systems. From Fig. 3.4, it can be observed that the BER for both legitimate users labeled as user-1 and user-2 are similar. Moreover, the figure also shows the BER performance for internal and external eavesdroppers. Internal eavesdropping is when a legitimate user tries to illegally acquire information that is intended for the other user. For instance, when user-1 try to get information intended for user-2 (depicted as "user-1 listenTo user-2") or when user-2 try to get information intended for user-1 (depicted as "user-2 listenTo user-1"). It can be observed that the performance of both internal eavesdroppers is highly degraded. In addition, the figure also shows the BER performance of an external eavesdropper trying to eavesdrop on information intended for user-1 and user-2, labeled as "Eve listenTo user-1" and "Eve listenTo user-2" respectively. Similarly, we observe tremendous BER degradation due to (3.27) and (3.28).

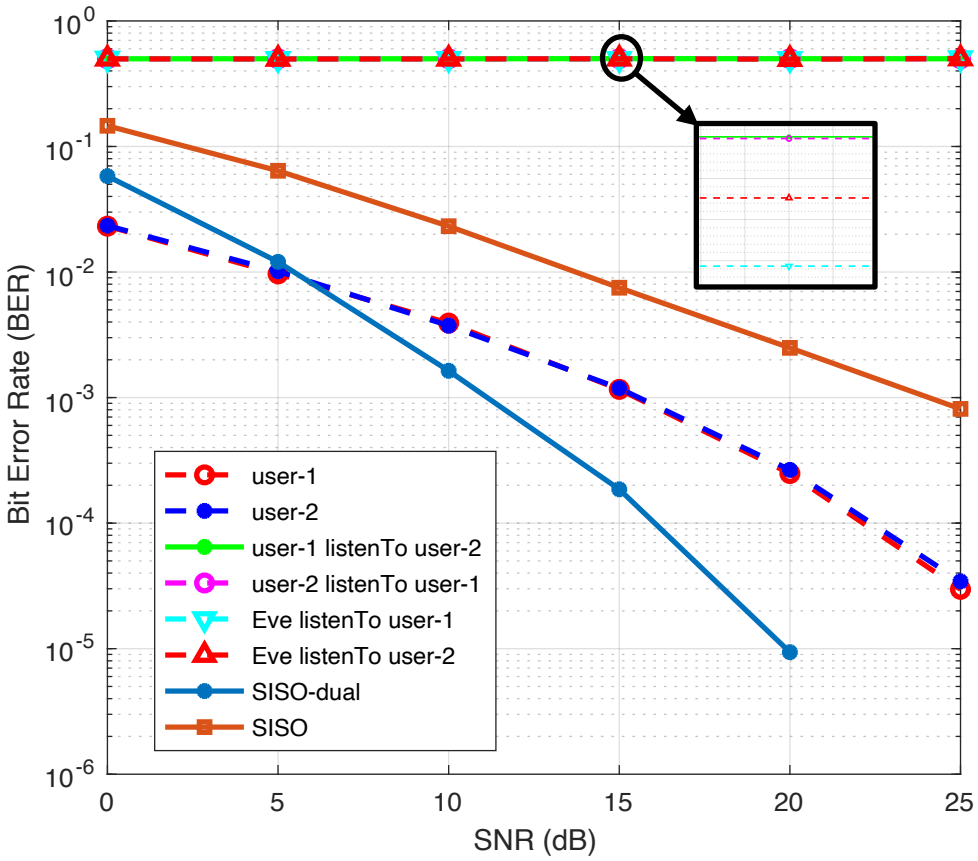

Figure 3.4: BER Vs SNR performance measure for the proposed algorithm

Fig. 3.4 also shows the BER performance of two distinct transmission mechanisms, where users are utilizing SISO with dual transmission (SISO-dual), and users utilizing SISO with single transmission. It can be observed that SISO-dual has better BER performance than SISO. Hence, the proposed system is implemented using dual transmission. Moreover, It can also be observed that users employing SISO-dual have better BER performance compared to the proposed algorithm. Nevertheless, it does not provide secure communication as the proposed scheme. Fig. 3.5 shows the throughput analysis for users utilizing the proposed algorithm, SISO, and SISO-dual systems. From Fig. 3.5, we can observe that the throughput performance for a SISO system performs better than an SISO-dual system. Nevertheless, the independent throughput performance of user-1 and user-2 outperforms the throughput performance for SISO. Moreover, it can be observed from the figure that the throughput performance of the external eavesdropper trying to obtain information intended for user-1 (Eve listenTo user-1) and user-2 (Eve listenTo user-2) is very degraded. Fig. 3.6 shows the packet error rate (PER) of the proposed algo-

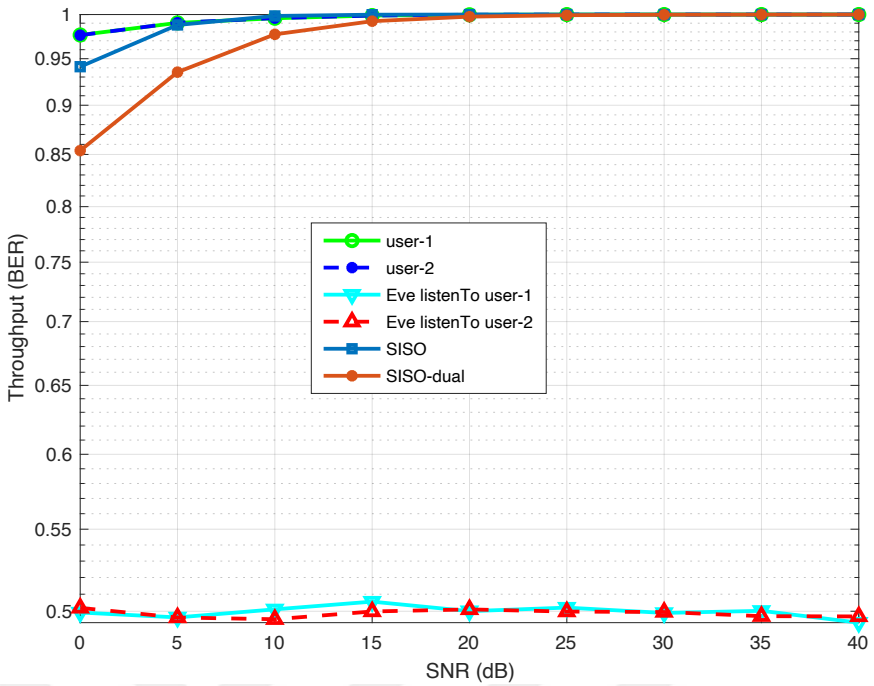

Figure 3.5: Throughput performance measure for the proposed algorithm in comparison with dual-SISO and SISO systems

rithm. From the figure, it can be observed that the PER for both user-1 and user-2 are similar and better than the PER of the eavesdropper. The PER of the eavesdropper trying to eavesdrop on the information of user-1 (Eve listenTo user-1) and user-2 (Eve listenTo user-2) are 1. This further demonstrates the security of the proposed system attained by utilising auxiliary superimposed signals obtained by exploiting the characteristics of the channel as shown in (3.21) and (3.22)

