ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

GROUP AUTHENTICATION FOR NEXT GENERATION NETWORKS

Ph.D. THESIS

Yücel AYDIN

Department of Applied Informatics

Cybersecurity Engineering and Cryptography Programme

MAY 2022

ISTANBUL TECHNICAL UNIVERSITY ★ GRADUATE SCHOOL

GROUP AUTHENTICATION FOR NEXT GENERATION NETWORKS

Ph.D. THESIS

Yücel AYDIN
(707172003)

Department of Applied Informatics

Cybersecurity Engineering and Cryptography Programme

Thesis Advisor: Assoc. Prof. Dr. Enver ÖZDEMİR
Thesis Co-Advisor: Prof. Dr. Güneş KARABULUT KURT

MAY 2022

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

GELECEK NESİL AĞLARDA GRUP KİMLİK DOĞRULAMASI

DOKTORA TEZİ

Yücel AYDIN
(707172003)

Bilişim Uygulamaları Anabilim Dalı

Bilgi Güvenliği Mühendisliği ve Kriptografi Programı

Tez Danışmanı: Doç. Dr. Enver ÖZDEMİR
Eş Danışman: Prof. Dr. Güneş KARABULUT KURT

MAYIS 2022

Yücel AYDIN, a Ph.D. student of ITU Graduate School student ID 707172003, successfully defended the dissertation entitled "GROUP AUTHENTICATION FOR NEXT GENERATION NETWORKS", which he prepared after fulfilling the requirements specified in the associated legislations, before the jury whose signatures are below.

Thesis Advisor : **Assoc. Prof. Dr. Enver ÖZDEMİR** ....
Istanbul Technical University

Co-advisor : **Prof. Dr. Güneş KARABULUT KURT** ....
Polytecnique Montreal

Jury Members : **Prof. Dr. Kemal BIÇAKÇI** ....
İstanbul Technical University

Prof. Dr. Muhammed Oğuzhan KÜLEKÇİ ....
İstanbul Technical University

Assoc. Prof. Dr. Ali Emre PUSANE ....
Boğaziçi University

Assis. Prof. Dr. Elif Segah ÖZTAŞ ....
Karamanoğlu Mehmet Bey University

Assis. Prof. Dr. Merve BULUT YILGÖR ....
Altınbaş University

Date of Submission : 05 March 2022
Date of Defense : 12 May 2022

To my lovely wife Latıfah

FOREWORD

Foremost, I would like to thank my esteemed advisors Professor Güneş KARABULUT KURT and Professor Enver ÖZDEMİR, who supported me during this thesis and responded to me in significantly detail, despite the COVID-19 epidemic. Thanks to their trust in me, their guidance, and their patience with me, it was possible to prepare this thesis and publications produced from this thesis. I want also to thank Professor Halim YANIKÖMEROĞLU, who has supervised me with all his advice and guidance throughout my studies.

I would like to convey my thanks to the dear members of the steering committee, Professor Oğuzhan KÜLEKÇİ, Professor Ali Emre PUSANE, and Professor Elif SEGAH ÖZTAŞ for their productive criticism and guidance throughout the proficiency exam, thesis proposal, and thesis progress reports.

I would like to thank my beautiful wife, who was with me at every step during this thesis and tried to overcome all the difficult processes with me. I would like to express my gratitude to my wife for being in my life, for always being patient with me and always standing by my side.

MAY 2022

Yücel AYDIN
(Cybersecurity Engineering and Cryptography)

TABLE OF CONTENTS

Page

ABBREVIATIONS

3GPP	: 3rd Generation Partnership Project
AAA	: Authentication, Authorization and Accounting
AKA	: Authentication and Key Agreement
AMF	: Access and Mobility Management Function
AuSF	: Authentication Server Function
AV	: Authentication Vector
BS	: Base Station
CK	: Encryption Key
CRT	: Chinese Remainder Theorem
ECC	: Elliptic Curve Cryptography
ECDH	: Elliptic Curve Diffie-Hellman
EPS	: Evolved Packet System
GAS	: Group Authentication Scheme
GM	: Group Manager
gNB	: eNodeB BS
HXRES	: Hashing of XRES
IMSI	: International Mobile Subscriber Identity
IoT	: Internet of Things
IK	: Integrity Key
LTE	: Long Term Evolution
MAC	: Message Authentication Code
Mbps	: Megabit per Second
MME	: Mobility Management Entity
mMTC	: Massive MTC
MR	: Measurement Report
MTC	: Machine Type Communication
NR	: New Radio
QoS	: Quality of Service
RAND	: Random
RFID	: Radio Frequency Identification
s-BS	: Serving BS
SGW	: Serving Gateway
SSS	: Secret Sharing Scheme
SUPI	: Subscription Permanent Key
t-BS	: Target BS
TEM	: Elliptic Curve Point Multiplication
UAS	: Unmanned Aerial System
UAV	: Unmanned Aerial Vehicle

UDM	**:** Unified Data Management
UE	**:** User Equipment
UxNB	**:** Radio Access Node Onboard Unmanned Aerial Vehicles
UPF	**:** User Plane Function
UTM	**:** Unmanned Aerial System Traffic Management
XRES	**:** Expected Response

SYMBOLS

r	: Threshold Value for CRT
y	: Secret Value for CRT
G	: A Cyclic Group
D	: Secret Value for SSS
k	: Threshold Value for SSS
n	: The number of users in G for SSS
f(x)	: A Function
g(x)	: A Function
p(x)	: A polynomial
P	: A generator point on elliptic curve
a	: An integer
Q	: Multiplication of integer a and generator P
b	: An integer
d_{ij}	: Random integer for user i
w_{ij}	: Random integer for user i
g_i	: Generator over a field for user i
$T_{mul,q}$	: Time for one multiplication for modq
$T_{mul,p}$	: Time for one multiplication for modp
m	: The number of users in G for Harn
R_v	: A random point on elliptic curve for Chien
E(.)	: Encryption operation
D(.)	: Decryption operation
H(.)	: Hashing operation
t	: Threshold Value for Group Authentication
s	: Secret Value for Group Authentication
U_i	: The user i
p	: A prime number
q	: A prime number

LIST OF TABLES

LIST OF FIGURES

Page

GROUP AUTHENTICATION FOR NEXT GENERATION NETWORKS

SUMMARY

The use of the internet of things and unmanned aerial vehicles will definitely increase in the next-generation networks. Security and usability are two balancing factors. While the offering of technological developments to humans makes life easier, it can raise usability and reduce safety. IoT devices and UAVs have limited resources and their numerical existing in a network is more than traditional network devices. Including these next-generation network devices to the mobile networks with authentication is one of the security issues due to their limitations and numbers.

