3-19-2021

Reliable and Secure Drone-assisted MillimeterWave Communications

Mai A. Abdel-Malek
Department of Electrical and Computer Engineering, Florida International University, mabde030@fiu.edu

FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

RELIABLE AND SECURE DRONE-ASSISTED MILLIMETERWAVE COMMUNICATIONS

A dissertation submitted in partial fulfillment of the

requirements for the degree of

DOCTOR OF PHILOSOPHY

in

ELECTRICAL AND COMPUTER ENGINEERING

by

Mai Abdel-Malek

2021

To: Dean John Volakis
College of Engineering and Computing

This dissertation, written by Mai Abdel-Malek, and entitled Reliable and Secure Drone-assisted MillimeterWave Communications, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

Elias Alwan

Leonardo Bobadilla

Selcuk Uluagac

Kemal Akkaya, Co-Major Professor

Ahmed S. Ibrahim, Co-Major Professor

Date of Defense: Mar 19, 2021

The dissertation of Mai Abdel-Malek is approved.

Dean John Volakis
College of Engineering and Computing

Andres G. Gil
Vice-President for Research and Economic Development
and Dean of University of Graduate School

Florida International University, 2021

DEDICATION

To my family.

ACKNOWLEDGMENTS

First and foremost, All praise be to Allah for his guidance and countless blessings. I would also like to express my profound gratitude to my parents and sisters for their continued support throughout my journey. I would like to express my sincere gratitude and appreciation to my advisor, Dr. Ahmed Ibrahim, for his guidance and support from the beginning until the end of this work. I would also like to thank my co-advisor, Dr. Kemal Akkaya, for his motivational and inspiring guidance and support and his support on both personal and academic levels.

Throughout my doctoral journey, I had a chance to work with great collaborators. Many thanks to the inspiring and strong team of Advanced Wireless and Security (ADWISE) Lab, especially to Dr. Nico Saputro and Dr. Mumin Cebe, for their contributions and assistance in building the NS-3 simulator experiments. I would also like to thank Dr. Arupjyoti Bhuyan from the Idaho National Lab Wireless Security institute (INL WSI) for his collaboration through the INL summer intern research. I would also like to thank my committee members, Dr.Elias Alwan, Dr. Leonardo Bobadilla, and Dr. Selcuk Uluagac.

I would like to thank the staff members of the Department of Electrical and Computer Engineering (ECE) for their assistance in all the paperwork through my five years in the doctoral program. Finally, I would like to thank Florida International University for financially supporting my research as well as the FIU community for providing a great environment for my research for this dissertation.

This work is supported by the National Science Foundation (NSF). The work in Chapters 7 and 8 are supported by a grant from the Idaho National Lab Wireless Security institute (INL WSI).

ABSTRACT OF THE DISSERTATION

RELIABLE AND SECURE DRONE-ASSISTED MILLIMETERWAVE COMMUNICATIONS

by

Mai Abdel-Malek

Florida International University, 2021

Miami, Florida

Professor Ahmed S. Ibrahim, Co-Major Professor

Professor Kemal Akkaya, Co-Major Professor

The next generation of mobile networks and wireless communication, including the fifth-generation (5G) and beyond, will provide a high data rate as one of its fundamental requirements. Providing high data rates can be accomplished through communication over high-frequency bands such as the Millimeter-Wave (mmWave) one. However, mmWave communication experiences short-range communication, which impacts the overall network connectivity. Improving network connectivity can be accomplished through deploying Unmanned Ariel Vehicles (UAVs), commonly known as drones, which serve as aerial small-cell base stations. Moreover, drone deployment is of special interest in recovering network connectivity in the aftermath of disasters. Despite the potential advantages, drone-assisted networks can be more vulnerable to security attacks, given their limited capabilities. This security vulnerability is especially true in the aftermath of a disaster where security measures could be at their lowest.

This thesis focuses on drone-assisted mmWave communication networks with their potential to provide *reliable* communication in terms of higher network connectivity measures, higher total network data rate, and lower end-to-end delay. Equally important, this thesis focuses on proposing and developing *security* measures needed for drone-assisted networks' secure operation. More specifically, we aim to employ a swarm of drones to have more connected, reliable, and secure communication over the mmWave band. Finally, we target both the cellular 5G network and Ad hoc IEEE 802.11ad/ay in typical network deployments as well as in post-disaster circumstances.

TABLE OF CONTENTS

LIST OF TABLES

TABLE PAGE

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

IAB	Integrated Access and Backhaul
NGMN	Next Generation of Mobile Networks
MiTM	Man in The Middle attack
ProSe	Proximity-based Services
KMF	Key Management Functions
TELNET	TELecommunication NETwork
FTP	File Transfer Protocol
DoS	Denial-of-service
ARP	Address Resolution Protocol
SBA	service-based architecture
AKA	Authentication and Key Agreement
SN	Serving Network
HN	Home Networks
SDN	Software-Defined Network
HetNet	Heterogeneous Network
WSN	Wireless Sensor Network
ML	Machine Learning
ECC	Elliptic Curve Cryptography
EAP	Extensible Authentication Protocol
TLS	Transport Layer Security
AUSF	Authentication Server Function
UDM	Unified Data Management
SEAF	Security Anchor Function
AMF	Access & Mobility Management Function
5G-GUTI	5G Global Unique Temporary Identifier
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier

SIDF	Subscription Identifier De-Concealing Function
NR	New Radio
PKMF	ProSe Key Management Function
SDP	Semi-Definite Programming
FAA	Federal Aviation Administration
S-NSSAI	Single Network Slice Selection Assistance Information
5G-RAN	5G-Radio Access Network
AAA-S	Authentication Authorization and Access Server
HMAC	Hash-based Message Authentication Code

CHAPTER 1

INTRODUCTION

1.1 Motivation

The Next Generation of Mobile Networks (NGMN), including the 5G system and beyond, needs to satisfy the demand for high traffic data that may emanate from the various Internet of Things (IoT) devices as well as mobile users Equipments (UEs) that are increasingly demanding streaming applications [WGA+15].Given the current wireless bandwidth crunch, [WM14,DP11], this is becoming a pressing issue that needs to be addressed for the sustainability of the current services. One promising solution is to tap into higher bands, such as MillimeterWave (mmWave). Communication over the mmWave spectrum band can support such high data rates due to its abundant bandwidth [WHQW14, GKZV08].

However, mmWave propagation suffers from a short communication range and can be easily blocked [BDRQL11,RSM+13,WWS+17,RSP+14]. If used in a multi-hop wireless ad hoc network (i.e., IEEE 802.11ad/ay-based mesh network), such short-range communication may result in weak connectivity. Therefore, if the mmWave band is to be utilized effectively for increasing the data rate in such environments, the first challenge to be addressed is to improve the connectivity of the underlying wireless network. Flying Unmanned Aerial Vehicles (UAVs) or drones, as commercially known, utilization in NGMN and ad hoc networks can contribute to such connectivity problem if utilized wisely. Once connectivity is improved, mmWave can become a more effective means to seek throughput maximization at the upper layer of the protocol stack by potentially utilizing multiple and/or parallel transmissions through the available alternative paths.

One of the most challenging circumstances in NGMN is post-disaster such as hurricanes and earthquakes, where the communication and power infrastructures could be damaged, disconnecting affected communities from the rest of the world. Hence, restoring communication on those networks is vital for damage assessment and to start the recovery process. Public safety agencies and local governments are currently considering deploying drones to address the need for rapid post-disaster recovery. Drones will act as relays among people in affected areas as well as with local authorities.

Nevertheless, drone deployment raises various security threats, which can go unnoticed and thus underexplored by primarily focusing on the 5G's and wireless

networks' performance aspects. Then, those under-explored security threats can become relevant, particularly in the post-disaster scenarios. For instance, as drones are commodity IoT devices, they can be easily obtained and deployed to eavesdrop on the network maliciously. In a post-disaster circumstance, as authorities and people's primary focus will be to facilitate aid efforts, security will not be a priority, as in regular communication networks. Authentication is particularly challenging in drone-assisted mmWave communication, given the short-range limitation of communication over the mmWave spectrum band. More precisely, not all optimally-positioned drones will have a direct communication link with the centralized authentication entity according to coverage or capacity constraints. Instead, drones will be connected to each other through a multi-hop mesh network. Therefore, there is a need to have drone-based short-range authentication mechanisms, which is one of our primary motivations.

1.2 Research Objective

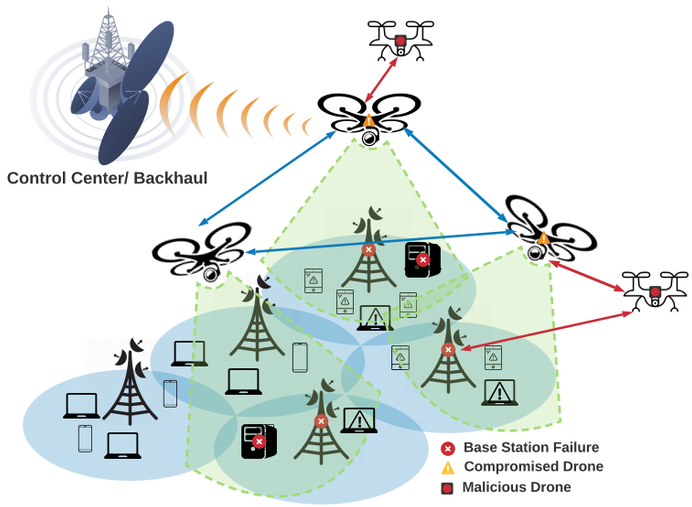


Fig. 1.1 System model of UAV-based mmWave network.

In this work, we aim to utilize a swarm of UAVs to have a more connected, reliable, and secure communication over the next generation mmWave frequencies for a higher data rate transmission. The targeted next-generation communication system is shown in Fig. 1.1. One of the main requirements for the next generation communication is restoring and enhancing the network connectivity to avoid isolated node scenarios and reduce networks congestion. To this end, we incorporate positioning a swarm of UAVs to increase the network connectivity and address the mmWave short communication range. Jointly, we consider the UAVs' interference management to avoid power loss due to communication over-

lapping. Moreover, we consider optimizing the UAVs' limited resources, such as transmission power. Once connectivity is boosted, mmWave can become a more effective means of seeking throughput maximization. We then aim to multiple and/or parallel transmissions through the available alternative paths to enhance reliability further.

Furthermore, UAVs' utilization raises various security threats as maliciously controlled drones in both the cellular 5G and ad hoc wireless networks. The malicious UAVs can collect information by acting in the middle (i.e., Man in The Middle attack (MiTM)). Those security threats increase the need for authentication and security mechanisms that can adequately eliminate suspicious UAVs. Hence, one of our research aims is to secure UAVs communication within the next generation mmWave communication. Therefore, we propose a fast, efficient, and lightweight distributed authentication mechanism for drones.

1.3 Research Approach

Our research approach through this dissertation proposal is described in the following subsections.

1.3.1 UAVs' Positioning

First, regarding the first challenge of the UAV swarm positioning, we utilize Optimization Theory. We optimally position the UAVs by providing mathematical processing considering the model limitations such as optimum power allocation. This model is Graph Theoretical-based, which provides an efficient connectivity framework that models and analyzes the relationship between the network nodes and links. Then, we further provide a Communication Theory interference and Quality of Service (QoS) constraints to optimize the network coverage and manage the interference between the nodes.

1.3.2 UAVs' Routing & Reliability

Once we enhanced the network connectivity, we tackle the reliability problem of mmWave communications by deploying additional UAVs and exploiting parallel multi-path transmissions through the help of these UAVs. Specifically, we maximize the initial network connectivity under an E2E delay constraint and a

maximum transmission power for the UAVs assuming IEEE 802.11ad-based connections. To this end, we propose ensuring End-to-End (E2E) delay through multi-path routing can ensure network reliability by increasing the redundant data through different routes. To cover the link reliability challenge, we consider a network layer mechanism to provide routing management. We then utilize a node-disjoint routing protocol that utilizes the mmWave PHY layer information and supports parallel multi-path transmissions for improved E2E delay and throughput performance.

1.3.3 UAVs' Authentication in Ad hoc Networks

Then, to implicate the security challenges over the ad hoc UAV network assuming potential imposters. We propose lightweight and fast authentication mechanisms that take into account the physical limitations of mmWave communication. We first consider an IEEE 802.11ad/ay post-disaster recovery of destroyed communication infrastructure, where drones are temporarily positioned within the affected area to create a wireless mesh network among public safety personnel. We opt for a delegation authentication called a proxy signature, where the proxy signer signs a message using a secret key of the original signer [DSP06, LY05]. Proxy signature provides data security and user privacy while not increasing computational loads. We propose a drone-to-drone authentication mechanism based on proxy signatures from the Control Center (CC).

1.3.4 UAVs' Authentication to The 5G Core

Then, toward a secure drone communication under the 5G network, we further propose a more robust authentication mechanism inspired by the idea of second-factor authentication in IT systems. Specifically, once the primary 5G authentication is executed, a slice specific is tasked to trigger a second-factor authentication utilizing different factors from the primary one. This trigger mechanism operates the re-authentication procedure as specified in the 3GPP 5G standards for easy integration.

1.3.5 Drone to Drone Authentication

We further propose a lightweight, fast, and reliable authentication mechanism compatible with the 5G Device-to-Device (D2D) Proximity-based Services (ProSe)

standard mechanisms. Specifically, we propose a distributed authentication with a delegation-based scheme instead of the repeated access to the 5G core network Key Management Functions (KMF). Hence, a legitimate drone is authorized by the core network via offering a proxy signature to authenticate itself to other drones as a leader drone and vice versa.

1.4 Dissertation Contribution

Our contributions in this dissertation can be summarized as follows:

1. Formulating a novel UAV-based Integrated Access and Backhaul (IAB) positioning problem, in which we aim to maximize the *backhaul* network connectivity while providing the desired SINR for all users in the *access* network.

    - Mathematically relaxing the formulated optimization problem to be an Semi-Definite Programming (SDP) one that can be solved numerically with reasonable complexity.
    - The proposed algorithm finds the best positions for the considered UAVs to enhance the backhaul network's algebraic connectivity. In the meantime, we are achieving the desired SINR for all the users on the mmWave access network.

2. We propose an analytical solution for the UAV-based *network topology formation* constrained optimization problem, where the minimum number of UAVs, along with their locations and transmission powers, are identified. This optimization is constrained to limit the acceptable E2E delay, and hence, increase the network throughput.

    - We model the expected delay between a source and destination using a queuing analysis;
    - We propose a multi-hop multi-path source routing scheme involving UAVs that will also allow parallel transmissions at the network layer for increased reliability, and hence, throughput.
    - We incorporate the PHY/MAC layers implementation of the IEEE 802.11ay protocol into the NS-3 simulator for developing a routing protocol with mmWave communication links and show that the developed analytical model closely matches the implementation results under NS-3.

3. We propose a proxy-based scheme for drone-to-drone and drones-to-ground authentication in ad hoc IEEE802.11ad/ay post-disaster circumstances.
    - We delegate one of the drones to sign the authentication warrant to authenticate other drones on behalf of a CC to reduce the communication time energy.
    - We propose a broadcast-based group authentication scheme for a drone to its associated ground nodes, where a proxy signature challenge-response authentication is followed.
4. We propose a second-factor authentication scheme to verify legal drones' and other IoT devices' authenticity as a part of the 5G network.
    - We propose a challenge-response based protocol that conforms with the current 5G authentication standard that utilizes drones' digital IDs.
    - We propose an authentication triggering mechanism based on the 5G re-authentication mechanism.
    - We implemented the proposed approach within the NS-3 simulation environment, which supports 5G radio access.
5. We propose a drones' D2D authentication in such a way that conjunct into the 5G D2D ProSe standards.
    - We add a delegation phase, after the mandatory 5G registration phase, in which we assign a delegation warrant and proxy parameters.
    - We propose a proxy signature authentication mechanism integrated into the ProSe discovery phase.

The rest of this dissertation is organized as follows. First, the related research works' literature review is in Chapter 2. Then, the background of the concepts utilized through the dissertation is in Chapter 3. The UAVs' positioning for enhancing the network connectivity is discussed in Chapter 4. Next, the UAVs' optimization challenge toward a reliable mmWave network is detailed in Chapter 5. Chapter 6 discuss the drone authentication in IEEE802.11ad/ay in a post-disaster circumstances. Then, The drones and IoT devices authentication to the core network and other swarm drones in a mmWave-based 5G network are in Chapter 7 and Chapter 8, respectively. Finally, the concluding remarks and future work are in Chapter 9.

CHAPTER 2

LITERATURE REVIEW

In this chapter, we examine the related work of the studies presented in this dissertation.

2.1 MmWave

The mmWave propagation suffers from a short communication range and can be easily blocked [BDRQL11, RSM+13, RSP+14]. If used in a multi-hop wireless ad hoc network (i.e., IEEE 802.11ad-based mesh network), such short-range communication may weaken connectivity or even lead to a disconnected wireless network defeating the purpose of supporting high data rates [WHQW14, GKZV08]. The mmWave communication has recently received significant attention in terms of its channel measurements, modeling, and system design. For example, in [WWS+17], the authors built an indoor communicating system to test and measure the mmWave 60 GHz propagation patterns. The authors introduced a statistical model for indoor multipath propagation. The ergodic capacity of an outdoor clustered mmWave network with directional antennas is proposed in [TH16], which utilizes the directional beamforming and uncoordinated channel access to provide cluster capacity gains.

There are ongoing researches on utilizing UAVs as relays to restore network functionality in mmWave communication. That requires a rapid temporary routing algorithm toward sustainable connection to retain the communication [XXX16a]. For example, in [KYW+17] an autonomous mobile relay scheme was proposed to extend the mmWave communication coverage. In [KOG17], UAVs are placed to explore ray-tracing simulations and assess Doppler effects for air to ground mmWave UAV communications. Similarly, the authors in [XXX16b] explored the blockage and Doppler effect depending on UAV positioning under mmWave spatial-division multiple access communication. In this work, we aim to optimally identify the minimum number of UAVs and their locations to maximize the mmWave network connectivity.

The 5G mmWave has many considered potential bands, such as 28 GHz, 38 GHz, and 60 GHz, including several channel modeling measurements. The most recent official 5G mmWave standard is adopting the 28 GHz. In [LMK+18],

the authors model the 5G mmWave cellular channel at 28 GHz using NYUSIM software [WoP18].

Moreover, the efforts are ongoing towards standardizing the mmWave communication with the development of new IEEE802.11 protocols such as 802.11ad [NCF+14]. For instance, IEEE802.ad is an extension to the IEEE 802.11-2012 specification that adds a new MAC/PHY to provide short-range, high capacity links in the 60 GHz unlicensed band [DGH14] for an ad hoc network of directional, short-range, point-to-point links. The limitations on the IEEE 802.11ad are regarding the transmission range, which is within $10 - 20$m. However, this problem was solved in IEEE 802.11ay using Multiple-Input Multiple-Output (MIMO) technology to obtain up to 300m.

2.2 Drones as Relays

Many techniques have been developed to promote the selection of the UAVs' positions towards network supporting and enhancing the network [RIG16, ARCP16]. Furthermore, the UAVs' positioning model plays a crucial role in evolving network performance [MV17, LKC+16, DYLS15]. In [PJSL17], the authors proposed an adaptive route recovery algorithm based on topology discovery and network hole replacement with UAV relays, where network hole occurs due to the terrestrial network broke links that lead to isolated sub-networks.

There have been recent works focusing on 3-dimensional (3D) UAV positioning to serve multiple purposes, either to increase the connectivity of the backhaul network [DYLS15, DCN07, Yan12], or to increase the coverage of the served UEs [RW12, MSBD16, KSYY17, MSBD15]. First, we start with exploring works on optimizing the UAVs positions only to enhance the *coverage*. In [ARCP16], the authors derived a closed-form expression for the UAV position to maximize the coverage radius in the presence of the Rician fading model. Optimal UAV positioning schemes to enhance the outage probability or Signal-to-Interference and Noise Ratio (SINR) were discussed in [RW12] and [MSBD16], respectively. In terms of achieving specific user data rates, a 3D positioning of UAVs' are investigated in [MSBD15], with users having different rate requirements for urban networks. Furthermore, the utilization of a UAV in D2D communication was considered in [KSYY17], in which the UAV acts as a flying base station for users in a D2D communication network.

Second, we explore works on UAV positioning for network *connectivity* enhancement. For example, steering UAV for offshore network recovery and rare territories with poor network construction was considered in [DYLS15] to improve the network connectivity. Utilizing the UAV to enhance the connectivity was also proposed in [DCN07]. The authors derived the probability of an arbitrary node being isolated as a representation of the network connectivity. In [Yan12], coverage-based and connectivity-based mobility models were introduced toward a UAV network monitoring. A comparison between both models is conducted to clarify the tradeoff between achievable area coverage for the connectivity-based model and achievable connectivity for the coverage-based model. As opposed to these approaches, our UAV deployment is geared for maximizing reliability for mmWave communication while also minimizing the E2E delay. In this work, the optimization problem also considers the E2E delay and UAV power consumption in addition to the UAV positioning.

2.3 Network Routing

Increasing network connectivity provides more routing options and enhances the communication experience with good utilization. Multiple works are focusing on UAVs' routing for reliable UAVs' networking. In [CCC+17], the authors developed a mathematical programming model for a time-dependent UAV heterogeneous fleet routing problem. A dynamic vehicle routing for UAVs performing spatially distributed tasks in dynamic environments is proposed in [FEPS15a]. For an energy-efficient routing, authors in [BHH19] proposed a UAV route determination algorithm by modifying a Voronoi diagram reflecting sensor energy information for Wireless Sensor Networks (WSNs). In [FEPS15b], the authors proposed a control policy to minimize the expected waiting time between the appearance of randomly-generated targets and the time the UAV visits them in both light and heavy loads. A novel and adaptive 3D UAV routing based on graph-theoretic complexity reduction are proposed in [RXE+18]. Finally, in [RS06], the authors proposed two approximated algorithms for a lower and upper bounding UAV routing.

Moreover, relying on single-path routing cannot handle the link congestion or failure, especially in ad hoc networks [HR08, WZSD00, CDS98, CRS99]. Hence, the need to have multipath routes increases with the use of mmWave frequencies; due to its short-range and high sustainability for link failure as aforementioned.

Multipath routing has been studied in different contexts for the traditional wireless frequencies either to enhance the link reliability or to obtain higher data rates [ND99, MD01]. More recent works are considering on-demand multipath routing in ad hoc networks to reduce routing overheads, which have more effectiveness and efficiency [MD06]. With all the advantages of multipath routing, when several paths share common resources, joint nodes, or links, performance may even degrade than single-path routing. Hence, when a link or a node is mutual among several paths, severe flow congestion occurs with high incoming traffic load. As a result, the shared node or link becomes a bottleneck [HF08]. Consequently, more recent research on multipath routing proposed node-disjoint path routing protocols to avoid interference among paths [LG01, LC04a, LC04b, HF08]. In [RDBL12], the authors summarize the related work on multipath routing for wireless networks for both the theoretical and practical sides of multipath routing. However, our work is different in terms of the impact on the lossy mmWave network. Moreover, our optimization problem formulation for the UAV positioning considers both the E2E delay and the UAV power consumption while finding suitable multipaths for proper communication.

2.4 Ad hoc Wireless Network Security

Security and privacy in wireless networks is a major concern, where the open nature of the wireless medium makes the wireless transmission vulnerable to eavesdropping and inimical attacks [WEDH14]. One approach to address wireless network security is physical layer security, where the characteristics of the wireless channel are exploited to transmit confidential messages [AEAH12, YE11]. The attacks related to wireless networks are such as TELecommunication NETwork (TELNET)/File Transfer Protocol (FTP) attack, Denial-of-service (DoS), Address Resolution Protocol (ARP) spoofing [HTZ+16], ad hoc network [KLX+02] and MiTM attack [GP15]. Hence, mutual authentication between the UAVs and the network nodes is required to assure communication security [CP08, BWB+11, WCMF17].

A survey of security requirements, attacks, and network integration in wireless mesh networks is discussed in [RK08]. An introduction to wireless mesh networks and present both the benefits enabled by this technology and the main hurdles that have to be overcome is introduced in [Sic05]. In [NL09], the authors proposed a heterogeneous wireless network integration model that integrates and clarifies

the security reference points at the network boundaries. The authors in [DCNR09] identified security goals and design challenges in achieving security for network coding systems. The authors revealed that both intra-flow and inter-flow network coding systems are vulnerable to a wide range of attacks at various stages of the protocol. In [NNS+07] the authors investigated the key challenges at each layer and discussed the feasibility of some proposed approaches in the literature to address these challenges.

In [DW11], the authors proposed using public networks for remote sensing-based UAV security operations. Several works attempted to develop practical and effective solutions for drone authentication in wireless networks. For instance, in [YLL+18], the authors propose a lightweight authentication scheme for the internet of drones deployment utilizing an efficient one-way cryptographic hash function. Other authors employed the elliptic curve Elliptic Curve Cryptography (ECC) for a legal drone digital identity proof as in [TJP+19]. In [LYK18], the authors investigated the secrecy outage performance achieved for opportunistic UAV relaying. The authors in [SGBW16] proposed a UAV position-aware, secure, and efficient mesh routing approach. This approach showed more attack mitigation than the well-known, secure routing protocol ARAN and the standardized security mechanisms of IEEE 802.11s/i. In [KGTK20], the authors proposed a blockchain-based cryptographic algorithm for a secure UAV network.

2.5 4G Vs. 5G Security Protocols

The authentication in the 4G network included a unified authentication framework, better UE identity protection, enhanced home-network control, and more key separation in key derivation [Ins19]. The proposed authentication for the 5G core network is based on a service-based architecture (SBA), enhancing the previous variant currently used in the 4G. The 5G network standardized the 5G AKA protocols for this purpose [Kou19]. These protocols work with the new structure of the 5G that includes the subscribers, the Serving Networks (SNs) with nearby base stations, and Home Networkss (HNs) that correspond to the subscribers' carriers. The AKA protocols enable the subscribers and HNs to mutually authenticate each other and let the subscribers and SNs establish a session key [BDH+18].

There are some recent studies on the authentication aspects of the 5G. For instance, Software-Defined Network (SDN) is utilized to enable efficient authentica-

tion handover, and privacy protection in [DW15]. The authors proposed a simplified authentication handover by global management of the 5G Heterogeneous Networks (HetNets) by sharing user-dependent security context information among related access points. Furthermore, in [NLS18], the authors proposed a secure service-oriented authentication framework for IoT services in the 5G network where a privacy-preserving slice selection mechanism is introduced to allow fog nodes to select proper network slices. The work in [SK18] proposes a two-factor authentication, but it is for Wireless Sensor Networks (WSNs) integrated with the 5G. The authentication is done for the user accessing this WSN, which is different from our work, exploring two-factor authentication within the 5G network itself. As seen, two-factor authentication has not been considered at all for the 5G core applications. Therefore, our work fills a significant gap to strengthen security to the 5G systems, especially for drone IoT applications.

2.6 UAVs Authentication

2.6.1 Message Authentication

Since drones are vulnerable to several kinds of attacks, drone authentication is studied within the context of message authentication and device authentication. For message authentication, in [WDK+19], the authors propose a lightweight authentication and key agreement scheme for the internet of drones deployment utilizing an efficient one-way cryptographic hash function. One message authentication solution is utilizing centralized techniques such as Mavlink protocol, which is a header-only protocol used to communicate with a ground control station [NA14, ANBDF05, ZYYY10]. Centralized techniques allow offshore authentication, which relief the load on the limited resources UAVs. Nevertheless, our goal in this work is not message authentication, as we aim to perform device authentication.

The authors in [YMM13] proposed a time-efficient privacy authentication protocol for secure communications, which achieves lower message latency and higher efficiency in terms of computational and communication resources. In [VHSV11], the authors proposed a simple, lightweight message authentication protocol based on Hash-based Message Authentication Code (HMAC) protocol for CAN bus. In [WY17], the authors proposed a local identity-based scheme, named LIAP, as an anonymous message authentication in Vehicular Ad hoc Networks (VANETs).

Another VANET message authentication mechanism was proposed in [WS11], where an Expedite Message Authentication Protocol (EMAP) was proposed. The authentication protocol in [WS11] expedites message authentication by replacing the time-consuming in the Certificate Revocation Lists (CRLs) with a fast revocation checking process employing the HMAC function. The authors in [ACK+20] proposed a two-stage mutual authentication protocol for SDN-based multi UAV networks in surveillance areas.

2.6.2 Device Authentication

For device authentication, in [TJP+19], the authors proposed an ECC digital certificate as the identity proof of the legal drone toward drone network identity authentication. Such an identity can easily be replaced or regenerated in a post-disaster scenario. Moreover, a Machine Learning (ML) mechanism for authentication in autonomous IoT systems is studied in [KAL+19]. This assessment is done for different ML algorithms by computing and reporting each algorithm's precision and recall rates. This approach will not work in a post-disaster scenario since the training needs to be done in advance.

There have been multiple works for different proxy signature approaches for device authentication purposes [DSP06]. For example, a short certificate base proxy signature is proposed in [VSKH19] with a low computational cost to overcome the integrity attacks on vehicular networks. In [ZK03], a blind ID-based partial delegation with warrant proxy signature is proposed, where ID-based proxy is to provide the anonymity of users. Also, in [HMMW19], the authors proposed a designated verified proxy blind signature scheme for drone network based on ECC that provides efficient computation. The assumptions and architecture in this work are different from our case and focus solely on computation calculations. Nevertheless, the blind proxy signature is a proxy signature mechanism designed to maintain user privacy, and hence, it only has the original signer signature and not the delegated/proxy signer itself. A powerful device authentication proxy signature should have information about the proxy signer along with the original signer. In [LMYT18], the authors proposed a new scheme to mitigate partial attacks not considered by the identity-based proxy signature. While our work utilizes proxy signature concepts like these studies, its proposed protocols are very different where the goal is to authenticate drones to an existing network.

2.6.3 D2D Authentication

A survey on variant state-of-the-art solutions to tackle security and privacy challenges in D2D communication spanning across a variety of D2D prospects is provided in [HWD+17]. An overview of the benefits of intelligent D2D communication in the IoT ecosystem is presented in [BZ16], where the authors focused on the routing state-of-the-art. Algorithms can achieve intelligent D2D communication in the IoT. In [BSD+20], the authors proposed a new blockchain-based secure framework for data management among a group of drones. In [SBSW17], the authors proposed a Body Area Network Device-to-device Authentication using Natural gAit (BANDANA). The BANDANA algorithm enables secure spontaneous pairing of devices worn on the same body. In [KHK+14], the authors proposed propose new D2D authentication protocols with a secure initial key establishment using ciphertext-policy attribute-based encryption(CP-ABE). The authors in [ADM19] proposed a lightweight elliptic-ElGamal-based authentication scheme using PKI (FHEEP) in D2D communication. In [LZLS12], the authors investigated the direct D2D communications between user equipments in the LTE-advanced cellular networks. A quick and safe handover authentication scheme to D2D out-band controlled communication mobility situations in the 5G-WLAN heterogeneous networks was presented in [KO18]. Most of those works aforementioned are general-purpose drone authentication for any network and do not apply to our case of D2D communication in 5G.

CHAPTER 3

PRELIMINARIES

This chapter gives a piece of background information related to the technologies used throughout the dissertation.

3.1 MmWave Channel

We utilize the mmWave channel model for the UAVs' communications links, where both the path loss and the small scale fading models are considered. The mmWave channel modeling was introduced in [SMR17] based on extensive real-world wide-band propagation channel measurements in various outdoor urban environments.

The close-in free space reference distance (CI) path loss PL model with a 1 m reference distance and an extra attenuation term due to various atmospheric conditions [SMR17]

$$\begin{aligned} PL^{CI}(f,d)[dB] =& FSPL(f,1m)[dB] + 10\alpha log10(d) \\ &+ AT[dB] + X_{\sigma}^{CI}, \end{aligned} \tag{3.1}$$

where f denotes the carrier frequency in GHz, d is the 3-D separation distance, α represents the path loss exponent(PLE). AT is the attenuation term induced by the atmosphere, X_{σ}^{CI} is a zero-mean Gaussian random variable with a standard deviation σ in dB, and $FSPL(f,1m)$ denotes the free space path loss in dB at a separation distance of 1 m at frequency f.

3.2 Graph Theory

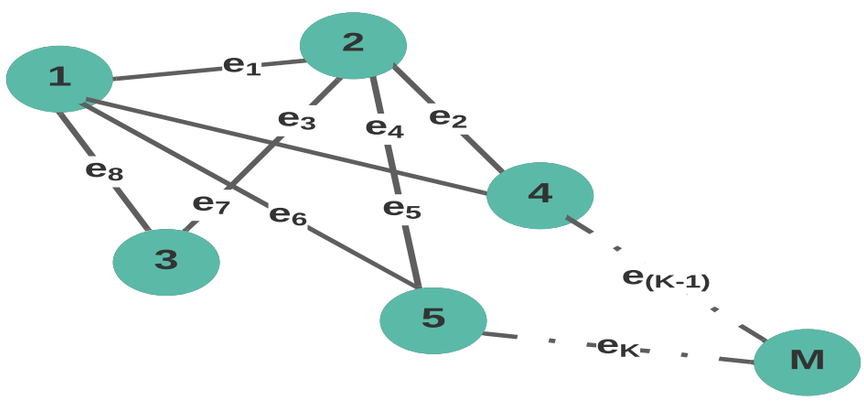


Fig. 3.1 Undirected Graph.