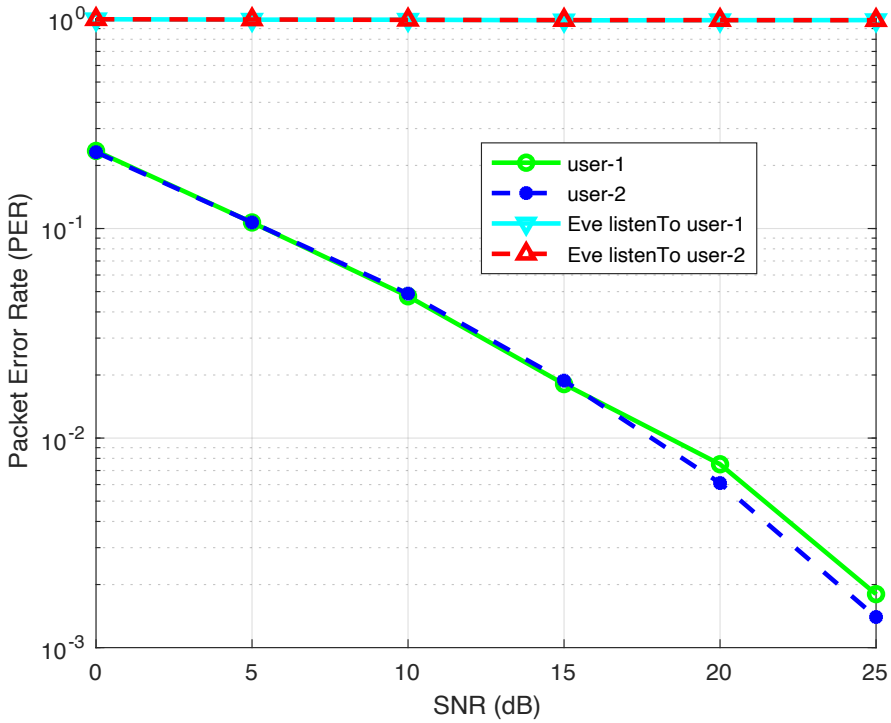

Figure 3.6: Packet error rate of the proposed algorithm.

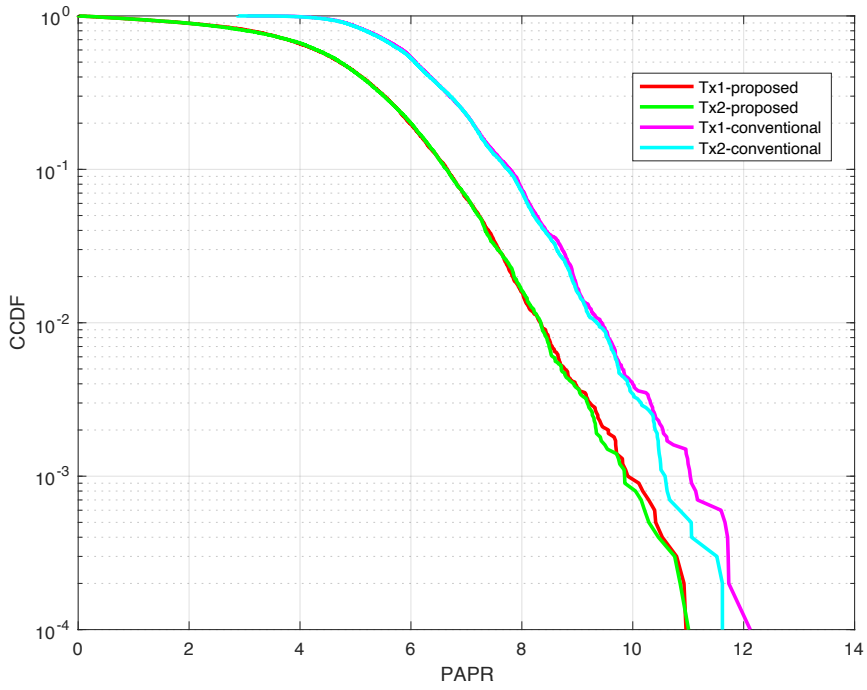

Figure 3.7: Peak to Average Power Ratio (PAPR) of the proposed algorithm.

Fig. 3.7 depicts the peak to average power ratio (PAPR) of a conventional OFDM

system and an OFDM system utilizing the proposed algorithm. Tx1-proposed and Tx2-proposed are the PAPR of the first and second antenna using the proposed NOMA technique, while Tx1-conventional and Tx2-conventional are the PAPR of the first and second antenna using a conventional OFDM system. Fig. 3.7 clearly indicates that users utilizing the proposed algorithm have better PAPR performance than these using conventional OFDM. Hence, the proposed system solves one major problem experienced by OFDM systems [54], by reducing the PAPR leading to better spectral and energy efficiency.

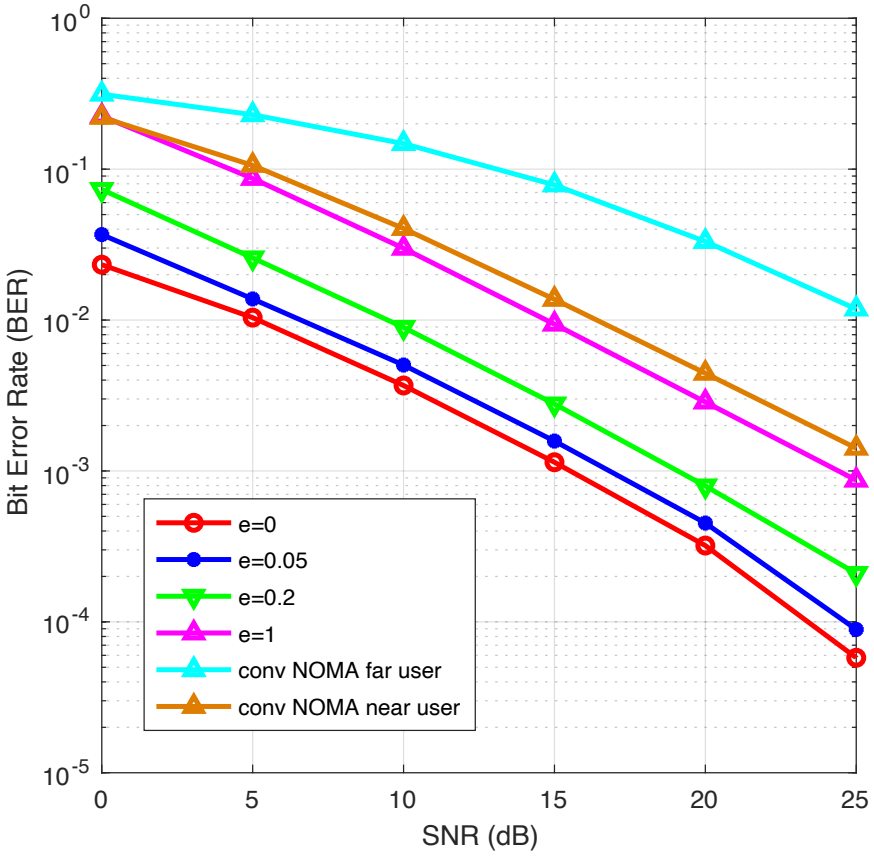

Figure 3.8: Robustness of the proposed algorithm under imperfect channel conditions.

Finally, it is critical to analyse the robustness of the proposed PLS algorithm to an imperfect channel. Therefore, a channel error $\triangle\mathbf{h}$ is injected into the actual channel $\mathbf{H}_{ij}$ based on the values of MSE of a least-square estimator, where i and j are the user number and transmission round respectively, and $i \leq 3$ and $j \leq 2$. The imperfect channel is given as: $\hat{\mathbf{H}}_{ij} = \mathbf{H}_{ij} +$ [55]. $\mathbf{H_{ij}}$ was used to calculate the auxiliary signals as shown in (3.21) and (3.22), but the signal is transmitted through $\hat{\mathbf{H}}_{\mathbf{ij}}$ which is not a similar channel since $\triangle\mathbf{h}$ was added. $\triangle\mathbf{h}$ can be modeled as an independent AWGN with zero mean and variance

σ^2, where $\sigma^2 = e \times 10^{\frac{-SNR_{dB}}{10}}$. e is used to measure the quality of the estimator, the lower the value of e, the higher the quality of the estimator. Hence Fig. 3.8 is drawn to measure the robustness of the proposed system.