Providing the confidentiality of communication in a network is possible with the encryption of the messages by the sender and decrypting by the receiver. In general, the encryption methods are divided into two sections as public-key encryption and symmetric key encryption. The main difference between these encryption methods is the existence of the same key in both sender and receiver. Each parties communicate with the symmetric key encryption should have the same security key to encrypt and decrypt the messages. The symmetric key encryption is preferred by the IoT and UAVs since the method uses fewer resources than public-key encryption. Although the symmetric key encryption has the advantage of consuming fewer resources, the distribution of the same key with each party in the communication is a challenge. If the number of parties is more than the traditional network as in IoT and UAVs, the key distribution is more challenging.

Authentication, authorization, and auditing are the steps of the access control chain. The security level of the chain begins with strong authentication solutions. A claimer shares its identity with the authentication authority to initiate the authentication process in traditional solutions. The authority verifies the identity according to the predetermined protocols or values. The agreement of a security key after the authentication is a best practice for the encryption of the messages between the claimer and authority.

Nowadays, the most common authentication schemes exploit the one-to-one authentication method. The authenticator can verify a claim at the same time in one-to-one authentication methods. One-to-one authentication methods are not preferred for dense networks such as IoT and UAVs since these networks may produce a large number of authentication requests at the same time. The authentication servers may not respond to the requests, which originates a scalability problem. Group authentication is a promising solution for next-generation networks to overcome scalability issues. Group authentication is a time and resource-saving solution since the members in a group may authenticate each other at the same time.

In this thesis, a new lightweight group authentication scheme is explained in detail by taking into account resource and time issues for IoT and UAVs. The group authentication scheme and most relevant group authentication solutions in the literature are implemented in omnetpp simulation application and the simulation results for time and energy consumption are compared. The results reflected that the group authentication solution required 80% less time and energy according to the other schemes. In addition to the advantages of time and energy, a group key is agreed upon by the group members in order to encrypt the messages in the group communication. The group authentication scheme is also resistant to eavesdropping, replay, and man-in-the-middle attacks since the private keys are kept secret by using discrete logarithm problem. The public value in the authentication is the multiplication of a private key with an elliptic curve generator point. The intruders with the public key cannot include in the authentication due to the lack of a private key. Also, a valid private key is required to recover the group key in order to decrypt the group communication. The updating of the group key in an interval also provides additional security for the group authentication.

The group authentication solutions in the literature require a group manager with preferable resources than other group members. The group manager usually is responsible for selecting the initial parameters of the scheme and verifying the group members. However, most of the networks with IoT devices or UAVs do not have a central authority to manage group authentication. A group authentication scheme should also propose solutions for both centralized and decentralized situations for the next-generation networks. In this thesis, a decentralized scenario for group authentication is presented for IoT devices and UAVs.

The number of IoT devices and UAVs will arise in the future mobile networks. Aerial devices are both service consumers and providers for mobile networks. The aerial devices are used for the capacity injection purposed in the places or scenarios such as disasters, high-dense or rural areas, where terrestrial networks cannot reach or are not sufficient. The UxNB, which is a radio access node onboard UAV, will be the first option to support the terrestrial base station consuming its resources.

During the handover process in 5G, the serving base station shares the security keys and parameters of user equipment with the new base station. In this thesis, a new handover solution for the UxNBs is presented without the requirement of sharing the security keys between UxNB and the terrestrial base station..

At first, the terrestrial base station should not begin to communicate with UxNBs without performing authentication. UxNB and terrestrial base station should authenticate each other and agree upon a security key for the encryption for further messages. After the authentication and key agreement, the devices in the coverage area of UxNB can perform handover from terrestrial to aerial base station. If the 5G handover solution is used for the handover operation, the security keys and parameters for each device should be sent from the terrestrial to the aerial base station. In this thesis, it is proposed and simulated to perform handover operations as a group to decrease time latency and the number of communication.

The security aspects of the authentication and handover for drone swarms are presented in the thesis. The reason to select drone swarms is to examine the authentication in a group and to raise the use of drones everywhere in daily life. The number of drones used for military or commercial applications is getting higher every day. Border security, visual shows, and cargo delivery can be some examples of drone applications. Due to their flying time and limited coverage area, a single drone cannot perform intensive tasks. While providing mobile service via aerial base stations, some UxNBs can turn back to the control station and new drones can be sent to the area to accomplish the tasks. Due to these reasons, it is preferred to use drone swarms for intensive tasks rather than a single drone.

The first security problem for the drone swarm is the authentication of the new drones sent by the drone control station join to the swarm. If it is possible to include a drone in the swarm without authentication, any intruders can impersonate a drone and send it to the swarm for various attacks. In addition to the authentication, the communication inside the swarm should be encrypted and each party should use a group key. The group key may also be shared with the new authenticated drone.

The next security requirement for the drone swarm is the mutual authentication of two drone swarms to perform more intensive tasks. If the authentication solution for the UAV authentication in 5G is exploited for mutual authentication, the number of communication and scalability should be taken into consideration since each party from a different swarm should perform authentication with the UAVs from another swarm. Group authentication solutions may be used to overcome scalability and the high number of communication issues.

Drone swarms also have security and latency issues for the handover operations. There are two kinds of handover operations for drone swarms. One is the handover of drone swarms from serving terrestrial base station to the new base station. The next one is the handover of UxNBs if the base station is not terrestrial but an aerial. The serving UxNB may be out of flying time and drone swarm may start to receive service from new UxNB.

The lightweight group authentication scheme is applied to the authentication and handover operations for the drone swarms in the thesis. 5G UAV authentication and handover methods and group-based solutions are implemented in the simulation and the results are compared. According to the results, the group authentication solutions provide better time, and less communication for the drone swarms.

GELECEK NESİL AĞLARDA GRUP KİMLİK DOĞRULAMASI

ÖZET

Nesnelerin interneti ve insansız hava araçlarının kullanımı gelecek nesil ağlarda şüphesiz ki artma gösterecektir. Güvenlik ve kullanışlılık birbirini dengeleyen iki unsurdur. Teknolojik gelişimlerin insanoğluna sunumu hayatı kolaylaştırırken kullanılışlıyı arttırıp güvenliği azaltabilmektedir. Geleneksel network yapılarına göre sayısal olarak çok fazla olan kaynak olarak ise kısıtlamalara sahip nesnelerin interneti ve insanlık hava araçlarının güvenli bir şekilde ağa dahil edilmesi için kimliklerinin doğrulanması gerekliliği bir problem sahası olarak karşımıza çıkmaktadır.