In graph theory models a number of nodes can be modeled as an undirected finite graph $\mathcal{G}(\mathbf{V},\mathbf{E})$ where $\mathbf{V} = \{v_1, \ldots, v_M\}$ is the vertices set of the M nodes

and $\mathbf{E} = \{e_1, \ldots, e_K\}$ is the set of K edges, as shown in Fig. 3.1. For any edge l connecting two vertices v_i and $v_j \in \mathbf{V}$, the edge vector $\mathbf{a_l} \in \mathbf{R}^M$ is all zeros vector except its i^{th} and j^{th} elements are $a_{l,i} = 1$ and $a_{l,j} = -1$, respectively. The graph incidence matrix of $\mathbf{A} \in \mathbf{R}^{M \times K}$ is given by $\mathbf{A} \triangleq [\mathbf{a}_1, \ldots, \mathbf{a}_K]$ and its the $M \times M$ Laplacian matrix can be written as follows [ISL09a]

$$\mathbf{L} = \mathbf{A}\,\mathrm{diag}(\mathbf{w})\mathbf{A}^T = \sum_{l=1}^{K} w_l \mathbf{a}_l \mathbf{a}_l^T, \tag{3.2}$$

where $\mathbf{w}$ denotes the $K \times 1$ weighting vector coefficients for the K edges and is given by $[w_1, w_2, \cdots, w_K]^T$. The Laplacian matrix is a positive semi-definite matrix, i.e., $\mathbf{L} \succeq 0$, with the smallest eigenvalue denoted by $\lambda_1(\mathbf{L})$ is equal to zero [ISL09a]. We term $\lambda_2(\mathbf{L})$ as the second smallest eigenvalue, also known as Fiedler value, of the graph Laplacian matrix which represents its algebraic connectivity. The smaller Fiedler value is, the less connected the network is, and vice verse. It is worth mentioning that when $\lambda_2(\mathbf{L}) = 0$, the graph is disconnected in which at least one of its vertices is unreachable from any other vertices in the graph.

3.3 5G Primary Authentication

The 5G authentication structure is a unified framework to support both 3GPP access and non-3GPP access networks such as Wi-Fi. The 5G authentication structure supports Extensible Authentication Protocol (EAP) that is also in use for IEEE 802.11 (WiFi) standard. In this regard, the 5G EAP authentication protocol supports both EAP-Transport Layer Security (TLS) and EAP-AKA protocols, where authentication process is executed between the UE (a client device) and the Authentication Server Function (AUSF)/Unified Data Management (UDM) (i.e., HN) through the Security Anchor Function (SEAF)/Access & Mobility Management Function (AMF) (i.e., SN) as an EAP authenticator [Ins19].

As 5G-AKA is widely used, we provide more info about its details, which is also shown in Fig. 3.2: 5G-AKA structure allows the SEAF function to trigger the authentication process once receiving any accessing message from a UE. In this message, the UE has to send its 5G Global Unique Temporary Identifier (5G-GUTI) temporary identifier to initiate the authentication procedure. If the UE is not provided with a 5G-GUTI, a Subscription Concealed Identifier (SUCI) can be used. The SUCI is an encrypted version of the Subscription Permanent Identifier (SUPI) provided to each UE using the public key of the home network

(i.e., it is encrypted using this key). Note that the SUPI should never be sent in plaintext to ensure UE's privacy.

Once SEAF receives the message, the authentication process is initiated by the SEAF function, and an authentication request is sent to the AUSF function in the home network. The AUSF then verifies that the serving network request is authorized. If it is a legitimate request, the AUSF proceeds with the authentication procedure by sending an authentication request to UDM. Next, the Subscription Identifier De-Concealing Function (SIDF) validates the SUCI by decrypting the SUCI and obtains the corresponding SUPI and selects the authentication method configured for the corresponding subscriber, which is 5G-AKA for our case. The UDM then sends an authentication response to the AUSF including an AUTH token, an $XRES$ token, the key K_{AUSF}, and the SUPI if not using the 5G-GUTI. K_{AUSF} is an important key material that can be further used to derive subsequent keys for different purposes. We will rely on this key in our approach.

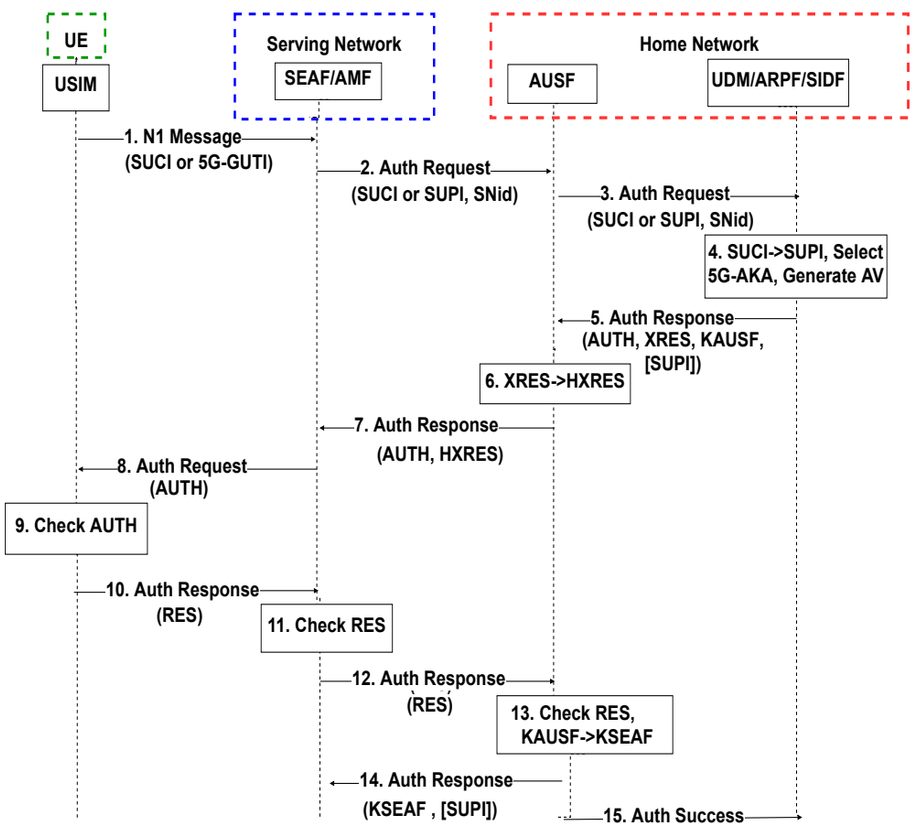


Fig. 3.2 5G-AKA Procedure for authentication [Ins19].

3.4 5G ProSe Standard

4G and 5G Cellular networks allow UEs to establish independent D2D connections for data exchange. For 4G and 5G networks the current D2D standard is 3GPP

ProSe standards (TS 33.303) [Off20a] and (TR 23.752) [Off20b], respectively. The ProSe is a D2D standard allowing LTE/5G devices to detect each other and to communicate directly. The ProSe standard comprises the ProSe discovery and the ProSe Direct Communication, which enables establish communication paths between two or more ProSe-enabled UEs. The 5G (TR 23.752) ProSe [Off20b] defines the following functions for D2D communication:

- **5G** ProSe Direct Discovery: A procedure employed by a ProSe-enabled UE to discover other ProSe-enabled UEs in its vicinity by using only the capabilities of the two UEs with New Radio (NR) technology.
- **5G ProSe UE-to-Network Relay**: A UE that provides functionality to support connectivity to the network for Remote UEs. Based on our network model, we focus on this case, where the leader drone represents the UE-to-Network relay. However, our approach can also work for the Direct Discovery mode.

The current 3GPP ProSe standards (TS 33.303) under the 4G ProSe [Off20a], includes the ability to use a UE node as a UE-network relay as well as connection establishment with it requires an in-advance key exchange process. The nodes which will use ProSe services first needs to register with ProSe Function and then make a *Key Request* to ProSe Key Management Function (PKMF), both of which are unique units residing within the 4G core [Off20a]. PKMF will issue a symmetric key with an ID (i.e., PKUK ID). Similarly, when a node acting as UE-network relay is contacted by a remote UE, it will need to make another *Key Request* to the PKMF for getting the same symmetric key corresponding to the PKUK ID. Hence, both nodes will agree on the same symmetric key and can move on to authenticate each other. Although the security mechanism for the ProSe is well defined for 4G/LTE, there is still no finalized security standard for the 5G standard yet [Off20b].

3.5 Proxy Signatures

We utilize Kim, Park and Won's proxy signature scheme [LKK01], where a proxy key pair depends on the signer private key for authentic information on the proxy signer's identity. Hence, in this model, the proxy signer's identity is protected using the node's authentic key pair (x_i, y_i). This is considered a strong proxy signature since it represents both original signer's in the form of a *warrant* w_i

and proxy signer's signatures (i.e., the node's private-public key pair (x_i, y_i)). Once a proxy signer creates a valid proxy signature, no one can ever repudiate his/her signature.

To further elaborate on this scheme, let the 5G core network (i.e., the original signer) be node A and the under authentication drone (i.e., the proxy signer) be node B. First, node A generates a random number K_A from a g generator of multiplicative subgroup Z_q^* with order of large prime q, and hence, $K_A \in Z_q^*$. Then, node A computes two proxy parameters $r_A = g^{K_A}$ and $s_A = x_A h(m_w w, r_A) + K_A$, where x_A is A's private key, $h()$ is a collision resistant hash function and m_w is A's signed warrant. The tuple (r_A, s_A) is A's signature for m_w, where (m_w, r_A, s_A) has to be sent secretly to node B. Next, once node B verifies the received tuple as $g^{s_A} \stackrel{?}{=} y_A^{h(m_w w, r_A)} r_A$, it then generates the proxy signature keys as follows:

$$\begin{aligned} x_p &= s_A + h(m_w, r_A) x_B \\ y_p &= (y_A y_B)^{h(m_w, r_A)} r_A \end{aligned} \tag{3.3}$$

This means, Node B can authenticate itself to other nodes on behalf of the original signer A using the proxy signature keys x_p and y_p.

Notation: Lower- and upper-case bold letters denote vectors and matrices, respectively, also $\mathbf{I}_M$ denotes the identity matrix of size M. The operations $(\cdot)^T$, $\mathbb{E}[\cdot]$, and $|\cdot|$ denote the transpose, statistical expectation and absolute value, respectively. The $\mathbf{A} \preceq \mathbf{B}$ denotes that $\mathbf{B} - \mathbf{A}$ is a positive semi-definite matrix. Finally, $\otimes$ denotes the Kronecker product operation.

CHAPTER 4

UAV POSITIONING FOR OUT-OF-BAND INTEGRATED ACCESS AND BACKHAUL MILLIMETER WAVE NETWORK

4.1 Introduction

This chapter aims to find the optimum locations for a set of UAVs operating in the mmWave frequency band to achieve an efficient coverage-connectivity tradeoff in an IAB mmWave network. On the one hand, the network connectivity is characterized in terms of the algebraic connectivity (Fiedler value) [GY04, Sli13], which is the second smallest eigenvalue of the Laplacian matrix representing the backhaul network graph. On the other hand, the coverage is defined by the threshold on the SINR. We consider an out-of-band (OOB) IAB network, in which there is no interference between the access and backhaul networks, as they operate on the different frequency bands. However, interference within the access network is considered and mitigated by optimizing the UAVs' locations. Given such system and considerations, we formulate the UAV optimization problem as finding the optimal UAVs' locations that maximize the backhaul network connectivity while maintaining the desired SINR above a certain threshold for all the served UEs. Given the complexity of the formulated UAV-based OOB IAB problem, we relax it through a number of steps to be prepared as a low-complexity SDP optimization problem. Computer simulations are conducted, taking into consideration the relevant mmWave frequency ranges and channel models. The proposed schemes' results show higher connectivity measures (Fiedler value) while achieving the UEs' desired SINR threshold. We point out that none of the previous works optimized the UAV position to jointly extend the access network coverage and enhance the backhaul network connectivity. To the best of our knowledge, this chapter is the first to address the tradeoff between coverage and connectivity and improve such tradeoff by utilizing and optimizing UAVs' positioning.

Our contributions in this chapter can be summarized as follows:

- Formulating a novel UAV-based IAB positioning problem, in which we aim to maximize the *backhaul* network connectivity while providing the desired SINR for all users in the *access* network.
- Mathematically relaxing the formulated optimization problem to be an SDP one that can be solved numerically with reasonable complexity.

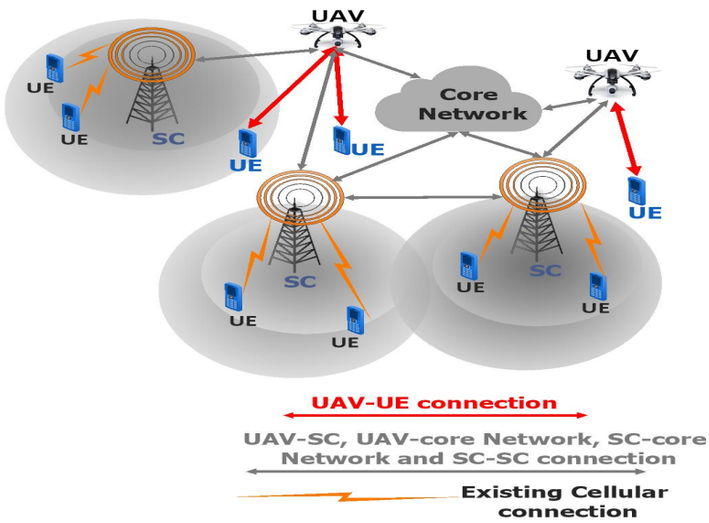


Fig. 4.1 System model of UAV-based integrated access and backhaul network.

- The proposed algorithm finds the best positions for the considered UAVs to enhance the backhaul network's algebraic connectivity. In the meantime, we are achieving the desired SINR for all the users on the mmWave access network.

The rest of this chapter is organized as follows; first, the system model describing both the access and backhaul networks is described in Section 4.2. The optimization problem is formulated in Section 4.3. Section 4.4 introduces the problem relaxation and the proposed solution. Finally, numerical results are provided in Sections 4.5.

4.2 System Model

In this section, we describe the system model covering both the access and backhaul networks. Fig. 4.1 depicts an IAB network which generally consists of N Small Cells (SCs) and M UEs. The N SCs are typically connected to each other as well as to the core network. The closest SC serves the UEs; however, the UE may lose the connection if they become out of the coverage range. In Fig. 4.1, we show that a UAV can be deployed to serve two purposes. First, it can enhance the backhaul network's connectivity by relaying information among the SCs and core network. Second, it can serve the UEs who are initially out of the SCs coverage.

We consider an OOB-IAB network, where the transmissions from the UAVs to SCs and UEs are assumed to be frequency division multiplexed (FDM), i.e., UAV-to-SC and UAV-to-UE communication links occur over different carrier frequencies with no interference between these two tiers. In the next subsection, we

introduce how to utilize graph theory in modeling the backhaul network while modeling the access network using communication theory. The notations used through this chapter are defined in Table 4.1.

Table 4.1 Notations.

Parameter	Definition
N	Number of SCs.
M	Number of UEs.
K	Total number of UAVs.
K_J	Number of UAVs assigned to serve both the UEs and SCs.
$P_{k,UE}$	Transmitted power from the k^{th} UAV
$h_{k,i}$	Channel coefficient channel between the k^{th} UAV and the i^{th} UE.
$d_{k,i}$	Distance between the k^{th} UAV and the i^{th} UE.
α	Path loss exponent.
I_i	Interference for the i^{th} UE.
$P_{j,UE}$	Transmitted power from the j^{th} UAV to other users.
γ	UEs' SINR matrix.
P_{I_i}	Interference power
σ^2	Additive white Gaussian noise (AWGN) variance
$\lambda_2(L)$	Algebraic connectivity (Fiedler value) of a graph that represents a network.
P_{UAV}	UAV maximum transmission power.
R_{SC}	SCs transmission range.
R_{UAV}	UAVss transmission range.
δ	Quantization step size.

4.2.1 Graph-theoretic Backhaul Network Modeling

The field of *graph theory* provides a good mathematical framework to analyze the connectivity of the backhaul network. Therefore in this chapter, we consider a graph-theoretic approach to model the backhaul network of small cells and UAVs as follows. Fig. 4.2 depicts the modeling of the SC backhaul network as an undirected weighted finite graph $\mathcal{G}(\mathbf{V}, \mathbf{E})$ where $\mathbf{V} = \{v_1, v_2, \cdots, v_N\}$ is the set of the SCs nodes and $\mathbf{E} = \{e_1, e_2, \cdots, e_Q\}$ is the set of all Q edges (links) among the SCs. The undirected graph implies that all the links in the network are bidirectional. Edges are defined based on the distance-based disk model [MSBD16]. In the considered disk model, an edge exists between two nodes if the distance between those nodes is less than R_{SC}. We point out that

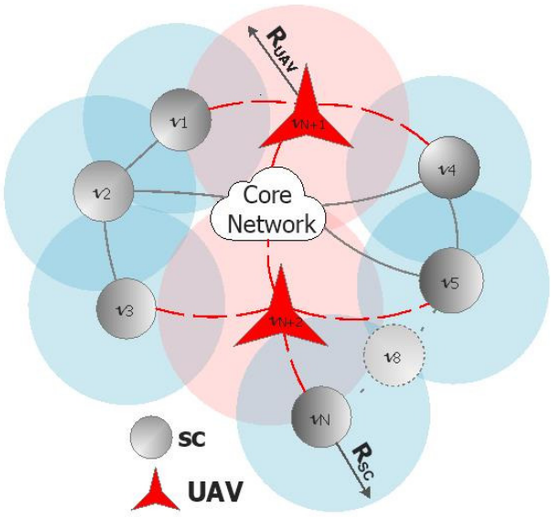


Fig. 4.2 Backhaul network modeling.

the orthogonal transmission among the SCs and UAVs results in no interference, and hence it is accurately represented by the distance-based model.

For an edge $q, 1 \leq q \leq Q$, connecting nodes $v_i, v_j \in V$, define the edge vector $\mathbf{a}_q \in \mathbf{R}^{N\times 1}$, where the i^{th} and j^{th} elements are given by $a_{q,i} = 1$ and $a_{q,j} = -1$, respectively, and the rest is zero. The relationship between the N vertices and the corresponding Q links between those vertices in $\mathcal{G}$ is captured in a matrix named the incidence matrix $\mathbf{A} \in \mathbf{R}^{N\times Q}$, where the q^{th} column is given by $\mathbf{a}_q$. For this undirected graph, the Laplacian matrix $\mathbf{L}(\mathbf{A}) \in \mathbf{R}^{N\times N}$ is defined as:

$$\mathbf{L}(\mathbf{A}) = \mathbf{A}\,\mathrm{diag}(\mathbf{w})\mathbf{A}^T = \sum_{q=1}^{Q} w_q \mathbf{a}_q \mathbf{a}_q^T, \tag{4.1}$$

where $\mathbf{w}$ denotes the $q\times 1$ weighting vector coefficients for the q edges and is given by $[w_1, w_2, \cdots, w_q]^T$ and diag $(\mathbf{w})$ is $Q \times Q$ diagonal matrix with the $\mathbf{w}$ as the diagonal elements. The Laplacian matrix for such graph is positive semi-definite, which is expressed as $\mathbf{L}(\mathbf{A}) \succcurlyeq 0$ and also its smallest eigenvalue is zero, i.e., $\lambda_1(\mathbf{L}(\mathbf{A})) = 0$. The second smallest eigenvalue of $\mathbf{L}(\mathbf{A})$, $\lambda_2(\mathbf{L}(\mathbf{A}))$, is the algebraic connectivity, or Fiedler value, of the graph $\mathcal{G}$ [Fie73, GB06]. In this chapter, the Fiedler value will be utilized to measure the backhaul network connectivity.

4.2.2 Interference-Based Access Network Modeling

This section introduces the downlink access network modeling, which consists of small cells or UAVs on one side and UEs on the other side. Our goal is to model the received SINR at UEs as the primary QoS metric for UEs. To calculate the SINR, we assume a distance-based association model in which each UE will be served by its closest serving station, which is either an SC or a UAV. Moreover, K_J

UAVs are jointly assigned to serve the UEs and SCs. The remaining $K - K_J$ UAVs are only used to enhance the SCs connectivity. In addition to the conventional association model, we also consider a *load balancing* scheme to have an equal share of users assigned to each serving station. More precisely, the UAVs serving the UEs are selected depending on their distance from each UAV, with an equal UEs distribution for each UAV. The maximum number of UEs attached to each UAV is equal to $\frac{M}{K_J}$.

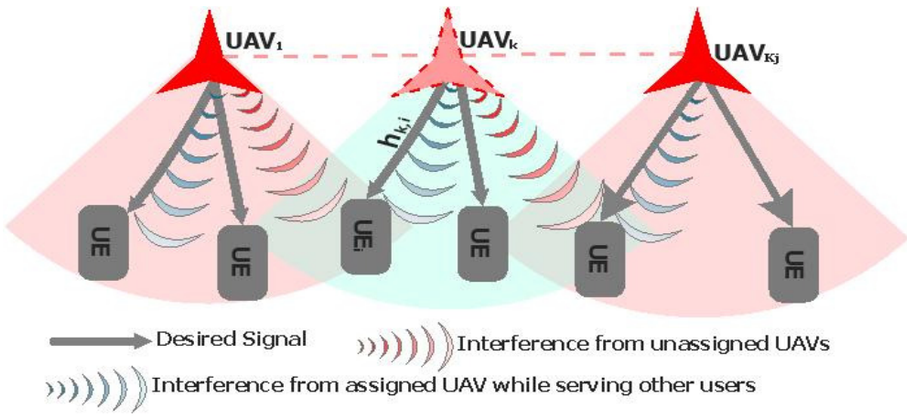


Fig. 4.3 Interference-based access network modeling.

Along with the considered distance-based association model, we also consider multiple interference sources. The interference-based model is shown in Fig. 4.3, where the received signal at any UE is the desired signal from the assigned UAV along with additional interfering signals. There are two different interference sources, as shown in Fig. 4.3. One is the interference from the same UAV assigned to the user while serving other trusted users. The second source of interference is from other UAVs that are serving their assigned users.

The received signal at a given UE, i, which is associated with the k^{th} UAV is modeled as

$$y_i = \sqrt{P_{k,UE}}\, h_{k,i}\, d_{k,i}^{-\alpha/2} x_{k,i} + I_i + n_i, \tag{4.2}$$

where $P_{k,UE}$ is the transmitted power from the k^{th} UAV. We assume equal power distribution among all UEs assigned to the k^{th} UAV. The $h_{k,i}$ is the channel coefficient corresponding to the channel between the k^{th} UAV and the i^{th} UE. Furthermore, $x_{k,i}$ represents the transmitted symbol from the k^{th} UAV towards its potentially-served i^{th} UE with a unit power $\mathbb{E}\{|x_{k,i}|^2\} = 1$ and $d_{k,i}$ denotes the distance between the k^{th} UAV and the i^{th} UE. n_i denotes complex zero-mean circularly-symmetric additive white Gaussian noise (AWGN) with variance σ^2,

representing the noise at the i^{th} UE, and it is assumed to be independent across the UEs. Moreover, I_i represents the interference for the i^{th} UE, where

$$I_i = \sum_{m=1, m\neq i}^{M/K_J} \sqrt{P_{k,UE}}\, h_{k,i} d_{k,i}^{-\alpha/2} x_{k,m} + \sum_{j=1, j\neq k}^{K_J} \sum_{m=1}^{M/K_J} \sqrt{P_{j,UE}}\, h_{j,i} d_{j,i}^{-\alpha/2} x_{j,m}, \quad (4.3)$$

where $P_{j,UE}$ is the transmitted power from the j^{th} UAV to other users.

As previously shown in Fig. 4.3, deploying multiple UAVs introduces two types of interference. The first interference is due to the same UAV users, which is the first part of I_i. The second type of interference is due to signals from other UAVs.

Then, the SINR of all the UEs is given by $\gamma \in \mathbf{R}^{M\times 1}$, where each element represents the i^{th} UE SINR and is given by

$$\gamma_i = \frac{P_{k,UE}\, d_{k,i}^{-\alpha} \left|h_{k,i}\right|^2}{P_{I_i} + \sigma^2}. \quad (4.4)$$

where P_{I_i} is the interference power given as

$$P_{I_i} = \sum_{m=1, m\neq i}^{M/K_J} P_{k,UE}\, d_{k,i}^{-\alpha} + \sum_{j=1, j\neq k}^{K_J} \sum_{m=1}^{M/K_J} P_{j,UE}\, d_{j,i}^{-\alpha}. \quad (4.5)$$

For an extensive network of multiple SCs and UAVs, we can assume that we will have a large number of short terms representing the interference in Eq. (4.3). Therefore, for simplicity of analysis and using the central limit theory, their addition can be represented by their average value. In other words, we can ignore the small-scale channel coefficients in the interference term Eq. (4.3) while calculating the interference power in Eq. (4.5). Therefore, the interference term in Eq. (4.3) depends only on large scale fading.

4.3 Problem Formulation

In this section, we formulate the UAV-based IAB positioning problem. We aim to maximize the backhaul network connectivity while providing the desired SINR for all access network users. For the backhaul network with K UAV deployment, a new graph $\mathcal{G}'$ is obtained with the same number of N nodes, a larger set of edges denoted by $\mathbf{E}'$ with Q' edges where $Q' \geq Q$, i.e., $\mathbf{E} \subseteq \mathbf{E}'$. As was shown previously in Fig. 4.2, a given UAV can create a new edge between two SCs, if they fall within its communication range, by relaying the information among them. Then, the optimization problem of deploying K UAVs to increase the backhaul

connectivity, while providing the desired SINR to the UEs, is formulated as

$$\begin{aligned} &\max_{\mathbf{E}'} \ \lambda_2(\mathbf{L}(\mathbf{E}')) \\ &\text{s. t. } \ \gamma_i \geq \gamma_{\text{th}}, \ \forall i \in \{1, \ \ldots, \ N\}, \\ &\qquad M \ P_{k,UE} + n \ P_{k,SC} \ \leq P_{UAV}, \ \forall k \in \{1, \ \ldots, \ K_J\}, \\ &\qquad (N-n) \ P_{k,SC} \ \leq P_{UAV}, \ \forall k \in \{K_J + 1, \ \ldots, \ K\}, \end{aligned} \tag{4.6}$$

where $P_{k,SC}$ is the transmission power from the k^{th} UAV to a single SC and P_{UAV} is the UAV maximum transmission power, we assume all the UAVs have the same maximum transmission power. Also, n is the number of SCs which the UAVs serve jointly with UEs and $(N-n)$ is the remaining SCs which are served separately by the extra UAVs.

The objective function is to maximize the SCs backhaul connectivity represented by the algebraic connectivity (Fiedler value), introduced in Section 4.2.1. Then, three constraints are considered: the first constraint is to provide a QoS to the UEs by assuring a certain SINR level to each UE. The next two constraints are to ensure that the maximum UAV power is not violated by either the SCs or the UEs connections. We assume the UAV power is equally distributed between the UAV-SC and UAV-UE connections. The total power allocated to the UAV-UE links is equally distributed over all UEs assigned to the UAV. Similarly, the total power allocated to the UAV-SC is equally allocated to all SCs. The total UAV power, P_{UAV}, is equally divided into two groups: UEs and the group of SCs. Half of the UAV power, $\frac{P_{UAV}}{2}$, is equally divided among the transmissions to all the UEs associated with the UAV. The second half of the UAV power, $\frac{P_{UAV}}{2}$, is equally divided among the transmissions towards all the SCs connected with the UAV.

4.4 Problem Relaxation and Proposed Solution

In the next section, we introduce the proposed approach to relax the optimization problem under consideration and then present the proposed solution.

4.4.1 Problem Relaxation

Since each UAV can be deployed anywhere in the 3-D network, the location of each UAV is considered as a continuous variable, which belongs to the interval $([0,h],[0,h],[0,h])$. It has been shown that this problem is NP-hard in [HSSM05].

To tackle this NP-hard problem [ISL09b], we convert the continuous optimization problem into a discrete one by considering that the SCs and UEs are distributed over $h \times h \times h$ volume. Moreover, the search space over the $x,\ y,$ and z axes is uniformly quantized with a step size δ to get a search grid consisting of β candidate positions for the UAV, which converts the continuous deploying to a discrete search in a finite number of available positions on the grid.

Thus, the Laplacian matrix is represented by the following formula:

$$\mathbf{L}(\mathbf{E}') = \mathbf{L}(\mathbf{E}) + \sum_{j=1}^{\beta} x_j \mathbf{A}_j \operatorname{diag}(\mathbf{w}_j) \mathbf{A}_j^T, \tag{4.7}$$

where $\mathbf{L}(\mathbf{E})$ is the original graph before UAV deployment and $x_j = 1$ if UAV is positioned in the j^{th} grid point, otherwise $x_j = 0$. Moreover, $\mathbf{w}_j$ and $\mathbf{A}_j$ are the weighting coefficients vectors and the incidence matrix when the UAV is deployed in this grid point. Collecting $x_j,\ j \in \{1,\ \ldots,\ \beta\}$, in the $\beta \times 1$ vector $\mathbf{x}$, Eqn. (4.7) can be written as follows:

$$\mathbf{L}(\mathbf{E}'(\mathbf{x})) = \mathbf{L}(\mathbf{E}) + (\mathbf{x} \otimes \mathbf{I}_M)\, \mathbf{\Gamma}, \tag{4.8}$$

where

$$\mathbf{\Gamma} \triangleq \left[\left(\mathbf{A}_1 \operatorname{diag}(\mathbf{w}_1) \mathbf{A}_1^T \right)^T,\ \ldots,\ \left(\mathbf{A}_\beta \operatorname{diag}(\mathbf{w}_\beta) \mathbf{A}_\beta^T \right)^T \right]^T. \tag{4.9}$$

Then the Backhaul connectivity enhancement problem can be formulated as

$$\begin{aligned} &\max_{\mathbf{x}}\ \ \lambda_2(\mathbf{L}(\mathbf{A}(\mathbf{x}))) \\ &\text{s. t.}\ \ \gamma_i \geq \gamma_{\text{th}},\ \forall i \in \{1,\ \ldots,\ N\}, \\ &\qquad M\ P_{k,UE} + n\ P_{k,SC}\ \leq P_{UAV},\ \forall k \in \{1,\ \ldots,\ K_J\}, \\ &\qquad (N-n)\ P_{k,SC}\ \leq P_{UAV},\ \forall k \in \{K_J+1,\ \ldots,\ K\}, \end{aligned} \tag{4.10}$$

where $\mathbf{x} \in \{0, 1\}$.

Furthermore, we accumulate the SINR levels between the i^{th} UE and the associated UAV in a matrix $\mathbf{V} \in \mathbf{R}^{\beta \times M}$ such that each column, $\mathbf{v}_i$, can be written as

$$\mathbf{v}_i = \left[\gamma_i|_{\{d_{k,i}, d_{k,j}\} \in \mathbf{D_1}}, \gamma_i|_{\{d_{k,i}, d_{k,j}\} \in \mathbf{D_2}}, \ldots, \gamma_i|_{\{d_{k,i}, d_{k,j}\} \in \mathbf{D}_\beta} \right]^T, \tag{4.11}$$

where $\mathbf{D_i} \in \mathbf{R}^{M \times K_J}, \forall i \in \{1, 2, \cdots, \beta\}$ is the distance between each UE and each UAV at only certain positions within the grid points only $(1, 2, \ldots, \beta)$. Hence, the optimization problem can be written in terms of the UAV position index vector

$\mathbf{x}$ as follows

$$\begin{aligned}
&\max_{\mathbf{x}} \ \lambda_2(\mathbf{L}(\mathbf{A}(\mathbf{x}))) \\
&\text{s. t. } \ \mathbf{x}^T\mathbf{V} \geq \mathbf{1}^T\gamma_{\text{th}}, \\
&\qquad \mathbf{1}^T\mathbf{x} \leq K, \ \mathbf{x} \in \{0,1\}, \\
&\qquad M \ P_{k,UE} + n \ P_{k,SC} \ \leq P_{UAV}, \ \forall k \in \{1, \ \ldots, \ K_J\}, \\
&\qquad (N-n) \ P_{k,SC} \ \leq P_{UAV}, \ \forall k \in \{K_J+1, \ \ldots, \ K\},
\end{aligned} \tag{4.12}$$

We relax the constraint on the entries of $\mathbf{x}$ and allow them to take any value in the interval $[0,1]$. $\lambda_2(\mathbf{L}(\mathbf{A}(\mathbf{x})))$ can be written as the point-wise infimum of a family of linear functions of $\mathbf{x}$ as

$$\lambda_2(\mathbf{L}(\mathbf{A}(\mathbf{x}))) = \inf_y [y^T\mathbf{L}(\mathbf{A}(\mathbf{x}))y, \parallel y \parallel_2 = 1, \mathbf{1}^T y = 0]. \tag{4.13}$$

Hence, it is a concave function in $\mathbf{x}$. In addition, the relaxed constraints are linear in $\mathbf{x}$. Therefore, the optimization problem is a convex optimization problem with linear constraints. Furthermore, the optimization problem in Eq.(4.6) can be written as a Semi-definite Programming (SDP), which is a subcategory of the convex optimization.

The relaxed SDP optimization problem can be written as follows [BV04]

$$\begin{aligned}
&\mathbf{P1}: \max_{\mathbf{x},s} \ s \\
&\qquad \text{s. t. } \ s(\mathbf{I} - \frac{1}{\beta}\mathbf{1}\mathbf{1}^T) \preceq \mathbf{L}(\mathbf{A}(\mathbf{x})), \\
&\qquad\qquad \mathbf{x}^T\mathbf{V} \geq \mathbf{1}^T\gamma_{\text{th}}, \\
&\qquad\qquad \mathbf{1}^T\mathbf{x} \leq K, \ 0 \leq \mathbf{x} \leq 1, \\
&\qquad\qquad M \ P_{k,UE} + n \ P_{k,SC} \ \leq P_{UAV}, \ \forall k \in \{1, \ \ldots, \ K_J\}, \\
&\qquad\qquad (N-n) \ P_{k,SC} \ \leq P_{UAV}, \ \forall k \in \{K_J+1, \ \ldots, \ K\}.
\end{aligned} \tag{4.14}$$

4.4.2 Proposed Solution

The relaxed SDP problem in Eq. (4.14) can be solved using an SDP solver such as CVX SDPT3 solver [GBY08]. Afterward, and since the entries of output vector $\mathbf{x}$ are continuous, we choose the maximum entry and set it to 1, while others are set to zero.