Fig. 3.8 depicts the BER versus SNR plot of the proposed paradigm under different qualities of the estimator, that is, e equals to 0, 0.05, 0.2, and 1. Moreover, the figure also shows the BER performance of near and far users utilizing conventional NOMA. It can be observed that there is a slight BER performance degradation as the quality of the estimator degrades. Nevertheless, there is a vast number of algorithms in literature used to enhance the performance of the estimator [55]. Also, it can be enhanced either by increasing the power of the training sequence or by using a pilot with a longer length. Nevertheless, the BER performance of the proposed design with an imperfect channel still outperforms the BER performance of convention NOMA users as can be observed from Fig. 3.8.

3.7 *SECTION SUMMERY*

This work proposes the design of a secure, resilient, effective, and low complexity NOMA communication scheme that can provide zero information leakage to both external and internal eavesdroppers (perfect secrecy) without having the receiver to do any additional processing. The scheme is made up of two transmitters, and transmission is carried out during two transmission rounds. Two distinct channel-dependent auxiliary signals are added to the sum of the transmitted signals of user-1 and user-2, one auxiliary signal during each transmission round such that each legitimate user gets their intended signal after the two transmission rounds, while the eavesdropper gets the much-degraded version of the signal. The paradigm is validated with mathematical models and simulations. The obtained results demonstrate that the proposed system is able to provide reliable and secure communication with minimum complexity than conventional communication techniques. Hence making the proposed model suitable for IoT applications with low complexity and low power requirements. In the future, we intend to model this communication technique for more than two users. In the next section, the optimal placement of drone BSs using heuristic algorithms is discussed.

CHAPTER 4

4. BS OPTIMAL PLACEMENT USING METAHEURISTIC ALGORITHMS

In a given city setting, there are area that are prone to emergency services, such places include market areas, rod intersections, congested streets, residential areas, banks, malls, and more. Therefore, the main question in setting up the proposed drone system will be where to set up drone BSs such that the entire city is able to receive services at any time while minimizing resources and consequently lowering cost. This problem will be exacerbated by the development of future mega-cities that are much bigger than current cities.

In this section, we determine the optimal position and number of drone base stations (BSs) in a given area with the constrains of time, power, and communication range such that the drones are able to reach a given location with minimal resources.

4.1 *OPTIMAL PLACEMENT*

In order to obtain an optimal number of drones to be used in maximizing the area covered, it is imperative that drone BSs are located in the correct position. This is of utmost importance so that the BS obtains maximum coverage while minimizing the number of UAVs and maximizing their operations. This in turn can reduce the cost. Considering the limited sensing and communication sensor range, as well as the restricted resources such as energy and coverage of the UAVs, makes optimization a more complex problem. In their study, Quaritsch et al.[56] investigates the use of UAVs in disaster management. They discuss the challenges facing the networked UAVs as well as focusing on their optimal placement. In doing so, Quaritsch et al. mathematically formulated the coverage problem and presented potential assessment results. Authors took into account two optimization criteria, the first one is the quality of the image taken, which refers to the coverage quality of the UAV. The second one is the consumption of resources, which involves the communication bandwidth and the energy used in flying. The observation area

and the forbidden area are drawn using worldwide coordinates, namely the longitude and latitude. However, as described by Quaritsch et al, the entire process of optimizing sensor placement is done using relative coordinates. Therefore, the first step is to transform the worldwide coordinates into the relative coordinates by selecting an arbitrary origin inside the observed region. Hence formulating the x- and y- axis to go eastwards and northwards respectively as shown in Fig. 4.1.

Figure 4.1: Virtual coordinates inside drone coverage area

Zorbas et al. [57] presents a study that determines the optimal static and dynamic drone positioning in a selected area to minimize cost and maximize coverage. It was shown that drones must have a maximum and a minimum observation altitude. This is because the height of the UAV is directly proportional to the coverage area it can observe. However, the higher the UAV's altitude, the more energy it consumes. Therefore, there must be a threshold on the maximum height/altitude an UAV can be placed at. Park et al. [58] propose a coverage decision algorithm, which aims at solving handover problems caused by time-varying aerial environments. The algorithm takes into account the height of the drone needed to provide a better coverage. Moreover, controlling the height of the drone helps to provide better drone coverage.

The relationship between the targeted area coverage and the height of the drone was

formulated by $A = \pi(R^2 - h^2)$, where A is the coverage area of the drone, h is the drone's height, and R represents the radius of the drone's observation area. The total area A is equal to πR^2 when the height h is equal to 0.

The main focus in [57] and [58], was to minimize the cost, and hence, the number of drones and energy consumed. Accordingly, our assumed UAVs can fly to a maximum height equal to h_{max}, and a minimum height equal to h_{min} that maintains a specific coverage radius r^{hu} [57]. Fig. 4.1 shows a rectangle with length x_{max} and width y_{max} , it represents the area of interest such as a city. Therefore, target critical areas could be in any arbitrary location in an area of $x_{max} * y_{max}$. An assumption can therefore be made that there is a position (x, y, h) that a drone can be located instantaneously. Let **U** denote a set of available drone BSs, and **T** is the set of target locations with high probability of an emergency.

Each location target $t_i \in \mathbf{T}$ has position (X_{t_i}, Y_{t_i}). Drone BSs $u \in \mathbf{U}$ has position (X_u, Y_u, h_u). For $h = 0$, the distance between the target and the drone is:

$$D_{t_i}^{u_x,u_y} = \sqrt{(x_{t_i} - x_u)^2 + (y_{t_i} - y_u)^2} \tag{4.1}$$

Each BS u, has an observation range θ in the area $x_{max} * y_{max}$ in form of a disc where UAVs from the BS can optimally access (see the blue area in Fig. 4.2). Moreover, it has a radius of r^{h_u}, which depends on the height of the BS h_u. The larger the value of h_u, the longer radius r^{h_u}. There are two important decisions that must be made at this point, the first one is to determine the position (X_u, Y_u, h_u) of the BS $u \in U$ (coordinates) and the second one is to find the target areas $t_i \in T$ in the area of interest.

For the first problem (Position of drone):

$$\delta_{xyh}^{u} = \begin{cases} 1, & if\ the\ BS\ u\ is\ located\ at\ (x,y,h) \\ 0, & otherwise \end{cases} \tag{4.2}$$

And for the second problem (Target areas):

$$\gamma_{t_i}^{u} = \begin{cases} 1, & if\ the\ target\ t_i\ is\ in\ the\ range\ of\ BS\ u \\ 0, & otherwise \end{cases} \tag{4.3}$$

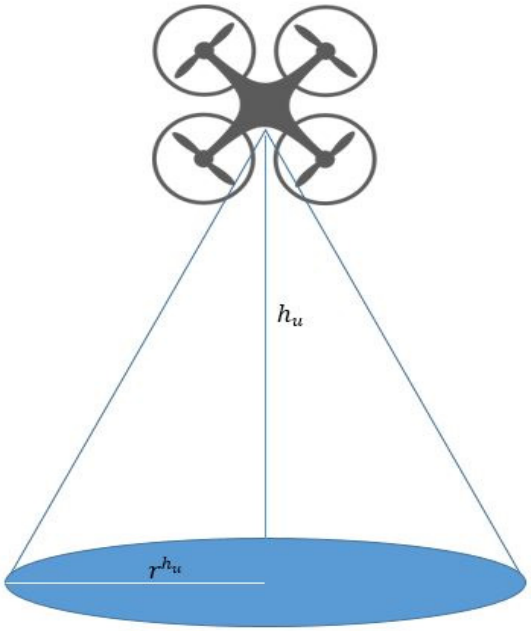

Figure 4.2: BS observation area

The objective is to cover all the target high-risk regions using at least one BS. Each drone consumes a total energy E formulated as:

$$E = (\beta + \alpha h)\, t + P_{max}\,(h/s)\,, \tag{4.4}$$

where β is the minimum power needed to hover at almost zero altitude, α is the motor speed multiplier, P_{max} is the maximum motor power, and s and t are speed and operating time, respectively. Also, h represents the drone's height. The term $P_{max}(h/s)$ is used to show the power used to rise the drone to a height h at speed s . It is worth pointing out here that β and α depend on the weight of the drone and the used motor characteristics. Therefore, we can formulate our placement problem as follows:

Minimize $f(\delta)$

Subject to,

$$\sum_{(x,y,h)} \delta^{u}_{xyh} \leq 1 \; and \; D^{u_x,u_y}_{u'} \leq r^{h_u} \quad \forall u, u' \in U. \tag{4.5}$$

Each BS u can be located in at most one position that is within the communication range of at least one neighbouring BS, where $D^{u_x,u_y}_{u'}$ is the Euclidian distance to the nearest

neighbouring BS u'. A single control center can be used to manage many multiple BS and drones where all the BSs can be used to form a routing path to the control centre.