Ağ içerisindeki bir haberleşmenin gizliliğinin sağlanması iletilen mesajların şifrelenip alıcı tarafında şifresinin çözülmesi ile mümkündür. Genel olarak açık anahtar şifreleme ve simetrik anahtar şifreleme olarak ikiye ayrılan şifreleme yöntemleri aynı anahtarın gönderici ve alıcı da bulunması gerekliliğine göre farklılık göstermektedir. Gönderici ve alıcının aynı anahtar ile şifreleme ve şifre çözme yaptığı simetrik anahtar şifreleme yöntemi açık anahtar yöntemine göre daha az kaynak tükettiği için nesnelerin interneti ve insansız hava araçları için tercih edilmektedir. Daha az kaynak tüketmesinin yanı sıra simetrik anahtarlama yönteminde aynı anahtarın haberleşmeye katılanlara dağıtılması problem oluşturmaktadır. Sayısal olarak kalabalık ortam olarak tanımlayabileceğimiz nesnelerin interneti ve insansız hava araçları için de bu problem etkisini daha fazla göstermektedir.

Kimlik doğrulama, yetkilendirme ve kayıt altında tutma giriş kontrol adımlarını oluşturmaktadır. Diğer adımların güvenliği başarılı bir kimlik doğrulamadan geçmektedir. Geleneksel olarak kimliğin doğrulanması önce doğrulama talebinde bulunanın kendini tanıtması için tanıtma bilgisini paylaşması ile başlar ve sonra tanıtma bilgisinin doğrulanması ile tamamlanır. Genel olarak kimlik doğrulama sonrası mesajların şifrelenmesi için ortak bir anahtar oluşturması tercih edilir.

Günümüzde kullanılan çoğu kimlik doğrulama yöntemleri birebir kimlik doğrulama yöntemini kullanmaktadır. Birebir kimlik doğrulama yönteminde, kimlik doğrulama yapan aynı anda sadece tek bir kimlik doğrulama yapabilmektedir. Sayısal olarak kalabalık ortamlarda kimlik doğrulama isteklerinin sayısı çok fazla olduğundan birebir doğrulama yöntemi yetersiz kalabilmektedir. Doğrulama yapacak olan sunucular gelen istekleri karşılayamadığından ölçeklenebilirlik problemi ortaya çıkmaktadır. Bu problemin çözümünde grup kimlik doğrulama yöntemleri ön plana çıkmaktadır. Grup içerisindeki bütün üyeler aynı anda birbirini doğrulayabildikleri için kaynak ve zamandan tasarruf sağlayabilmektedir.

Bu tez çalışmasında nesnelerin interneti ve insansız hava araçlarındaki kaynak kısıtlamaları göz önünde bulundurularak yeni bir grup kimlik doğrulama çözümü sunulmaktadır. Bu yöntem literatürdeki diğer çözümlerle birlikte omnetpp simülasyon

ortamında gerçekleştirilerek elde edilen sonuçlar karşılaştırılmıştır. Elde edilen sonuçlara göre önerilen çözüm yüzde 80 zaman ve enerji tasarrufu sağlamaktadır. Aynı zamanda diğer grup kimlik çözümlerinden farklı olarak kimlik doğrulama sonrası mesajların şifrelenmesi de dikkate alınmıştır. Grubu oluşturan tüm üyelerin aynı anda elde ettikleri grup anahtarı sayesinde grup haberleşmesi şifreli yapılabilmektedir. Grup üyelerine ait özel anahtarlar eliptik eğri ayrık logaritma problemi ile gizlendiği için ortam dinlemesi, ortadaki adam ve tekrarlama saldırıları ile elde edilen açık anahtarlarla kimlik doğrulaması ve gruba üyelik mümkün olmamaktadır. Grup anahtarının elde edilmesi geçerli bir özel anahtar bulunmasını gerektirmektedir. Grup anahtarının periyodik olarak güncellenmesi de güvenliği bir katman daha arttırmaktadır.

Literatür içerisindeki grup kimlik doğrulama çözümleri genellikle grup içerisinde diğer üyelere göre kaynakları daha fazla olan bir grup yöneticisine ihtiyaç duymaktadır. Bu grup yöneticisi kimlik doğrulama başlangıç değerlerini belirleyip doğrulamayı yapmaktadır. Ancak gelecek nesil ağlarda kullanılan nesnelerin interneti ve insansız hava araçları genellikle merkezi bir yöneticiye sahip olmayacaktır. Her biri aynı kaynağa sahip bir grup insansız hava aracı veya nesnelerin interneti araçları merkezi olmayan bir grup kimlik doğrulama çözümüne ihtiyaç duyacaktır. Bu tez çalışmasındaki grup kimlik doğrulama çözümü hem merkezi bir yöneticinin olduğu senaryolar için hem de merkezi olmayan grup kimlik doğrulamaları için kullanılabilmektedir.

Gelecek nesil ağlarda, nesnelerin interneti ve insansız hava araçları mobil ağ altyapısında kendilerini daha fazla hissettirmeye başlayacaktır. Hava araçları mobil ağ içerisinde hem hizmet alan bir unsur olarak karşımıza çıkarken aynı zamanda mobil ağların bir parçası olmaya başlamıştır. Karasal ağların gidemediğinden veya zaman kısıtlaması nedeniyle yetişemediğinden doğal afet, kırsal alanlar veya kalabalık haberleşme ortamlarında karasal olmayan ağlar mobil ağları takviye maksadıyla kullanılacaktır. Hava araçlarına monte edilmiş baz istasyonları hava baz istasyonları karasal baz istasyonlarının yetersiz kaldığı veya gidemediği noktalarda devreye girecektir.

5G çözümlerinde bir baz istasyonundan başka bir baz istasyonuna geçerken yetki devir aşamasında şifreleme için kullanılan güvenlik anahtarları ve değişkenleri baz istasyonları arasında paylaşılmaktadır. Bu tez içerisinde UxNB ile karasal baz istasyonu arasında mobil cihaz yetki devri işlemi için güvenlik anahtarlarının paylaşımına ihtiyaç duymayacak yeni bir çözüm sunulmuştur.