Algorithm 1 summarizes the solution steps as follows; first, the total 3-D area is quantized to the $h \times h \times h$ cubes as mentioned in Section 4.2. Then, the new network, including both the SCs and the UAVs, is defined using the incidence matrix $A(x)$ for all the permutations of possible positions (cubes) in the grid,

Algorithm 1 K UAVs Positioning

Input: (X_{SC}, Y_{SC}, Z_{SC}) and (X_{UE}, Y_{UE}, Z_{UE})
$\mathbf{A} \leftarrow$ the graph incidence Matrix
$\lambda_2(\mathbf{L}(\mathbf{A})) \leftarrow$ connectivity of SCs
Quantize:
$\beta \leftarrow$ Grid positions
$\mathbf{x} \leftarrow \beta \times 1$ vector
$P(\beta) \leftarrow$ permutation of all grid positions
for $\forall k \leq K_J \& \forall P(\beta)$ **do**
Link Matrix:
    $A(\mathbf{x}) \leftarrow$ Link matrix after adding $UAVs$
    $\mathbf{L}(\mathbf{x}) \leftarrow$ Laplacian matrix after adding $UAVs$
Association $\forall k \leq K_J$:
    $\mathbf{D} \leftarrow$ Distance matrix after adding $UAVs$
    $\gamma(\mathbf{D}) \leftarrow$ The UEs SINR
    $\mathbf{S}(\mathbf{D}) \leftarrow$ association matrix after adding $UAVs$
    $I\mathbf{S}(\mathbf{D}) \leftarrow$ Interference matrix
end for
for K **do**
Optimization:
    $\max_{\mathbf{x}} \ \lambda_2(\mathbf{L}(\mathbf{A}(\mathbf{x})))$
    if $\gamma(\mathbf{D}) \geq \gamma_{th}$ & UAV total power $\leq P_{UAV}$ **then**
        Break
    else
        goto *Optimization*.
        $(X_{UAV}, Y_{UAV}, Z_{UAV}) \leftarrow \max_K(\mathbf{x})$.
    end if
end for
Output: $(X_{UAV}, Y_{UAV}, Z_{UAV})$

$P(\beta)$. Next, we construct the distance matrix, $\mathbf{D}$, of all possible locations for the UAVs. Also, we construct the association matrix, $\mathbf{S}(\mathbf{D})$, to find the UEs assigned to each UAV depending on the distance matrix and the maximum load assigned to each UAV.

Next, the optimization solver is executed to find the maximum backhaul network connectivity while providing the desired SINR, γ_{th}, for all users in the access network. The output optimized UAVs' locations in the grid system is obtained as a probability distribution of $0 \leq \mathbf{x} \leq 1$ due to the SDP relaxation. Hence, We receive the UAVs' locations by finding the maximum K values of $\mathbf{x}$. Then, the UAVs' Cartesian locations are calculated by reversing the griding quantization operation.

In terms of the complexity of the proposed algorithm, first, we point out that the interior point algorithms for solving SDP optimization problems are shown to be polynomial in time [FFK$^+$00]. Therefore, the proposed UAV positioning scheme, which applies a small number of iterations, requires solving the SDP optimization problem and has a polynomial complexity in time.

Finally, we point out that the proposed solution will be implemented via a central node (e.g., core network) that has access to all the information in the network, which is needed to solve the optimization problem in Eq. (4.14). The central node will accordingly direct the UAVs to take their positions according to the obtained solution.

Table 4.2 Simulation parameters.

Parameter	Value
h	100 m
N	10
M	2
K	1
R_{SC}	40 m
R_{UAV}	40 m
α	4
σ^2	-130 dBm
P_{UAV}	30 dBm
δ	6 m
γ_{th}	30 dB

4.5 Simulation Results

This section presents simulation results to demonstrate the achievable performance of the proposed UAV-based IAB positioning algorithm. Our goal is to show the performance improvement in the backhaul network connectivity while providing the desired SINR for all access network users. For comparison purposes, we also consider a *random* positioning approach, in which the UAVs are deployed randomly while the SINR threshold constraints are satisfied for all the UEs. The simulation is executed using MATLAB SDPT3 solver with the simulation parameters listed in Table 4.2. The results are averaged over 10^3 different backhaul network realizations and UEs deployment locations. The 28 GHz mmWave channel coefficients are obtained through NYUSIM [SMR17], which is a developed channel model simulator for the mmWave wireless communications.

Next, we present the results for the single UAV deployment in Section 4.5.1. The multiple UAV simulation results are presented in Section 4.5.2.

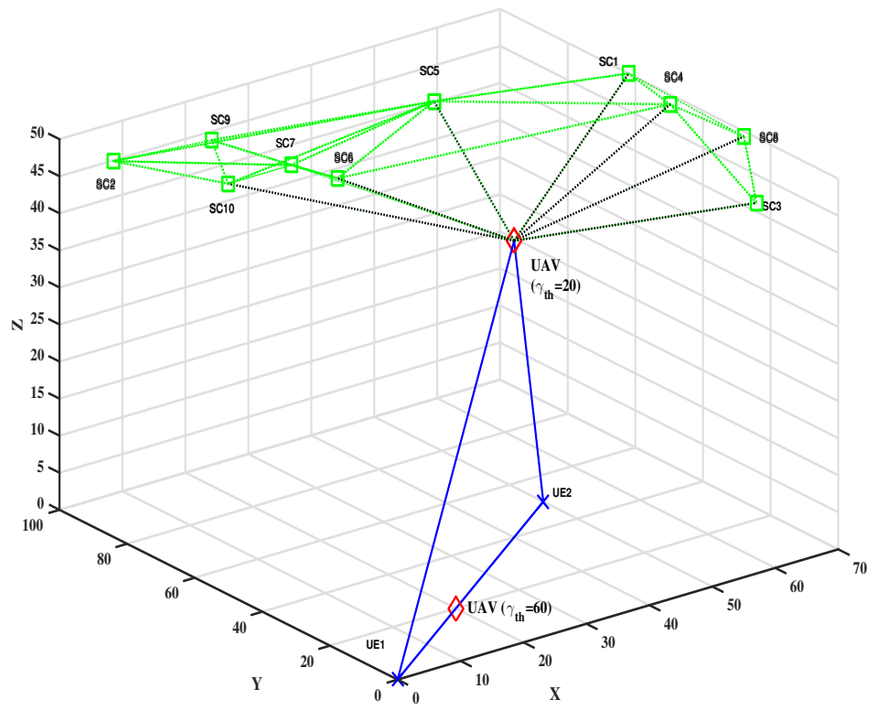


Fig. 4.4 UAV positioning for different γ_{th}. The square, cross and diamond markers represent SC, UE and UAV, respectively.

4.5.1 Single UAV Simulation Results

This section shows the approximated SDP optimization solution in Eq. (4.14) to find the optimal deployment of a single UAV deployment problem. We assume no interference case, and hence, the SINR threshold is treated as only SNR threshold. The impact of changing γ_{th} on the UAV positioning is shown in Fig. 4.4, where the UAV position in the 3-D search grid with red diamond markers is plotted for two extreme cases for the UEs constraints. In the first case, $\gamma_{th} = 20$ dB corresponding to low QoS constraint. In this case, the UAV gets closer to the SCs to enhance the backhaul network connectivity. The original network connectivity is $\lambda_2(\mathbf{L}(\mathbf{x})) = 2.015$ and the UAV deployment achieves $\lambda_2(\mathbf{L}(\mathbf{x})) = 6.476$, which is more than three times the original backhaul connectivity. In the other case at $\gamma_{th} = 60$ dB, which represents a high QoS constraint, the UAV gets closer to the UEs to satisfy their tight constraints with no improvement for the backhaul network connectivity.

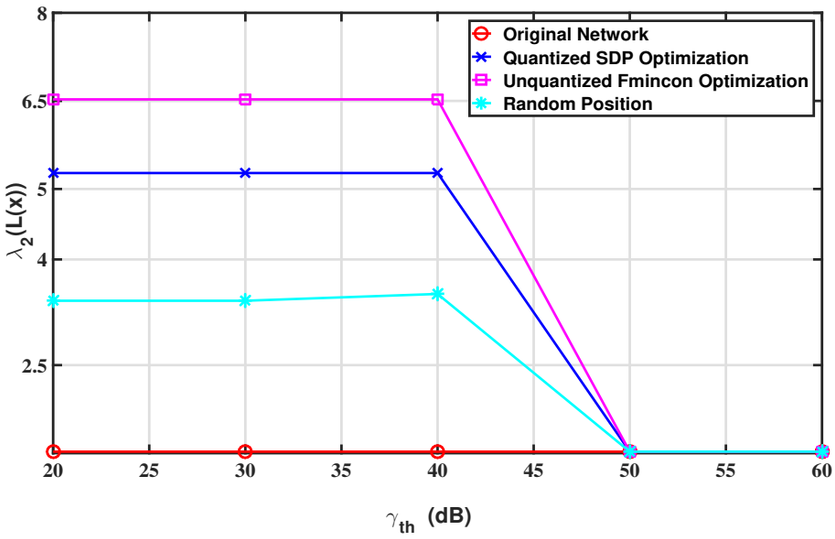


Fig. 4.5 The connectivity of the SCs versus the UEs SNR constraint for $\beta = 2197$, $\delta \cong 8$ m.

Quantization Step Size

Fig. 4.5 investigates the performance of the quantizing relaxation as compared to the unquantized optimization problem in Eq. (4.6). It depicts the Fiedler value of the SCs backhaul network graph as a function of the UEs SNR threshold γ_{th}. The unquantized optimization is solved using the non-convex *fmincon* numerical solver in MATLAB, with multi-initial point searching to avoid local minima situations. Assuming $\delta = 8$m in Eq. (4.14) for the quantized SDP optimization, Fig. 4.5 shows that increasing the γ_{th} decreases the connectivity for the different schemes. It is shown that the SDP-based quantized solution achieves nearly 35% gain compared to the random positioning scheme, for $\gamma_{th} = 30$ dB. It is also shown the that proposed SDP-algorithm achieves algebraic connectivity of 5.25, while the non-convex solver achieves 6.5. Hence, there is a performance gap of 24% due to relaxing the original non-convex optimization problem in this case.

To reduce the performance gap between the unquantized optimization and the SDP-based solution, we decrease the step size to $\delta = 6$ m, which results in a higher quantization resolution. As shown in Fig. 4.6, the output from the SDP optimization is the same as the unquantized optimization for all values of γ_{th}. Furthermore, at SNR threshold $\gamma_{th} = 30$ dB and considering $\delta = 6$ m, the quantized SDP-based solution achieves a gain of 60%, compared to the random positioning scheme. All the simulation results presented in the rest of this chapter will be based on the quantization step of $\delta = 6$ to avoid any performance gap due to relaxing the original non-convex optimization problem.

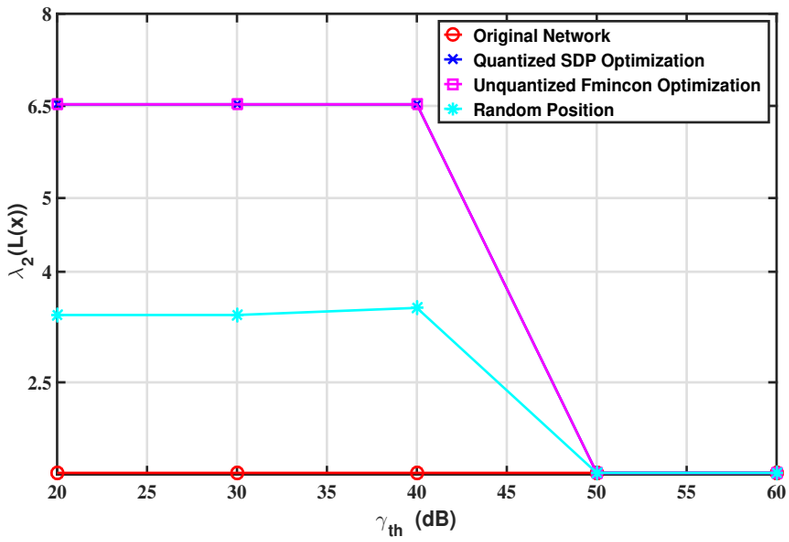


Fig. 4.6 The SCs connectivity versus the UEs SNR constraint for $\beta = 3,375$, $\delta \cong 6$ m.

Convergence of the Proposed SDP-based Algorithm

This subsection shows the convergence of the proposed solution, which is an integral characteristic of any iterative solution. In implementing the proposed solution, we have utilized the SDPT3 solver. Such solver produces its iterations' status, once concluded, which can be "solved", "Failed", or "unbounded". In an attempt to characterize the convergence of the proposed iterative solution, we show in Table 4.3 the ratio of the "solved" status, as opposed to the other ones, for 500 different network deployment scenarios. As shown, 90% of the iterations have resulted in a "solved" status leading to an optimum solution.

Table 4.3 Convergence analysis of the SDP algorithm.

SDPT3 status	Percentage
Solved	90%
Failed/Unbounded	10%

UAV Transmission Range

In this subsection, we investigate the effect of the UAV transmission range on the backhaul connectivity. In Fig. 4.7 the algebraic connectivity of the SCs backhaul network is plotted against the UAV transmission range, R_{UAV}. As shown, the backhaul connectivity enhances with the increase of the UAV transmission range. As the UAV transmission radius increases beyond a certain threshold, the

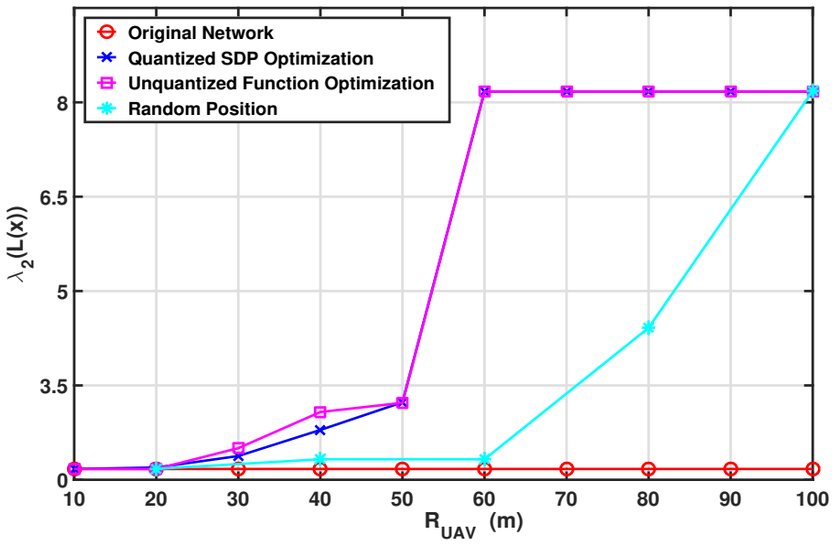


Fig. 4.7 The SCs connectivity versus the UAV transmission range for $\beta = 3,375$, $\delta \cong 6$ m.

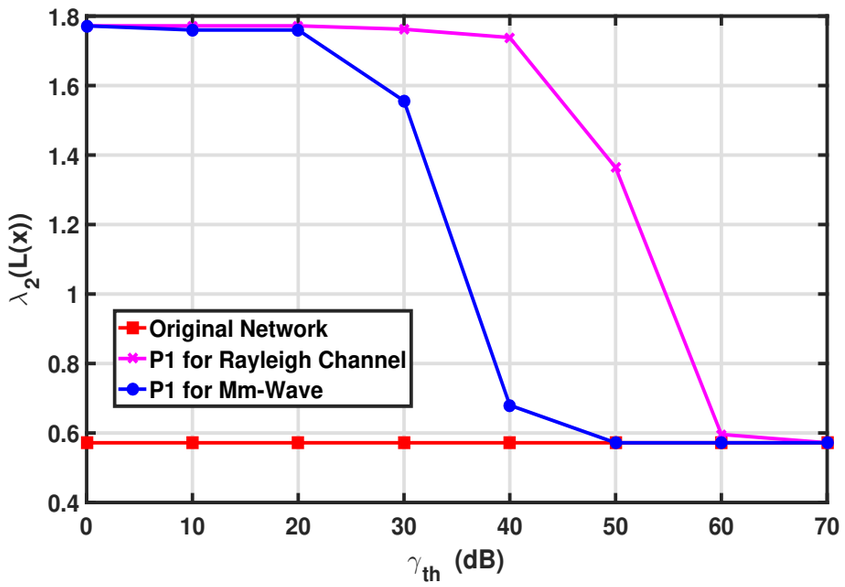


Fig. 4.8 The Rayleigh fading channel versus the mmWave channel.

network algebraic connectivity saturates at its maximum possible value. Similar to the above results, the proposed SDP-based solution outperforms the random positioning scheme.

Millimeter Wave Channel Impact

In this subsection, we will investigate the mmWave channel's impact on the SCs backhaul network's connectivity. The mmWave channel model at 28 Ghz is obtained through NYUSIM [SMR17]. Fig. 4.8 depicts the algebraic connectivity considering both the *Rayleigh* and the mmWave channel fading channel and assuming $\alpha = 4$. As a result of the higher-frequency of the mmWave signal, the

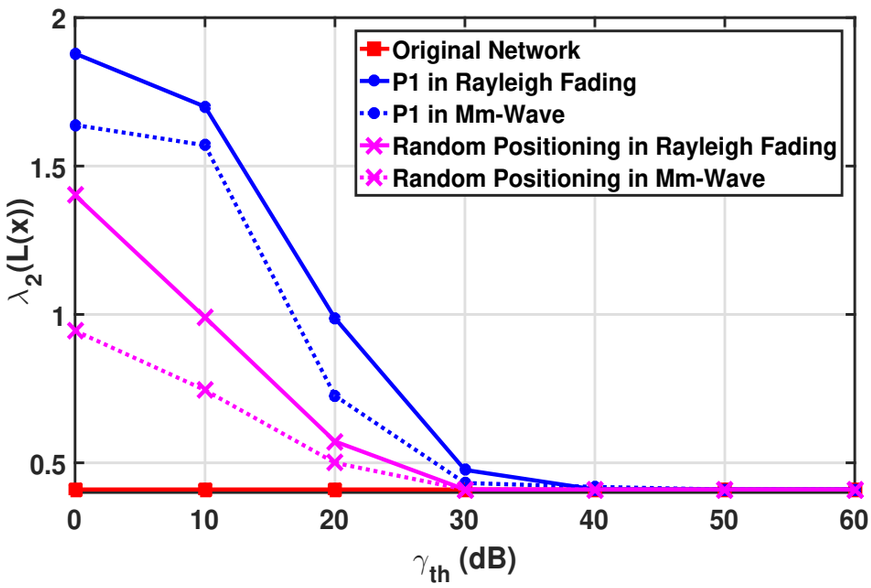


Fig. 4.9 The connectivity of the SCs versus the UEs γ_{th} for $K = 2$ UAVs.

transmission range is smaller compared to the Rayleigh model. Accordingly, the algebraic connectivity is less for the mmWave transmission.

4.5.2 Multiple UAV Simulation Results

This section provides the simulations results after solving Eq. (4.14) for multiple UAVs. Our goal is to find the optimal locations for the multiple UAVs that maximize the backhaul algebraic connectivity, subject to providing a certain SINR threshold for all the UEs.

Fig. 4.9 aims to show the performance of the proposed algorithm in the multiple UAV case. We consider the deployment of $K = 2$ UAVs seeking to serve $M = 8$ UEs. Fig. 4.9 shows that the proposed algorithm provides a better SCs connectivity compared to the UAVs' random positioning in both Rayleigh and mmWave channels. Similar to the single-UAV case in Fig. 4.8, the mmWave achieves lower connectivity than the Rayleigh fading. Compared to the random positioning scheme, Fig. 4.9 shows that deploying 2 UAVs achieve a performance gain of 100% for the Rayleigh channel and 80% for the mmWave channel, at an SINR threshold of 20 dB. The achieved performance over the random positioning is almost 60% for both mmWave and Rayleigh channels.

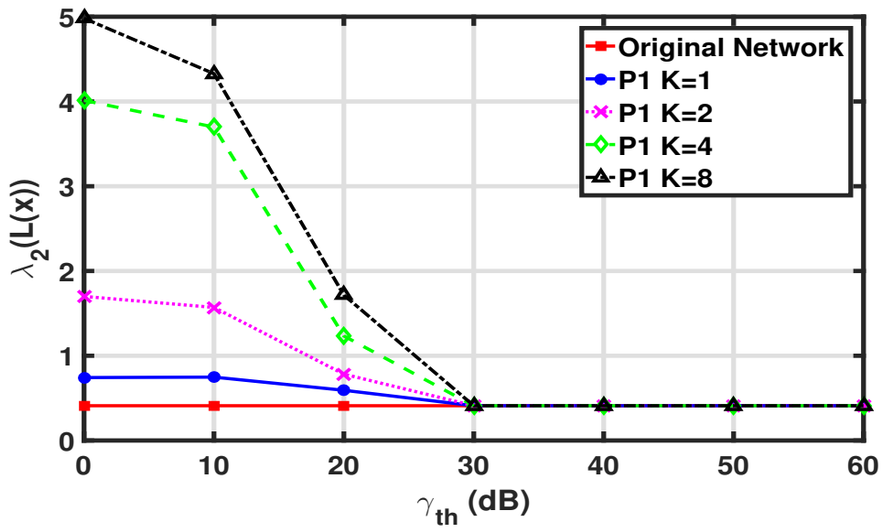


Fig. 4.10 The connectivity of the SCs versus the UEs γ_{th} for different number of UAVs.

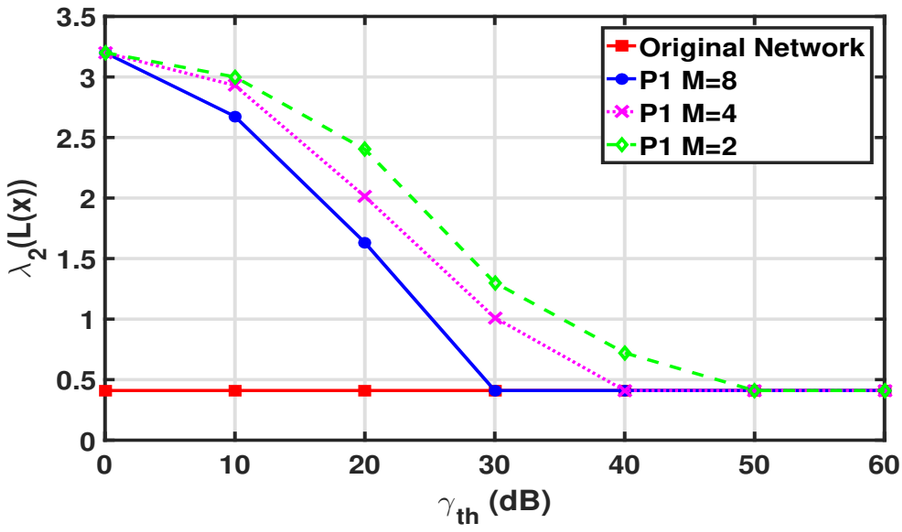


Fig. 4.11 The connectivity of the SCs versus the UEs γ_{th} for different number of UEs.

Impact of Number of UAVs

In Fig. 4.10, the SCs connectivity is plotted against the UEs SINR threshold for different number of UAVs, $K = 1, 2, 4$ *textsand*8, with the mmWave channel model. In this scenario, the connectivity of the SCs network grows with increasing the number of UAVs. For example, deploying $K = 4$ achieves a connectivity gain of almost 3 times (200% gain) the original network connectivity at the SINR threshold of 20 dB.

Dependency on the Number of UEs

Furthermore, we investigate the impact of the number of UEs served by each UAV by increasing the number of UEs,M, and keeping K fixed. In Fig. 4.11, the SCs connectivity is plotted versus the UEs SINR threshold γ_{th} at $K = 2$ UAVs. In this scenario, we notice a degradation in the algebraic connectivity as the number of UEs increases, which can be clarified as follows, increasing the number of UEs forces more UAVs to come closer to them to achieve the required UEs SINR. Consequently, the UAVs move away from the SCs, which leads to lower algebraic connectivity for the SCs backhaul network.

CHAPTER 5

UAV-ASSISTED MULTI-PATH PARALLEL ROUTING FOR MMWAVE-BASED WIRELESS NETWORKS

5.1 Introduction

This chapter investigates how the protocol stack's upper layers can improve the mmWave network throughput, particularly in an ad hoc network where streaming might be needed in cases of emergencies or post-disaster scenarios. That not only implies enhancing the reliability of mmWave communications (i.e., reduce packet losses due to mmWave short range) but also modeling the data traffic to support more traffic within a given period. Both purposes can be achieved by relying on the deployment of additional relays in the network. The most suitable relays for wireless ad hoc networks would be Unmanned Aerial Vehicles (UAVs), as they can be used on-demand for temporary purposes. That is particularly relevant for emergency applications, military setups, or Intelligent Transportation Systems (ITS) where additional connectivity is required [Bis00, BTM+06]. Therefore, we study the optimization problem for UAVs' deployment to improve network connectivity. Then, we find the most appropriate routes for data transmissions that can also exploit parallel routing to boost throughput.

We consider a UAV-assisted ad hoc network with mmWave links, where we aim to enhance the network connectivity by maximizing the algebraic connectivity of the UAV-based network graph. Second, a constraint is added to limit the acceptable E2E delay, and hence increase the network throughput. Jointly with choosing the minimum number of UAVs and their optimal positions, we also aim to define the UAVs *transmission powers* optimally. The problem of finding the design aspects of the UAV-based topology, as explained above, can be formulated as a complex constrained optimization problem. However, it can be relaxed to a SDP optimization problem, which can be solved efficiently using one of the available numerical SDP solvers.

Once the UAVs are optimally deployed, we propose forming multiple paths among each source-destination pair to provide alternative data paths in case of link failures. To this end, we propose a modified node-disjoint routing approach to minimize potential interference among inter-routes, which will enable *parallel* transmissions from the same source. In other words, we send the duplicate packets through multiple paths simultaneously to increase the likelihood of successful

reception at the receiver. To the best of our knowledge, the parallel transmission idea has not been exploited before for mmWave communications.

For the performance evaluation of the proposed approach, we used two simulation platforms. The first platform is MATLAB, which is utilized to solve the SDP optimization problem and find the deployed UAVs design parameters (3D positions and transmission powers). The second platform is the NS-3 network simulator, where we implement the IEEE 802.11*ay* mmWave communication protocol at 60 GHz, assuming an ad hoc network. Through the NS-3 simulations, we were able to show a significant increase in the network throughput while reducing the E2E delay when alternative or parallel paths are used for data transmission.

To the best of our knowledge, we are the first work that utilizes parallel routing for mmWave communications and incorporates this idea within the IEEE 802.11ad/ay standard. The limitations on the IEEE 802.11ad are regarding the transmission range, which is within $10 - 20$m. However, this problem was solved in IEEE 802.11ay using MIMO technology to obtain up to 300m. Nevertheless, since the IEEE 802.11ay implementation over NS-3 is not available to utilize yet, we utilized the IEEE 802.11ad implementation [AW16], where we updated the physical layer to have a MIMO transmission.

Based on the discussion aforementioned, the contributions of this chapter can be summarized as follows

- We propose an analytical solution for the UAV-based *network topology formation* constrained optimization problem, where the minimum number of UAVs, along with their locations and transmission powers, are identified; For this goal, we model the expected delay between a source and destination using a queuing analysis;
- We propose a multi-hop multi-path source routing scheme involving UAVs, that will also allow parallel transmissions at the network layer for increased reliability, and hence, throughput;
- We incorporate the PHY/MAC layers implementation of the IEEE 802.11ay protocol into the NS-3 simulator for developing a routing protocol with mmWave communication links and show that the developed analytical model closely matches the implementation results under NS-3.

The rest of this chapter is organized as follows. The system model is described in Section 4.2. The optimization problem and the routing model are described in

Table 5.1 Notations.

Parameter	Definition
K_V	Number of UAVs.
N	Number of nodes in the network.
s	Transmitter node.
r	Receiver node.
n	Path loss exponent.
$SINR_r$	Signal to interference-plus-noise ratio at the receiver.
$R_{s,r}$	Maximum rate between the transmitter and receiver.
W	MmWave transmission bandwidth.
f	MmWave transmission frequency.
D_{E2E}	End-to-End delay between the transmitter and receiver nodes.
(M/G/1,....)	Markov chain standard representation for the queue type.
$\lambda_2(L)$	Algebraic connectivity (Fiedler value) of a graph that represents a network.
P_V	UAV maximum transmission power
D_{th}	E2E delay threshold.

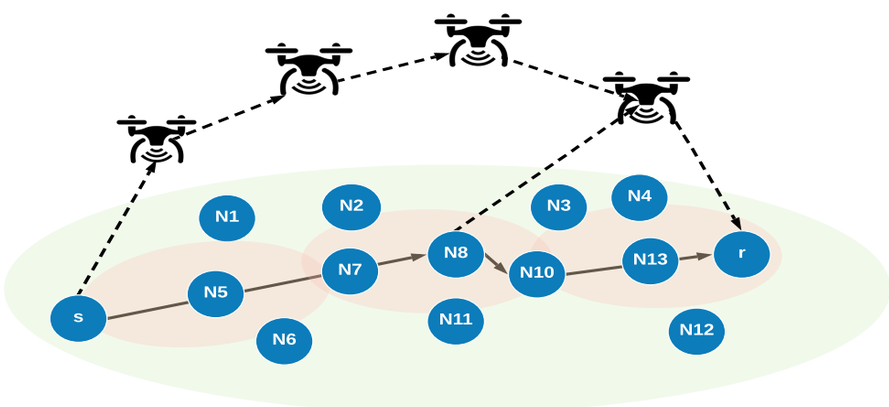


Fig. 5.1 System model.

Section 5.3. Then, the proposed solution and algorithms are described in Section 5.4. Finally, numerical results are provided in Section 5.5.

5.2 System Model

Fig. 5.1 depicts the assumed system model of an ad hoc wireless mesh network, which consists of N nodes. A number of UAVs, K_V, are deployed to increase network connectivity. Each wireless link is assumed to utilize the mmWave frequency band at a frequency of 60 GHz. Before we detail the link model, delay model, and network model used later in the computation of the number and locations of the UAVs, we also briefly define the used notation in Table 5.1

5.2.1 mmWave Channel Model

We consider a 60 GHz mmWave channel model for both the small scale and large scale fading [SMR17], where the authors addressed the channel variation and beamforming tracing for both line-of-sight (LoS) and non-line-of-sight (NLoS). The fluctuation and beamforming model is then discussed in the channel coefficient representing the mmWave ray tracing. Then, the received baseband signal from a source, s, at a destination, r, within a transmission radius R is as follows

$$y_r = \sqrt{P_{i,r}} h_{i,r} d_{i,r}^{-n/2} x_{s,r} + \sum_{j=1, j\neq i}^{N} \sqrt{P_{j,r}} h_{j,r} d_{j,r}^{-n/2} x_{j,r} + n_0, \tag{5.1}$$

where $p_{i,r}$ is the transmitted power from the last node in the path i to the destination node r and $p_{j,r}$ is the transmitted power from any other node j to the destination node r which is considered as interference to node r. $x_{s,r}, x_{j,r}$ are the transmitted unit-power symbols from node s and j to node r, respectively, and $d_{i,r}, d_{j,r}$ represent the distance between i and j nodes and r. Moreover, n_0 denotes zero-mean circularly-symmetric additive-white-Gaussian noise (AWGN) with variance σ_0^2 and it is assumed to be independent across the nodes. Furthermore, $h_{i,r}$ and $h_{j,r}$ are the channel coefficient representing the small scale fading corresponding to the channel between node i and r, or node j and r, respectively. Finally, n is the path loss exponent.

The SINR at the input of the receiver is given by

$$\text{SINR}_r = \frac{P_{i,r}|h_{i,r}|^2 d_{i,r}^{-n}}{\sum_{j=1, j\neq i}^{N} P_{j,r}|h_{j,r}|^2 d_{j,r}^{-n} + \sigma_0^2}. \tag{5.2}$$

Following an information-theoretic model, the maximum rate for the communication between nodes r and s is computed as

$$R_{s,r} = W \log_2 \left(1 + \frac{P_{i,r}|h_{i,r}|^2 d_{i,r}^{-n}}{\sum_{j=1, j\neq i}^{N} P_{j,r}|h_{j,r}|^2 d_{j,r}^{-n} + \sigma_0^2} \right), \tag{5.3}$$

where W is the transmission bandwidth for the mmWave standard.

5.2.2 Delay Link Model

In this section, we model the expected delay for a packet between the source and the destination which may include multiple intermediate hops. The E2E delay can be written as [KR10],

$$D_{E2E} = D_t + D_p + D_q, \tag{5.4}$$

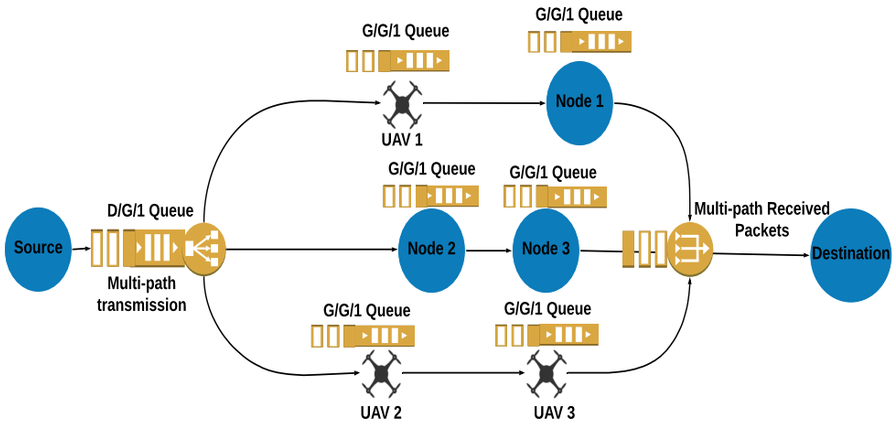


Fig. 5.2 Multi-path queuing model

where D_t, D_P and D_q are the transmission delay, propagation delay and queuing delay, respectively. Moreover, the transmission delay, D_t, represents the time required to put an entire packet into the communication media and can be written as,

$$D_t = N' \frac{m}{\min_{\{i,j\} \in \mathbf{s}} R_{i,j}}, \tag{5.5}$$

where, N' is the number of nodes in the route between the source and the destination nodes, m is the packet size and $\mathbf{s}$ is the set of nodes in the source and destination route including the UAVs.