With the above constrain, we set the value for $\gamma_{t_i}^{u}$ in (4.6). If r^{hu}(radious_range) is less than $D_{t_i}^{u_x,u_y}$(distance) , then $\gamma_{t_i}^{u}$ is equal to 0. In other words, if the target region is outside the observation range of a BS, then the target region cannot be covered by that BS.

$$\gamma_{t_i}^{u} \leq \sum_{(x,y,h)} \delta_{xyh}^{u} \left(\frac{r^{h_u}}{D_{t_i}^{u_{x,u_y}}} \right) \quad \forall u \in U, t_i \in T. \tag{4.6}$$

Therefore, the variable $\gamma_{t_i}^{u}$, can get either the value 0 or 1.

$$\sum_{u \in \mathbf{U}} \gamma_{t_i}^{u} \geq 1 \; t_i \in \mathbf{T}. \tag{4.7}$$

The above constrain ensures there exists at least one BS covering each target. The following equations show the solution space of the aforementioned $\gamma_{t_i}^{u}$ and δ_{xyh}^{u} decision variables.

$$\begin{aligned} \delta_{xyh}^{u} \quad &= \{0,\ 1\}, \quad \forall (x,y,h), 1 \leq x \leq x_{max}, 1 \leq y \leq y_{max}, \\ &\qquad h_{min} \leq h \leq h_{max}, \quad u \in U \end{aligned} \tag{4.8}$$

$$\gamma_{t_i}^{u} = \{0,\ 1\}, \quad \forall t_i \in T, u \in U. \tag{4.9}$$

Hence, $f(\delta)$ to be minimized can be formulated as follows:

$$f(\delta) = A - \sum_{u \in \mathbf{U}} \delta_{xyh}^{u} * A'_i, \tag{4.10}$$

where A is the total area to be covered, and A'_i is the area covered by the i_{th} BS. By integrating (4.10) and (4.4), to minimize the total energy consumed by a UAV, while considering the movement time of the drone, $f(\delta)$ becomes:

$$\begin{aligned} f(\delta) \quad &= \beta \textstyle\sum_{(x,y,h)} \sum_{u \in U} \delta_{xyh}^{u} t + \alpha \sum_{(x,y,h)} \sum_{u \in U} h \delta_{xyh}^{u} t \\ &\quad + \frac{p_{\max}}{s} \textstyle\sum_{(x,y,h)} \sum_{u \in U} h \delta_{xyh}^{u}. \end{aligned} \tag{4.11}$$

Two alternatives to solve the placement problem are proposed. Genetic algorithm (GA) and Simulated Annealing (SA) would be used to calculate the number of drones BSs and their respective position in a given area while maintaining coverage and lifetime constrains in the 3D deployment area.

4.1.1 *SIMULATED ANNEALING (SA)*

In Algorithm 3, SA is used to find the minimum number of drones where line 1 is initializing the aforementioned placement problem parameters. T_0 is the selected initial temperature of the system. This parameter is used to enable the acceptance or rejection of a certain BS placement solutions. The higher the value of T_0 , the higher the probability of accepting a bad solution. Hence, a maximum temperature to T_0 is initially allocated. The temperature of the system is gradually reduced using the cooling factor α, which was selected in this work as 0.95. As the temperature reduces, so does the probability of accepting bad solutions. In line 1, the initial solution δ_0 is also initialized, which is heuristically selected for better results. Moreover, m is representing the number of stages and n is the count of moves per stage with a certain temperature in SA algorithm. The number of moves allows for the exploration of the neighbourhood for possible solutions (i.e., UAVs' locations). Therefore, it is important that this value is carefully chosen. Line 2 assigns the initial solution to δ and to the final solution δ_F. It assigns also the initial temperature to the current temperature T_1. Line 3 – 17 iterates over the initialized number of stages, where the temperature value is decremented after every stage. Lines 4 – 15 iterates over the number of moves at a given stage, where the neighbouring solutions is explored under a constant temperature. In line 5, a neighbouring solution is found using the move operator $\sigma(\delta)$, where $\sigma(\delta) = \delta + N(0,1)$. This solution is assigned to a temporary solution δ_{Temp}. Line 6 checks if the temporary BS placement solution is better than the current one. To achieve this, both the temporary and the current solution are substituted to the fitness function shown in (4.10). Line 7 assigns the temporary solution to the current solution, if the condition in line 6 is satisfied. Line 8 to 10 covers an "Else if" statement. Line 8 uses the current temperature T_t, which represents the temporary solution and the current solution to find an exponential value. The value is compared with a random number (between 0 and 1 exclusive) to determine whether the temporary bad solution shall be accepted or rejected. Line 9 assigns the temporary solution to the current solution if the condition in line 8 is true. Line 10 ends the "Else if" statement. Line 11 – 13 represents another "If" statement. Line 11 checks if the current drone BS placement solution is better than the final solution using the fitness function. Line 12 assigns the current solution to the final one if the condition in line 11 is true. Line 13 ends

Algorithm 3 Simulated Annealing Pseudo Code

Initialize: $T_0, \delta_0, \alpha, m, n$
$\delta = X_0, \delta_F = X_0, T_1 = T_0$
for $i = 1 : m$ **do**
  for $j = 1 : n$ **do**
    $\delta_{Temp} = \sigma(\delta)$
    if $f(\delta_{Temp}) \leq f(\delta)$ **then**
      $\delta = \delta_{Temp}$
    else if $U(0,1) \leq e^{-\frac{f(\delta_{Temp}) - f(\delta)}{T_t}}$ **then**
      $\delta = \delta_{Temp}$
    end if
    if $f(\delta) \leq f(\delta_F)$ **then**
      $\delta_F = \delta$
    end if
  end for
  $T_{t+1} = \alpha \cdot T_t$
end for
Return : δ_F

the “If” statement while line 14 ends the second “for” loop. Line 15 computes the next stage temperature of the system T_{t+1} using the cooling factor. Line 16 ends the first “for” loop and finally line 17 returns the selected final solution δ_F after all iterations have been completed.

4.1.2 *GENETIC ALGORITHM (GA)*

In Algorithm 4, GA is applied on the same problem to find the minimum number of drone BSs and their optimal positions for the maximum coverage. The aforementioned parameters are initialized in line 1. PS is the population size, which represents the count of the initial solutions to be selected. G_{max} is the maximum generation number for which an optimal solution is obtained. PC and PM are the probability of crossover and probability of mutation, respectively. These parameters are selected in order to evolve from one generation to the next. In line 2, the initial solution is generated in accordance with PS. This solution is represented by the set of 0’s and 1’s. In line 3, the fitness of all initial solutions are computed, and in line 4, the solution with the best fitness value is selected. Lines 5 – 10 iterate over a specific generation number, while line 6 – 13 iterates for a number of times equal to half of the population size.