Karasal ve hava baz istasyonları birbirlerini doğruladıktan sonra karasal baz istasyonundan hizmet alan ama hava baz istasyonu kapsama alanında olan cihazların karasal baz istasyonundan hava baz istasyonuna devir edilmesi gerekmektedir. Bu noktada yine 5G standartlarındaki yetki devir çözümünü kullanmak her bir cihaz için baz istasyonları arasında o cihaza ait güvenlik değerlerinin paylaşımını gerektirmektedir. Bu tez içerisinde yetki devir işleminin grup kimlik doğrulama yöntemleriyle grup halinde yapılmasının yetki devir işlemi için gerekli zamanı azalttığı ve yetki devir için gereken haberleşme sayısını da azalttığı simule edilerek gösterilmiştir.

Bu tez çalışmasında incelenen bir diğer husus ise insansız hava araçlarının grup olarak kullanıldığı dron kümelerinin kimlik doğrulama ve yetki devir işlemlerinin güvenliğidir. Günümüzde dronların askeri ve ticari birçok alanda kullanıldığını görmekteyiz. Sınır güvenliğinin sağlanması, görsel gösterilerin yapılması ve kargoların teslimi bu uygulama alanlarına birkaç örnek olarak verilebilir. Dronlar havada kalma sürelerindeki veya kapsama alanındaki sınırlamalar nedeniyle tek başlarına belli görevleri yapmaları mümkün olmamaktadır. Bir bölgeye hava baz istasyonu ile mobil ağ hizmeti sağlanırken kesintisiz hizmet için dron veya hava aracının havada kalma süresi bitmeden yenisi ile değişimi gerekmektedir. Kesintisiz hizmet sağlamak ve yoğun görevleri yerine getirmek için birden fazla dronun grup olarak kullanımı karşımıza çıkmaktadır.

Dron kümelerinin kimlik doğrulama ihtiyaçları başında gruba dahil olacak yeni dronların doğrulanması gelmektedir. Bir görev yerine getirilirken dron kümesinden bazı dronlar kontrol istasyonuna dönecek ve gruba yeni üyeler dahil olacaktır. Sahte dronların küme içerisinde bulunmasının engellenmesi için bir kimlik doğrulama aşamasını geçmesi gerekmektedir. Kimlik doğrulama sonrası yeni dron ile grup içerisindeki haberleşmenin şifrelenmesinde kullanılan grup anahtarı paylaşılmalıdır. Diğer bir kimlik doğrulama ihtiyacı ise iki farklı dron kümesinin daha geniş ölçüdeki bir görevi yapması için birbirini doğrulamasında ortaya çıkmaktadır. Ölçeklenebilirlik ve haberleşme sayısındaki fazlalık sebebiyle her iki gruptaki dronların birbirini 5G standartlarına göre 5G ağı ile tek tek doğrulaması yerine grup kimlik doğrulama yöntemlerinin kullanımı daha olumlu sonuçlar vermektedir.

Dron kümeleri için yetki devri iki şekilde karşımıza çıkmaktadır. Birincisi, bir dron kümesinin hizmet aldığı karasal baz istasyonunu bırakıp yeni bir baz istasyonuna devir olması ile oluşmaktadır. Diğeri ise hizmet sağlayan baz istasyonunun hava baz istasyonu olması nedeniyle hava baz istasyonunun yerine yeni bir hava baz istasyonu gelince tüm dron kümesinin yeni hava baz istasyonuna devir edilmesidir.

Bu tez çalışmasında önerilen grup kimlik doğrulama yönteminin hava ve karasal baz istasyonlarının birbirini doğrulamasında ve yetki devri işleminde kullanılmasının zaman ve haberleşme sayısında tasarruf sağladığı 5G çözümleri ile önerilen yöntemler omnetpp ortamında gerçekleştirilip gösterilmiştir. Aynı şekilde dron kümelerindeki kimlik doğrulama ve yetki devir işlemleri 5G standartları yerine önerilen grup kimlik çözümü ile yapılması kaynak olarak sınırlı insansız hava araçları için avantaj sağlamaktadır.

1. INTRODUCTION

This thesis in general focuses on the scalability, resource, and latency issues of authentication schemes actively used in wireless sensor and 3rd generation partnership project (3GPP) networks. Group authentication solution for the resource-limited internet of things (IoT) devices, group handover solution from terrestrial base stations (BS) to the radio access node onboard unmanned aerial vehicles (UxNB), and authentication and handover solution for drone swarms are presented in the other chapters.

The relevant studies with the presented schemes are explained in a summary in this chapter. In each chapter, the simulation results of the presented schemes and most related works are compared, and acquired results and conclusions are given.

1.1 Related Works

In this section, the studies conducted before on the group authentication, handover, and the security aspects of the drone swarms are explained in order to compare the related studies with the presented schemes later in the other chapters.

1.1.1 Group authentication

A group of users might utilize a secret sharing algorithm for secure group communication. In this respect, a group key is divided into a number of shares via a secret sharing algorithm, and private shares are distributed among users. Users exchange their private keys with each other, and each user can recover the group key after having its peers' private keys up to a threshold value. Group members can communicate with each other securely by symmetric key algorithm.

The foundation of the studies in the secret-sharing area was initiated in 1979 by two different researchers. The Shamir secret sharing method was proposed by Adi Shamir in [1]. In the same year, the concept of key safeguarding was revealed by George

Robert Blakley in [2]. Both secret sharing and key safeguarding schemes are called threshold schemes.

Shamir's secret sharing scheme is exploited by Harn for efficient group authentication. Harn proposes three different group authentication schemes in [3]. His first scheme is a solution if group users share their private keys with each other at the same time. Otherwise, the first scheme is not secure. An intruder can capture keys and compute a legitimate secret key if the transmissions between group members are asynchronous. The intruder can share the computed key as the last group member and participate in the group authentication. The other two schemes proposed by Harn are designed for asynchronous key sharing. The group members share their private keys with each other and conduct group authentication in a time span, not at the same time as the first scheme. The second scheme can generate a secret key while the last scheme generates a distinct key for each trial. Chien proves in his study [4] that Harn's schemes are not secure, and an intruder can recover the security parameters. He proposes a new scheme based on elliptic curve cryptography (ECC) and bilinear mapping. Chien also compares the computational costs of Harn's approach and his proposed method.

A key establishment scheme in wireless group communication is proposed in [5]. Rather than using traditional secret sharing schemes, a linear secret sharing scheme is proposed using the Vandermonde matrix. The computational complexity of the employed secret sharing scheme is reduced in the proposed approach.

A selective group authentication scheme for IoT-based medical information systems is proposed in [6]. The scheme is based on Shamir's secret sharing method. The proposal provides an authentication solution for one user to access multiple IoT nodes. There are several communications between entities in the system to authenticate only one user.