The propagation delay, D_p, is the time that takes a signal to propagate through the communication media from one node to the next one and can be written as,

$$D_p = \frac{\sum_{\{i,j\} \in \mathbf{s}}^{N'} \|\mathbf{u}_i - \mathbf{u}_j\|_2}{c}, \tag{5.6}$$

where $\mathbf{u}_i = [X_i, Y_i, Z_i]$ and $\mathbf{u}_j = [X_j, Y_j, Z_j]$ are the i^{th} and j^{th} nodes 3×1 position vector in the Cartesian coordinate system, respectively.

Furthermore, the queuing delay, D_q, is the waiting time for the packet spent in a queue to be transmitted, which is usually obtained by performing queue model analysis [BGH92]. This type of analysis includes an investigation of the status of the arriving packet queue and the service/drain rate, as shown in Fig. 5.2.

After investigating the queue model at the source point, we considered a queue of $M/G/1$ model. The queue has a Poisson distribution with λ_i arrival rate at the i^{th} node represented by the symbol 'M' and a general service rate depending on the mmWave channel between the source node and the next hop represented by the symbol 'G'. Moreover, towards our aim for a reliable mmWave network, each packet from the source is transmitted on all the available multi-paths. In other words, in the queuing model, we copy the queue output to all the available

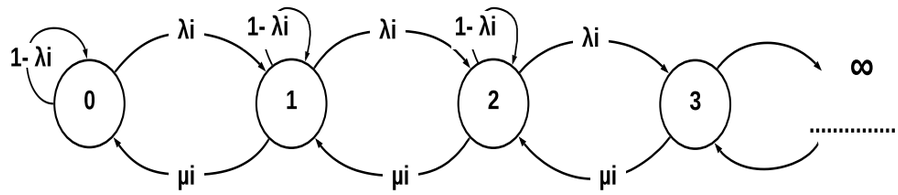


Fig. 5.3 Markov chain representation for M/G/1 and G/G/1

paths instead of splitting the queue for all the multi-path connections. Hence, our model is $M/G/1$ and not $M/G/M$, where M is the number of available multi-paths. The $M/G/1$ model is a Markov chain standard representation for the queue type depending on the input and output rates, shown in Fig. 5.3.

Furthermore, all the nodes in the path except for the source node have a $G/G/1$ queuing model as the arrival rate depends on the arrived packets through the channel.

Then, the queuing delay at the source point is given by

$$W_s = \frac{\lambda_i(\sigma_X^2 + \mathbf{E}\{X\}^2)}{2(1-\rho)} + \frac{1}{\mu_i}. \tag{5.7}$$

where λ_i, $\mathbf{E}\{X\}$ and σ_X^2 are the arriving rate to the source node queue, the service process expectation, and variance at node i which is the source node in this case, respectively. Moreover, $\rho = \lambda_i/\mu_i$ is the service utilization, where μ_i is the service rate of the queue and $0 \leq \rho < 1$.

The total delay at any node i (except the source node s) is as follows (see Appendix I for more detailed explanation):

$$W_i = \sigma_Y^2 \left(\frac{d_{r,i}}{d_{s,i}|d_{s,i} - d_{r,i}|} \right)^n + \mathbf{E}\{Y\} d_{s,i}^{-n}, \tag{5.8}$$

where $\mathbf{E}\{Y\}$ and σ_Y^2 are the expectation and the variance of the queue service process, respectively. Moreover, $d_{s,i}$ and $d_{r,i}$ are the distance between the source s or the destination r and the i^{th} node in the network, respectively. Hence, the total queue delay on any path is:

$$D_q = \min_M \left(\sum_{i=1}^{N'} W_i + W_s \right). \tag{5.9}$$

where M is the number of available paths.

5.2.3 Graph-theoretic Network Model

The baseline network can be modeled as an undirected finite graph $\mathcal{G}(\mathbf{V}, \mathbf{E})$, where $\mathbf{V} = \{v_1, v_2, \cdots, v_N\}$ is the set of the N nodes constructing the network

Table 5.2 Comparison of 802.11g at 2.4Ghz and mmWave at 60 Ghz

Path Loss Exponent (n)	E2E Delay (msec)					
	IEEE 802.11g			IEEE 802.11ay		
	Path 1	Path 2	Path 3	Path 1	Path 2	Path 3
2	1.65	1.12	1.67	0.34	0.234	0.348
3	1.65	1.12	1.67	0.34	N/A	0.4122
4	1.65	1.12	1.67	N/A	N/A	N/A

and $\mathbf{E} = \{e_1, e_2, \cdots, e_Q\}$ is the set of all Q edges (links). For an edge $q, 1 \leq q \leq Q$, connecting nodes $v_i, v_j \in V$, we define the corresponding edge vector $\mathbf{a}_q \in \mathbf{R}^{N\times 1}$, where the i^{th} and j^{th} elements are given by $a_{q,i} = 1$ and $a_{q,j} = -1$, respectively, and the rest is zero. The relationship between the N vertices and the corresponding Q links between those vertices in $\mathcal{G}$ is captured in a matrix named the incidence matrix $\mathbf{A} \in \mathbf{R}^{N\times Q}$, where the q^{th} column is given by $\mathbf{a}_q$. For this undirected graph, the Laplacian matrix $\mathbf{L}(\mathbf{A}) \in \mathbf{R}^{N\times N}$ is defined as:

$$\mathbf{L}(\mathbf{A}) = \mathbf{A}\mathbf{A}^T = \sum_{q=1}^{Q} \mathbf{a}_q \mathbf{a}_q^T. \tag{5.10}$$

The Laplacian matrix for such graph is positive semi-definite, which is expressed as $L \succcurlyeq 0$ and also the smallest eigenvalue is zero, i.e., $\lambda_1(L) = 0$. The second smallest eigenvalue of L, $\lambda_2(L)$, is the algebraic connectivity of the graph $\mathcal{G}$ also called Fiedler value [Fie73], which will be used in the rest of this chapter to represent the network connectivity.

A UAV, as a hovering relay, can relay data packets between two nodes in the network. Accordingly, deploying a UAV can create one or more links (edges) in the baseline graph $\mathcal{G}(\mathbf{V}, \mathbf{E})$, which results in a new graph $\mathcal{G}'(\mathbf{V}, \mathbf{E}')$. The new graph $\mathcal{G}'$ has the same number of N nodes, but with a larger set of edges denoted by $\mathbf{E}'$ with Q' edges where $Q' \geq Q$, i.e., $\mathbf{E} \subseteq \mathbf{E}'$. The potential increase in the network connectivity, due to deploying UAVs, can be computed as $\lambda_2(\mathbf{L}') - \lambda_2(\mathbf{L})$.

5.3 Problem Motivation and Formulation

5.3.1 Motivation

The motivation behind combining the UAVs' deployment and multiple paths is based on the potential impact of the upper layers for routing on enhancing the

mmWave channel behavior. To demonstrate this, we conducted a simple experiment where IEEE 802.11g and IEEE 802.11ay MAC layer are used for routing in an ad hoc network. We created a 10-node ad hoc network topology in the NS-3 simulator and established 3 different routes from a source to its destination. We transmitted data from the source to the destination under different path loss exponents using Transmission Control Protocol (TCP) as the transport layer protocol. The results for packet delay are shown in Table 5.2. From these results, we can see that the E2E delay when IEEE 802.11g is used is higher, but there is always a successful packet routing. On the other hand, when IEEE 802.11ay is used, we observe reduced E2E delay due to the higher transmission rate. However, the packet receiving is not always guaranteed, even though TCP is used to ensure re-transmissions in case of failures. For instance, under $n = 4$, no routes were successful in transporting the packets. These results suggest that under mmWave channels, the three routes need to be available for backup, and even this may not be enough (i.e., see the case when $n = 4$), and thus additional relays might be needed. Connectivity becomes a crucial concern to be able to benefit from high-bandwidth mmWave communications. Next, we formulate our problem to address the aforementioned concerns.

5.3.2 Problem Formulation

First, we introduce the optimization problem to enhance the network connectivity with a maximum allowed constraint on the E2E delay between the desired source and destination. We also consider finding the minimum number of K_V UAVs, the UAVs' optimal locations, and transmission power.

Mathematically, this optimization problem can be formulated as follows:

$$\begin{aligned} \max_{\mathbf{U}, P_q, K_V} \quad & \lambda_2(\mathbf{L}'(\mathbf{U})) \\ \text{s. t.} \quad & D_{E2E} \leq D_{\text{th}}, \\ & d_{i,j} \leq R, \\ & \sum_{q=1}^{Q_V} P_q \leq P_V, \end{aligned} \tag{5.11}$$

where $\mathbf{U}$ is the $3 \times K_V$ UAVs position matrix in the Cartesian coordinate system and D_{th} is the E2E delay threshold. In this chapter, we consider the Cartesian coordinates to specify the UAV position and transmission direction, hence, we assume a fixed UAV antenna angle.. Moreover, $d_{i,j}$ where $i, j \in 1, 2, \cdots, K_V$ denotes the distance between any 2 UAVs i and j. The maximum UAV transmission

power is P_V, and P_q is the UAV transmission power over each link q of Q_V, which represents the total number of links provided by the UAV.

Once the UAVs are deployed through the optimization problem, we tackle the improving reliability at the network layer problem. In order to increase the network reliability for mmWave communication, a modified node-disjoint routing multi-path protocol is proposed. Note that the same data will be sent through all these node-disjoint paths simultaneously to increase the success rate. In this way, the receiver can also select the minimum E2E delay path for multiple packets that arrive for the same data. This approach also minimizes the potential interference among inter-routes since the same nodes and links are not shared by different routes.

5.4 Proposed Solution

In this section, we describe, in detail, the proposed solutions and algorithms to find the optimal UAVs' positions and the multi-path/parallel routing between a particular source and a destination. The optimization problem solution is detailed in Algorithm 2 in Section 5.4.1 while the routing technique is detailed in Algorithm 3 in Section 5.4.2.

5.4.1 Connectivity Optimization Relaxation and Solution

To address the indirect relation between the graph Laplacian matrix and the UAVs position, we use a quantized grid such that the nodes are distributed over $h \times h \times h$ volume. Moreover, the search space over the x, y, and z axes is uniformly quantized with a step size δ to get a search grid consisting of β candidate positions for the UAV. This simplifies the Laplacian matrix to be represented by the following formula:

$$\mathbf{L}' = \mathbf{L} + \sum_{j=1}^{\beta} x_j \mathbf{A}'_j \mathbf{A}'^T_j, \tag{5.12}$$

where $\mathbf{L}$ is the original graph before UAV deployment, and x_j is equal to one if a UAV is positioned in the j^{th} grid point, otherwise $x_j = 0$. Moreover, $\mathbf{A}'_j$ is the incidence matrix when the UAV is deployed in this grid point.

Collecting $x_j,\ j \in \{1,\ \ldots,\ \beta\}$, in the $\beta \times 1$ vector $\mathbf{x}$, Eq. (5.12) can be written as follows:

$$\mathbf{L}' = \mathbf{L} + (\mathbf{x} \otimes \mathbf{I}_M)\, \mathbf{\Gamma}, \tag{5.13}$$

where $\mathbf{\Gamma} \triangleq \left[\left(\mathbf{A}'_1\mathbf{A}'^T_1\right)^T,\ \ldots,\ \left(\mathbf{A}'_\beta\mathbf{A}'^T_\beta\right)\right]^T$.

Furthermore, we apply the quantized grid model over the E2E delay in a $\mathbf{b} \in \mathbf{R}^{\beta\times 1} = [b_1, b_2, \cdots, b_\beta]^T$ such as

$$b_i = D_{E2E}|_{\beta=i}. \tag{5.14}$$

where $\mathbf{b}$ is the vector of the minimum E2E delay over all the available paths through the destination for all the β possible UAVs positions.

Hence, the optimization problem can be written in terms of the UAVs position index vector $\mathbf{x}$ rather than its actual 3-D physical locations as follows:

$$\begin{aligned} \max_{\mathbf{x},P_q,K_V} \quad & \lambda_2(\mathbf{L}'(\mathbf{x})) \\ \text{s. t.} \quad & \mathbf{x}^T\mathbf{b} \le D_{\text{th}}, \\ & \mathbf{x}^T\mathbf{d}_{i,j} \le R, \\ & \sum_{q=1}^{Q_V} P_q \le P_V, \\ & \mathbf{x} \in \{0,1\}, \end{aligned} \tag{5.15}$$

where, $\mathbf{d}_{i,j}$ is $\beta \times K_V$ matrix representing the distance between any 2 UAVs. Furthermore, the first constraint $\mathbf{x}^T\mathbf{b} \le D_{\text{th}}$ represents the E2E delay constraint, where $\mathbf{b}$ is the vector of the E2E delay over all the available paths through the destination.

Moreover, $\lambda_2(\mathbf{L}'(\mathbf{A}'(\mathbf{x})))$ can be written as the point-wise infimum of a family of linear functions of $\mathbf{x}$ as:

$$\lambda_2(\mathbf{L}'(\mathbf{A}'(\mathbf{x}))) = \inf_y [y^T\mathbf{L}'(\mathbf{A}'(\mathbf{x}))y, \parallel y \parallel_2 = 1, \mathbf{1}^T y = 0]. \tag{5.16}$$

Hence, it is a concave function in $\mathbf{x}$. The optimization problem can be written as follows:

$$\begin{aligned} \max_{\mathbf{x},\log(P_q),K_V,\gamma} \quad & \gamma \\ \text{s. t.} \quad & \gamma(\mathbf{I} - \frac{1}{\beta}\mathbf{1}\mathbf{1}^T) \preceq \mathbf{L}'(\mathbf{x}, P_q, K_V) \\ & \mathbf{x}^T\mathbf{b} \le D_{\text{th}}, \\ & \mathbf{x}^T\mathbf{d}_{i,j} \le R, \\ & \sum_{q=1}^{Q_V} P_q \le P_V, \\ & \mathbf{1}^T\mathbf{x} <= K_V,\ \mathbf{x} \in [0,1]. \end{aligned} \tag{5.17}$$

Investigating the problem convexity, the objective function, γ, is linear in the optimization variables. Moreover, the first constraint is a semi-definite constraint. The second constraint, $\mathbf{x}^T\mathbf{b} \leq D_{\text{th}}$ is also a linear constraint in its general form as proven in details in Appendix II.

In addition, the rest of the constraints are linear in $\mathbf{x}$. Therefore, the optimization problem is a convex optimization problem with linear constraints. The optimization problem in Eq.(5.17) can be written as a Semi-definite Programming (SDP), a sub category of the convex optimization, after relaxing the binary constraint in $\mathbf{x}$ to be real value between 0 and 1, as follows:

$$\begin{aligned}
\max_{\mathbf{x},\log(P_q),K_V,\gamma} \quad & \gamma \\
\text{s. t.} \quad & \gamma(\mathbf{I} - \frac{1}{\beta}\mathbf{1}\mathbf{1}^T) \preceq \mathbf{L}'(\mathbf{x}, P_q, K_V) \\
& \mathbf{x}^T\mathbf{b} \leq D_{\text{th}}, \\
& \mathbf{x}^T\mathbf{d}_{i,j} \leq R, \\
& \sum_{q=1}^{Q_V} P_q \leq P_V, \\
& \mathbf{1}^T\mathbf{x} <= K_V,\ 0 \leq \mathbf{x} \leq 1.
\end{aligned} \tag{5.18}$$

The relaxed SDP problem in Eq. (5.18) can be solved using an *SDP* solver such as CVX SDPT3 solver [GBY08].

Algorithm 2 summarizes the solution presented above as follows: The first step is to quantize the 3-D grid to the $h \times h \times h$ cubs. In the next step, every time a UAV is added to the grid, a new graph incidence matrix $A'(x)$ is reconstructed for all the permutations $Perm(\beta)$ of all possible UAV positions on the grid. Additionally, the distance matrix $\mathbf{D}$ of the network is established for all $Perm(\beta)$. The algorithm, then, strives to optimize the maximum network connectivity that satisfies the requirement of the network E2E delay to be less than D_{th} by adding more UAVs. After the optimization is done and all the UAVs' positions are found in the grid, a post-processing algorithm is performed to obtain the UAVs' Cartesian coordinates by choosing the maximum K_V elements in $\mathbf{x}$.

5.4.2 Parallel Multi-path Routing

After the UAVs' positions have been determined, the next step is to find the multi-path routing to increase the mmWave links' reliability. The aim is to increase the

Algorithm 2 UAVs Positioning

Input: $(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$ and $K_V = 1$
$\mathbf{A} \leftarrow$ the graph incidence Matrix
$\lambda_2(\mathbf{L}(\mathbf{A})) \leftarrow$ Network connectivity of $\mathcal{G}$
$K \leftarrow$ The maximum available UAVs
Quantize:
$\beta \leftarrow$ Grid positions; $\mathbf{x} \leftarrow \beta \times 1$ vector
$Perm(\beta) \leftarrow$ permutation of all grid positions
for $\forall K_V \leq K$ & $\forall P(\beta)$ **do**
Link Matrix:
    $A'(\mathbf{x}) \leftarrow$ Link matrix after adding $UAVs$
    $\mathbf{L}'(\mathbf{x}) \leftarrow$ Laplacian matrix after adding $UAVs$
    $E2E \leftarrow$ The E2E delay
end for
Optimization:
$\max_{\mathbf{x}} \quad \lambda_2(\mathbf{L}'(\mathbf{A}'(\mathbf{x})))$
if $\mathbf{x}^T\mathbf{b} \leq D_{th}$ & UAV total power $\leq P_V$ **then**
    Break
else
    goto *Optimization*.
    $(X_V, Y_V, Z_V) \leftarrow \max_{\mathbf{x}}$.
end if
Loop:
if $d_{i,j} > R$ **then**
    $K_V \leftarrow K_V + 1$
    $(X_V, Y_V, Z_V) \leftarrow \max_{\mathbf{x}}$.
    goto *Loop*.
end if
Output: $(\mathbf{X_V}, \mathbf{Y_V}, \mathbf{Z_V})$, P_q and K_V

network reliability for the mmWave communication by sending the same data packets in parallel over multiple alternative paths.

Sending packets through multiple paths will be challenging at the upper layers in terms of implementation. For instance, if TCP is to be used, some changes will be needed since TCP establishes a connection that is maintained during data transmission at all times. If a node has multiple IP interfaces, the current multi-path TCP (MPTCP) standard [PJZ17] can be utilized for parallel transmission. However, in our case, drones and other mobile nodes may not have such resources, and thus, new approaches are needed.

To this end, we assume that a node will use source routing (such as dynamic source routing (DSR) [JM96, JMB+01]) to pick among multiple available paths, labeling them separately just like multi-protocol layer switching (MPLS)-based routing [DR00, XHBN00]. Those labels can be incorporated in the TCP header's unused bits so that the receiving party can differentiate between different route packets. In the case of User Datagram Protocol (UDP), there is still a need for MPLS with fewer bits needed to be added to the UDP header.

We propose a multi-path protocol that is a modified node-disjoint routing ap-

Algorithm 3 Multi-path Routes

Input: $(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$, $(\mathbf{X_V}, \mathbf{Y_V}, \mathbf{Z_V})$, D_{th} and K_V
$Q'' \leftarrow$ The total number of links after adding the UAVs
$\mathcal{G}'' \leftarrow (\mathbf{V}'', \mathbf{E}'')$ The network graph including the UAVs
$root \leftarrow$ The source node s
$\mathbf{t} \leftarrow []$ initial empty spanning tree
$\mathbf{c} \leftarrow$ Initial cost $= 0$
for $i \leq N + K_V$ **do**
    if $root \notin \mathbf{t}$ **then**
        $\mathbf{t} \leftarrow root$
        $\mathbf{c} \leftarrow \mathbf{c} + D_{E2E}$
    end if
end for
$\mathbf{TC} \leftarrow$ Total Cost vector on all the paths
$\mathbf{ST} \leftarrow$ Spanning Tree
for $\forall \mathbf{t} \in \mathbf{ST}$ **do**
    if $\mathbf{ST} \cap \mathbf{t} \neq \Phi || \mathbf{c} > D_{th}$ **then**
        $\mathbf{ST} \leftarrow \mathbf{ST} - \mathbf{t}$
        $\mathbf{TC} \leftarrow \mathbf{TC} - \mathbf{c}$
        $H \leftarrow$ The number of hops $\forall \mathbf{ST}$
    end if
end for
$\mathbf{path}_i \leftarrow \mathbf{ST}|_{\min(H,c)}$
for $\forall$ **ST do**
    if $[N+1 : N+K_V] \in \mathbf{ST}$ & $\mathbf{ST} \cap [1:N] - [s,r] = \Phi$ **then**
        $\mathbf{path}_{i+1} \leftarrow \mathbf{ST}|_{\min(H,c)}$
    end if
end for
Output: $\mathbf{path}_1, \mathbf{path}_2, \cdots, \mathbf{path}_i$.

proach to minimize potential interference among inter-routes; to enable parallel transmissions from the same source. In this setting, original network nodes are allowed to be used only once, while UAVs are considered to be reusable on several paths. The justification of such a model is that the UAVs are movable and adjustable to avoid link failure, whereas the nodes in the network can not be easily adjusted. Here, we propose an algorithm to determine the available paths that are independent of each other (i.e., they do not share any links or intermediate nodes) so that there will be very diverse options to send the packets, increasing the chances to make it to the receiver. Note that, given that all the nodes and their locations are known in advance; then, this will be a centralized algorithm running at the source node, which is in line with the source routing concept we offer. Basically, the source will determine the routes, label each route, and maintain them locally. Whenever a packet is to be sent, the route will be included in the packet header.

The proposed algorithm to find the multiple paths is shown in Algorithm 3. In this algorithm, an undirected finite graph $\mathcal{G}''(\mathbf{V}'', \mathbf{E}'')$ is created to represent this new network topology that consists of the original network and the deployed UAVs. $\mathbf{V}'' = \{v_1, v_2, \cdots, v_{N+K_V}\}$ is the set of the N nodes constructing the

original network and $\mathbf{E}'' = \{e_1, e_2, \cdots, e_{Q''}\}$ is the set of all Q'' edges (links). The new graph $\mathcal{G}''$ is different from $\mathcal{G}'$ in the connectivity calculations as it has $N + K_V$ nodes.

Moreover, the weights of each link represent the E2E delay of the data transmission over this link. Our algorithm will find all the spanning trees, **ST**, and the corresponding cost (E2E delay) for each tree, **TC**, between the source s and destination r. Next, we only choose the spanning trees with disjoint vertices (except for the UAVs) and have a total cost less than the E2E delay threshold, D_{th}. Finally, we select the i routes with the lowest number of hops to be our paths of transmission, $\mathbf{path}_1, \mathbf{path}_2, \cdots, \mathbf{path}_i$.

By using the constraint in Eq. (5.18):

$$\mathbf{x}^T \mathbf{d}_{i,j} \leq R \tag{5.19}$$

a direct path over the UAVs can be formed as a backup route that guarantees the independence of this route from any other routes uses existing nodes. Thus, potential link failures that may happen within the existing network among the nodes will not impact this route. Finally, while power consumption is vital in the UAV deployment optimization, once they are on-site, they can be replaced when their batteries approach critical levels.

5.5 Performance Evaluation

5.5.1 Simulation Setup

In this section, we present the simulation results to demonstrate the effectiveness of the proposed scheme. The two algorithms presented in Section 5.4 are first implemented in MATLAB to obtain the UAVs' positions and the multi-path routes. Then, for testing our model in a realistic scenario, the obtained data from MATLAB is fed into a widely used NS-3 simulator to calculate the actual throughput and E2E delay. The optimization approaches are implemented in MATLAB R2016a using the CVX solver.

For NS-3, we used version 3.26 and have adopted the IEEE 802.11ad implementation described in [AW16] and updated the physical layer to match the IEEE 802.11ay MIMO transmission. To the best of our knowledge, this is the first multi-hop implementation of IEEE 802.11ad/ay in NS-3.

Table 5.3 Simulation Parameters.

Parameter	Value
MATLAB Parameters	
W	2.16 GHz
f	56.16 GHz
P_V	30 dBm
σ_0^2	-130 dBm
n	4 (suburban environment)
D_{th}	3 msec
NS-3 Parameters	
Simulation time	10 sec
Video size	290 MB
Number of frames	2000
Image resolution	352×288
Frame size	30 fps
Modulation and Coding Scheme (MCS)	$18 - 25$
PHY Type	"DMG-MCS"
Antennas	1
Antenna Sectors	3
Transmission (Tx) Power	10 dBm
Tx Gain	23
Rx Gain	23

The system parameters used throughout the experiments for MATLAB and NS-3 are listed in Table 5.3. N nodes are deployed with a uniform random distribution within an area of 100×100 m. For the evaluation on NS-3, we created a scenario to send data between a source and destination over multi hops using the same setting as in the MATLAB evaluation. As mmWave is a better match for high-bandwidth traffics, we investigated the proposed approaches under the high-rate multimedia transmission. We utilized the *Evalvid* tool-set [KRW03] that is designed for video management. In this scenario, the **highway** reference video from Evalvid which is around 290 MB and consists of 2000 frames, is used as the multimedia traffic.

The following metrics are used to evaluate our approach:

- *Connectivity*: The connectivity, $\lambda_2(\mathbf{L}(\mathbf{x}))$, refers to Eq. (5.10) used in Section 5.2.3. That parameter shows whether the nodes are highly connected or not and indicates the level of connectedness. This parameter demonstrates the effectiveness of the optimal positioning optimization problem in Eq. (5.11). The increase of this parameter indicates better coverage between nodes in the network, resulting in better communication performance.
- *E2E Delay*: This is the total delay between the source and the destination nodes. In MATLAB, we calculate the E2E delay as in Eq. (5.4) in Section

5.3. In NS-3, it is calculated from the receiver's perspective after receiving the real packet from the sender. The effectiveness of our proposed routing solution along with the optimal position reflects in a better E2E delay.

- *Throughput*: The throughput is used within NS-3 to represent the number of bits successfully received at the receiver side in a second.

5.5.2 Baselines for Comparison

We consider two types of network topologies. The first type is the original network before the UAV deployment, while the second type is the network with UAVs after the optimization. In these networks, the following paths are compared:

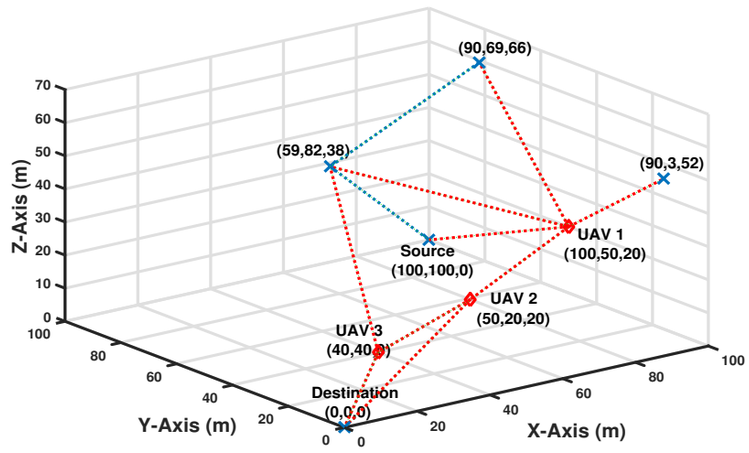
- *Baseline path*: refers to the shortest path in the original network to reach the destination;
- *Hybrid path*: refers to the optimized path with the minimum number of hops that includes the node(s) in the original network and UAV(s) to reach the destination.
- *UAV-only path*: refers to the path that uses only UAV(s) to reach the destination. This path type is critical when there are not enough nodes to form an adequate route.
- *Parallel Multi-path*: This path represents the multi-path communication where the data is sent over both the Hybrid and UAV-only paths in parallel to ensure reliability.

5.5.3 Performance Results

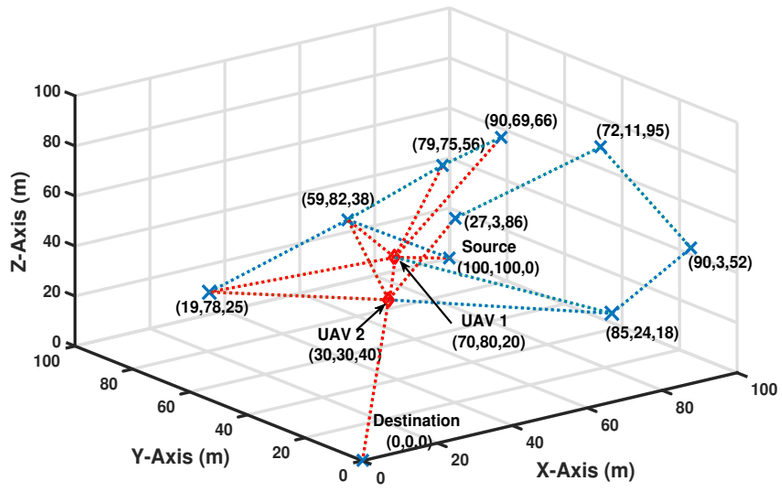
UAVs Placement Evaluation

We considered several network topologies with a different number of nodes, and we computed the optimal number and the UAVs' location.

To initially investigate our proposed solution, we first conducted a simple experiment. Specifically, we compare the number of UAVs needed for an initial network with 5 nodes to the same network after adding 5 more nodes to have a total of 10 nodes. We assume the same positions for the source and the destination nodes. The number of UAVs added for the first case (Fig.5.4a) is 3 while it is 2 for the second case (in Fig.5.4b), depending on the need of the network. Fig. 5.5



(a) $N = 5$



(b) $N = 10$

Fig. 5.4 UAV positioning for different number of nodes. The cross and diamond markers represent nodes and UAVs, respectively.

further investigates the UAV transmission range on the number of UAV needed in both 5 and 10 nodes network. As shown in the figure, the number of UAVs required decreases with the UAV range extension; and it settles to only 1 UAV when the range is almost covering the whole area.

Next, the achieved enhancement in the network algebraic connectivity is assessed before and after using the UAVs with the network growth. As seen in Fig. 5.6, the algebraic connectivity after adding the UAVs with optimal positioning is higher than that of the original network without the UAVs. The connectivity for our approach is enhanced by almost 200% at $N = 10$ and 66% at $N = 30$ compared to the original network.

Furthermore, the results depicted in Fig. 5.7 shows that the average number of UAVs needed tends to decrease with the increased number of nodes. That is

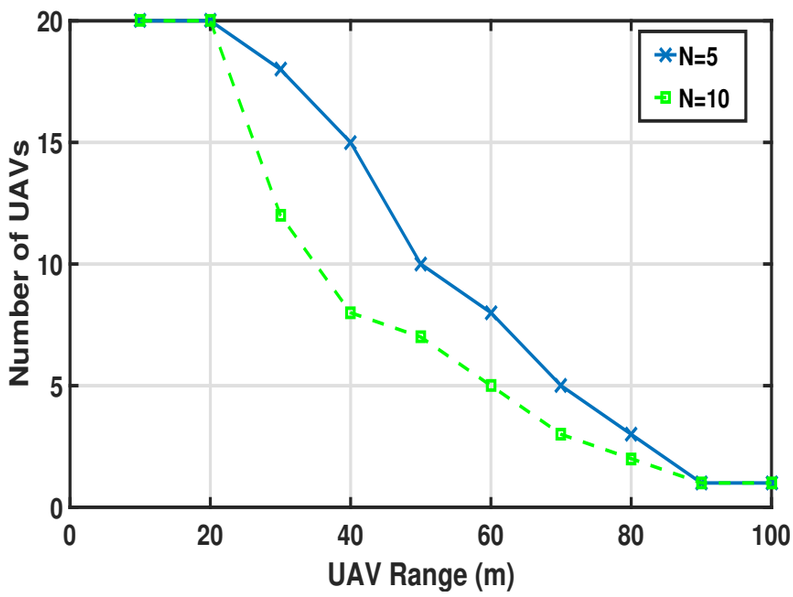


Fig. 5.5 The number of UAVs required for different UAV transmission range.

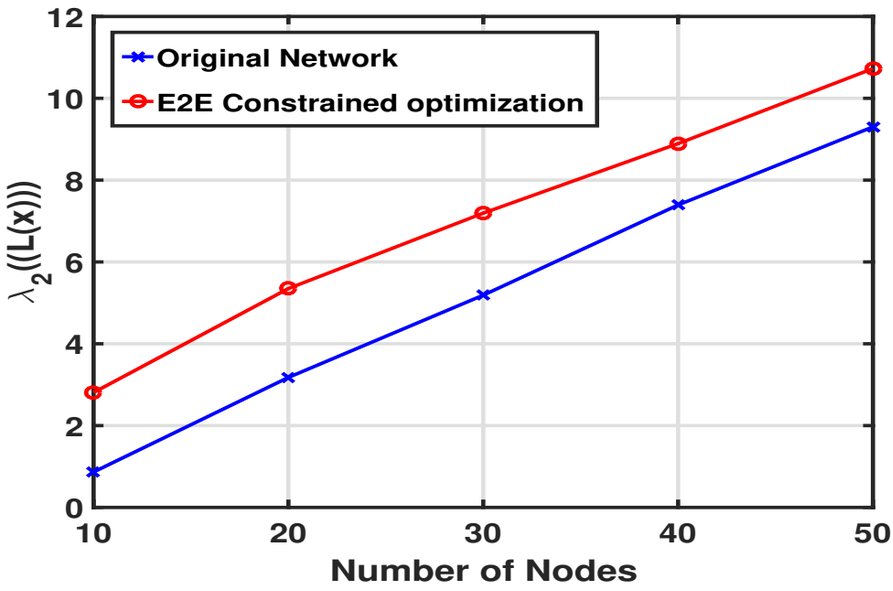


Fig. 5.6 The network connectivity enhancement through UAVs.

due to increasing the number of nodes in the same area, and as a result, more links are created between original nodes and decreases the need for UAVs to support the network connectivity.