Iterations over half the population size are done because at every generation two parents are selected for the crossover operation. In line 7, two parents are selected, then in line 8, two children are produced by applying the crossover operation. In line 9, the produced children are mutated using a probability equal to PM. In this case, each element in each solution is considered. In line 10, the second “for” loop is terminated. In line 11, all the parents are replaced with the newly produced children, forming the next generation of the evolved drone BSs placement solutions. In line 12, the best-found solution (BFS) are updated by substituting the newly produced solutions in the fitness function (i.e., (4.10)) so that the best solution can be found. This solution is compared with the previous BFS, if it is better, the BFS is updated. In line 13, the first “for” loop is ended, and in line 14, the BFS is returned.

Algorithm 4 Genetic Algorithm Pseudo Code

Initialize: PS, G_{max}, PC, PM

$\delta = (\delta^{u}_{x\,yh})^{+} : Generate - initial - random - solutions$

$f(\delta) : Calculate - fitness - for - random - solutions$

$Select - BFS$

for $g = 1 : G_{max}$ **do**

  for $i = 1 : PS/2$ **do**

    $Select - two - parents$

    $Crossover - with - PC$

    $Mutate - with - PM$

  end for

  $Replace - parent - with - children$

  $Update - BSF$

end for

Return : BSF

4.1.3 *RESULTS AND DISCUSSIONS*

In this section, an in-depth analysis of the simulated results is presented. MATLAB and Python software were used to execute the SA and GA algorithms. An area of 80 kilometres squared (km^2) was selected to be observed, with each BS having a coverage area of 10 km^2 squared. For Simulated Annealing, initialization was done as follows, an initial temperature of 300 was chosen, and an initial solution in terms 0s and 1s was chosen (1 indicating the presence of a drone in that vertex, 0 indicating its absence). The movement operator (α) in SA was set to be equal to 0.95, while m and n were set as 500 and 200 respectively. Additionally, initialization for GA was done as follows: a population size of 8 was selected, stopping criteria (i.e. (G_{max})) was 50, PC (Probability of Crossover) of 0.5 and PM (Probability of Mutation) was chosen as 1.

In Figures 4.3 to 4.5, the number of BSs required for a randomly generated count of targets on the ground are shown. Fig. shows three targets that need to be covered. It can be observed that these targets have been located far away from each other. Therefore, one BS is not enough to cover all of them, hence three BSs have been used in order to cover

all targets. In Fig. 4.4 and 4.5, the randomly distributed number of targets are increased to 10 and 22 respectively. It can be observed that the optimal number of drones required for this configuration increases to six in both figures. Accordingly, it can be concluded that if the number of targets is equal to x, then the required number of drones to cover all targets can range from 1 to x. For example, if two targets are out of the coverage range of a single BS, then two BS are needed to cover all targets. However, if the two targets are within the range of a single BS, then only one drone is needed. Therefore, it can be conclude that the configuration (distribution) of the targets in the covered area has a key influence on the minimum number of BSs required to cover these targets.

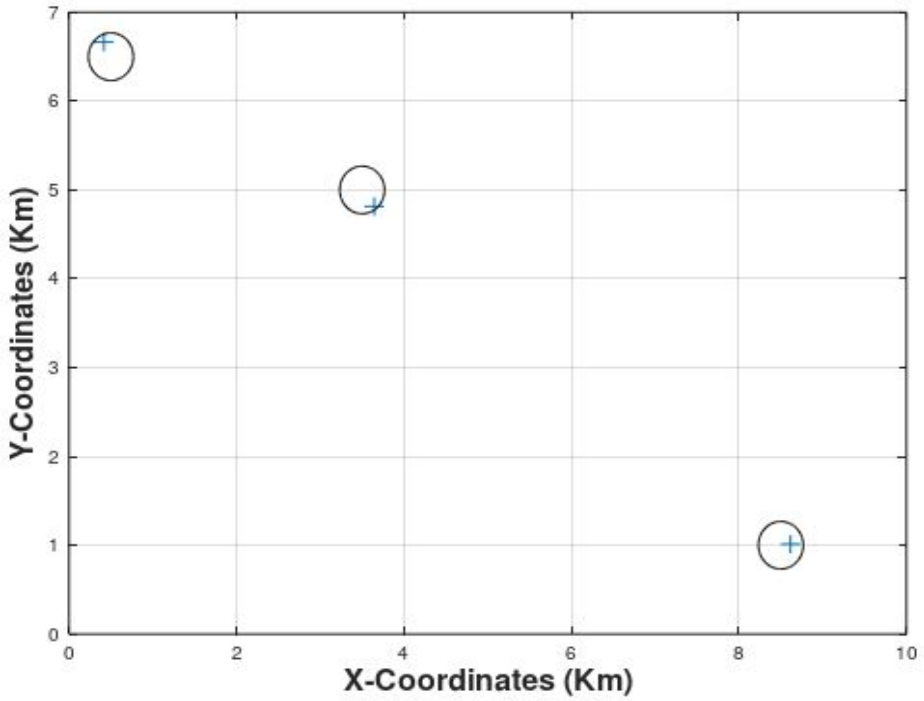

Figure 4.3: Three targets to cover

Fig. 4.6 and Fig. 4.7 shows the average execution time and fitness value over 100 runs for both SA and GA respectively. The relative precision stopping criterion is used. Simulation runs are stopped at the first checkpoint when the condition $\delta \leq \delta_{\max}$ is met, where $\delta_{\max}$, which can have a value between 0 and 1, is the maximum acceptable value of the relative precision for confidence intervals at the $100(1-\alpha)\%$ significance level. All obtained results from the simulations are within the confidence interval of 5% with a confidence level of 95%. Thus, both default values for α and δ are set to 0.05. This

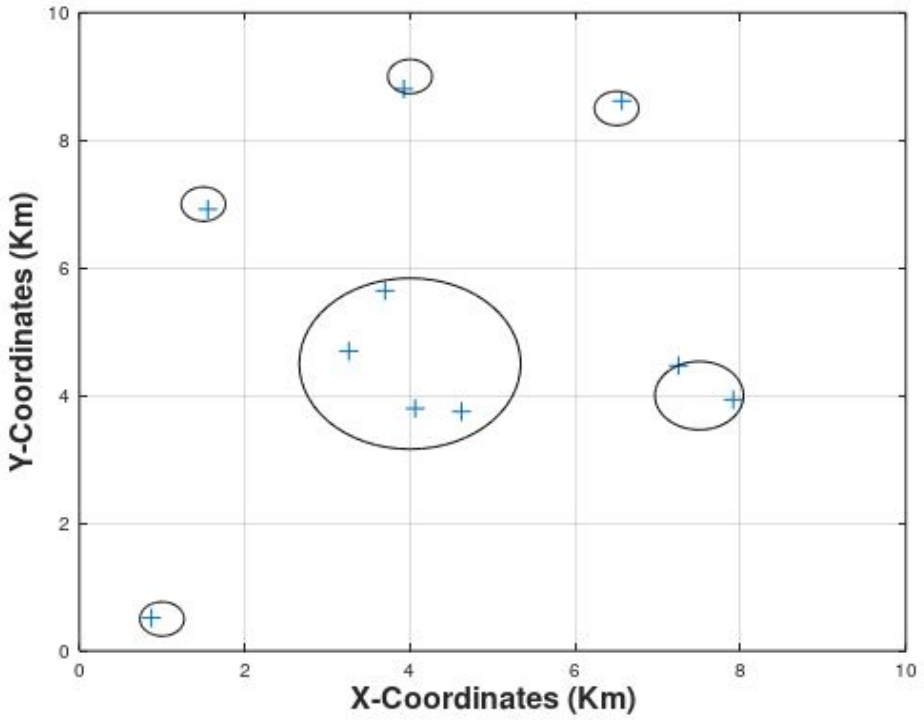

Figure 4.4: Ten targets to cover

can help in assessing the evolutionary convergence for algorithms. Fig. 4.6 below shows the execution time for both SA and GA with a varied coverage area. In this setup, the area covered by each BS is held constant, while the total area of interest is increased from 20 to 80 (km^2). It can be observe that the execution time for both algorithms lie between approximately 0.29 seconds and 1.2 seconds, with SA recording the fastest and GA recording the slowest time. From the obtained graph it can also be seen that SA records the fastest time until the total area of interest is equal to 44 (km^2), where both algorithms have the same execution time. However, when the coverage area is increased further, the execution time for SA slows drastically, while that of GA also slows but not as fast as that of SA. Consequently, GA realizes a faster execution time than SA for a coverage area greater than 44 (km^2).