Asmuth and Bloom propose a key safeguarding scheme, which is based on the Chinese remainder theorem (CRT) in [7]. If anyone has shadows up to r, the secret value y can be computed easily using CRT. But anyone with $r-1$ shadows cannot know the secret [7].

The authors propose an algorithm using the Paillier threshold cryptography in [8]. They compare their results with Harn's group authentication method and present experimental results. The results from [8] show that their algorithm has a better running time result than Harn's group authentication algorithm. However, the authors did not take into account the computational cost of public and private key encryptions or scalability issues. Note that the public key is a key that is known by everyone, but the private key is known only by the owner of the key.

The aggregation of credentials is another solution for group authentication. The approach is mostly used for mobile networks. A trusted group member by the long term evolution (LTE) network collects all the credentials from the group members. Then, the trusted member computes an aggregated value, which is the combination of the credentials. The computed value is confirmed by the authentication server in the LTE network. Here, we also provide an overview of the research based on the aggregation of the credential approach. The authors [9] propose a dynamic group based efficient and secure protocol to authenticate a group of machine type communication (MTC) devices. The protocol authenticates group members by sharing a symmetric key and verifies an aggregate message authentication code. An authentication and key agreement protocol to provide secure communication for a group of mobile station is proposed in [10]. The serving network authenticates mobile stations through the home network component.

A group-based authentication protocol with dynamic policy updating for MTC in LTE networks to provide distributed authentication and session key establishment is proposed in [11]. The authors exploit asynchronous secret sharing and Diffie-Hellman key exchange schemes in their proposal. The group manager (GM), which has better sources than other group members, collects the credentials from the MTC devices and tries to authenticate group members through mobility management entity and home subscriber server.

The work [12] proposes a lightweight group authentication scheme for machine-to-machine communication. Each MTC device computes its message authentication code and sends it to the GM. The manager authenticates the group members through the home subscriber server. A fast mutual authentication and data transfer scheme for massive narrow-band IoT devices is proposed in [13]. The study is also a group-based authentication scheme. A group of IoT devices can be authenticated at the same time according to the scheme.

A group authentication and key distribution solution based on physically unclonable function and CRT is proposed in [14]. Although the solution is named group authentication, the group members are proved one by one with a challenge-response method. After the group members are authenticated, a group key is distributed to the members for group communication. Another study [15] with two steps required to recover a group key is proposed. The satellites as group members are authenticated by the ground control station one by one by sending a challenge to the satellite and verifying the response. After succeeding authentications, the ground control station generates a group key and distributes the key with the satellites by the proposed secret sharing scheme. The secret polynomial for group key agreement is shared with each satellite and the first coefficient of the polynomial is the group key. The security of the group depends on the security of each satellite. If one of the satellites is owned by the intruders, the secret polynomial can be captured and the group communication can be monitored. Further, the handover solution is also based on the group key. The key derivation functions in the handover are using the group key as a key. The security of the handover operations depends also on the security level of each satellite.

1.1.2 Handover studies for UxNBs

There are few studies on the security aspect of UxNB since the usage of UxNB is a new emerging topic. In [16], the authors investigate the scenario in which user equipments(UE) move from one UxNB to another one. The difficulty of using the X_2 logical interface as in LTE is explained in the study.

The studies [17, 18] are related to the selection the best time for the handover. The aim of the papers is to decrease the handover latency. The security aspect of the handover process is not taken into account.

The authentication between a drone and 5G BS is provided by physical unclonable functions in the study [19]. The number of transmissions between drones and BS, XOR operations, mapping, and non-linear functions is time and resource-consuming for drones with limited capabilities. The solution may be used for single drones but it is not scalable to use with the handover of drone groups.

There exist some researches which investigate the security link between a unmanned aerial vehicle (UAV) and control station and the handover key management in

LTE-based aerial vehicle control network [20, 21]. In the studies, authentication between UAV and BS is accomplished by key pairs instead of international mobile subscriber identity (IMSI). With key pairs, which UAV and BS already know before communication, the main authentication key is created and authentication and handover are performed with the new authentication key. According to the presented simulation results, the handover of UAVs is mostly performed between BSs.

One of the gaps in the previous studies is the lack of the authentication solution between UxNB and terrestrial BS. An intruder can impersonate a UxNB and be involved to the system without authentication. Also, the scalability problem for terrestrial BSs is not addressed in the studies. In high-density areas, BSs can drop the requests from UEs. Besides, the scalability is also an issue for handover in high-denstiy areas. These points are not taken into consideration in the previous studies.

1.1.3 Studies on security aspects of drone swarms

The importance of broadcasting for the drone swarm is stated in the study [22]. Following a leader in a swarm is a natural behavior of group communication. The leader prefers to send messages to drones in the swarm as broadcast messages rather than communicating with drones one by one. The authors proposed a broadcast protocol to solve the key distribution issue for the drone swarm. Anytime a new drone participates in the swarm, a new group key is produced and used by the drones. If we take into consideration the dynamic structure of a swarm, all drones will participate in the reconstruction phase of the group key and this will cause too much communication and computational cost for the swarm.

The secure transmission of aggregated data is accomplished by blockchain in the study [23]. The sensing layer of the internet of things and drones as swarms monitor a predefined region and collect data. The data is sent to the cloud servers via gateways and be part of a blockchain. The security solution is commonly based on the application layer. The security of the sensing and network layers is not taken into consideration.

A defense system via drone swarms in order to detect and block malicious drones outside of a flight zone is presented in the paper [24]. The study proposes a clustering approach to realize the interceptions of malicious drones. If the drone swarm detects a UAV with malicious activities, the drone is forced to leave the area. The authors present a security model for the drone swarm [25]. The drones in the swarm store a trust table concerning their neighbor drones. The trust table is generated by the positive and negative votes for each drone in the swarm. If a drone has a trust value less than a threshold value, the drone is assumed an untrusted entity.

1.2 Main Contributions and Outline of the Thesis

The main objective of this thesis is to propose authentication and handover solutions for the next generation networks. The next-generation networks mean the wireless sensor networks and non-terrestrial networks in the thesis.

In the second chapter of the thesis, group-based authentication solutions are examined. A lightweight and flexible group authentication scheme is given and compared with the most relevant group authentication schemes. The content of the second chapter is published in the following paper.

Aydin, Y., Kurt, G. K., Ozdemir, E., Yanikomeroglu, H. (2020). A Flexible and Lightweight Group Authentication Scheme, *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10277-10287.

The main contributions of the second chapter are as listed:

- A flexible lightweight authentication scheme to overcome the possible issues in one-to-one authentication and a scheme can be used in the groups with or without central authority is presented.