Routing Performance

Next, we investigate the E2E delay and throughput performance for the proposed routing algorithm compared to the original network.

First, we study the performance of using a single path with the deployment of UAVs while parallel multi-paths are available. To this end, we fixed N to 50 and

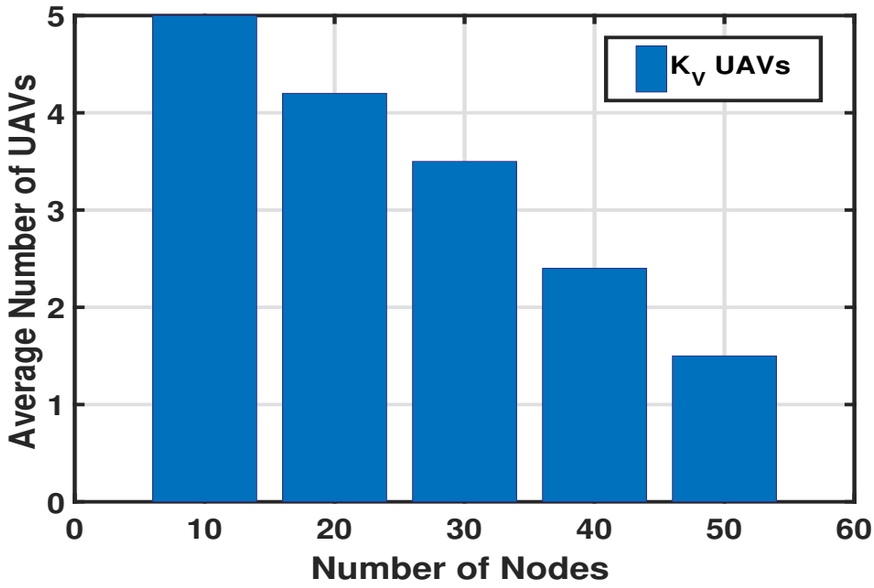


Fig. 5.7 Average number of UAVs needed for different N.

determined three node-disjoint paths (i.e., Path 1, Path 2, and Path 3) with the lowest E2E delay (from MATLAB results) from the same source and destination in the original network topology. We report the NS-3 results of the throughput (TP) and E2E delay per frame transmission for these paths when UDP is used as the transport layer protocol in Table 5.4.

Table 5.4 Path Performance Comparison.

	Path 1	Path 2	Path 3
Original Network (No UAVs)			
TP (MB/s)	0.31	0.23	0.17
E2E (ms)	0.4664	0.63	0.83
Network with UAVs			
TP (MB/s)	0.73	0.58	0.8
E2E (ms)	0.20	0.25	0.18

The results show a significant improvement in both TP and E2E for the network after adding the UAVs. In some cases, the TP triples on average, and the E2E delay reduces to less than half. Because the UAVs are placed in locations that will reduce the E2E delay based on the proposed solution/ optimization. The decrease in E2E delay also enables increased TP. In addition, we speculate that the paths for the original network might have fewer hops and thus the longer distance between nodes, which impacts the packet delivery ratio (PDR) in mmWave links. That is not the case in our approach since the number of hops increases while the distance between nodes decreases, enabling better PDR. Hence, we in-

vestigated the effect of the Modulation and Coding Scheme (MCS) index on the PDR for the baseline, original network, and our approach for $N = 10$ in Table 5.5. The results show that the original network has a high packet loss for the MCS index under 18, while the proposed optimal UAVs positioning optimization has no packet loss even with a low-quality MCS index. The reason behind the high packet loss in the original network is that the nodes are long distanced, and the mmWave channel is lossy.

Table 5.5 Original Network Packet Delivery Ratio

MCS Index	Transmitted frames	Received Frames	PDR
Original Network (No UAVs)			
10	2106	151	7 %
11	2106	679	32%
12	2106	1697	81%
18	2106	2106	100%
Network with UAVs			
10-18	2106	2106	100%

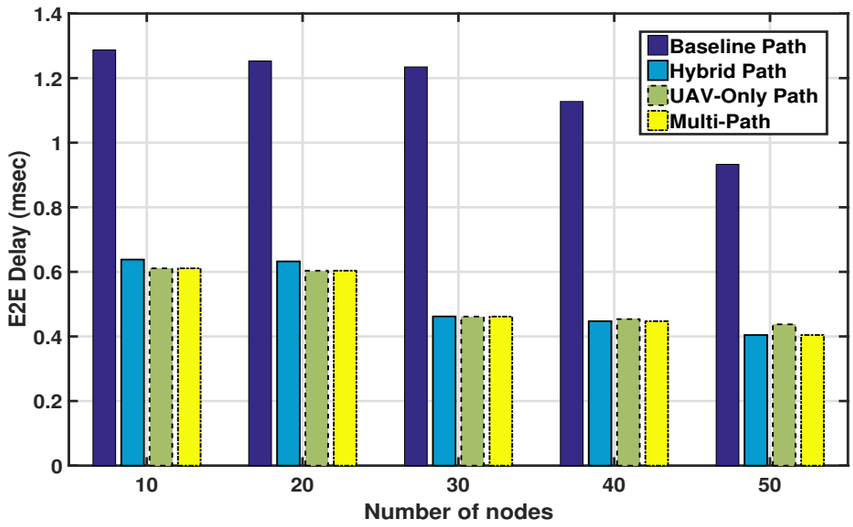
On the other hand, using TCP transmission may add extra overhead to the E2E delay due to the TCP handshake process for the network with UAVs. To investigate this point, we transmit $10,000$ packets with a packet rate of 4 MB/sec and a packet interval of 16 µsec/packet for both UDP and TCP NewReno for $N = 50$. The results in Table 5.6 shows a lower E2E delay for the UDP connection due to the TCP setup process.

In the next experiment, we investigated the achieved enhancement in the E2E delay and TP between the source and destination nodes

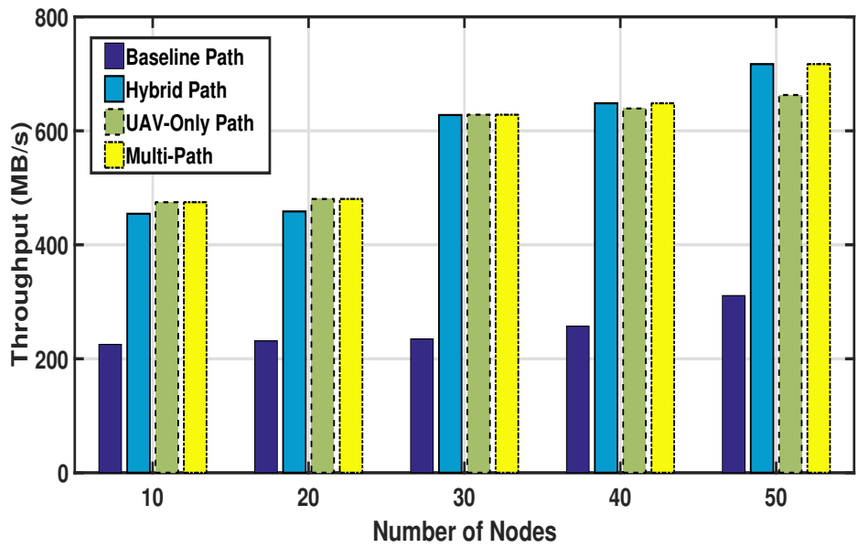
Table 5.6 UDP vs. TCP Performance Comparison

	E2E (ms)	
Min. delay paths	UDP	TCP NewReno
Path 1	0.018	0.034
Path 2	0.015	0.025
Path 3	0.038	0.072

As shown in Fig. 5.8(a), the multi-path approach uses parallel communication over both the hybrid and UAV-only paths. Then, the E2E delay achieved will be equal to the minimum E2E delay of both paths. In other words, the receiver would



(a) The E2E delay.



(b) The throughput.

Fig. 5.8 The E2E delay and throughput for different N.

pick the frame which arrives first. So in all cases, our proposed approach achieved the least E2E delay. The improvement concerning no UAV-case (baseline) is particularly significant when the network size is smaller (i.e., above 50%) as there are no alternative path options for such smaller sizes. Comparing the Hybrid Path and UAV-only path, we see that the results are close to each other. But Hybrid Path performs better as the number of nodes increases, giving more path options to be used.

Looking at the TP in Fig. 5.8(b), we observe that it increases for the Hybrid Path approach as better paths are becoming available with the increased number of nodes. In such cases, our multi-path approach benefits from such an increase in terms of TP as it utilizes that path instead of the UAV-only one. The UAV-only path does not benefit from the growth of the network as it solely relies on

UAVs. These results are consistent with the E2E delay results. As a result, we can conclude that the parallel multi-path approach performs the best in terms of E2E delay and TP in all cases, which indicates its effectiveness. These results further emphasize our model appropriateness for emergency management and first responder applications with high bandwidth streaming requirements.

On the other hand, multi-path parallel transmission adds an extra overhead by introducing redundant transmissions. However, these parallel transmissions are needed to guarantee the delivery and increase the overall throughput, as shown in the experiments aforementioned (Fig. 5.8). Hence, to justify our multi-path parallel transmission overhead, we conducted some experiments to include results on how TCP performance improves by reporting the number of re-transmissions compared to actual transmissions. For this set of experiments, we used the following TCP settings: TCP NewReno with a total of $10,000$ transmitting packets with a packet rate of 4 MB/sec and a packet interval of 16 µsec/packet. As shown in Fig. 5.9, the baseline TCP re-transmissions are much higher than our proposed scheme, even for the multi-path transmission. For example, at $N = 30$ nodes, the TCP re-transmissions are around 350 packets; but with our proposed scheme, the TCP re-transmissions are around $50 - 60$ packets on the Uav-Only and the Hybrid paths. Moreover, even with the two parallel paths, the total TCP re-transmissions are just a little above 100 packets, which is almost 75% fewer re-transmissions.

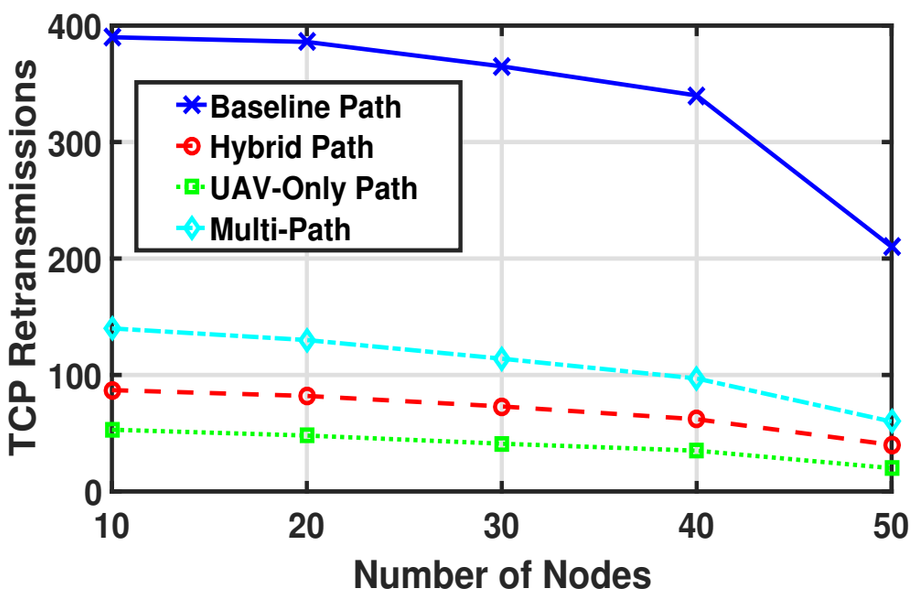


Fig. 5.9 TCP re-transmissions overhead for different N.

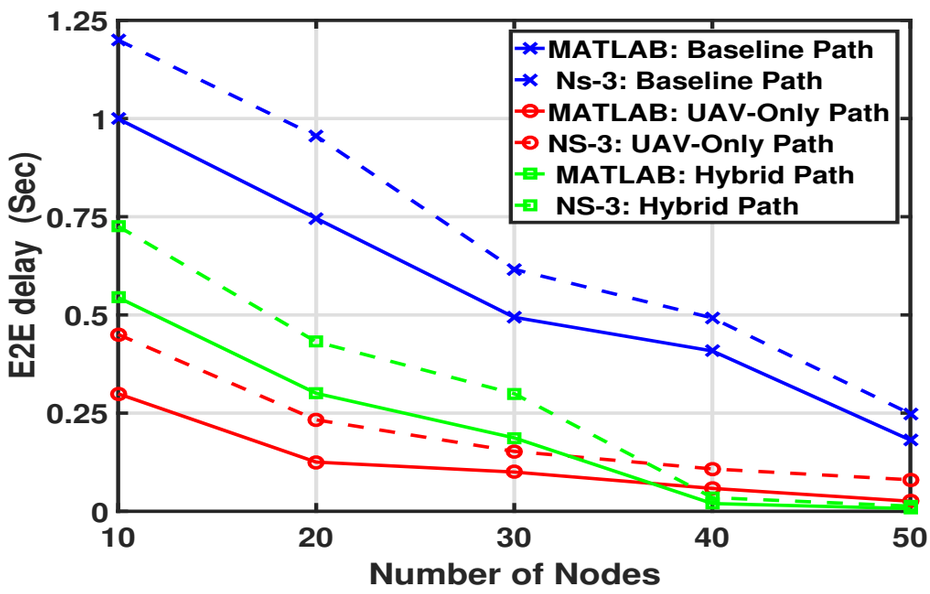


Fig. 5.10 Optimization vs NS-3 E2E delay for different N.

Comparison of Optimization and NS-3 Results

An important factor in the evaluation is the accuracy of optimization results concerning a real-life situation. Thus, we compared the NS-3 results with other optimization results from MATLAB on the same topologies. Fig. 5.10 shows the E2E delay from the MATLAB optimization compared to the NS-3 simulator. As can be seen, the optimization results show slightly lower E2E delays since the deployment in a realistic environment faces uncertainties and complexities that could not be captured within analytical models. However, the trends match perfectly and indicate the validity of the optimization results. The slight difference can be attributed to various overheads in actual transmissions: For instance, the delay may be due to half-duplex operations in NS-3 and the processing delay at the receiver side when dealing with multiple redundant transmissions. In addition, the processing of packet headers at the receiver side adds to the total delay.

Appendix I

Here, we investigate the delay performance for the packet transmit over each path of the multi-path communication with a total queue delay is,

$$D_q = \min_M \left(\sum_{n=1}^{N'} W_N + W_s \right) \tag{5.20}$$

where D_q is the total queuing delay at any node i and W_s is the total queuing delay at the source node. Furthermore, calculating the total queuing delay for

each path requires the queuing delay for each node in that path, hence, the need for queuing analysis at each node.

Source node with $M/G/1$ queue

We begin the queuing analysis with the queuing model at the source node with the $M/G/1$ model shown in Fig. 5.3. The $M/G/1$ waiting delay at the source node is as follows [JS96],

$$W_{q,s} = \frac{\lambda_i(\sigma_{s,i}^2 + \mathbf{E}\{Z\}^2)}{2(1-\rho)}, \tag{5.21}$$

where λ_i, $\mathbf{E}\{Z\}$ and $\sigma_{s,i}^2$ are the arriving rate to the queue, the service process expectation and the service process variance at node i which is the source node in this case, respectively. Moreover, $\rho = \lambda_i/\mu_i$ is the service utilization, where μ_i is the service rate of the queue and $0 \leq \rho < 1$. Then, the total queue delay at node s is,

$$W_s = W_{q,s} + \frac{1}{\mu_i}. \tag{5.22}$$

Furthermore, this model's service process depends on the mmWave channel statistics and the probability distribution density function (PDF) of proper transmission. In this chapter, we utilize the 10° transmit antenna. The K-factor expresses the relative strength of both the direct and the scattered components of the received signal with a Rician distribution [TAG03, ABA+15]. The K-factor provides an indication of link quality and the received power in a reach scattering environment. Hence, the K-factor is fitted to a Gaussian distribution with mean of $\mathbf{E}\{X\}$ and variance of σ_X where $X = P_{Rx}$ of $\mathcal{P}rob\{X \leq P_{th}\}$ where P_{th} is the threshold received power for a proper communication.

Nodes with $G/G/1$ queue

Now, we investigate the queuing analysis with the queuing model at all other nodes with the $G/G/1$ model shown in Fig. 5.3. The $G/G/1$ waiting delay is following Kingman's formula [Kin62], which is an approximation formula for the mean waiting time in a $G/G/1$ queue and is known to be generally very accurate. Then, the queue waiting time at any node i is as follows

$$W_{q,i} = \frac{\rho_i}{1-\rho_i} \cdot \frac{C_a^2 + C_s^2}{2} \cdot \frac{1}{\mu_i}, \tag{5.23}$$

where $\rho_i = \lambda_i/\mu_i$ is the service utilization and C_a and C_s are the coefficient of variation for the arrival and service processes, respectively. The coefficient

of variation is a standardized measure of the dispersion of random variable g a probability distribution function and equal to the standard deviation of the distribution divided by its mean, $C = \sigma_g / \mathbf{E}\{g\}$.

Then the queue waiting time can be approximated as follows

$$W_{q,i} = \sigma_Y^2 \left(\frac{d_{r,i}}{d_{s,i}|d_{s,i} - d_{r,i}|} \right)^n. \tag{5.24}$$

Hance, the queue waiting time is a linear function of the distances. Then, the total delay at any node N (except the source node s) is,

$$W_i = \sigma_Y^2 \left(\frac{d_{r,i}}{d_{s,i}|d_{s,i} - d_{r,i}|} \right)^n + \mathbf{E}\{Y\} d_{s,i}^{-n}. \tag{5.25}$$

Appendix II

In order to establish convexity of the constraints of the proposed optimization problem, the following constraints are linear so no need for further convex investigation,

$$\begin{gathered} \mathbf{x}^T \mathbf{d}_{i,j} \leq R, \\ \sum_{q=1}^{Q_V} P_q \leq P_V, \\ \mathbf{1}^T \mathbf{x} <= K_V, \ \mathbf{x} \in [0,1]. \end{gathered} \tag{5.26}$$

Hence, we only need to establish the convexity of the E2E delay constraint with respect to the optimization variables, $\mathbf{x}$, $\log(P_q)$, and K_V. Moreover, as aforementioned in Section 5.4.1 the problem is solved for one UAV at a time, then the optimization variables that affect the optimization are only $\mathbf{x}$ and $\log(P_q)$.

From Eq. (5.4), the E2E delay, D_{E2E}, is given by:

$$D_{E2E} = D_t + D_p + D_q, \tag{5.27}$$

where,

$$D_t = N' \frac{m}{\min_{\{i,j\} \in \mathbf{S}} R_{i,j}}, \tag{5.28}$$

$$D_p = \frac{\sum_{\{i,j\} \in \mathbf{S}}^{N'} \|\mathbf{u}_i - \mathbf{u}_j\|_2}{c}, \tag{5.29}$$

$$D_q = \sum_{i=1}^{N'} W_i + W_s. \tag{5.30}$$

Furthermore, the E2E delay has three terms, it suffices to prove that each term is convex in $\mathbf{x}$ and $\log(P_q)$; this follows from the fact that the sum of convex functions is also convex [BV04]. We can validate the convexity of D_{E2E} by examining the

Hessian of each term. The hessian matrix for two optimization variables is as follows

$$\mathbf{H}_n(\mathbf{x}, \log(P_q)) = \begin{bmatrix} \frac{\delta^2 F(\mathbf{x}, \log(P_q))}{\delta \mathbf{x}^2} & \frac{\delta^2 F(\mathbf{x}, \log(P_q))}{\delta \mathbf{x} \delta \log(P_q)} \\ \frac{\delta^2 F(\mathbf{x}, \log(P_q))}{\delta \log(P_q) \delta \mathbf{x}} & \frac{\delta^2 F(\mathbf{x}, \log(P_q))}{\delta \log(P_q)^2} \end{bmatrix}, \tag{5.31}$$

if the hessian matrix of a function is positive semi-definite in the optimization variables, $\mathbf{H}_n(\mathbf{x}, \log(P_q)) \succeq 0$, that means it is a convex function. Also, if the hessian matrix of a function is negative definite in the optimization variables, $\mathbf{H}_n(\mathbf{x}, \log(P_q)) \preceq 0$, that means it is a concave function.

First for D_t in Eq. (5.28), from the convex set properties the function $1/f(x)$ is convex if and only if the function $f(x)$ is a function convexity preserving and its interior is also convex.

The min function is a convexity preserving function [BV04], i.e., we only need to prove that the interior function, $R_{i,j}$, is convex. The $R_{i,j}$ can be written as

$$\begin{aligned} R_{uav,j} \leq W \Big[& \log_2(P_q) + 2\log_2(|h_{i,r}|) - n\log(d_{uav,j}) \\ & - \log_2\left(\sum_{j=1, j\neq i}^{N} \exp^{P_q |h_{i,r}|^2 d_{j,r}^{-n}} \right) - \log(\sigma_0^2), \Big] \end{aligned} \tag{5.32}$$

Whereas, the only rate, $R_{i,j}$, that depend on the UAV location and power are the links that connects the nodes through the UAV Then, applying the hessian matrix on Eq. (5.32) $\mathbf{H}_n(D_{Tx}(\mathbf{x}, \log(P_q)))$, then the function is convex as it can be shown as a zero matrix, Which indicate that it is a linear function, hence, $R_{i,j}$ is convex. Second, we inspect D_P which can be written as follows

$$D_p = \frac{\sum_{\{i,j\} \in \mathbf{S}}^{N'} \mathbf{x}^T \mathbf{D}_{i,j}}{c} \tag{5.33}$$

where, $\mathbf{D}_{i,j} \in \mathbf{R}^{\beta \times N}$ is the quantized distances between any 2 nodes i and j. Moreover, this term is linear $\mathbf{x}$, hence, it is convex. The convex investigation for the queue delay model is a quadratic function of the distances. Furthermore, the convexity investigation for D_p fit for the second and third constraints in Eq. (5.19), is a linear constraint as it sums over $\log(P_q)$. Moreover, D_q is a positive quadratic function in $\mathbf{x}$ and $\log(P_q)$.

CHAPTER 6

EFFICIENT AUTHENTICATION OF DRONES TO MMWAVE WIRELESS MESH NETWORKS IN POST-DISASTER SCENARIOS

6.1 Introduction

In post-disaster circumstances such as hurricanes and earthquakes, the communication and power infrastructures could be damaged, disconnecting affected communities from the rest of the world. Hence, restoring communication networks is vital for damage assessment and to start the recovery process. Public safety agencies and local governments are currently considering the deployment of UAVs, commonly known as drones. In a rapid post-disaster recovery, drones can act as relays among people in affected areas and local authorities. Therefore, in this chapter, we first propose a proxy-based scheme for drone-to-drone authentication. We delegate one of the drones to sign the authentication warrant on behalf of a CC to reduce the communication time energy. In this way, we ensure that a newcomer drone's authentication with one of the existing drones would suffice as it represents others in the network through the proxy features. The second scenario, considered in this chapter, focuses on trust among the deployed drones and the ground nodes. A drone may act as an imposter to deceive ground nodes. Therefore, there is a need for authentication of drones to ground nodes. This chapter aims to find an efficient way of authentication between a drone and its associated ground nodes, based on group authentication that significantly reduces the authentication's overhead. Thus, we propose adopting a broadcast-based group authentication scheme where a simple challenge-response authentication is followed. The signed messages in the broadcast utilize the proxy signature of the CC.

We implemented the two proposed authentication schemes in the NS-3 network simulator by utilizing an underlying IEEE 802.11ad communication environment that enables mesh networking among the ground nodes and drones. We implemented other baselines to compare with our approaches and assessed the overhead that comes with authentication. The results indicate that our mmWave-based authentication approaches can significantly reduce the authentication time and energy consumption.

The rest of this chapter is organized as follows. The system and attach models are described in Section 4.2. The proposed authentication schemes are introduced in Section 6.3. Finally, the evaluation and the security analysis are in Section 6.4.

6.2 System and Attack Models

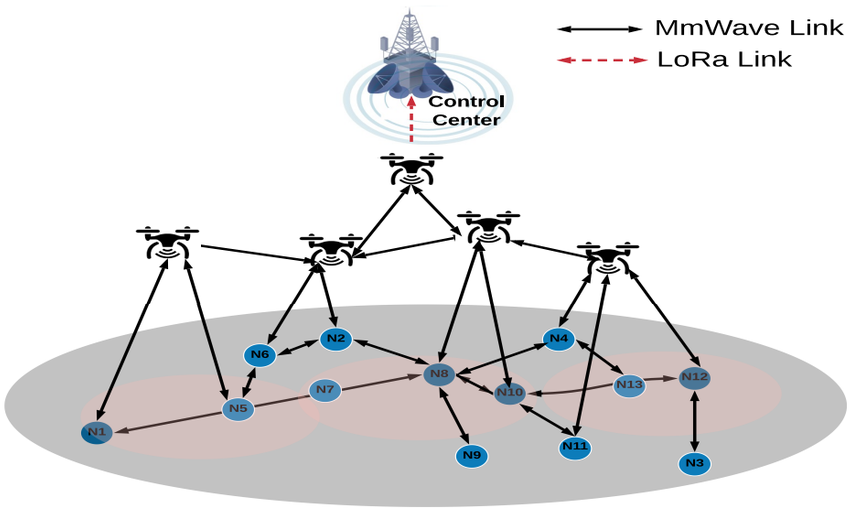


Fig. 6.1 Envisioned adhoc wireless mesh network of drones and ground users.

6.2.1 System Model

We assume a post-disaster scenario where most of the cellular base-stations and cable/DSL infrastructure have been damaged and not functioning. To enable communication among citizens and emergency crew, we assume that a certain number of drones could be deployed within a neighborhood in order to form a temporary ad hoc wireless mesh network among user smartphones/laptops or WiFi routers in their homes. We assume these drones can act semi-autonomously to make their own decisions once deployed. For providing high bandwidth multimedia communications, we assume these drones are capable of supporting mmWave communications such as IEEE 802.11ad standard, which operates at the 60GHz frequency. We consider that each user (ground) node has installed an emergency client application in advance to be used in the aftermath of a disaster where there is no Internet access. We assume a control center, CC, maintained by public-safety personnel, which can send drones to the region of interest to form a wireless mesh network where these drones serve as relay nodes to ground user nodes shown in Fig. 6.1. One of the drones can act as a gateway to connect to the CC using a

wide area communication standard such as LoRa [MCV17]. The notations used through this chapter are defined in Table 6.1.

Table 6.1 Notations.

Parameter	Definition
D_0	Observer drone.
Pub_{D0}	Observer drone public key.
ID_{D0}	Observer drone pseudonym.
CC	Control center.
$cert_{cc}$	CC's certificate.
G_j	j^{th} ground node.
ID_{Gj}	Ground node ID.
Pub_{Gj}	Ground node public key.
w_{Di}	The CC warrant.
(r_i, s_i)	The CC delegation keys pair.
$(Pub_{Dproxy_i}, Priv_{Dproxy_i})$	Proxy signature public-private key pair.

6.2.2 Attack Model

We assume that there may be malicious drones as they are deployed externally, but the ground nodes will be trusted. The drones do not collude, and there is time synchronization among the nodes. The following attacks are considered:

- A malicious drone can act as an imposter and become part of the wireless mesh network. Once becoming a mesh node, a malicious drone may not honor routing and forwarding (i.e., block messages, change the messages, etc.). It also can be a passive attack to collect private information coming from ground users.
- Without becoming part of the wireless mesh network, a malicious drone can broadcast messages to ground nodes claiming to be a gateway for them. In such cases, private user data can be collected from the ground users.

6.3 Proposed Authentication Schemes

The drone authentication problem with the presence of new drones and ground users to form an IEEE 802.11ad-based wireless mesh network can be divided into two sub-problems: (1) the mutual authentication among drones for new and legitimate drone deployment; and (2) the drone-to-ground nodes authentication. Our

proposed idea of the authentication scheme is based on proxy delegation from the CC for both cases. As such, rather than allowing each drone pair to authenticate each other mutually, we follow a more efficient approach where authentication with any of the drones would suffice. Given the nature of mmWave links, this process will be much faster and enable energy-efficiency in terms of drone movement. To enable this delegation, we utilize the proxy signature concept [LKK01]. The motivation comes from the fact that one can designate a proxy to sign messages on behalf of him/herself. The delegation can be in different forms, but eventually, the proxy's signature can be traced back to the original signer for verification. In our case, we will utilize the signature as an indication for device (source) authentication. We propose that the CC designate the drones as their proxies so that the drones can authenticate themselves to the post-disaster wireless mesh network as new devices. The details proposed approaches are discussed next.

6.3.1 Registration Phase

The first step in the network formation is the *registration phase* where the ground nodes within the envisioned mesh network are determined. To this end, the control center will designate an *observer drone*, D_0, which will hoover above the region of interest to collect information from the interested ground nodes. Specifically, the observer drone D_0 broadcasts a message that includes its public key Pub_{D0}, its unique pseudonym ID_{D0}, and the CC's certificate, $cert_{cc}$. The observer drone then collects the responses from any ground node which would like to become part of this mesh network. Note that the emergency client application on a ground node comes pre-installed with the public key of a certificate authority (CA) that can be used to verify any signature coming from the CC. Through this client app, any ground node, G_j will send a reply message that includes its unique ground node ID ID_{Gj}, public key Pub_{Gj}, its location, and its received signal strength indicator (RSSI) value. In the end, all the collected ground node info will be sent to the control center using LoRa by the observer drone. Based on the collected data, the CC optimally computes the number of $(M-1)$ new drones that need to be deployed and the best M locations for these new drones and the observer drone to maximize the communication throughput and enhance the link qualities by utilizing some of the existing solutions [AMIMA19].

6.3.2 Delegation Phase

Before the CC releases the additional $(M-1)$ drones to these locations, it performs some initial configurations to these drones first simply by manually accessing the drones and installing the needed parameters for the proxy signature creation as used in [LKK01]. To enable this, we assume that each drone D_i, $i = 1, 2, ..., (M-1)$ has a pair of public-private key $(Pub_{D_i}, Priv_{D_i})$.

As part of this proxy signature, the CC creates a *warrant* w_{Di} for each D_i by signing the drone's public key with its private key $Priv_{cc}$: $w_{Di} = \mathbf{S}(Pub_{Di}, Priv_{cc})$, where $\mathbf{S()}$ is any digital signature function. Then, a pair of *CC delegation keys* (r_i, s_i) is created for drone D_i as follows: Let g be a generator of a multiplicative subgroup of Z_p^* with order p. The CC chooses a random number $k_i \in_R Z_p^*$ and calculates these keys:

$$\begin{aligned} r_i &= g^{k_i}, \\ s_i &= Priv_{cc}\mathbf{H}(w_{D_i}, r_i) + k_i, \end{aligned} \tag{6.1}$$

where, $\mathbf{H}()$ is a collision resistant hash function.

Along with these keys, a *delegation message* of a tuple $(w_{D_i}, r_i, s_i, cert_{cc})$ is created and installed in each drone D_i, which can now create a *proxy public-private key pair*

$$(Pub_{Dproxy_i}, Priv_{Dproxy_i})$$

using the info in the delegation message to sign any message on behalf of the CC as follows:

$$\begin{aligned} Priv_{Dproxy_i} &= s_i + \mathbf{H}(w_{D_i}, r_i)Priv_{D_i} \\ Pub_{Dproxy_i} &= (Pub_{cc}Pub_{D_i})^{\mathbf{H}(w_{D_i}, r_i)}r_i \end{aligned} \tag{6.2}$$

Since $Priv_{Dproxy_i}$ is only known by D_i, the proxy signature can be only created by a legitimate drone D_i. Note that the same process was used to create the proxy key pair of the observer drone D_0.

6.3.3 Drone-to-Drone Mutual Authentication

Once the drones go to their locations, each drone D_i initiates the authentication process by creating a timestamp nonce t_{Di}, and then signs this nonce with its proxy private key $Priv_{Dproxy_i}$: $\sigma_i = \mathbf{S}(t_{Di}, Priv_{Dproxy_i})$. D_i then broadcasts a proxy signature that contains the following tuple: $(t_{Di}, \sigma_i, w_{Di}, r_i, Pub_{Di})$. Any other drone, say D_j, within the vicinity will be able to verify this proxy signature by verifying whether the proxy signature is valid. The following equation can do

this verification:

$$\mathbf{V}(t_{Di}, \sigma_i, (cert_{cc} Pub_{Di})^{\mathbf{H}(w_{D_i}, Pub_{Di})} r_i) \stackrel{?}{=} True \tag{6.3}$$

where $\mathbf{V}()$ is a digital signature verification algorithm. Note that this process can happen simultaneously for every drone, which can save significant time. However, due to drones' potential varying arrival times to their locations, some drones may not receive these broadcasts on time. Therefore, the broadcasts from D_i should continue until the neighboring drone(s) such as D_j replies back with the same message but with a different timestamp. The timestamps are used to prevent any replay attacks from malicious drones. This process is shown in Fig. 6.2. In this way, both drones are authenticated each other and can now become part of the mesh network.

Note that as long as a drone broadcasts a proxy signature, it can be authenticated with the rest of the drones without needing individual authentications. This model saves us time and energy in the context of the public safety application.