Therefore, it can clearly be concluded that SA is capable of generating relevant solutions faster than GA when the coverage area is small. However, for larger areas to be covered by the BSs, it is efficient to use GA as its time to generate optimal solutions is much shorter than SA.

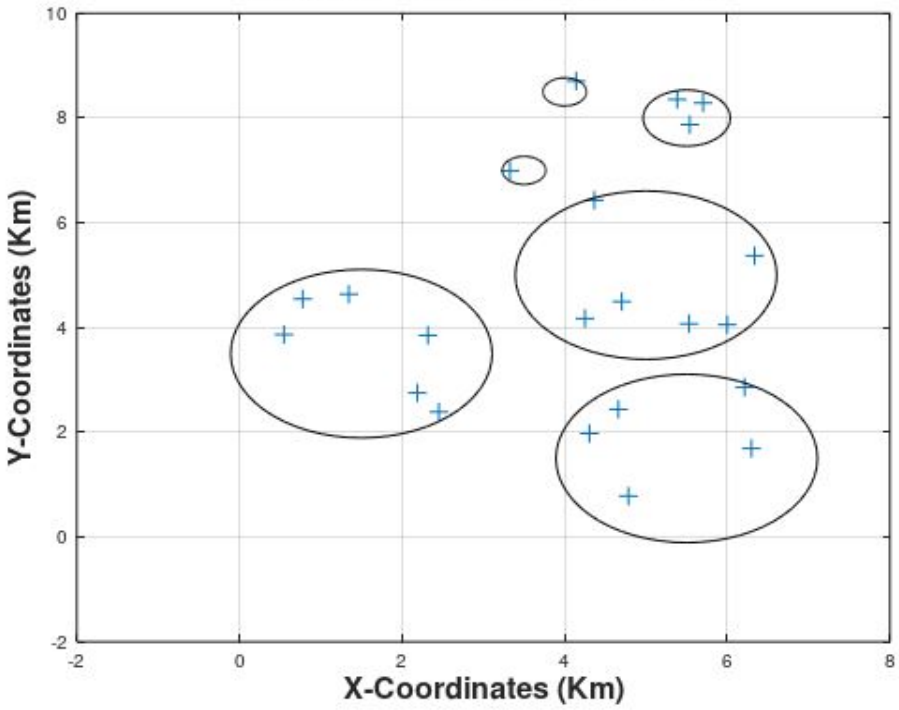

Figure 4.5: 22 targets to cover

In Fig. 4.7, both algorithms are analyzed on how they produce optimal solutions by tracking the fitness functions against the number of iterations. From the figure, it can be observed that GA consistently produces a better fitness function output than the previous one until the fifth iteration, where a slight deterioration is observed. However, the general form of the GA function depicts that the parent selection and replacement method used in our algorithm produced optimal solutions in each iteration. On the other hand, it can be observed that SA is more unpredictable in comparison to GA. This instability can be attributed to the nature of SA algorithm in finding the optimal value. That is why SA requires more computation power in comparison to GA as reported in [59], where the major drawback of SA is its slow convergence towards an optimal value [60]. This appears clearly in Fig. 4.7, where SA algorithm experiences more local optimal values than GA. Hence, it is more likely to get stuck on a local optimal value in SA than in GA. The figure therefore suggests that there is a better probability to get the global optimal value when GA is applied rather than SA.