- At the end of the group authentication, each group member can recover the same group key for further communications. The group nodes communicate with each other by symmetric key encryption once they have a group key.

- Lightweight schemes are vital for the wireless sensor networks due to the presence of resource constrained nodes. When we compare the proposed scheme in the chapter with other group authentication solutions, the energy consumption of one node can be reduced by up to 80%. Additionally, energy consumption remains constant even if the number of group members increases.

The procedures for the handover management and key exchange between base stations in 3GPP are mentioned in the third chapter. In addition, the use of UxNB for capacity injection purposes and group-based handover from terrestrial to aerial BS are given as well. The content of the third chapter is published in the following paper.

Aydin, Y., Kurt, G. K., Ozdemir, E., Yanikomeroglu, H. (2021). Group Handover for Drone Base Stations, *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 13876-13887.

The main contributions of the third chapter are as listed:

- A fast and energy-efficient handover scheme is explained in the chapter for the high-density areas where UxNB can be exploited efficiently to provide service to the UEs. The current handover solution in 5G new radio (NR) requires to share UE data from the serving-BS *(s-BS)* to the target BS *(t-BS)*. However, there is no data-sharing between BSs in our presented method, which saves time and energy. Besides, confirming UEs by the *t-BS* as a group decreases the time for handover.

- Fake BS attack is a security issue for current mobile networks. Using UxNB also creates the same problem. Any intruder can impersonate a UxNB and try to control UEs. The presented scheme offers an authentication solution between BSs. UxNB can obtain public and private key pair from the core network before becoming active. When UxNB comes over a high-density area, the *s-BS* can authenticate UxNB easily by using the public key of the *t-BS*.

- As the *s-BS* shares the group secret information with the *t-BS*. By using this function, the *t-BS* can authenticate UEs easily in the group handover phase. The authentication can be accomplished as a group. Thanks to having a private function, there is no phase for the control packet transmissions of data between BSs. While the *s-BS* sends data for each UE to the *t-BS* in 3GPP Release 17, no data-sharing between BSs is required in the presented method. Therefore, in the presented method, the number of control packet transmissions between BSs is zero.

- In all authentication solutions for mobile networks, UE must have a private key. In the presented method, it is recommend that UE turns the private key into a public key with a powering operation in the elliptic curve group for handover operation.

Handover operation is carried out when the *t-BS* verify the public key. These private keys must be distributed to UEs before authentication. In the presented method, it is possible to use a subscription permanent identifier (SUPI) belonging to each UE as a private key. This solution eliminates the need for private key distribution before authentication.

In the fourth chapter, the steps for the UAV authentication with the 3GPP network and drone control station in 3GPP standards are given. The security aspects of drone swarms and the authentication and handover solutions are presented in the chapter. The content of the fourth chapter is published in the following papers.

Aydin, Y., Kurt, G. K., Ozdemir, E., Yanikomeroglu, H. (2021). Group Authentication for Drone Swarms, *IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*, pp. 72-77.

Aydin, Y., Kurt, G. K., Ozdemir, E., Yanikomeroglu, H. (2022). Authentication and Handover Challenges and Methods for Drone Swarms, *IEEE Journal of RFID*, under review.

The main contributions of the fourth chapter are as listed:

- A group key is distributed between drones in the swarm to provide a secure channel for the communication and a solution to share the group key with the new participants is presented.

- Authentication of a new drone participating in the swarm requires two steps if the 5G NR solution is used. The first step is the confirmation of the new drone by the core network and the next step is the authentication via the drone control station. The group-based authentication solution in the chapter offers better time and communication complexities than 5G NR.

- During handover operation for the drone swarm, sharing the data for each drone between s-BS and t-BS may cause latency for the communication. Rather than authentication of each drone one-by-one and sharing information between BSs, the network drones can perform group authentication with the target-BS in the presented method.

- If the service providing BS is a UxNB, the handover steps in 3GPP cost time and service latency. A group-based handover solution is presented in the chapter to provide seamless handover from serving-UxNB to target-UxNB.

The overall overview of the thesis and the recommendations for future works are presented in the last chapter. The comparison results from the other chapters are summarized and assessed in the chapter.

2. LIGHTWEIGHT GROUP AUTHENTICATION

2.1 Introduction

In the second chapter, the advantages of using group authentication rather than traditional authentication are dedicated. The fundamentals for lightweight group authentication solutions such as secret sharing and elliptic curve cryptography can be found in the chapter. The authentication in 5G new radio (NR) and a flexible and lightweight group authentication solution are presented and the three most relevant studies for group authentication and 5G NR authentiction are compared in the last section of the chapter.

Confidentiality, integrity and availability features must be fulfilled in order to ensure the security of a communication between parties. Access control and key agreement are the main points of these features. Access control of a system consists of authentication, authorization and accounting (AAA). Authentication is the most important step of the access control chain. Other steps proceed according to the accuracy of this stage.

Traditional authentication methods include one server and one client. The client shares a confidential information it has with the server and the server verifies the client according to private information. Therefore, the server can only authenticate one client at the same time. This authentication process is called one-to-one authentication [3]. The 5G authentication and key agreement (5G-AKA) protocol [26] is currently used for the security of 5G NR communications, which is also one-to-one authentication method.

One-to-one authentication method is used effectively in communications where the number of clients is limited. For example, a computer with windows operating system acts as a server and authenticates the client. Username and password are used in the simplest way for this process. Another example is the authentication of our smartphone, which we constantly use. The phone is authenticated before providing service by the mobile network. This authentication process is accomplished through the chip card in the phone. The phone shares the key in this card with the mobile network and the phone is authenticated. There are many examples of one-to-one authentication such as these. Considering the millions of Internet of Things (IoT) devices, authentication of these devices one by one causes some problems. Especially, the secure communication of massive machine type communication (mMTC) devices with each other, which is also a large number, requires more scalable authentication methods. In the current 3rd generation partnership project (3GPP) standards for 5G NR networks, there is no solution for the concurrent authentication request of mMTC devices [27].

Scalability is one of the problems for one-to-one authentication method. If tens of thousands of clients simultaneously request authentication, it will consume the server's resources and the server may be out of order. Another problem arises from the operations to be made by clients with limited resources for authentication. IoT devices generally have limited storage and energy capacity. It is time, resource, and energy-consuming to use methods such as public key encryption methods for the authentication of these devices [28]. Lighter encryption methods are required.

According to IMT-2020's mMTC requirements, over 1 million nodes can operate in a single km^2 [29]. Although the security issues of mMTC networks are already visible and currently being studied by the research community [30], there are no standardization efforts targeting the scalability of device authentication in these networks [26]. Each mMTC node must perform individual authentication with an authentication server according to the current evolved packet system authentication protocol (EPS-AKA) in mobile networks [31]. This can cause high signaling overhead on the server.