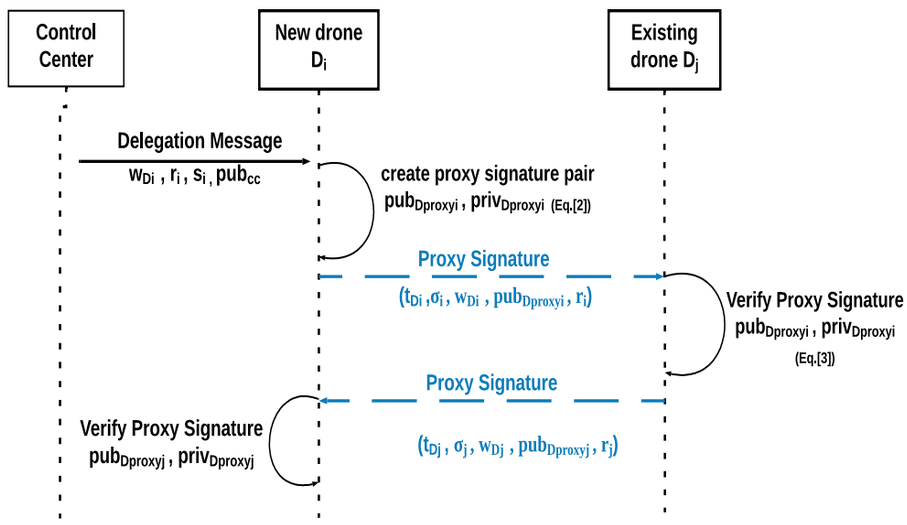


Fig. 6.2 Message exchanges among drones for mutual authentication.

6.3.4 Drone-to-Ground Authentication

The next step in forming the proposed wireless mesh networks is to ensure that the ground nodes trust the newly joining drones. In this section, we propose a device authentication mechanism to legitimize the drones to the ground nodes in the network and avoid any illegitimate drone communicating with these nodes in the context of the disaster applications. Given the nature of mmWave communications, we opted for a group authentication scheme where we can easily reach

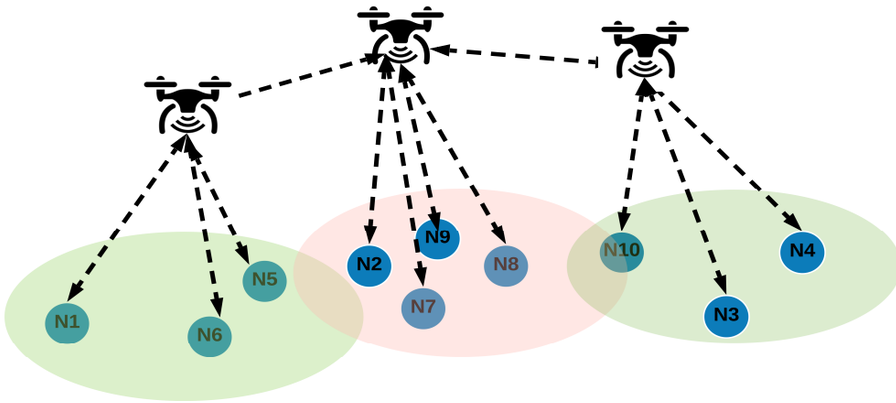


Fig. 6.3 Clustering of ground nodes to be served by a particular drone.

out to many nodes with a single message to achieve faster processing and eliminate any redundant messages as they can be easily lost. Note that authenticating nodes pair by pair is time and power-consuming for both the drones and the nodes in a disaster situation, particularly in the context of the mmWave channel.

To enable group authentication, we first need to divide the ground nodes into the clusters where a drone will be responsible for serving each cluster, as shown in Fig. 6.3. In order to enable this, each ground node should select a drone. When a drone does a broadcast, a ground node may hear from multiple of these drones depending on its location. We assume that the ground node will pick the drone whose message arrives first.

As the goal is to authenticate drones as entities that these ground nodes can trust, we propose using a one-time challenge-response protocol based on public-key cryptography. The motivation also comes from the fact that the ground nodes and the drones cannot agree on a symmetric key easily. This will introduce extra communication or other mechanisms that may not be suitable for disaster cases. Thus, we opt for a group-based challenge-response as we do not want to perform this process one-by-one with each ground node.

Nevertheless, we still rely on the proxy-signatures generated by the CC. The idea is to send a challenge to each ground node from their respective drone through a broadcast message. This challenge will include a proxy signature from the drone (i.e., delegated by the CC) that needs to be verified by each ground node. To this end, each drone D_i prepares and broadcast a proxy signature to its cluster that contains the following tuple:

$$D_i \rightarrow \forall nodes : (ID_{D_i}, t_i, w_{D_i}, \beta_i, cert_{CC}, Pub_{D_i}) \tag{6.4}$$

where $\beta_i = \mathbf{S}((ID_{Di}||w_{Di}||t_i), Priv_{Dproxy_i})$ is a signed message consisting of drone ID, its warrant, and a timestamp t_i using the drone's proxy private key $Priv_{Dproxy_i}$.

On receiving this broadcast proxy signature, a ground node, G_j, first verifies the *warrant* to ensure that it is signed by the private key of the CC: $\mathbf{V}(Pub_{D_i}, w_{D_i}, cert_{cc}) \stackrel{?}{=} True$. Next, it verifies the proxy signature to ensure that it is signed by the proxy private key of D_i:

$$\mathbf{V}((ID_{Di}||w_{D_i}||t_i), \beta_i, (cert_{cc}Pub_{D_i})^{\mathbf{H}(w_{D_i}, r_i)} r_i) \stackrel{?}{=} True. \tag{6.5}$$

Note that it can also verify the signature of CC using CA's private key which was pre-installed.

6.4 Security and Performance Analysis

In this section, we first discuss the security analysis of the proposed schemes and then present the simulation results to demonstrate the proposed scheme's effectiveness.

6.4.1 Security Analysis

In order to join the network, a legitimate drone D_i will need to show that it has a valid and unique pair of proxy key, which is created based on a unique pair of delegation key given by the CC to the drone D_i. A malicious drone D_m needs to broadcast a proxy signature message (either to other drones or ground nodes) that can be verified using the D_m's proxy public key. Since the delegation phase is conducted manually and securely prior to the drones' release to the new location, D_m will not be able to create its pair of the proxy key since it does not have the unique pair of delegation key. Hence, it cannot join and become part of the mesh network.

D_m may also try to impersonate a legitimate drone D_i by performing a *replay attack* where it replays a captured message from D_i either for joining the network or claiming as the gateway for ground nodes. In both cases, D_m broadcasts the whole proxy signature of drone D_i, $(t_{Di}, \sigma_i, w_{Di}, Pub_{DProxy_i}, Pub_{Di})$. Let us assume a verifier node (either drone or ground node) X_k receives this broadcast for the first time. This proxy signature will not pass the verification using Eq. 6.3 due to stale timestamp value in the message. That applies to Eq. 6.5 in the same manner.

6.4.2 Experimental Setup

We used NS-3 [NSN16] network simulator to performed the evaluations. We adopted the IEEE 802.11ad mmWave implementation described in [AW16] as the underlying communication for the drone-to-drone and drone-to-ground nodes communications. We used the following IEEE 802.11ad parameters for the experiments: *PHY Type* = DMG-MCS18, *Antenna Sector*=8, *Transmission Power*=10 dBm, and *Transmitter and Receiver gain*=23. The LoRa connection from observer drone to CC is also implemented using the NS-3 LoRa module. The CC is assumed at 1km from the observer node. We used a Raspberry Pi IoT device to mimic constrained drone processing power and measure the required cryptographic operations' authentication times. These collected authentication times are then utilized in NS-3 to make a realistic simulation scenario. We used ECC for signatures. The key size is set to 260 bits.

N_D number of drones are placed to cover the whole area of interest. Each drone covers an area of 100×100 m^2. The ground node density in an area is varied in terms of the number of ground nodes. We used different number of ground nodes (i.e., $(10, 20, \cdots, 50)$) for the evaluations. The positions of the ground nodes are randomly distributed. The drone is assumed to be placed in a specific location above the area with a varying altitude below 60m to ensure the coverage of all ground nodes within the area.

6.4.3 Metrics and Baselines

To assess the performance, we considered the *total authentication time*, which includes all the communication and computation delays. In addition, we considered the energy metric for drones, which indicates the energy consumption for running the proposed approaches. To this end, we mainly counted the *number of messages* sent (TX) and received (RX) by all drones as computation energy is almost negligible compared to communication energy costs. To compare with our proposed approach, we considered some baselines as follows:

1. *Drone-to-Drone mutual authentication*: For this case, we considered a baseline approach where all the newcomer drones are authenticated to the CC through the observer drone using multi-hop/ long-distance communication. This communication to the CC is based on a challenge-response mechanism referred to as *centralized authentication*. As a second baseline, we also considered our proxy

approach but in a sequential manner where drones authenticate themselves in a sequence starting from the observer drone's first neighbor using unicast messages. This approach is referred to as *sequential proxy signature* in the figures, while our approach is shown as *parallel proxy signature*.

2. *Drone-to-ground node authentication*: For this case, as a baseline, we considered a pairwise proxy authentication from a drone to each of the ground nodes using unicast messaging. We refer to this approach as *unicast-based proxy signature* in the figures. Moreover, we consider a traditional group authentication through the CC where the drone asks the observer drone to request a signed message from CC. The CC sends it back to the drone via the observer, which can then broadcast it to the cluster's ground nodes. This baseline is referred to as *centralized group authentication* in the figures. Our approach is labeled as *broadcast-based proxy signature*.

6.4.4 Performance Results

Drone-to-Drone Mutual Authentication results

Fig. 6.4 shows the authentication time plotted with the increasing number of drones for all approaches. As can be seen, our parallel proxy scheme can provide significant time savings compared to a centralized challenge-response approach and sequential proxy. With the increased number of drones, the reduction is almost doubled. This reduction can be attributed to the fact that our approach performs authentications in parallel, thanks to consent from CC, which reduces the authentication time.

Table 6.2 shows the total number of messages sent and received for each approach. As can be seen, proxy-based approaches are much more energy-efficient. The parallel proxy approach reduces the transmission messages, TX more than 13 fold when the # of drones is 11 compared to the centralized approach. Again this is due to eliminating the need to reach observer drone or CC for any authentication purposes. Moreover, the parallel proxy approach results in more received messages, RX, more than the sequential proxy signature as we broadcast the messages, and more nodes can receive it. However, as TX energy cost is typically much higher than RX, the parallel proxy approach is still more energy efficient as it almost halves the TX count.

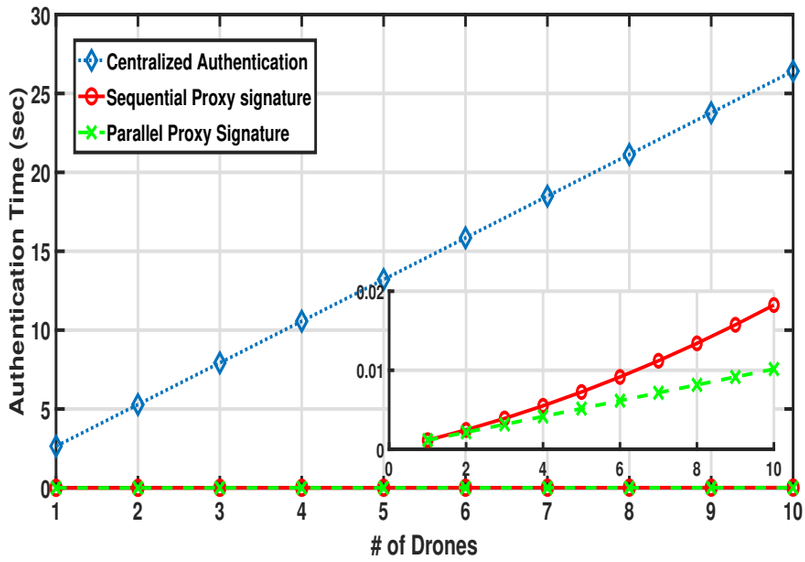


Fig. 6.4 Drone-to-Drone mutual authentication time under varying # of drones.

Table 6.2 Total # of messages for drone-to-drone authentication.

	Centralized Authentication		**Sequential Proxy Signature**		**Parallel Proxy Signature**	
# of Drones	TX	RX	TX	RX	TX	RX
2	6	6	2	2	2	2
3	14	14	4	4	3	6
4	24	24	6	6	4	12
5	36	36	8	8	5	18
6	50	50	10	10	6	24
7	66	66	12	12	7	29
8	84	84	14	14	8	34
9	104	104	16	16	9	39
10	126	126	18	18	10	44
11	150	150	20	20	11	49

Drone-to-Ground Authentication Results

In this subsection, we present the performance of the authentication mechanism for Drone-to-Ground authentication. We assessed the effect of a different number of ground nodes on the drone-to-ground node authentication time. As seen in Fig. 6.5, the time for *Unicast-based Proxy Signature* increases linearly with the increasing number of ground nodes since, in this mechanism, the drone authenticates to each ground node separately. However, for our *broadcast-based proxy signature* approach, the authentication time stays stable even though the number of ground nodes increases. This stability is because we use a broadcast-based

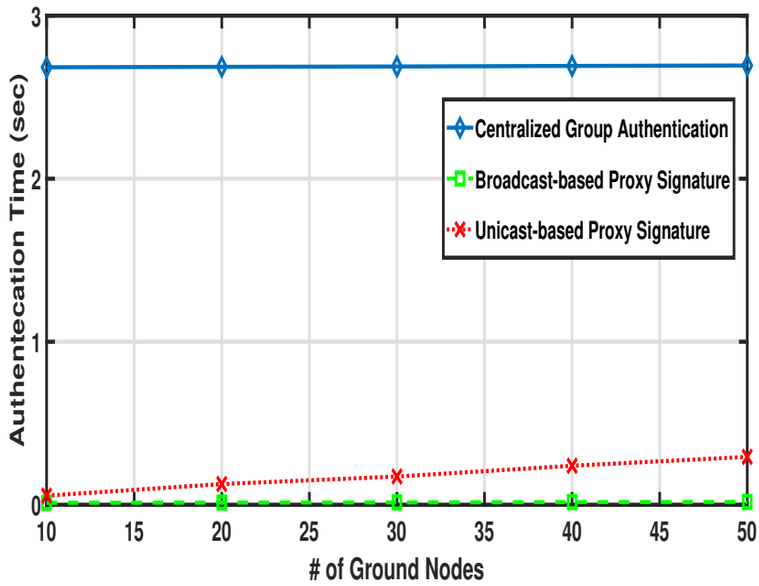


Fig. 6.5 Drone-to-Ground authentication time under varying # of ground nodes

approach where each ground node can become part of one of the existing clusters served by a drone. Increasing the number of nodes will only increase a cluster's size, yet the broadcast will still reach them in one message. Note that compared to these proxy cases, the *centralized group authentication* performs much worse due to the need for long-distance communication to the CC. Nonetheless, since each drone uses broadcasts, the authentication time is fixed.

Looking at the total number of messages exchanged, as seen in Table 6.3, our approach requires a single transmission message from each drone. At the same time, this will increase with the number of ground nodes in the unicast-based authentication. Moreover, a drone in centralized group authentication needs to reach the observer and the CC, which increases the TX count. Given that RX count is similar for all approaches, our broadcast-based proxy approach consumes the least energy.

Table 6.3 Total # of messages for drone-to-ground authentication.

	Centralized Authentication		**Unicast-based Proxy Signature**		**Broadcast-based Proxy Signature**	
# of Ground Nodes	TX	RX	TX	RX	TX	RX
10	5	14	10	10	1	10
20	5	24	20	20	1	20
30	5	34	30	30	1	30
40	5	44	40	40	1	40
50	5	54	50	50	1	50

CHAPTER 7

DRONE AUTHENTICATION TO THE 5G NETWORKS

The 5G infrastructure with both UEs and the various IoT devices will pose threats to the 5G network infrastructure and expose users' privacy. Recognizing this risk, the current 5G also comes with new security protocols to ensure primary security services for confidentiality, integrity, and authentication [SH15, JM19]. Nevertheless, the current focus of these security services is primarily about users and their data. While there are defined procedures for M2M communication security, their assurance will not be verified until large-scale M2M applications with 5G are deployed. Hence, there is a need for additional security services for drone applications that will utilize separate network slices in 5G.

Therefore, in this chapter, we propose a second-factor authentication scheme to verify legal drones' authenticity as a part of the 5G network. This second-factor authentication is inspired by multi-factor authentication mechanisms currently employed in IT systems for enhanced security. The goal is to double-check a drone's authenticity by utilizing various factors from the primary authentication that comes with 5G authentication services. Unlike second-factor systems where the entire authentication depends on both first and second factors, the proposed mechanism will be in addition to the primary one. The main challenges for such an authentication scheme are twofold: 1) To provide a lightweight scheme that will not bring additional burden to drones, and 2) integrate the mechanisms to the current 5G standard based on 3GPP specifications [SH15].

To this end, for the first challenge, we propose a challenge-response based protocol that conforms with the current 5G authentication standard that utilizes drones' digital IDs, which will be enforced by Federal Aviation Administration (FAA) in the US [Fed20]. We include mechanisms such as simultaneously using a seed and nonce to prevent any replay attacks. We exploit the re-authentication triggering mechanism currently in place for the 5G authentication for the second challenge. This trigger is used to initiate our second-factor authentication without making any other system changes. We implemented the proposed approach in the NS-3 simulation environment, which supports 5G radio access. The evaluation indicated that the proposed approach brings almost negligible overhead in both computation and communication and can be easily integrated with network slicing.

This chapter is organized as follows: Section 7.1 is dedicated to the system models. In Section 7.2, we explain the details of our proposed authentication approach. is dedicated to of the approach. Finally, the security evaluation and authentication performance evaluation are in Section 7.4 and Section 7.3, respectively.

7.1 System and Attack Models

7.1.1 System Model

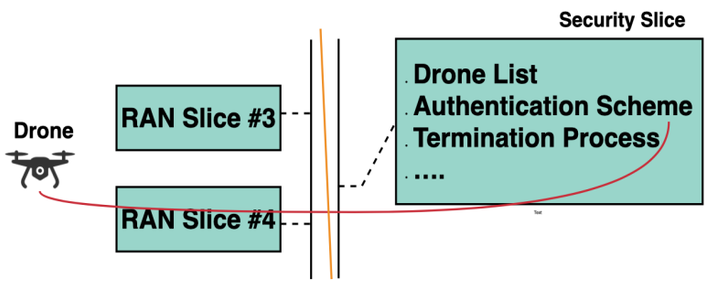


Fig. 7.1 Assumed network slicing for drones.

We assume a 5G cellular infrastructure where drones could connect through the standard 5G Authentication procedure (EAP-AKA or EAP-TLS). Each drone is considered to have a digital ID assigned by FAA. This digital ID assignment is due to a recent announcement from FAA in the US that each drone accessing the 5G system shall be assigned a drone Remote Identifier (Remote ID) to register drones [Fed20] legally. Moreover, all drones are initially registered as UE devices through the SEAF/AMF in the network core for proper cellular communication. Hence, the primary 5G authentication protocols are executed for all the drones before any communication attempts throughout the network.

In 5G, the service model is based on virtual network slices [LSC+17], allowing flexibility for providing differentiated services based on applications' needs and requirements. A virtual network slice is a network customized to serve a defined business purpose or customer, consisting of an end-to-end composition of all the available network resources required to satisfy the specific performance [LSC+17]. These virtual network slices are the major re-haul from 4G/LTE systems and enable flexibility and efficiency. Each network slice is identified by a Single Network Slice Selection Assistance Information (S-NSSAI), which could be used by a UE when requesting access to the 5G Core and the 5G-Radio Access Network (5G-RAN) [3GP20]. In our case, we assume that there is a specific network slice for the drones to provide additional authentication services as shown in Fig.

7.1 managed by the third party mentioned above. This slice information is provided by the drone when connecting to the 5G network core.

7.1.2 Attack Model

We assume that the 5G Core network is trusted, but the drones are not trusted, and they can try to bypass the system to become part of the 5G network. We identify any malicious drone as a drone that is not pre-registered in a friendly drone database administered by a third party and is trying to access the network to communicate with other parties. We also assume that adversaries may impersonate a drone or core network to replay authentication messages back and forth.

7.2 Slice Specific Second-Factor Authentication

When a drone acting as a UE requests connectivity through a specific slice in 5G, the slice manager may also want to further authenticate the device for increased security in addition to 5G primary authentication. Note that this is somewhat analogous to the second-factor (or multi-factor) authentication concept used in modern IT systems. However, it is in addition to primary one (i.e., primary and secondary are not linked), which is not the case in IT systems. In a sense, it can be considered as a re-authentication mechanism for more specific purposes. Nevertheless, there needs to be diversity in this additional authentication request, as in the case of second-factor authentication. The goal is to increase security by using a different factor each time (e.g., asking for a text message after entering your password). To support this concept in our case, we would like to request information from the drones in this second authentication that is different from the primary authentication (e.g., ID, keys, fingerprints, etc.) while still following the EAP-based authentication used in the 3GPP standard. However, as the current 3GPP specifications do not explicitly support this type of second-factor authentication [3GP20], we propose utilizing specific existing 3GPP procedures to integrate our second-factor authentication protocol to the current standard. Next, we explain how we can trigger this second-factorby following the standard's specifications (i.e., not requesting any changes), and then we describe our authentication protocol in detail.

7.2.1 Initiating Slice Specific Second-Factor Authentication

Current 3GPP standard specifications allow a re-authentication procedure for a device based on its S-NSSAI [3GP20]. Specifically, suppose there is a specific S-NSSAI for drones other than the default one. In that case, this specific drone slice could dictate the Authentication Authorization and Access Server (AAA-S) to initiate another application-specific authentication. Note that AAA-S is in charge of authentication in 5G and maybe sitting in the operator's network or a separate third party network. This procedure is called AAA-S triggered *Network Slice-Specific Re-authentication and Re-authorization procedure* [3GP20] and its details are shown in Fig. 7.2. We adopt this procedure for our initiation purposes so that our approach can be easily integrated with the envisioned implementations of 5G Core.

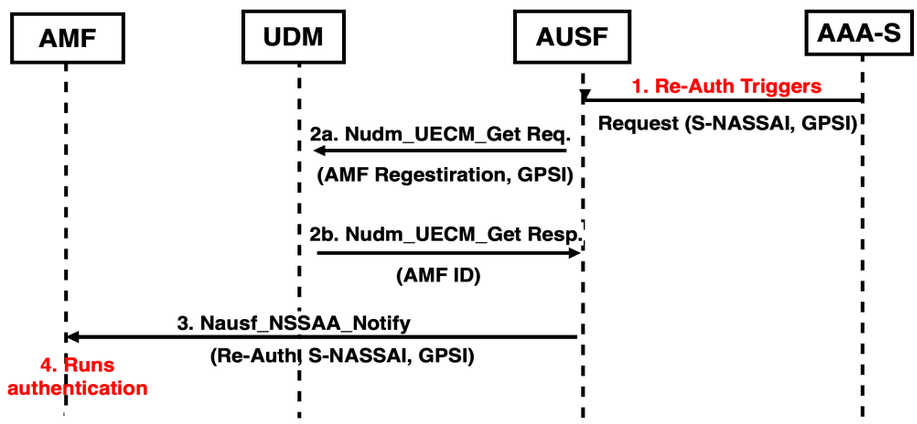


Fig. 7.2 AAA-S triggered Network Slice-Specific Re-authentication and Re-authorization procedure in 3GPP. We use this procedure to integrate our second-factor into the system.

In our approach, before AAA-S initiates the second-factor authentication, the slice functions will need to check whether the SUPI of the device registered exists in a drone database created in advance. If the SUPI of the registered drone is within this database, then a second-factor will be mandated. That is precisely where our approach kicks in: We exploit the 5G standard's ability to re-authenticate to trigger a mandatory second-factor authentication for drones to secure their communication further. This approach will be initiated by AAA-S, which requests Generic Public Subscription Identifier (GPSI) for the devices. Note that GPSI is used for addressing a 3GPP subscription in different data networks outside of the 3GPP system. But since the 3GPP system stores within the subscription data the association between the GPSI and the corresponding SUPI, it is easy to map. The initiation process follows the procedure in 3GPP

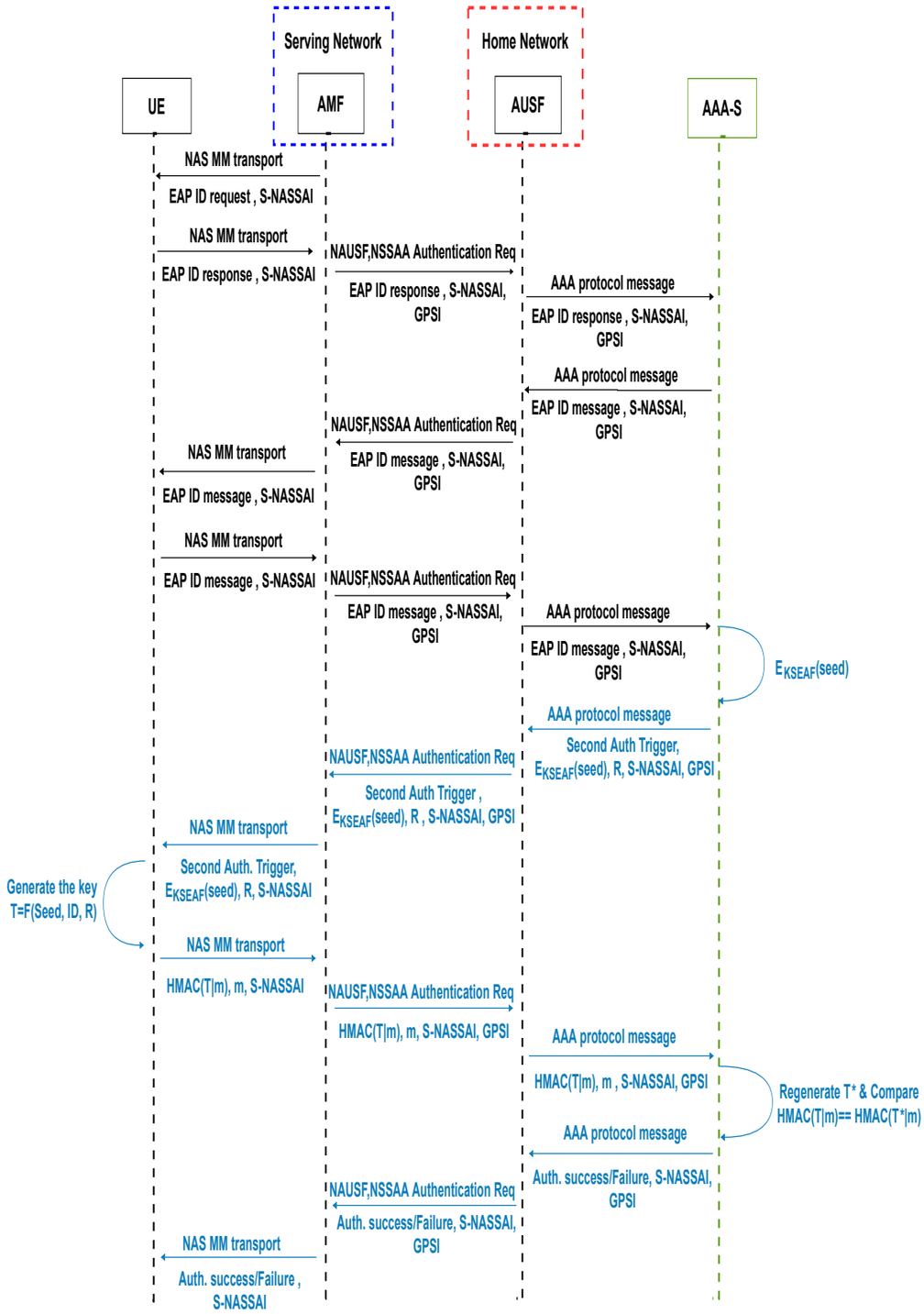


Fig. 7.3 second-factorauthentication registration shown in black messages and proposed protocol shown in blue messages

standards, where AAA-S informs the AMF to request registration from the drone. AMF will initiate a *challenge-response* EAP protocol to the newly authenticated drone that will follow our proposal to differentiate it from the primary one. This EAP-compliant procedure is explained in the next subsection.

7.2.2 Second-factor authentication protocol

Our protocol follows a challenge-response type authentication procedure since it needs to conform with the current EAP framework for 5G authentication. This framework is flexible because it allows replacing the underlying authentication protocol such as AKA or TLS. Our approach's main motivation is to enable a more restricted authentication specific to our application that will rely on different information from the primary 5G authentication. To this end, we utilize two new items that have no relationship with the prior material generated during primary authentication: 1) The digital ID of the drone: As mentioned before, this unique ID will be different than any other IDs that the 5G system might assign; and 2) A new symmetric key different from the existing key hierarchy: This key is produced from a unique seed generated by the machine managing the related network slice function so that it will not have any relation with the key seed K_{SEAF} produced during the primary authentication.

Our challenge-response protocol kicks in after AMF (i.e., the party responsible for handling the process after AAA-S informs it about the second authentication request) follows the drone's standard registration procedure. It sends an EAP ID request message and gets an EAP Response from the drone, passed to AUSF and AAA-S as part of the initiation procedures. This process is shown in Fig. 7.3 in black messages. The rest of the authentication process between the AAA-S and the drone, shown in blue in Fig. 7.3, is detailed below. Note that we could directly initiate the authentication from the AAA-S without resorting to EAP-Request and Response messages. Since this is part of the initiation process, we follow the standard's messages to ensure that our protocol can be fully integrated.

- **Challenge from AAA-S**: The AAS-S prepares a challenge to be relayed to the drone by the intermediate components AUSF/UDM and AMF/SEAF. This includes a random number R and a seed $Seed$ generated by the hosting computer using pseudo-random generator each time there is a need for a secondary authentication. The $Seed$ is encrypted using the symmetric key, K_{SEAF} which was produced in the primary authentication phase and then sent to drone D_{ID} along with R. Moreover, ID is the FAA remote identifier assigned to the drone:

$$AAA - S \rightarrow E_{K_{SEAF}}(Seed), R \tag{7.1}$$

- **Challenge Response Preparation**: The receiving drone, D_{ID} calculates the challenge reply based on a unique symmetric key T which is created by using private ID, $Seed$ and R sent to it:

$$T = F(Seed, ID, R) \tag{7.2}$$

where F is a deterministic random bit generator (DRBG) function [BFW15]. The drone then uses this T as a symmetric key and m as a dummy message and creates a secure message authentication code (HMAC) [KF07]. This HMAC and m are then relayed to the AAA-S as follows: The drone then uses this T and creates a secureHMAC [KF07] message using T as a symmetric key and m as a dummy message.

$$HMAC(T|m), m \rightarrow AAA - S \tag{7.3}$$

- **Response Verification**: AAA-S receives these $HMAC(T|m)$ and m pair and recomputes a new HMAC by using the info stored locally in the database (i.e., drone ID, $Seed$ and R to re-generate T). If the new HMAC and the received one matches, then it sends an ACK message to the drone to finish the second-factor authentication:

$$ACK \rightarrow Drone \tag{7.4}$$

If they do not match, then a de-registration procedure is initiated. The AAA-S contacts AMF to initiate this process for the UE, which is already part of the 3GPP standard.

7.2.3 Security Analysis of the Proposed Protocol

Our second-factor authentication utilizes unique information from drones and AAA-S. Therefore, any drone whose unique ID is not in the database will be de-registered from the network when our second-factor is triggered. The protocol is also resilient against any replay or integrity attacks. Any adversary that tries to create an HMAC will fail due to lack of access to the secret key T. In addition, each time, the AAA-S will generate a new seed $Seed$, so any replay attack from an imposter server will fail due to mismatching of $Seed$ values. Similarly, since the drone is using a new R each time, any replay attack from the drone side will also not be possible. These values ensure that authentication messages are all fresh. Finally, even if a drone ID is compromised, this can not be used in future authentications because the system requires new $Seed$ and R values (i.e., forward secrecy).

7.3 Security Analysis

The security analysis, the proposed authentication model is qualified to sustain the following security issues,

1. *Message Integrity*: Any adversary that tries to create an HMAC will fail due to lack of access to the secret key T. Hence, integrity is achieved.
2. *Strongness*: During the verification process, the encrypted K_SEAF secret key and D_{ID} needed. Thus, any entity other than the designated drone is incapable of successfully complete the validation. Hence, the proposed scheme is strong enough against the resilience of various types of attacks.
3. *Modification attack*: The warrant comprises the message scope, and verification needs the secret key of the core network. Thus, during verification, message alteration will not be successful. Thus, the proposed scheme prevents modification attacks.
4. *Replay Attack*: Each time, the AAA-S will generate a new seed *Seed*, so any replay attack from an imposter server will fail due to mismatching of *Seed* values. Similarly, since the drone is using a new R each time, any replay attack from the drone side will also not be possible. These values ensure that authentication messages are all fresh. Finally, even if a drone ID is compromised, this can not be used in future authentications because the system requires new *Seed* and R values (i.e., forward secrecy). Thus, a replay attack is not successful in the proposed scheme.
5. MiTM attack: To prevent MiTM attack, authentication of source, identifiability, and unforgeability should be satisfied. Since the proposed authentication scheme satisfies all these attacks as aforementioned, therefore, an eavesdropper can not alter the message signature pair. Hence, the proposed scheme prevents the MiTM attack.

Furthermore, the *Seed* and R values ensure that authentication messages are all fresh. Hence, even if a drone ID is compromised, this can not be used in future authentications because the system requires new *Seed* and R values (i.e., forward secrecy).