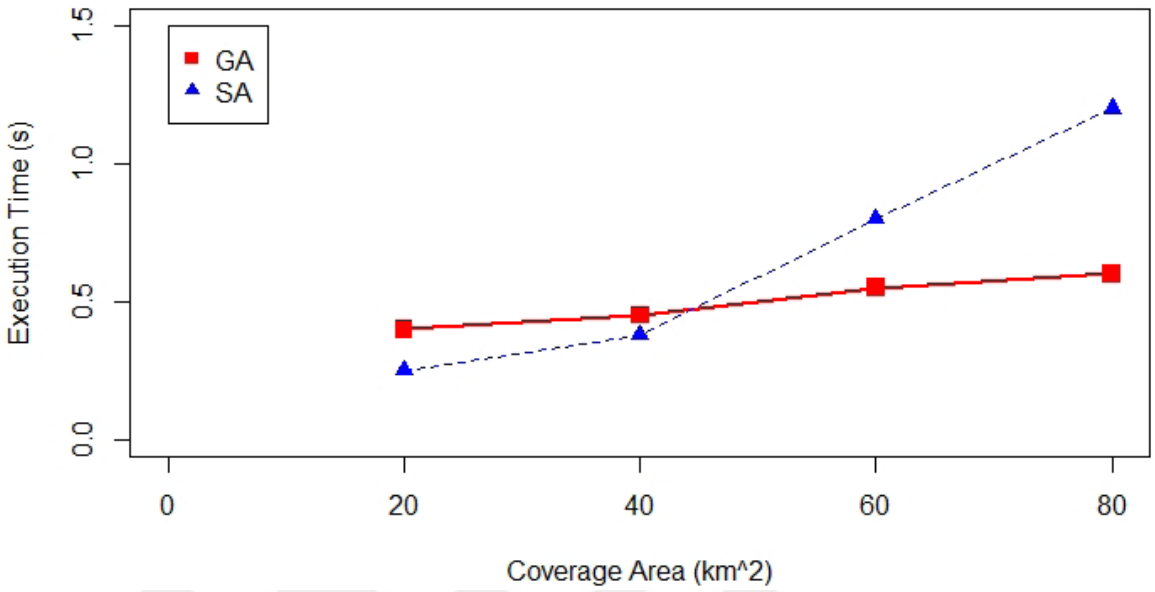

Figure 4.6: Execution time vs coverage area

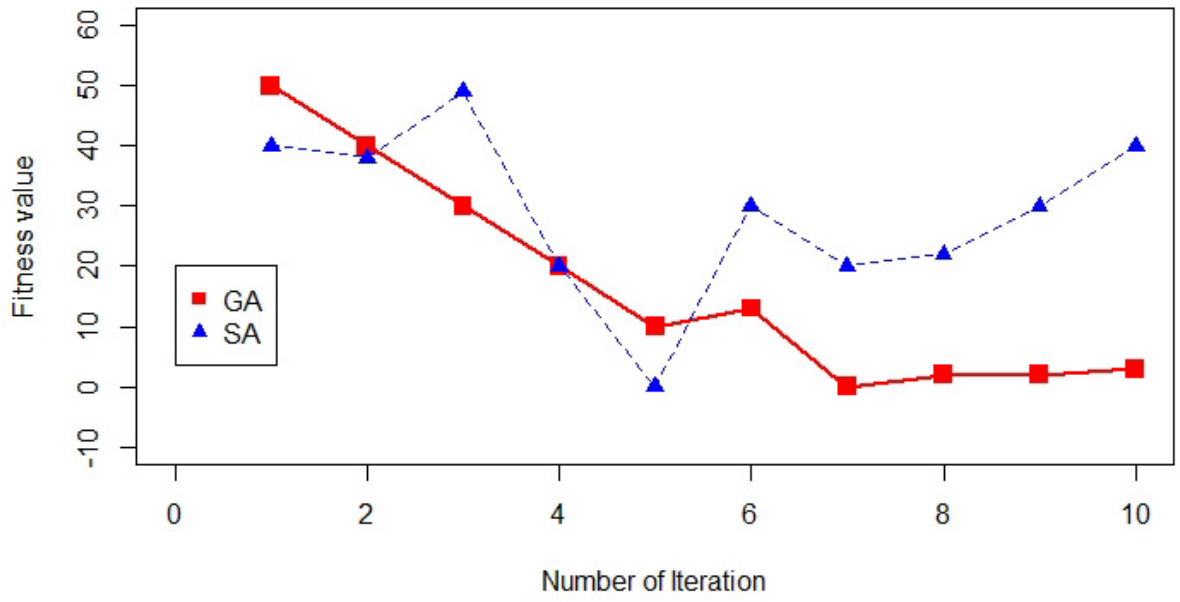

Figure 4.7: Fitness function behaviour

CHAPTER 5

5. PROPOSED MODEL MAIN CHALLENGES

Even though the autonomous first response drone-based paradigm proves to be effective in handling critical situations, the system still faces some challenges. One limitation is the unreliability nature of the GPS module to provide accurate location coordinates. GPS signals can be critically weakened by the surrounding environment which blocks the satellite link. Such environmental obstacles include tall buildings, tunnels, tree cover, and weather elements such as clouds and humidity.

However, proposed solutions to overcome this challenge include the use of satellite networks such as the Russian GLONASS network [61]. Moreover, there are GPS modules that can communicate with more than one GPS network. This means that the GPS receiver can pick up multiple satellite signals and improve its reliability and performance. Modules such as the Ublox Neo 7N and Ublox Neo M8N 436 modules support both GPS and GLONASS networks. Moreover, optic flow which is a vision-based motion estimation system can be used to decrease the GPS location errors [62]. Drones like DJI Phantom 3, and Inspire one 155 have inbuilt Optic flow features, that allows them to fly indoors.

Another challenge faced by the Auto-FRD paradigm is the loss of transmitted packets. As shown by Fig. 2.8 and Fig. 2.9, location coordinates send from the transmitter can fail to reach the receiver due to NLoS and distance. Proposed solutions to combat this challenge include the use of MIMO (Multiple transmitter and receiver antennas) to increase the path of the signals, consequently increasing the rate of packets received at the receiver.

CHAPTER 6

6. CONCLUSION AND FUTURE WORKS

This study shows that using Autonomous First Response Drones-based smart rescue system for critical situation management is a novel idea that can be used to save many lives by significantly reducing emergency response time. In addition, the paradigm is inexpensive, secure and reliable compared to conventional response-time-reduction methods. Moreover, a novel wireless communication paradigm was developed. The communication technique was designed to provide complete security (zero information leakage) against internal and external eavesdroppers while minimizing complexity. Results indicate that the proposed technique outperforms convention wireless communication methods by having better bit error rate, throughput, and peak to average power ratio.

Future works of this project include implementing a network of BSs, drones, and sensors using LoRaWAN by further utilizing IoT systems and smarter city paradigms. Moreover, we intend to modify the drones to autonomously deliver more services to a critical situation such as fire extinguishing balls.

APPENDIX A

NOTATIONS

Notation	Description
T_0	Initial temperature
δ_0	Initial solution
α	Cooling factor
m	Number of stages
n	Number of moves
δ_F	Finale solution
δ	Current solution
δ_{Temp}	Temporary solution
σ	Move operator
f	Fitness function
T_t	Temperature at time t
PM	Probability of mutation
PC	Probability of crossover
PS	Population size
G_{max}	Maximum generation number
BSF	Best fit function

BIBLIOGRAPHY

[1] Haji M Furqan, Jehad Hamamreh, Huseyin Arslan, et al. “Physical Layer Security for NOMA: Requirements, Merits, Challenges, and Recommendations”. In: *arXiv preprint arXiv:1905.05064* (2019).

[2] Mehmet Mert Şahin and Hüseyin Arslan. “Waveform-Domain NOMA: The Future of Multiple Access”. In: *arXiv preprint arXiv:2003.05548* (2020).

[3] Seoungjun Lee, Dongsoo Har, and Dongsuk Kum. “Drone-assisted disaster management: Finding victims via infrared camera and lidar sensor fusion”. In: *2016 3rd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE)*. IEEE. 2016, pp. 84–89.

[4] Fadi Al-Turjman et al. “Optimal Placement for 5G Drone-BS Using SA and GA”. In: *Drones in IoT-enabled Spaces*. CRC Press, 2019, pp. 43–58.

[5] Xiaowei Li et al. “A near-optimal UAV-aided radio coverage strategy for dense urban areas”. In: *IEEE Transactions on Vehicular Technology* 68.9 (2019), pp. 9098–9109.

[6] Jesús San-Miguel-Ayanz et al. “Forest fires in Europe”. In: *Middle East and North Africa* 2018 (2017).

[7] Abdulla Al-Kaff et al. “Emergency Support Unmanned Aerial Vehicle for Forest Fire Surveillance”. In: *Electronics* 9.2 (2020), p. 260.

[8] Arman Nedjati, Bela Vizvari, and Gokhan Izbirak. “Post-earthquake response by small UAV helicopters”. In: *Natural Hazards* 80.3 (2016), pp. 1669–1688.

[9] Paolo Bellezza Quater et al. “Light Unmanned Aerial Vehicles (UAVs) for cooperative inspection of PV plants”. In: *IEEE Journal of Photovoltaics* 4.4 (2014), pp. 1107–1113.

[10] Béla Vizvári et al. “Top-down approach to design the relief system in a metropolitan city using UAV technology, part I: the first 48 h”. In: *Natural Hazards* 99.1 (2019), pp. 571–597.

[11] Gabriele Ermacora et al. “A cloud based service for management and planning of autonomous UAV missions in smart city scenarios”. In: *International Workshop on Modelling and Simulation for Autonomous Systems*. Springer. 2014, pp. 20–26.

[12] Nour Charara et al. “Adabev: Automatic detection of abnormal behavior in video-surveillance”. In: *International Journal of Computer and Information Engineering* 6.8 (2012), pp. 946–952.

[13] Yuanwei Liu et al. “Non-orthogonal multiple access for 5G and beyond”. In: *arXiv preprint arXiv:1808.00277* (2018).

[14] Ertuğrul Güvenkaya, Jehad M Hamamreh, and Hüseyin Arslan. “On physical-layer concepts and metrics in secure signal transmission”. In: *Physical Communication* 25 (2017), pp. 14–25.

[15] Lemayian Joel Poncha et al. “5G in a convergent internet of things Era: An Overview”. In: *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE. 2018, pp. 1–6.

[16] Adrienne Welch. “A cost-benefit analysis of Amazon Prime Air”. In: (2015).

[17] Abdullah Cihan, Yan Zhang, and Larry Hoover. “Police response time to in-progress burglary: A multilevel analysis”. In: *Police Quarterly* 15.3 (2012), pp. 308–327.

[18] Joel Poncha Lemayian and Jehad M Hamamreh. “Autonomous First Response Drone-Based Smart Rescue System for Critical Situation Management in Future Wireless Networks”. In: *RS Open Journal on Innovative Communication Technologies* (2020).

[19] Emel Aktaş et al. “Optimizing fire station locations for the Istanbul metropolitan municipality”. In: *Interfaces* 43.3 (2013), pp. 240–255.

[20] Jordi Blanes i Vidal and Tom Kirchmaier. “The effect of police response time on crime clearance rates”. In: *The Review of Economic Studies* 85.2 (2018), pp. 855–891.

[21] Gang Xiang et al. “Design of the life-ring drone delivery system for rip current rescue”. In: *2016 IEEE Systems and Information Engineering Design Symposium (SIEDS)*. IEEE. 2016, pp. 181–186.

[22] Md Nafiz Hasan Khan and Carman Neustaedter. “Exploring Drones to Assist Firefighters During Emergencies”. In: 2019.