One of the current methods used to deal with these problems is to perform the authentication process as a group. In this method, which is expressed as a group authentication method, each user in the group authenticates all users in the group at the same time. This method is called many-to-many authentication [3].

Existing group authentication approaches do not take the resource constraints of the network into account. However, sensing nodes in an IoT environment frequently have limited memory, tight energy constraints, and very limited processing capability. So during the authentication process, the communication overhead on the nodes should be as little as possible. Furthermore, the energy consumption of the group authentication algorithm should be as low as possible. For this reason, traditional cryptographic systems, along with existing group authentication methods, are not well-suited for IoT, and lightweight systems must be proposed.

Group authentication in wireless communication environments is more vulnerable to attacks by unauthorized entities. Man-in-the-middle attacks can be performed by anyone who can capture group credentials. Hence, group authentication algorithms must provide security for attacks on the wireless channel. Existing group authentication approaches remain vulnerable to such attacks.

Another challenge for IoT networks is the need for secure communication between nodes without any human intervention. For secure communication between millions of mMTC nodes, each node must have a private key. In such a crowded environment, key distribution and key management consume a wast amount of time and energy. A key agreement scheme is also required to ensure the confidentiality of the data.

2.2 5G Authentication and Key Agreement Protocol

The 5G-AKA protocol is an example of the one-to-one authentication method. The initial authentication steps for each user equipment (UE) should be performed to provide service to the UEs. The details about the initial authentication and key derivation in 5G-AKA are given in this section in order to indicate the number of communications and computations to verify only one UE.

Each UE has an identity number, which is embedded in a chip card by the service provider and stored also in the database. This identity number is subscription permanent identifier (SUPI) for 5G NR. Entire authentication and generation encryption, message authentication keys for further communications depend on the long term key K.

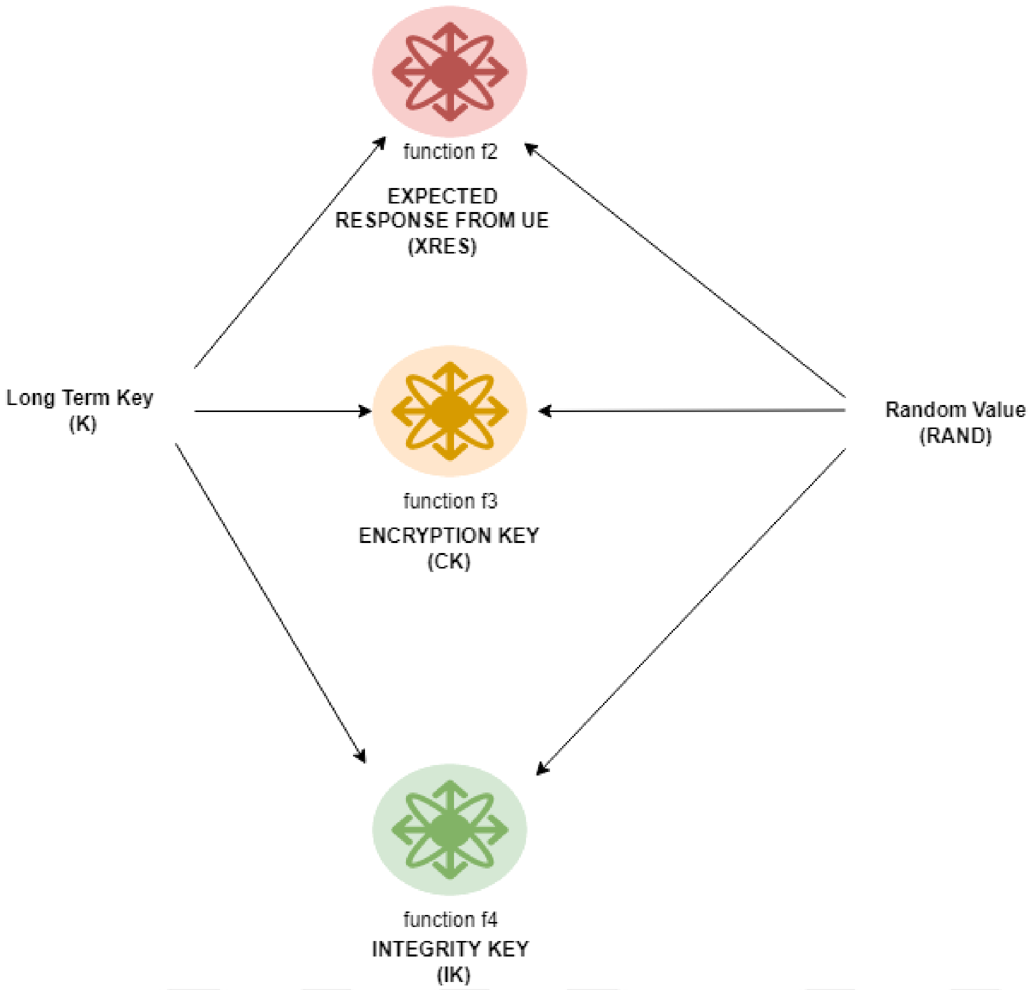

Figure 2.1 : Authentication Vector Generation.

UE, 5G eNodeB base station (gNb), authentication server function (AuSF), and unified data management (UDM) are the members of the initial authentication. The gNb is the actor of the serving network and AuSF, UDM are the actors of the core network in the authentication. The authentication begins with the authentication request from UE. The public key infrastructure is used in 5G NR to overcome the user tracking attacks. The UE encrypts the SUPI using the operator's public key. The UDM decrypts the value transferred from UE. After decryption operation, the SUPI is shared with AuSF. The UDM generates an authentication vector (AV) [32,33] with a random value (RAND) and long term key by using predetermined functions as show in Figure 2.1. The expected response (XRES), encryption key (CK), and integrity key (IK) are the pieces of the vector.