7.4 Performance Analysis

7.4.1 Experiment Setup

In order to assess the performance of the proposed second-factor authentication, we utilized the NS-3 network simulator, which has recently implemented 5G-RAN module [WoP18]. Nevertheless, it still does not support the new 5G Core, and thus we needed to simulate the slicing on the server-side. Specifically, we created a UE node (node 1) to represent a drone and another server node (node 2) to define the core network's AUSF server, all of which serve as NS-3 nodes. This AUSF is connected to another server (node 3), representing the AAA-S and specific network slice for drones. We created an Ethernet connection from the AUSF server to AAA-S to indicate connections between them, assuming AAA-S can represent a virtual function. The overall architecture for this implementation setup is shown in Fig. 7.4. In this implementation, we initiate the process by sending

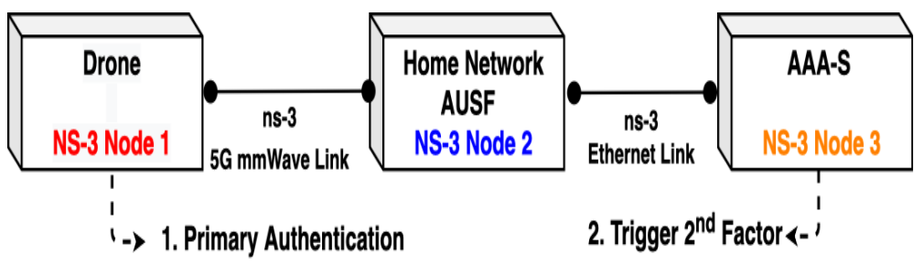


Fig. 7.4 NS-3 implementation setup.

a message from UE to AUSF assuming this will be the completion of primary authentication, which then contacts AAA-S through the Ethernet connection for slice specific authentication. Our implementation starts with AAA-S contacting core network (i.e., AMF) to contact the UE which will start running messaging shown in Fig. 6.1. Table 7.1 lists the system parameters for NS-3 simulation as well as the bit sizes for keys used in the experiments.

7.4.2 Metrics and Baselines

To assess our proposed authentication mechanism's overhead, we considered the *total authentication time*, which includes all the communication and computation delays during the authentication process. Note that the computational delay is crucial in determining the proposed authentication scheme's overhead due to lim-

Table 7.1 Simulation Parameters

Parameter	Value
Packet size	1000 bit
Data rate	30 Mb/sec
Background nodes traffic	10
gNodeB distance	300 m
inter packet interval	100
Seed size	440 bits
Remote ID size	32 bit
K_{SEAF} size	256 bit
HMAC type	SHA256

ited battery and resources on a drone. Hence, toward a more realistic assessment, we used a Raspberry-Pi3 IoT device to mimic the drone's behavior.

7.4.3 Performance Results

Drone Computational Overhead

The drone's computational delays through the second-factor authentication are in Table 7.2. Hence, the total processing delay for our proposed secondary authentication is 0.942msec. Moreover, the utilization of the DRBG hash provides a faster computational time, and hence, the total computational time is less than 1msec, which is even less than the total time for primary 5G-AKA authentication.

Table 7.2 Computational Overhead Comoarison

Approach	Operation	Delay (msec)
2^{nd} Factor	DRBG-Hash	0.16
2^{nd} Factor	HMAC	0.78
2^{nd} Factor	**Total**	**0.94**
5G-AKA	**Total**	**1.02**

Communication Delay

The communication delays experienced between the AAA-S and the drone throughout the second-factor authentication are in Table 7.3. As seen, the total authentication delay is 7msec for one drone authentication. Note that since our approach also uses challenge-response based authentication, the communication delay is almost similar due to the same number of messages exchanged for primary authentication. The only additional delay for our approach is the triggering time, which is 3.62msec in total. Overall, the total time of 7msec is an important figure since this is the amount of time provided to drone to act maliciously until the second-factor authentication de-registers it if the drone is malicious. During that 7msec, the drone can't collect and transmit any meaningful data, which indicates our approach's effectiveness.

Table 7.3 Second-Factor Communication Overhead

Approach	Connection	Delay(msec)
2^{nd} Factor	AUSF to AAA-S Ethernet	1.50
2^{nd} Factor	Drone to AUSF	1.12
2^{nd} Factor	TCP Handshake Time	2.18
2^{nd} Factor	**Total Communication Delay**	**7.00**
5G-AKA	**Total Communication Delay**	**3.38**

Impact of Background Traffic Delay

Another factor we investigated is the impact of background traffic from other existing nodes within the same cell during the second-factor authentication. We simulated both Uplink and Downlink background traffic connecting to the AUSF server simultaneously while starting the second-factor authentication to investigate this point further. The traffic frequency at each node is set to 1msec interval between packets transmissions, and the maximum number of packets sent by each node is set to 100000. This setup is considered a heavy bulk background traffic over the server. As shown in Table 7.4, the total authentication delay based on the high background traffic up to 100 nodes is within 0.4 µsec. Hence, under heavy background traffic, the additional delay is negligible, which means no extra delay overhead on the proposed authentication.

Table 7.4 Delay under varying Background Traffic

Background Nodes	Delay (msec)
10	7.000753
50	7.000810
100	7.000968

CHAPTER 8

DRONE TO DRONE AUTHENTICATION IN THE 5G NETWORKS

8.1 Introduction

The 5G ProSe security extension scheme is still under development, which opens a wide area for research and contributing. This chapter proposes an authentication scheme that fits in the 5G D2D ProSe anticipated standard. We propose a delegation based authentication for lightweight, fast and reliable authentication instead of the existing LTE/5G ProSe centralized scheme. In particular, we propose a proxy signature algorithm where each legal drone will assign a delegation warrant and parameters to derive the proxy signature keys to be used in the authentication process. Moreover, the proxy signature keys take into calculations the drone's private key, and hence, we prevent malicious drones and repudiation attacks. We follow the ProSe discovery model for the drone discovery phase, in which the drone detects other drones in the network for D2D communication. The ProSe discovery model has two models, Model A and Model B. In Model A, each drone announces its existence in the network, wherein in Model B, each drone sends a discovery message to the nearest drones. Our proposed authentication protocol would work for both Models. We follow Model A in our simulations; however, Model B applies to our proposed model as well. We assume a leader drone as a relay between the 5G core network and all other drone swarms. We propose a proxy signature-based message exchange mechanism between the leader drone and the swarm drones.

In this chapter, We target the security challenges in the drones' D2D communication in such a way that conjunct into the 5G D2D ProSe standards. We assume having a swarm-of-drones where only one of them is within the cellular coverage (i.e., a data relay) and others establish D2D links with this leader drone. The leader drone acts as a UE-to-Network Relay between the 5G network core and all other drones in the swarm. We propose mutual authentication of leader drone and others in the swarm. Given the resource limitations of drones, we must provide an efficient and lightweight solution for scalability purposes.

As opposed to following an approach similar to the 4G ProSe security standards where there is a requirement to have access to the network core, we opt for a solution that will minimize the message exchanges among the drones and

the core network. To achieve the above objectives, we propose a delegation-based authentication using proxy signatures. A proxy signature enables a party to delegate its authentication credentials to other parties while still providing the same security services as digital signatures (i.e., source authentication and message integrity). Specifically, the proxy signer signs a message using a secret key of the original signer and its own private key [DSP06, LY05]. Our solution is similar to the existing OpenID [RR06] type authentication mechanisms. In the sense that they rely on an OpenID server, which issues identities to be presented as evidence (i.e., like a proxy signature) for authentication. However, we do not want to access this server each time, in our case, since we would like to minimize the number of messages.

Therefore, after the mandatory 5G registration phase, we add a delegation phase, in which we assign a delegation warrant and proxy parameters. Those delegation parameters are used to derive the proxy signature keys for the authentication process. Then, we follow the existing ProSe device discovery model where a drone detects other drones in the network for D2D communication. The ProSe discovery model has two options: Model A and Model B. In Model A, a drone announces its existence in the network, wherein in Model B, each drone sends a discovery message to the nearest drones. Our proposed authentication protocol would work for both models. The authentication process is integrated into the discovery phase by attaching a drone's proxy signature and verifying it by the receiving drones. We assessed our scheme through implementation with the NS-3 5G network simulator under the D2D communication model [Dio17]. For a realistic assessment of computations times for the proxy signature keys, we performed all the computations on a Raspberry-Pi3 IoT device. We also set a baseline comparison to the 4G ProSe security standard. Our results show an overall much lower device authentication delay compared to this baseline.

The rest of this chapter is organized as follows. The system and attack models are described in Section 4.2. The proposed authentication schemes are introduced in Section 8.3. Finally, the security analysis and performance evaluation are in Section 8.4 and Section 6.4, respectively.

8.2 System and Attack Models

8.2.1 System Model

We assume a drone-to-drone communication model under a 5G cellular infrastructure network. The drones can communicate directly through D2D communication. One of the drones, *leader drone*, will act as a *UE-to-Network relay* to the 5G core network. The described communication model for the proposed 5G D2D drone communication is in Fig. 8.1. Each drone i is assumed to have a pair of public and private asymmetric keys: y_i and x_i respectively.

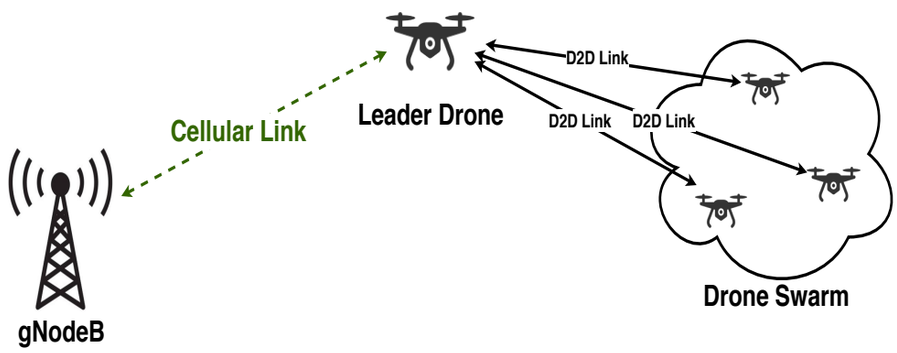


Fig. 8.1 Assumed drone communication model.

8.2.2 Attack Model

We assume the following threats to the drones:

1. *Malicious Leader Drone*: A malicious drone can broadcast messages to other drones claiming to be a UE-network relay for them. In such cases, private data is collected from the drones.
2. *Replay Attack*: A malicious drone sniffs the communication between other legitimate drones to maliciously transmit a repeated or delayed signature to verify itself to the leader drone.

8.3 D2D Authentication Protocol

8.3.1 Motivation and Overview

As described under the ProSe security standard, the authentication solution is time-consuming and introduces additional message overhead. The ProSe security

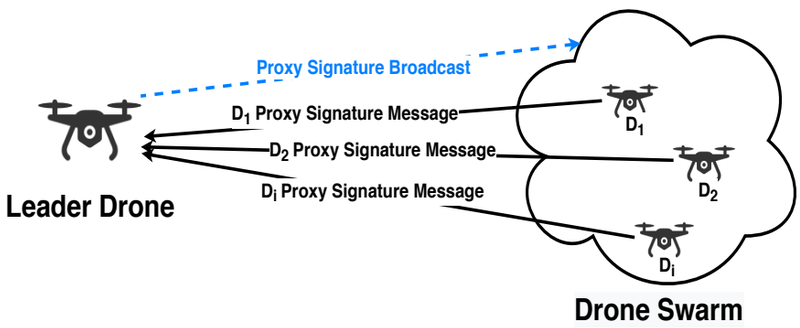


Fig. 8.2 Drones authentication messages.

standard further requires maintaining the state information about all the keys. As a result, following a similar approach will not be useful to IoT devices, which require a fast and scalable authentication mechanism. Therefore, in this chapter, we propose a new model for the 5G standard, with no pre-messaging to sustain IoT devices that may be resource-constrained, such as drones.

In this way, we also minimize the message count to ensure scalability for the 5G Core and support an increased number of nodes.

Specifically, we propose a proxy signature-based device authentication where the leader drone first authenticates itself to the swarm of drones by only broadcasting a proxy signature. Hence, other drones in the swarm initiate the authentication to this leader drone by using a similar proxy signature to be ready for communication, as shown in Fig. 8.2. In both cases, the original signer of these proxy signatures is the 5G Core (i.e., the elements that will replace PKMF in 4G). Therefore, we allow the nodes to authenticate themselves to the PKMF existing within 4G through the leader drone. We provide the details of this process in the next subsections.

8.3.2 Registration and Delegation Phase

After the drones are registered and authenticated through 5G authentication services (i.e., 5G-AKA [Kou19] mechanism), they are checked against their digital drone IDs to initiate a delegation phase for D2D communication. A specific slice function is triggered based on the drone IDs kept in a list by the network function operator. In the delegation phase, all these drones receive the needed parameters for the proxy signature creation. Those parameters are fetched specifically from the AAA-S in the 5G core network, as shown in Fig. 8.3.

Let us assume that AAA-S has a private-public key pair (x_c, y_c). The proxy signature keys are created for a drone D_i by first generating a random number

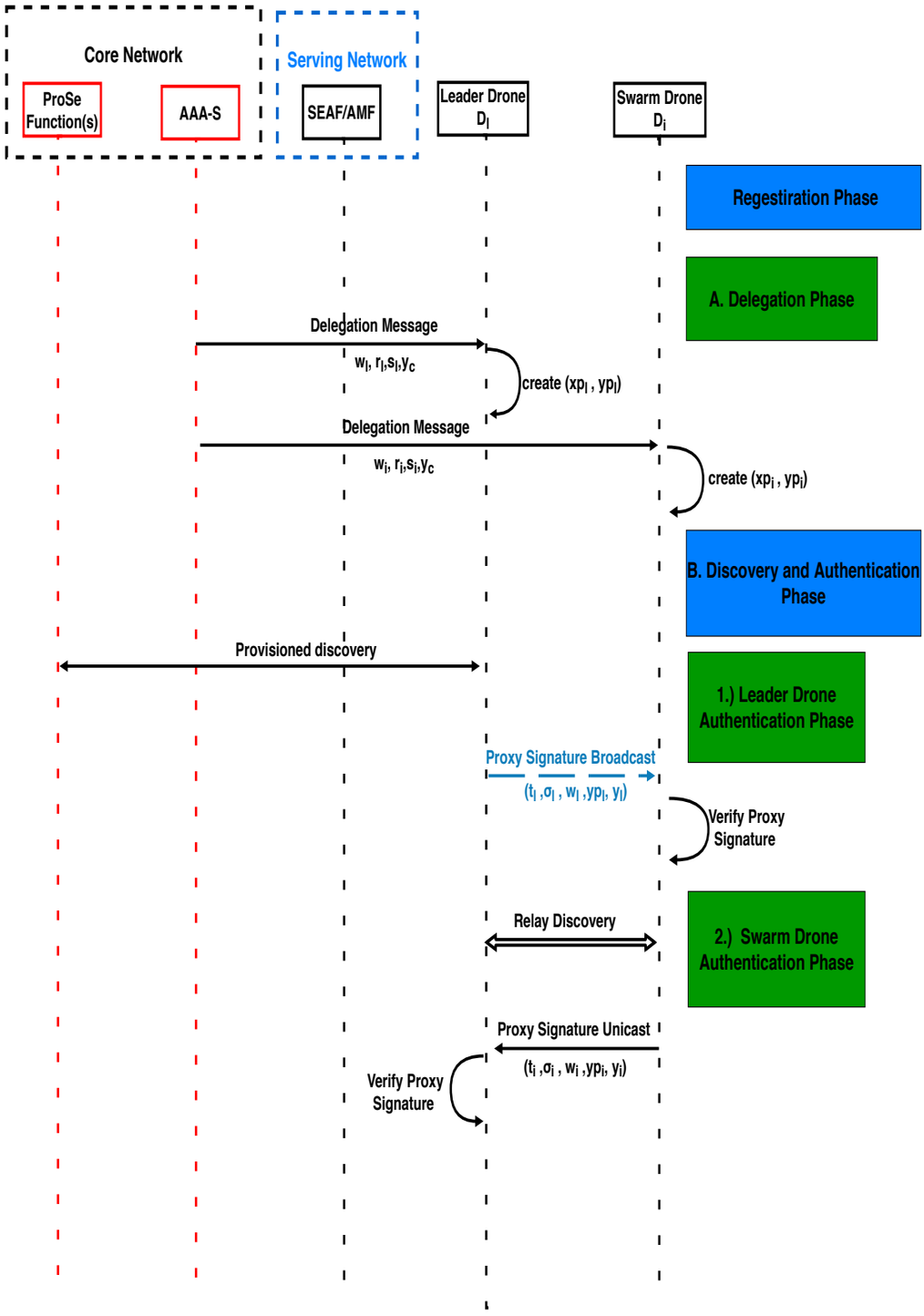


Fig. 8.3 Proxy Signature exchange messages within 5G Core and the involved drones.

as a seed for the proxy signature parameters. The details of this process are as follows:

- Let g be a generator of a multiplicative subgroup of Z_p^* with order p. Then a random number $k_i \in_R Z_p^*$ is selected from this set.
- The proxy signature parameters are generated as follows:

$$r_i = g^{k_i},$$
$$s_i = x_c h(w_i, r_i) + k_i, \tag{8.1}$$

where, $h()$ is a collision resistant hash function. In addition, as part of this proxy signature, the AAA-S creates a unique *warrant* w_i for each drone D_i, as follows:

$$w_i = \mathbf{S}(r_i, s_i), \tag{8.2}$$

where $\mathbf{S()}$ is any digital signature function. Note that this warrant is specific to drone D_i as it uses the (r_i, s_i).

- Then, the delegation parameters (i.e., the proxy parameters, the warrant, and the core network public key) are sent securely to the drone D_i as a tuple of (w_i, r_i, s_i, y_c). We use the K_{SEAF} key produced during the 5G primary authentication for this encrypted communication.
- The leader drone D_l that will act as a UE-to-Network relay receives a similar uniquely created tuple of (w_l, r_l, s_l, y_c).

8.3.3 Discovery and Device Authentication Phase

The next phase after the registration and delegation phases is the discovery phase, where the drones can search for the other available UE-to-Network relay drones for D2D connection. This phase is done through the ProSe standard in the cellular network. The second part of Fig. 8.3 shows the 5G ProSe D2D discovery process. The ProSe standard has two models of discovery: Model A and Model B. In Model A, the UE-network relay announces its presence, while in Model B, the UE/drone sends a discovery message to the nearest nodes. Our proposed authentication protocol would work for both models. In discovery messages for both models, each drone (leader or not) attaches the proxy signature. Anyone who replies will attach its proxy signature as well. We explain this protocol in two parts below:

Leader Drone Authentication

The leader drone message exchange for the proposed proxy signature authentication protocol is shown in Fig. 8.3 under the leader drone authentication phase.

- The leader drone D_l creates the proxy signature keys, (xp_l, yp_l), using the delegation parameters as follows:

$$\begin{aligned} xp_l &= s_l + h(w_l, r_l)x_l \\ yp_l &= (y_c y_l)^{h(w_l, r_l)} r_l \end{aligned} \tag{8.3}$$

- The leader drone then creates the following signature:

$$\sigma_l = \mathbf{S}(t_l, xp_l). \tag{8.4}$$

  where t_l is a timestamp nonce using its private key xp_l. Note that since xp_l is only known by D_l, the proxy signature can be only created by a legitimate D_l.

- The leader drone D_l broadcasts this proxy signature (blue doted message in Fig. 8.3) that contains the following tuple:

$$(t_l, \sigma_l, w_l, yp_l, y_l)$$

- Then, each drone D_i in the swarm receives the proxy signature and verifies the leader's proxy signature as follows:

$$\mathbf{V}(t_l, \sigma_l, (y_c y_l)^{h(w_l, y_l)} yp_i) \stackrel{?}{=} True, \tag{8.5}$$

  where $\mathbf{V()}$ is a digital signature verification algorithm.

Swarm Drones Proxy Signature-based Authentication

Next, in response to the leader's broadcast signature, the swarm drones send a reply to be authenticated to the leader drone. The swarm drones authentication to the leader drone is shown in Fig. 8.3 under the swarm drone authentication phase.

- Initially, each drone D_i creates the proxy signature keys, (xp_i, yp_i), using the delegation parameters as follows:

$$\begin{aligned} xp_i &= s_i + h(w_i, r_i)x_i, \\ yp_i &= (y_c y_i)^{h(w_i, r_i)} r_i. \end{aligned} \tag{8.6}$$

- Next, each drone prepares a signed nonce with its proxy private key, xp_i as follows:

$$\sigma_i = \mathbf{S}(t_i, xp_i). \tag{8.7}$$

- Next, after receiving the leaders broadcast message, the drone D_i then sends the proxy signature message that contains the following tuple: $(t_i, \sigma_i, w_i, yp_i, y_i)$ in its reply.
- Then, the leader drone D_l verifies this proxy signature, as follows:

$$\mathbf{V}(t_i, \sigma_i, (y_c y_i)^{h(w_i, y_i)} yp_i) \stackrel{?}{=} True, \tag{8.8}$$

  where **V()** is a digital signature verification algorithm.

Since both the leader drone and the drones in the swarm are already mutually authenticated, they can start message communication securely. The leader drone can create a symmetric key and send it to the other drones using its private key, to be used for message encryption, authentication, and integrity. We do not discuss these details as message authentication is beyond our scope.

8.3.4 Proxy key Revocation

Whenever asymmetric keys are used, there is a need for a key revocation mechanism if they are compromised. Revocation is the declaration for the existing proxy signature keys as obsolete (i.e., not valid anymore). We propose that the AAA-S in the core network can revoke y_p, which is the public proxy signature of a proxy drone B. Simultaneously as the leader drone verifying the proxy signature of B using its public proxy key y_p, it will also check whether this key is in a proxy revocation list. This revocation process is similar to the case of certificate revocation lists (CRLs) [MAM+99] in usual public-key systems.

8.4 Security Analysis

The security analysis, the proposed authentication model is qualified to sustain the following security issues,

1. *Authentication of source*: During the delegation phase, the drones are assigned with the network core (original signer) warrant and delegation parameter. Therefore, during the drone authentication stage, the verifier drone can verify the delegation source. Thus, the proposed scheme proves the authentication of the source.
2. *Identifiable*: The construction of the proposed authentication scheme is warrant and private key-based. Therefore, any drone can identify both the original signer and the proxy signer. Thus, identifiability is satisfied.

3. *Message Integrity*: The authentication message alteration can result in a rejected authentication in the verification stage in Eq. (8.8) and Eq. (8.5). A malicious drone D_m needs to send a proxy signature message that can be verified using the D_m's proxy public key. However, since the delegation phase is held securely before the drones' release to its location, D_m will fail to create its pair of the proxy keys since it does not have the unique delegation parameters. Hence, integrity is achieved.

4. *Prevention of misuse*: The scope of message is only comprised in the warrant, and therefore, the drone (proxy signer) can not sign an illegal document. Our proposed D2D drone authentication utilizes information distributed by the core network itself through delegation. Hence, to join the network, a legitimate drone D_i needs to show its valid and unique pair of proxy keys along with the warrant. The proxy keys are created based on the unique delegation parameters, r_i and s_i, given by the SEAF/AMF serving network to the drone D_i. Thus, the proposed scheme prevents the misuse of proxy signing.

5. *Strongness*: During the verification process, the verifier's secret key is needed. Thus, any entity other than the designated verifier (drone) is incapable of verifying the message signature pair's validity. Hence, the proposed scheme is strong enough against the resilience of various types of attacks.

6. *Modification attack*: The warrant comprises the message scope, and verification needs the secret key of the core network. Thus, during verification, message alteration will not be successful. Thus, the proposed scheme prevents modification attacks.

7. *Replay Attack*: The protocol is also resilient against any replay or integrity attacks. Any adversary D_m that tries to impersonate a legitimate drone in the swarm D_i by performing a *replay attack* where it replays a captured message from D_i either for joining the network or claiming to be the leader drone. In both cases, D_m broadcasts the whole proxy signature of drone D_i, $(t_i, \sigma_i, w_i, yp_i, y_i)$. Let us assume a verifier node receives this broadcast for the first time. This proxy signature will not pass the verification using Eq. (8.8) due to stale timestamp value in the message. Similarly, for replay attack of the leader drone broadcast message, the signature will not pass the verification at Eq.(8.5) in the same manner. Thus, a replay attack is not successful in the proposed scheme.

8. *Impersonation attack*: Due to the correctness of verification and that it is based on several parameters from both the signer drone (proxy signer) and the core network (original signer), the impersonation attack can not be successful.

9. MiTM attack: To prevent MiTM attack, authentication of source, identifiability, and unforgeability should be satisfied. Since the proposed authentication scheme satisfies all these attacks as aforementioned, therefore, an eavesdropper can not alter the message signature pair. Hence, the proposed scheme prevents the MiTM attack.

8.5 Performance Analysis

8.5.1 Experiment Setup

We simulated the proposed approach using the NS-3 5G network simulator, which has recently implemented 5G RAN module [WoP18]. We also utilized the D2D implementation in [Dio17] for a node to node communication between drones. We created 2 UE nodes representing the leader drone and one swarm drone, respectively. For our experiment, we added a server node representing the AAA-S for the proxy authentication computation. We selected Model A, where the leader announces itself first, then the others join. We also assume that the proxy signature parameters are pre-installed to the nodes. The system parameters for the NS-3 simulation used in the experiments are listed in Table 8.1. We further used a Raspberry-Pi3 IoT device to mimic the drone's behavior for complexity convenience and realistic assessment.

8.5.2 Metrics and Baselines

To assess the proposed authentication mechanism overhead, we consider the *total authentication time*, which includes all the communication and computation delays during the authentication process.

Moreover, as a baseline comparison to our proposed D2D authentication mechanism, we use the 4G ProSe D2D security as a centralized authentication model.

Table 8.1 Simulation Parameters

Parameter	Value
Packet size	56 Byte
Data rate	30 Mb/sec
gNodeB distance	300 m
drone to drone distance	150 m
K_{SEAF} size	256 bit
Proxy Signature Hash Function	SipHash [AB12]

8.5.3 Performance Results

Drone Computational Overhead

The drones computational delay experienced through the proxy signature authentication are listed in Table 8.2. As seen, the total processing delay for our proposed drone D2D authentication is 2.012 msec, which includes all the proxy signature parameters and keys calculations. These results indicate that the computational complexity is almost negligible.

Table 8.2 Computational Overhead

Operation	Delay (msec)
SipHash Function	0.13
Proxy Private Key Creation xp_i&xp_l	1.02
Proxy Public Key Creation yp_i& yp_l	0.992
Total	**2.012**

Communication Delay

The communication delays experienced between the drones are listed in Table 8.3. The total delay for the proposed proxy signature authentication communication delay is 6.35 msec. Hence, the total delay for the proposed authentication mechanism after adding the computation delay is 8.362 msec. In comparison, the ProSe mechanism with a total authentication time of 12.46 msec, while our proposed

authentication mechanism is almost 33% faster. The reason for this delay is due to the 4G-based ProSe connection to the core network.

Table 8.3 Communication Overhead

Approach	Connection	Delay(msec)
Proxy Signature	Discovery Phase	2.32
Proxy Signature	D2D Message Exchange	4.03
Proxy Signature	**Total Communication Delay**	**6.35**
4G-based ProSe	**Total Communication Delay**	**12.46**

Impact of Background Traffic Delay

We further investigate the impact of background traffic from other existing communication to the leader drone during the D2D drone authentication. We simulated an uplink and downlink background traffic over the leader drone simultaneously while starting the D2D proxy authentication. The traffic frequency at each background node is set to 1 msec intervals between packet transmissions. As shown in Table 8.4, the total authentication communication delay based on the background traffic up to 40 nodes is within 0.8 µsec. Hence, under background traffic, the additional delay is negligible, which means no extra delay overhead on the proposed authentication.

Table 8.4 Authentication Delay under varying Background Traffic

Background Nodes	Delay (msec)
1	6.350012
10	6.350064
20	6.350207
40	6.35089

CHAPTER 9

CONCLUSIONS AND FUTURE WORK

9.1 Conclusions

This dissertation utilized a swarm of drones to have a more connected, reliable, and secure communication over the next generation mmWave frequencies for a higher data rate transmission. We targeted next-generation communication in both the 5G cellular and Ad hoc IEEE 802.11ad/ay networks. We further considered a typical communication situations as well as post-disaster circumstances, where drones are temporarily positioned within an affected area to create a wireless mesh network among public safety personnel. We started with restoring and enhancing the network connectivity to avoid isolated node scenarios and reduce network congestion resulting from mmWave channel statistics. We incorporated positioning a swarm of UAVs to increase the network connectivity and address the mmWave short communication range. Jointly, we considered the UAVs' interference management to avoid power loss due to communication overlapping while taking into account UAVs' limited resources, such as transmission power. Once the network is well connected and ready for communication, we ensured network reliability by optimizing the drones' communication E2E delay through multipath routing, which increases the redundant data through different routes.

For guaranteeing the drones' security, we interpreted the security challenges over the ad hoc UAV network, assuming potential imposters. We proposed a fast, efficient, and lightweight distributed authentication mechanism for drones that took into account the physical limitations of mmWave communication. We adopted a delegation authentication mechanism, named proxy signature, to provide data security and user privacy while not increasing computational loads. We further considered a post-disaster recovery for destroyed communication infrastructure, where we relied on IEEE 802.11ad/ay ad hoc network. We further proposed a drone-to-drone proxy signature-based authentication mechanism delegated by the control center.

Toward a secure next-generation communication, we further proposed a more robust authentication mechanism inspired by the idea of second-factor authentication in IT systems. This second-factor authentication mechanism is dedicated to IoT devices over the 5G network, which kicks in once the primary 5G authentication is executed. The proposed trigger mechanism utilizes the re-authentication

procedure specified in the 3GPP 5G standards for easy integration. We proposed a reliable authentication mechanism compatible with the 5G D2D ProSe standard mechanisms for the communication within the drones' swarm. The proposed authentication is distributed-based authentication with a delegation-based scheme instead of the repeated access to the 5G core network KMF.

For results insights, the considered drone positioning optimization in Chapter 4 was related to an SDP problem and solved numerically with reasonable complexity on MATLAB CVX-SDP solver. The provided simulation results have shown that deploying one UAV can enhance the backhaul algebraic connectivity by 80%, compared to random positioning schemes. Higher performance was indicated for the multiple UAVs; for example, at $K = 4$ UAVs, 200% improvement gain in the backhaul connectivity was achieved, compared to the random positioning scheme. The indicated connectivity enhancements are achieved while guaranteeing the desired SINR for all the users over the mmWave access network.

In Chapter 5, we implemented the proposed multipath routing protocol and tested it on NS-3 by relying on the MATLAB's optimization output. The results demonstrated the feasibility and effectiveness of multipath routing to achieve better throughput while minimizing the E2E delay. Moreover, the results showed that the network connectivity enhanced by 66% after adding the UAVs. Furthermore, the E2E delay is reduced by 50% to 66% depending on the number of nodes.

The proposed authentication mechanism in Chapter 6 was also implemented and tested under NS-3 by utilizing mmWave channel from IEEE 802.11ad/ay standard and relying on a Raspberry Pi's computations. The results showed that our proposed authentication is fast, reliable, and, more importantly, scalable to more extensive ad hoc networks. The second-factor authentication approach in Chapter 7 was implemented in NS-3 using the 5G mmWave radio access. The evaluation of the approach indicated its efficiency and feasibility. We further implemented the drones' D2D authentication scheme in Chapter 8 using the NS-3 5G D2D communication. The evaluation of the authentication model indicated its efficiency and feasibility over the 4G Standard ProSe scheme.

9.2 Future Work

The work in this dissertation can be further investigated in the future in one or more of the following extensions,

- The positioning work in Chapter 4 can be extended in the future by
  - Considering in-band IAB scenarios, where both the access and backhaul networks operate on the same spectrum band. Formulating the backhaul connectivity maximization problem while considering the access network's interference impact will be more challenging than the considered problem formulation in this work.
  - Also, considering optimal power allocation of the UAVs instead of the equal power allocation policy is a further optimization aspect.
- The routing and positioning work in Chapter 5 can be extended as,
  - The proposed model can be implemented and tested on the IEEE 802.11*ay* mmWave communication protocol at 60 GHz, once it is officially available on NS-3, assuming an ad hoc network.
  - Models using intelligent schemes such as ML can bring new management intelligence to the optimization. ML algorithms allow the UAVs to gain more intelligence through the learning process to update their position and routing on-the-fly.
  - Moreover, Software-defined networking (SDN) can bring new centralized techniques to manage the networking system.
- The work in Chapter 6 can be investigated as follows,
  - An updating model can be considered based on UAVs' mobility. A model for relocating or replacing UAVs in the network, if necessary.
- The work in Chapter 7 can be implemented on a 5G core-based simulation platform, such as the Free5GC (free5gc.org). The 5G-based NS-3 platform is based on an LTE core network for its simulation.
- In Chapter 8, the D2D security is essential to notice that the 5G ProSe security extensions are still under development, which opens a wide area for research and contribution.

Furthermore, drone security challenges in the next-generation cellular networks are still open to provide on-fly lightweight schemes that will not bring additional burden to drones. This research point is highly demanding for publishing as it still has significantly open and parching for more enhancement.

[3GP20] 3GPP. TS 23.502-V16.7.0 - Procedures for the 5G System (5GS), 2020.

[AB12] Jean-Philippe Aumasson and Daniel J Bernstein. Siphash: a fast short-input prf. In *International Conference on Cryptology in India*, pages 489–508. Springer, 2012.

[ABA+15] N. F. Abdullah, D. Berraki, A. Ameen, S. Armour, A. Doufexi, A. Nix, and M. Beach. Channel parameters and throughput predictions for mmWave and LTE-A networks in urban environments. In *IEEE Vehicular Technology Conference (VTC Spring)*, pages 1–5, 2015.

[ACK+20] Tejasvi Alladi, Vinay Chamola, Neeraj Kumar, et al. Parth: A two-stage lightweight mutual authentication protocol for uav surveillance networks. *Computer Communications*, 160:81–90, 2020.

[ADM19] Adeel Abro, Zhongliang Deng, and Kamran Ali Memon. A lightweight elliptic-elgamal-based authentication scheme for secure device-to-device communication. *Future Internet*, 11(5):108, 2019.