[23] W Stan Crowder and Brent E Turvey. “False 9-1-1 Calls”. In: *False Allegations*. Elsevier, 2018, pp. 65–88.

[24] Jehad M Hamamreh. “Improving the Physical Layer Security of IoT-5G Systems”. In: *Artificial Intelligence in IoT*. Springer, 2019, pp. 25–44.

[25] Jehad M Hamamreh, Zekeriyya Esat Ankarali, and Huseyin Arslan. “CP-less OFDM with alignment signals for enhancing spectral efficiency, reducing latency, and improving PHY security of 5G services”. In: *IEEE Access* 6 (2018), pp. 63649–63663.

[26] Jehad M Hamamreh, Ertugrul Basar, and Huseyin Arslan. “OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services”. In: *IEEE Access* 5 (2017), pp. 25863–25875.

[27] SM Riazul Islam et al. “Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges”. In: *IEEE Communications Surveys & Tutorials* 19.2 (2016), pp. 721–742.

[28] Jehad M Hamamreh et al. “Cross MAC/PHY layer security design using ARQ with MRC and adaptive modulation”. In: *2016 IEEE Wireless Communications and Networking Conference*. IEEE. 2016, pp. 1–7.

[29] M Furqan, J Hamamreh, and Huseyin Arslan. “Adaptive OFDM-IM for enhancing physical layer security and spectral efficiency of future wireless networks”. In: *Wirel Commun Mob Comput* 2018 (2018), pp. 1–16.

[30] Li Sun and Qinghe Du. “Physical layer security with its applications in 5G networks: A review”. In: *China Communications* 14.12 (2017), pp. 1–14.

[31] Jehad M Hamamreh and Huseyin Arslan. “Joint PHY/MAC layer security design using ARQ with MRC and null-space independent PAPR-aware artificial noise in SISO systems”. In: *IEEE Transactions on Wireless Communications* 17.9 (2018), pp. 6190–6204.

[32] Jehad M Hamamreh, Haji M Furqan, and Huseyin Arslan. “Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey”. In: *IEEE Communications Surveys & Tutorials* 21.2 (2018), pp. 1773–1828.

[33] Zhongwu Xiang et al. “Physical layer security in cognitive radio inspired NOMA network”. In: *IEEE Journal of Selected Topics in Signal Processing* 13.3 (2019), pp. 700–714.

[34] Lu Lv et al. “Secure MISO-NOMA transmission with artificial noise”. In: *IEEE Transactions on Vehicular Technology* 67.7 (2018), pp. 6700–6705.

[35] Linglong Dai et al. “A survey of non-orthogonal multiple access for 5G”. In: *IEEE communications surveys & tutorials* 20.3 (2018), pp. 2294–2323.

[36] Allen W Scott and Rex Frobenius. “Multiple access techniques: FDMA, TDMA, and CDMA”. In: (2008).

[37] Anass Benjebbour et al. “NOMA: From concept to standardization”. In: *2015 IEEE conference on standards for communications and networking (CSCN)*. IEEE. 2015, pp. 18–23.

[38] 3GPP R1-153332. “Evaluation methodologies for downlink multiuser superposition transmissions”. In: 3GPP. (Online) https://www.3gpp.org/DynaReport/TDocExMtg–R1-81–31256.htm (Access Date:25.08.2020).

[39] Mahmoud Aldababsa et al. “A tutorial on nonorthogonal multiple access for 5G and beyond”. In: *wireless communications and mobile computing* 2018 (2018).

[40] SM Riazul Islam et al. “Power-domain non-orthogonal multiple access (NOMA) in 5G systems: Potentials and challenges”. In: *IEEE Communications Surveys & Tutorials* 19.2 (2016), pp. 721–742.

[41] Yuya Saito et al. “System-level performance evaluation of downlink non-orthogonal multiple access (NOMA)”. In: *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE. 2013, pp. 611–615.

[42] 3GPP RP-160680. “Downlink multiuser superposition transmissions for LTE”. In: 3GPP. (Online)https://portal.3gpp.org/ngppapp/CreateTDoc.aspx?mode=viewcontributionUid=RP-160680(Access Date:25.08.2020).

[43] 3GPP R1-154537. “Link-level evaluation results for downlink transmissions”. In: 3GPP. (Online)https://www.3gpp.org/ftp/tsg_ran/WG1_RL1/TSGR1_82/Docs/ (Access Date:25.08.2020).

[44] Behrooz Makki et al. “A survey of NOMA: Current status and open research challenges”. In: *IEEE Open Journal of the Communications Society* 1 (2020), pp. 179–189.

[45] Yuya Saito et al. “System-level performance evaluation of downlink non-orthogonal multiple access (NOMA)”. In: *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE. 2013, pp. 611–615.

[46] Peng Xu et al. “NOMA: An information theoretic perspective”. In: *arXiv preprint arXiv:1504.07751* (2015).

[47] Yifei Yuan and Chunlin Yan. “NOMA study in 3GPP for 5G”. In: *2018 IEEE 10th International Symposium on Turbo Codes & Iterative Information Processing (ISTC)*. IEEE. 2018, pp. 1–5.

[48] Shanzhi Chen et al. “Pattern division multiple access—A novel nonorthogonal multiple access for fifth-generation radio networks”. In: *IEEE Transactions on Vehicular Technology* 66.4 (2016), pp. 3185–3196.

[49] 3GPP R1-164688. “Resource Spread Multiple Access, Qualcomm”. In: 3GPP. May 2016.

[50] Zhifeng Yuan et al. “Multi-user shared access for internet of things”. In: *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*. IEEE. 2016, pp. 1–5.

[51] R1-163992 3GPP. “Non-Orthogonal Multiple Access Candidate for NR,Samsung”. In: 3GPP. May 2016.

[52] Zhanji Wu et al. “Comprehensive study and comparison on 5G NOMA schemes”. In: *IEEE Access* 6 (2018), pp. 18511–18519.

[53] Xiangming Li et al. “Welch bound analysis on generic code division multiple access codes with interference free windows”. In: *IEEE transactions on wireless communications* 8.4 (2009), pp. 1603–1607.

[54] Imran Baig et al. “A DST precoding based uplink NOMA scheme for PAPR reduction in 5G wireless network”. In: *2017 7th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO)*. IEEE. 2017, pp. 1–4.

[55] Jehad M Hamamreh and Huseyin Arslan. “Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond”. In: *IEEE Communications Letters* 21.5 (2017), pp. 1191–1194.

[56] Markus Quaritsch et al. “Networked UAVs as aerial sensor network for disaster management applications”. In: *e & i Elektrotechnik und Informationstechnik* 127.3 (2010), pp. 56–63.

[57] Dimitrios Zorbas et al. “Optimal drone placement and cost-efficient target coverage”. In: *Journal of Network and Computer Applications* 75 (2016), pp. 16–31.

[58] Kyung-Nam Park et al. “Optimal coverage control for net-drone handover”. In: *2015 Seventh International Conference on Ubiquitous and Future Networks*. IEEE. 2015, pp. 97–99.

[59] AE Gamal et al. “Using simulated annealing to design good codes”. In: *IEEE Transactions on Information Theory* 33.1 (1987), pp. 116–123.

[60] Geir Storvik. “A Bayesian approach to dynamic contours through stochastic sampling and simulated annealing”. In: *IEEE Transactions on Pattern Analysis and Machine Intelligence* 16.10 (1994), pp. 976–986.

[61] Yuri Urlichich et al. “GLONASS modernization”. In: *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*. 2011, pp. 3125–3128.

[62] Hsiu-Wen Cheng, Tsung-Lin Chen, and Chung-Hao Tien. “Motion estimation by hybrid optical flow technology for UAV landing in an unvisited area”. In: *Sensors* 19.6 (2019), p. 1380.