[AEAH12] Salam Akoum, Omar El Ayach, and Robert W Heath. Coverage and capacity in mmwave cellular systems. In *2012 conference record of the forty sixth Asilomar conference on signals, systems and computers (ASILOMAR)*, pages 688–692. IEEE, 2012.

[AMIMA19] Mai A. Abdel-Malek, Ahmed S. Ibrahim, Mohamed Mokhtar, and Kemal Akkaya. UAV positioning for out-of-band integrated access and backhaul millimeter wave network. *Physical Communication*, 35:100721, 2019.

[ANBDF05] Chris Augeri, Danial Neebel, Leemon Baird, and Adrian De Freitas. UAV communications: Integrating a real-world scenario with computer architecture. In *Proceedings Frontiers in Education 35th Annual Conference*, pages F2H–F2H. IEEE, 2005.

[ARCP16] Mohammad M. Azari, Fernando Rosas, Kwang-Cheng Chen, and Sofie Pollin. Optimal UAV positioning for terrestrial-aerial communication in presence of fading. In *IEEE Global Communications Conference (GLOBECOM)*, pages 1–7, 2016.

[AW16] Hany Assasa and Joerg Widmer. Implementation and evaluation of a wlan IEEE 802.11 ad model in ns-3. In *ACM Proceedings of the Workshop on ns-3*, pages 57–64, 2016.

[BDH+18] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. A formal analysis of 5G authentication. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 1383–1396, New York, NY, USA, 2018. Association for Computing Machinery.

[BDRQL11] Eshar Ben-Dor, Theodore S Rappaport, Yijun Qiao, and Samuel J Lauffenburger. Millimeter-wave 60 GHz outdoor and vehicle AOA propagation measurements using a broadband channel sounder. In

IEEE Global Telecommunications Conference (GLOBECOM), pages 1–6, 2011.

[BFW15] Elaine Barker, Larry Feldman, and Gregory Witte. Recommendation for random number generation using deterministic random bit generators. Technical report, National Institute of Standards and Technology, 2015.

[BGH92] Dimitri P Bertsekas, Robert G Gallager, and Pierre Humblet. *Data Networks*, chapter 3, pages 187–188. Prentice Hall, 1992.

[BHH19] Jaeuk Baek, Sang Ik Han, and Youngnam Han. Energy-efficient UAV routing for wireless sensor networks. *IEEE Transactions on Vehicular Technology*, 69(2):1741–1750, 2019.

[Bis00] Richard Bishop. A survey of intelligent vehicle applications worldwide. In *Proceedings of the IEEE Intelligent Vehicles Symposium (Cat. No.00TH8511)*, pages 25–30, 2000.

[BSD+20] Basudeb Bera, Sourav Saha, Ashok Kumar Das, Neeraj Kumar, Pascal Lorenz, and Mamoun Alazab. Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled internet of drones environment. *IEEE Transactions on Vehicular Technology*, 69(8):9097–9111, 2020.

[BTM+06] B Braunstein, T Trimble, R Mishra, BS Manoj, L Lenert, and R Rao. Challenges in using distributed wireless mesh networks in emergency response. In *Proceedings of the 3rd International ISCRAM Conference*, pages 30–38, 2006.

[BV04] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge university press, 2004.

[BWB+11] Andreas Birk, Burkhard Wiggerich, Heiko Bülow, Max Pfingsthorn, and Sören Schwertfeger. Safety, security, and rescue missions with an unmanned aerial vehicle (UAV). *Journal of Intelligent & Robotic Systems*, 64(1):57–76, 2011.

[BZ16] O. Bello and S. Zeadally. Intelligent device-to-device communication in the internet of things. *IEEE Systems Journal*, 10(3):1172–1182, 2016.

[CCC+17] Bruno N Coelho, Vitor N Coelho, Igor M Coelho, Luiz S Ochi, Roozbeh Haghnazar, Demetrius Zuidema, Milton SF Lima, and Adilson R da Costa. A multi-objective green UAV routing problem. *Computers & Operations Research*, 88:306–315, 2017.

[CDS98] Johnny Chen, Peter Druschel, and Devika Subramanian. An efficient multipath forwarding method. In *Proceedings of IEEE INFOCOM'98, the Conference on Computer Communications. Seventeenth Annual Joint Conference of the IEEE Computer and Communications Societies. Gateway to the 21st Century*, volume 3, pages 1418–1425. IEEE, 1998.

[CP08] Chris Constantinides and Paul Parkinson. Security challenges in UAV development. In *2008 IEEE/AIAA 27th Digital Avionics Systems Conference*, pages 1–C. IEEE, 2008.

[CRS99] Israel Cidon, Raphael Rom, and Yuval Shavitt. Analysis of multi-path routing. *IEEE/ACM Transactions On Networking*, 7(6):885–896, 1999.

[DCN07] Jingbo Dong, Qing Chen, and Zhisheng Niu. Random graph theory based connectivity analysis in wireless sensor networks with rayleigh fading channels. In *Asia-Pacific Conference on Communications*, pages 123–126, 2007.

[DCNR09] Jing Dong, Reza Curtmola, and Cristina Nita-Rotaru. Secure network coding for wireless mesh networks: Threats, challenges, and directions. *Computer Communications*, 32(17):1790–1801, 2009.

[DGH14] Bob Cutler David Grieve and John Harmon. Understanding IEEE802.11ad physical layer and measurement challenges. Technical report, keysight, 2014.

[Dio17] Makhtar Diouf. mmWave cellular network simulator. `https://github.com/makhtardiouf/d2d`, 2017.

[DP11] Robert A DiFazio and Philip J Pietraski. The bandwidth crunch: Can wireless technology meet the skyrocketing demand for mobile data? In *2011 IEEE Long Island Systems, Applications and Technology Conference*, pages 1–6. IEEE, 2011.

[DR00] Bruce S Davie and Yakov Rekhter. *MPLS: technology and applications*. Morgan Kaufmann Publishers Inc., 2000.

[DSP06] Manik Lal Das, Ashutosh Saxena, and Deepak B Phatak. Algorithms and approaches of proxy signature: A survey. *arXiv preprint cs/0612098*, 2006.

[DW11] Kai Daniel and Christian Wietfeld. Using public network infrastructures for UAV remote sensing in civilian security operations. Technical report, DORTMUND UNIV (GERMANY FR), 2011.

[DW15] Xiaoyu Duan and Xianbin Wang. Authentication handover and privacy protection in 5G hetnets using software-defined networking. *IEEE Communications Magazine*, 53(4):28–35, 2015.

[DYLS15] Zhang Dejin, N. Yang, Wu Liaoni, and Zhou Shenglu. A kind of moving net recovery technology for unmanned aerial vehicle. In *International Conference on Information and Communications Technologies (ICT)*, pages 1–5, 2015.

[Fed20] Federal Aviation Administration. UAS remote identification. `https://www.faa.gov/uas/research_development/remote_id/`, 2020.

[FEPS15a] E Frazzoli, J Enright, M Pavone, and K Savla. UAV routing and coordination in stochastic, dynamic environments, 2015.

[FEPS15b] E Frazzoli, J Enright, M Pavone, and K Savla. UAV routing and coordination in stochastic, dynamic environments, 2015.

[FFK+00] K Fujisawa, Yoshiaki Futakata, M Kojima, Satoshi Matsuyama, S Nakamura, K Nakata, and M Yamashita. SDPA-M (semidefinite programming algorithm in MATLAB) user's manual—version

6.2. 0. *Research Reports on Mathematical and Computing Sciences, Series B: Operation Res., Dep. Math. and Computing Sci., Tokyo Institute of Technol., Japan*, 10, 2000.

[Fie73] Miroslav Fiedler. Algebraic connectivity of graphs. *Czechoslovak mathematical journal*, 23(2):298–305, 1973.

[GB06] Arpita Ghosh and Stephen Boyd. Growing well-connected graphs. In *Proceedings of the 45th IEEE Conference on Decision and Control*, pages 6605–6611. IEEE, 2006.

[GBY08] Michael Grant, Stephen Boyd, and Yinyu Ye. Cvx: Matlab software for disciplined convex programming, 2008.

[GKZV08] Suiyan Geng, Jarmo Kivinen, Xiongwen Zhao, and Pertti Vainikainen. Millimeter-wave propagation channel characterization for short-range wireless communications. *IEEE transactions on vehicular technology*, 58(1):3–13, 2008.

[GP15] Stephen GergoVemi and Christo Panchev. Vulnerability testing of wireless access points using unmanned aerial vehicles (UAV). In *ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015*, page 425. Academic Conferences Limited, 2015.

[GY04] Jonathan L Gross and Jay Yellen. Handbook of graph theory crc press. *Boca Raton*, 2004.

[HF08] Xiaoxia Huang and Yuguang Fang. Performance study of node-disjoint multipath routing in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 58(4):1942–1950, 2008.

[HMMW19] Lei He, Jianfeng Ma, Ruo Mo, and Dawei Wei. Designated verifier proxy blind signature scheme for unmanned aerial vehicle network based on mobile edge computing. *Security and Communication Networks*, 2019, 2019.

[HR08] Jiayue He and Jennifer Rexford. Toward internet-wide multipath routing. *IEEE network*, 22(2):16–21, 2008.

[HSSM05] Yiwei T. Hou, Yi Shi, Hanif D. Sherali, and Scott F. Midkiff. Prolonging sensor network lifetime with energy provisioning and relay node placement. In *IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON)*, volume 5, pages 295–304, 2005.

[HTZ+16] Michael Hooper, Yifan Tian, Runxuan Zhou, Bin Cao, Adrian P. Lauf, Lanier Watkins, William H. Robinson, and Wlajimir Alexis. Securing commercial wifi-based uavs from common security attacks. In *MILCOM 2016-2016 IEEE Military Communications Conference*, pages 1213–1218. IEEE, 2016.

[HWD+17] Michael Haus, Muhammad Waqas, Aaron Yi Ding, Yong Li, Sasu Tarkoma, and Jörg Ott. Security and privacy in device-to-device (d2d) communication: A review. *IEEE Communications Surveys & Tutorials*, 19(2):1054–1079, 2017.

[Ins19] Informed Inside. A comparative introduction to 4G and 5G authentication., WINTER 2019.

[ISL09a] A. S. Ibrahim, K. G. Seddik, and K. J. R. Liu. Connectivity-aware network maintenance and repair via relays deployment. *IEEE Transactions on Wireless Communications*, 8(1):356–366, 2009.

[ISL09b] Ahmed S. Ibrahim, Karim G. Seddik, and KJ Ray Liu. Connectivity-aware network maintenance and repair via relays deployment. *IEEE Transactions on Wireless Communications*, 8(1):356–366, 2009.

[JM96] David B. Johnson and David A. Maltz. Dynamic source routing in ad hoc wireless networks. In *Mobile computing*, pages 153–181. Springer, 1996.

[JM19] Roger Piqueras Jover and Vuk Marojevic. Security and protocol exploit analysis of the 5G specifications. *IEEE Access*, 7:24956–24963, 2019.

[JMB+01] David B. Johnson, David A. Maltz, Josh Broch, et al. DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks. *Ad hoc networking*, 5:139–172, 2001.

[JS96] Gautam Jain and Karl Sigman. A Pollaczek–Khintchine formula for M/G/1 queues with disasters. *Journal of Applied Probability*, 33(4):1191–1200, 1996.

[KAL+19] Mehdi Karimibiuki, Michal Aibin, Yuyu Lai, Raziq Khan, Ryan Norfield, and Aaron Hunter. Drones' face off: Authentication by machine learning in autonomous IoT systems. In *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 0329–0333. IEEE, 2019.

[KF07] S Kelly and S Frankel. Using hmac-sha-256, hmac-sha-384, and hmac-sha-512 with ipsec. Technical report, RFC 4868, 2007.

[KGTK20] Aparna Kumari, Rajesh Gupta, Sudeep Tanwar, and Neeraj Kumar. A taxonomy of blockchain-enabled softwarization for secure uav network. *Computer Communications*, 161:304–323, 2020.

[KHK+14] Hyunsoo Kwon, Changhee Hahn, Daeyoung Kim, Kyungtae Kang, and Junbeom Hur. Secure device-to-device authentication in mobile multi-hop networks. In *International Conference on Wireless Algorithms, Systems, and Applications*, pages 267–278. Springer, 2014.

[Kin62] John FC Kingman. On queues in heavy traffic. *Journal of the Royal Statistical Society: Series B (Methodological)*, 24(2):383–392, 1962.

[KLX+02] Jiejun Kong, Haiyun Luo, Kaixin Xu, Daniel Lihui Gu, Mario Gerla, and Songwu Lu. Adaptive security for multilevel ad hoc networks. *Wireless Communications and Mobile Computing*, 2(5):533–547, 2002.

[KO18] Amit Kumar and Hari Om. Handover authentication scheme for device-to-device outband communication in 5g-wlan next generation heterogeneous networks. *Arabian Journal for Science and Engineering*, 43(12):7961–7977, 2018.

[KOG17] Wahab Khawaja, Ozgur Ozdemir, and Ismail Guvenc. UAV air-to-ground channel characterization for mmWave systems. In *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, pages 1–5, 2017.

[Kou19] Adrien Koutsos. The 5G-AKA authentication protocol privacy. In *IEEE European Symposium on Security and Privacy (EuroS P)*, pages 464–479. IEEE, 2019.

[KR10] James F. Kurose and Keith W. Ross. *Computer networking: a top-down approach*. Addison-Wesley Reading, 2010.

[KRW03] Jirka Klaue, Berthold Rathke, and Adam Wolisz. valVid – a framework for video transmission and quality evaluation. In *Computer Performance Evaluation. Modelling Techniques and Tools*, pages 255–272. Springer Berlin Heidelberg, 2003.

[KSYY17] Elham Kalantari, Muhammad Zeeshan Shakir, Halim Yanikomeroglu, and Abbas Yongacoglu. Backhaul-aware robust 3d drone placement in 5G+ wireless networks. In *IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 109–114, 2017.

[KYW+17] Linghe Kong, Linsheng Ye, Fan Wu, Meixia Tao, Guihai Chen, and Athanasios V Vasilakos. Autonomous relay for millimeter-wave wireless communications. *IEEE Journal on Selected Areas in Communications*, 35(9):2127–2136, 2017.

[LC04a] Xuefei Li and Laurie Cuthbert. On-demand node-disjoint multipath routing in wireless ad hoc networks. In *29th Annual IEEE International Conference on Local Computer Networks*, pages 419–420, 2004.

[LC04b] Xuefei Li and Laurie Cuthbert. Stable node-disjoint multipath routing with low overhead in mobile ad hoc networks. In *The IEEE Computer Society's 12th Annual International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (MASCOTS). Proceedings.*, pages 184–191, 2004.

[LG01] S-J Lee and Mario Gerla. Split multipath routing with maximally disjoint paths in ad hoc networks. In *IEEE International Conference on Communications (ICC)*, volume 10, pages 3201–3205 vol.10, 2001.

[LKC+16] Gino J Lim, Seonjin Kim, Jaeyoung Cho, Yibin Gong, and Amin Khodaei. Multi-UAV pre-positioning and routing for power network damage assessment. *IEEE Transactions on Smart Grid*, 9(4):3643–3651, 2016.

[LKK01] Byoungcheon Lee, Heesun Kim, and Kwangjo Kim. Strong proxy signature and its applications. In *Proceedings of SCIS*, volume 2001, pages 603–608, 2001.

[LMK+18] Mir M Lodro, Nahdia Majeed, Aziz A Khuwaja, Ali Hassan Sodhro, and Steve Greedy. Statistical channel modelling of 5G mmWave MIMO wireless communication. In *2018 International*

Conference on Computing, Mathematics and Engineering Technologies (iCoMET), pages 1–5. IEEE, 2018.

[LMYT18] Weiwei Liu, Yi Mu, Guomin Yang, and Yangguang Tian. Strong identity-based proxy signature schemes, revisited. *Wireless Communications and Mobile Computing*, 2018, 2018.

[LSC+17] Xin Li, Mohammed Samaka, H Anthony Chan, Deval Bhamare, Lav Gupta, Chengcheng Guo, and Raj Jain. Network slicing for 5G: Challenges and opportunities. *IEEE Internet Computing*, 21(5):20–27, 2017.

[LY05] Wei-Bin Lee and Chang-Kuo Yeh. A new delegation-based authentication protocol for use in portable communication systems. *IEEE Transactions on Wireless Communications*, 4(1):57–64, 2005.

[LYK18] H. Liu, S. Yoo, and K. S. Kwak. Opportunistic relaying for low-altitude UAV swarm secure communications with multiple eavesdroppers. *Journal of Communications and Networks*, 20(5):496–508, 2018.

[LZLS12] L. Lei, Z. Zhong, C. Lin, and X. Shen. Operator controlled device-to-device communications in lte-advanced networks. *IEEE Wireless Communications*, 19(3):96–104, 2012.

[MAM+99] Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams. X. 509 internet public key infrastructure online certificate status protocol-ocsp. Technical report, RFC 2560, 1999.

[MCV17] Davide Magrin, Marco Centenaro, and Lorenzo Vangelista. Performance evaluation of lora networks in a smart city scenario. In *2017 IEEE International Conference on communications (ICC)*, pages 1–7. ieee, 2017.

[MD01] Mahesh K Marina and Samir R Das. On-demand multipath distance vector routing in ad hoc networks. In *Proceedings Ninth International Conference on Network Protocols (ICNP)*, pages 14–23. IEEE, 2001.

[MD06] Mahesh K Marina and Samir R Das. Ad hoc on-demand multipath distance vector routing. *Wireless communications and mobile computing*, 6(7):969–988, 2006.

[MSBD15] Mohammad Mozaffari, Walid Saad, Mehdi Bennis, and Merouane Debbah. Drone small cells in the clouds: Design, deployment and performance analysis. In *2015 IEEE global communications conference (GLOBECOM)*, pages 1–6. IEEE, 2015.

[MSBD16] Mohammad Mozaffari, Walid Saad, Mehdi Bennis, and Mérouane Debbah. Unmanned aerial vehicle with underlaid device-to-device communications: Performance and tradeoffs. *IEEE Transactions on Wireless Communications*, 15(6):3949–3963, 2016.

[MV17] Silvia Mignardi and Roberto Verdone. On the performance improvement of a cellular network supported by an unmanned aerial base station. In *2017 29th International Teletraffic Congress (ITC 29)*, volume 2, pages 7–12. IEEE, 2017.

[NA14] S Nirmala and CM Ananda. Communication methodology in formation of flying of micro air vehicles. In *The 3rd International Conference on Recent Advances in Design, Development and Operation of Micro Air Vehicle*, pages 63–67, 2014.

[NCF+14] T. Nitsche, C. Cordeiro, A. B. Flores, E. W. Knightly, E. Perahia, and J. C. Widmer. IEEE 802.11ad: directional 60 GHz communication for multi-gigabit-per-second wi-fi [invited paper]. *IEEE Communications Magazine*, 52(12):132–141, 2014.

[ND99] Asis Nasipuri and Samir R Das. On-demand multipath routing for mobile ad hoc networks. In *Proceedings Eight International Conference on Computer Communications and Networks (Cat. No. 99EX370)*, pages 64–70. IEEE, 1999.

[NL09] Tahir Naeem and Kok-Keong Loo. Common security issues and challenges in wireless sensor networks and IEEE 802.11 wireless mesh networks. *3; 1*, 2009.

[NLS18] Jianbing Ni, Xiaodong Lin, and Xuemin Sherman Shen. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. *IEEE Journal on Selected Areas in Communications*, 36(3):644–657, 2018.

[NNS+07] N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D. P. Agrawal. Wireless mesh networks: Current challenges and future directions of web-in-the-sky. *IEEE Wireless Communications*, 14(4):79–89, 2007.

[NSN16] NSNAM. ns-3: network simulator 3. Release 3.24.1, 2016.

[Off20a] 3GPP Support Office. 3rd generation partnership project; technical specification group services and system aspects; proximity-based services (ProSe); security aspects. Technical report, 3GPP TS 33.303 V16.0.0 Technical Specification (Release 16), 2020.

[Off20b] 3GPP Support Office. 3rd generation partnership project; technical specification group services and system aspects; study on system enhancement for proximity based services (ProSe) in the 5G system (5GS). Technical report, 3GPP TR 23.752 V0.3.0 Technical Specification (Release 16), 2020.

[PJSL17] So-Yeon Park, Dahee Jeong, Christina Suyong Shin, and HyungJune Lee. DroneNet+: adaptive route recovery using path stitching of UAVs in Ad-Hoc networks. In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pages 1–7. IEEE, 2017.

[PJZ17] Michele Polese, Rittwik Jana, and Michele Zorzi. TCP and MP-TCP in 5G mmWave networks. *IEEE Internet Computing*, 21(5):12–19, 2017.

[RDBL12] Marjan Radi, Behnam Dezfouli, Kamalrulnizam Abu Bakar, and Malrey Lee. Multipath routing in wireless sensor networks: survey and research challenges. *Sensors*, 12(1):650–685, 2012.

[RIG16] N. Rupasinghe, A. S. Ibrahim, and I. Guvenc. Optimum hovering locations with angular domain user separation for cooperative UAV

networks. In *IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, 2016.

[RK08] H. Redwan and K. Kim. Survey of security requirements, attacks and network integration in wireless mesh networks. In *2008 New Technologies, Mobility and Security*, pages 1–5, 2008.

[RR06] David Recordon and Drummond Reed. Openid 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management*, pages 11–16, 2006.

[RS06] Sivakumar Rathinam and Raja Sengupta. Lower and upper bounds for a multiple depot UAV routing problem. In *Proceedings of the 45th IEEE Conference on Decision and Control*, pages 5287–5292. IEEE, 2006.

[RSM+13] Theodore S Rappaport, Shu Sun, Rimma Mayzus, Hang Zhao, Yaniv Azar, Kevin Wang, George N Wong, Jocelyn K Schulz, Mathew Samimi, and Felix Gutierrez. Millimeter wave mobile communications for 5G cellular: It will work! *IEEE access*, 1:335–349, 2013.

[RSP+14] Wonil Roh, Ji-Yun Seol, Jeongho Park, Byunghwan Lee, Jaekon Lee, Yungsoo Kim, Jaeweon Cho, Kyungwhoon Cheun, and Farshid Aryanfar. Millimeter-wave beamforming as an enabling technology for 5G cellular communications: theoretical feasibility and prototype results. *IEEE communications magazine*, 52(2):106–113, 2014.

[RW12] Sebastian Rohde and Christian Wietfeld. Interference aware positioning of aerial relays for cell overload and outage compensation. In *IEEE vehicular technology conference (VTC Fall)*, pages 1–5. IEEE, 2012.

[RXE+18] Sohail Razzaq, Costas Xydeas, Michael E Everett, Anzar Mahmood, and Thamer Alquthami. Three-dimensional UAV routing with deconfliction. *IEEE Access*, 6:21536–21551, 2018.

[SBSW17] D. Schürmann, A. Brüsch, S. Sigg, and L. Wolf. BANDANA — body area network device-to-device authentication using natural gAit. In *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 190–196, 2017.

[SGBW16] M. Sbeiti, N. Goddemeier, D. Behnke, and C. Wietfeld. Paser: Secure and efficient routing approach for airborne mesh networks. *IEEE Transactions on Wireless Communications*, 15(3):1950–1964, 2016.

[SH15] Peter Schneider and Günther Horn. Towards 5G security. In *IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 1165–1170. IEEE, 2015.

[Sic05] Mihail L Sichitiu. Wireless mesh networks: opportunities and challenges. In *Proceedings of World Wireless Congress*, volume 2, page 21. Citeseer, 2005.

[SK18] Sooyeon Shin and Taekyoung Kwon. Two-factor authenticated key agreement supporting unlinkability in 5G-integrated wireless sensor networks. *IEEE Access*, 6:11229–11241, 2018.

[Sli13] Brian Slininger. Fiedlers theory of spectral graph partitioning, 2013.

[SMR17] Shu Sun, George R. MacCartney, and Theodore S. Rappaport. A novel millimeter-wave channel simulator and applications for 5G wireless communications. In *IEEE International Conference on Communications (ICC)*, pages 1–7. IEEE, 2017.

[TAG03] Cihan Tepedelenlioglu, Ali Abdi, and Georgios B Giannakis. The Ricean K factor: estimation and performance analysis. *IEEE Transactions on Wireless Communications*, 2(4):799–810, 2003.

[TH16] Andrew Thornburg and Robert W Heath. Capacity and coverage in clustered LOS mmWave ad hoc networks. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2016.

[TJP+19] Li Teng, Ma Jianfeng, Feng Pengbin, Meng Yue, Ma Xindi, Zhang Jiawei, Chenyang Gao, and Lu Di. Lightweight security authentication mechanism towards UAV networks. In *2019 International Conference on Networking and Network Applications (NaNA)*, pages 379–384. IEEE, 2019.

[VHSV11] Anthony Van Herrewege, Dave Singelee, and Ingrid Verbauwhede. Canauth-a simple, backward compatible broadcast authentication protocol for can bus. In *ECRYPT Workshop on Lightweight Cryptography*, volume 2011, page 20, 2011.

[VSKH19] Girraj Kumar Verma, BB Singh, Neeraj Kumar, and Debiao He. Cb-ps: An efficient short-certificate-based proxy signature scheme for uavs. *IEEE Systems Journal*, 2019.

[WCMF17] Qian Wang, Zhi Chen, Weidong Mei, and Jun Fang. Improving physical layer security using UAV-enabled mobile relaying. *IEEE Wireless Communications Letters*, 6(3):310–313, 2017.

[WDK+19] Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Athanasios V Vasilakos, and Joel JPC Rodrigues. Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment. *IEEE Internet of Things Journal*, 6(2):3572–3584, 2019.

[WEDH14] Lifeng Wang, Maged Elkashlan, Trung Q Duong, and Robert W Heath. Secure communication in cellular networks: The benefits of millimeter wave mobile broadband. In *2014 IEEE 15th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pages 115–119. IEEE, 2014.

[WGA+15] Cheng-Xiang Wang, Ammar Ghazal, Bo Ai, Yu Liu, and Pingzhi Fan. Channel measurements and models for high-speed train communication systems: A survey. *IEEE communications surveys & tutorials*, 18(2):974–987, 2015.

[WHQW14] Lili Wei, Rose Qingyang Hu, Yi Qian, and Geng Wu. Key elements to enable millimeter wave communications for 5G wireless systems. *IEEE Wireless Communications*, 21(6):136–143, 2014.

[WM14] Kevin Werbach and Aalok Mehta. The spectrum opportunity: Sharing as the solution to the wireless crunch. *International Journal of Communication*, 8:22, 2014.

[WoP18] NYU Wireless and The University of Padova. mmWave cellular network simulator. `https://apps.nsnam.org/app/mmwave/`, 2018.

[WS11] Albert Wasef and Xuemin Shen. Emap: Expedite message authentication protocol for vehicular ad hoc networks. *IEEE transactions on Mobile Computing*, 12(1):78–89, 2011.

[WWS+17] Xianyue Wu, Cheng-Xiang Wang, Jian Sun, Jie Huang, Rui Feng, Yang Yang, and Xiaohu Ge. 60-GHz millimeter-wave channel measurements and modeling for indoor office environments. *IEEE Transactions on Antennas and Propagation*, 65(4):1912–1924, 2017.

[WY17] Shibin Wang and Nianmin Yao. Liap: A local identity-based anonymous message authentication protocol in vanets. *Computer Communications*, 112:154–164, 2017.

[WZSD00] Lei Wang, Lianfang Zhang, Yantai Shu, and Miao Dong. Multipath source routing in wireless ad hoc networks. In *2000 Canadian Conference on Electrical and Computer Engineering. Conference Proceedings. Navigating to a New Era (Cat. No. 00TH8492)*, volume 1, pages 479–483. IEEE, 2000.

[XHBN00] Xipeng Xiao, A. Hannan, B. Bailey, and L. M. Ni. Traffic engineering with MPLS in the internet. *IEEE Network*, 14(2):28–33, 2000.

[XXX16a] Zhenyu Xiao, Pengfei Xia, and Xiang-Gen Xia. Enabling UAV cellular with millimeter-wave communication: Potentials and approaches. *IEEE Communications Magazine*, 54(5):66–73, 2016.

[XXX16b] Zhenyu Xiao, Pengfei Xia, and Xiang-Gen Xia. Enabling UAV cellular with millimeter-wave communication: potentials and approaches. *IEEE Communications Magazine*, 54(5):66–73, 2016.

[Yan12] Evşen Yanmaz. Connectivity versus area coverage in unmanned aerial vehicle networks. In *2012 IEEE International Conference on Communications (ICC)*, pages 719–723. IEEE, 2012.

[YE11] Melda Yuksel and Elza Erkip. Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel. *IEEE Transactions on Wireless Communications*, 10(3):762–771, 2011.

[YLL+18] Guang Yang, Xingqin Lin, Yan Li, Hang Cui, Min Xu, Dan Wu, Henrik Rydén, and Sakib Bin Redhwan. A telecom perspective on the internet of drones: From lte-advanced to 5G. *arXiv preprint arXiv:1803.11048*, 2018.

[YMM13] Bidi Ying, Dimitrios Makrakis, and Hussein T Mouftah. Privacy preserving broadcast message authentication protocol for VANETs. *Journal of Network and Computer Applications*, 36(5):1352–1364, 2013.

[ZK03] Fangguo Zhang and Kwangjo Kim. Efficient id-based blind signature and proxy signature from bilinear pairings. In *Australasian Conference on Information Security and Privacy*, pages 312–323. Springer, 2003.

[ZYYY10] Zhang Zhixian, Wang Yajun, Yao Yuan, and Wang Yuzhou. Implementation of uavs communication network based on dynamic tdma mac protocol. In *The 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)*, volume 6, pages V6–551. IEEE, 2010.

VITA

MAI A. ABDELMALEK

2013 B.S., Electrical Engineering
Faculty of Engineering
Alexandria University
Alexandria, Egypt

2015 M.Sc., Wireless Technology
Wireless Intelligent Networks Center (WINC)
Nile University (NU)
Giza, Egypt

2021 Ph.D., Electrical and Computer Engineering
Florida International University (FIU)
Miami, Florida

PUBLICATIONS AND PRESENTATIONS

- Mai A. Abdel-Malek, Kemal Akkaya, Arupjyoti Bhuyan, and Ahmed S. Ibrahim, "Proxy Signature-Based Swarm-of-Drone Authentication Schemes in 5G D2D Networks" under preparation, IEEE Internet of Thing (IoT) journal, 2021.
- Mai A. Abdelmalek, Nico Sapurto, Ahmed Ibrahim and Kemal Akkaya, "UAV-assisted Multi-path Routing for MmWave-based Wireless Networks", Elsevier Internet of Thing (IoT) journal, 2021.
- Mai A. Abdel-Malek, Kemal Akkaya, Arupjyoti Bhuyan, and Ahmed S. Ibrahim, "A Proxy Signature-Based Drone Authentication in 5G D2D Networks", IEEE Vehicular Technology Conference: VTC2021-Spring, 2020.
- Mai A. Abdel-Malek, Kemal Akkaya, Arupjyoti Bhuyan, Mumin Cebe and Ahmed S. Ibrahim, "Enabling Second Factor Authentication for Drones in 5G using Network Slicing", IEEE Global Communications Workshop, 2020.
- Mai Abdelmalek, Nico Sapurto, Ahmed Ibrahim and Kemal Akkaya "Efficient Authentication of Drones to mmWave Wireless Mesh Networks in Post-Disaster Scenarios",IEEE Global Communications Conference, 2020.
- Mai A. Abdel-Malek, A. S. Ibrahim, M. Mokhtar, and K. Akkaya, "UAV positioning for out-of-band integrated access and backhaul millimeter wave network", Physical Communication, vol. 35, p. 100721, Aug. 2019, doi: 10.1016/j.phycom.2019.100721.
- Mai A. Abdel-Malek, K. G. Seddik, T. ElBatt, and Y. Mohasseb, "Effective capacity optimization for cognitive radio networks under primary QoS provisioning", Wireless Networks, vol. 26, no. 3, pp. 2171–2190, Jun. 2019, doi: 10.1007/s11276-019-02002-w.
- Mai A. Abdel-Malek, Nico Sapurto, Ahmed S. Ibrahim, and Kemal Akkaya, "UAV-assisted authentication for Millimeter Wave Wireless Mesh Networks", The first Warren B. Nelms Annual IoT Conference, Dec 2019.
- Mai A. Abdelmalek, Nico Saputro, Kemal Akkaya and Ahmed Ibrahim,"UAV-assisted Secure Routing for Millimeter Wave Wireless Mesh Networks", The Third Workshop for Women in Hardware and Systems Security (WISE), May 9, 2019.
- Mai A. Abdel-Malek, Ahmed S. Ibrahim, Mohamed Mokhtar, and Kemal Akkaya, "UAV Positioning for Out-of-Band Integrated Access and Backhaul Millimeter Wave Network", FIU Graduate Student Appreciation Week GSAW, April 2019.

- Mai A. Abdel-Malek, Ahmed S. Ibrahim, Mohamed Mokhtar, and K. Akkaya, “Uav positioning for outof-band integrated access and backhaul millimeter wave network”, in the Fourth NSF millimeter-wave Workshop, Jul. 2018.
- Mai A. Abdel-Malek, Ahmed S. Ibrahim, and Mohamed Mokhtar. “UAV Positioning for Improving Coverage-Connectivity Tradeoff in Millimeter-Wave Wireless Channel”, The second NSF millimeter-wave Workshop, 2017.
- Mai A. Abdel-Malek, Ahmed S. Ibrahim, and Mohamed Mokhtar. "Optimum UAV positioning for better coverage-connectivity tradeoff." In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1-5. IEEE, 2017.
- Mai Abdel-Malek, Karim Seddik, Tamer ElBatt, and Yahya Mohas seb. "Effective capacity and delay optimization in cognitive radio networks." In International Conference on Cognitive Radio Oriented Wireless Networks, pp. 30-42. Springer, Cham, 2015.