UDM computes expected response star (XRES*) by predetermined function as shown in Figure 2.2. The RAND and XRES as input and $CK||IK$ is used as key for the function

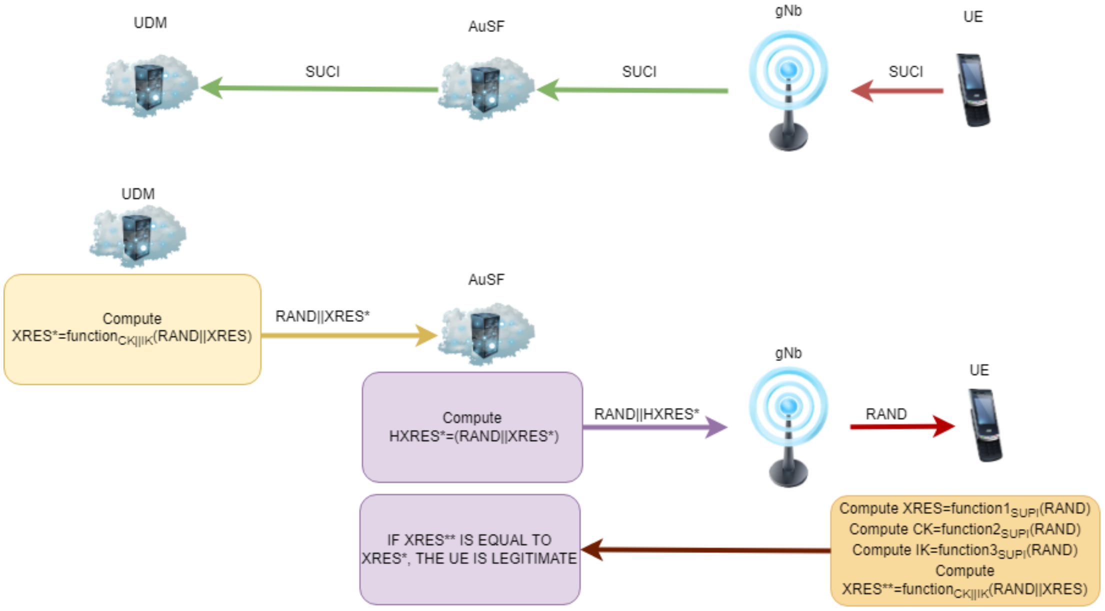
UDM
AuSF
gNb
UE
SUCI
SUCI
SUCI
UDM
Compute
XRES*=function$_{CK||IK}$(RAND||XRES)
RAND||XRES*
AuSF
gNb
UE
Compute
HXRES*=(RAND||XRES*)
RAND||HXRES*
RAND
IF XRES** IS EQUAL TO
XRES*, THE UE IS LEGITIMATE
Compute XRES=function1$_{SUPI}$(RAND)
Compute CK=function2$_{SUPI}$(RAND)
Compute IK=function3$_{SUPI}$(RAND)
Compute
XRES**=function$_{CK||IK}$(RAND||XRES)

Figure 2.2 : 5G NR AKA key derivation functions.

to generate XRES*. The computed XRES* and RAND is shared with the AuSF. The AuSF stores the XRES* and compute the hashing of expected response star (HXRES*) by hashing of $RAND||XRES*$. The AuSF shares the RAND and HXRES* with the gNb. The gNb stores the HXRES* and shares the RAND with the UE. Once the UE has the RAND, the XRES, CK and IK are generated. With the predetermined function XRES* is computed by the UE. The computed XRES* is shared with gNb and AuSF. If the shared value from UE is valid, AuSF confirms the UE and gNb begins to provide service to the UE.

2.2.1 5G NR AKA time complexity

The total time required for the authentication of one UE by the core network with 5G AKA is analyzed in this subsection. The main objective of the analysis is to have the 5G authentication time for the comparison with the group authentication. The operations to complete the UE authentication are one asymmetric key encryption to compute SUCI from SUPI, one asymmetric key decryption to compute SUPI back, 8 keyed-hash mac authentication code256 (HMAC256) with 256 bits output for the key derivation functions, and one hashing with SHA256 to compute the hash of expected response.

Table 2.1 : 5G NR AKA Time Analysis.

Operation	Entity	Time
One Asymmetric Key Encryption	UE	0.1ms
One Asymmetric Key Decryption	g-Nb	1.5ms
Expected Response (XRES) Computation	UDM	67μs
Encryption Key (CK) Computation	UDM	67μs
Integrity Key (IK) Computation	UDM	67μs
Expected Response Star (XRES*) Computation	UDM	67μs
Hash Expected Response Star (HXRES*) Computation	AuSF	50μs
Expected Response (XRES) Computation	UE	67μs
Encryption Key (CK) Computation	UE	67μs
Integrity Key (IK) Computation	UE	67μs
Expected Response Star (XRES*) Computation	UE	67μs
SUPI Transmission to UDM	UE-gNb-AuSF-UDM	10ms
RAND Transmission to UE	UDM-AuSF-gNb-UE	10ms
XRES Transmission to AuSF	UE-gNb-AuSF	10ms
Total Authentication Time	UE-gNb-AuSF-UDM	33ms

According to the computations in [34, 35], one asymmetric key encryption is 0.1ms, one asymmetric key decryption is 1.5ms, one HMAC256 is 67μ, and one SHA256 is 50μ. In addition to the computations, 3 transmissions are performed to complete UE authentication. According to the simulation in omnet++, one transmission requires 10ms. The total authentication time is 33ms as shown in Table 2.1.

2.3 Authentication Requirements for IoT and Non-Terrestrial Networks

The thing in the concept of the IoT can be defined as the node that has an internet connection and is capable of communicating with other things. The purpose of this approach is to connect many objects used in daily life with the cyber world. These IoT devices have the ability to securely communicate with each other. While this communication is taking place, they also make use of the group communication method. The communication between things can be either unicast or multicast. In multicast communication, IoT devices can form a group and share a message with all devices in the group. Generally, this method can be called group communication [36].

In order for IoT devices to communicate securely with each other within the group, a key should be known by both sender and receiver to encrypt the unicast communication. As the number of devices that make up the group increases, the problem of distribution of these keys arises. In addition, in order for the multicast communication to be encrypted by the sender and decrypted by other group members, a group key should be known by all group members. In summary, the group authentication method to be used for group communication should use the source of IoT devices at the minimum level and should distributed the relevant keys with related devices in order to ensure unicast and multicast communication.

In addition to widespread use of IoT technology in next generation networks (5G and beyond 5G) and creating a large volume in internet traffic, the number of non-terrestrial networks will also increase in cellular networks. Non-terrestrial networks consist of space and aerial networks. The use of unmanned aerial vehicles (UAV) in the field of wireless communication also occurs in aerial networks. UAVs can be included in the cellular network as user equipment (UE) and receive services. In addition, it can serve as a radio access node on-board UAV (UxNB) or relay with a base station (BS) deployed on the UAV [37, 38]. Security is one of the first considerations when using UAVs as BS or UE. Since UAVs can be anywhere at any time, the chances of encountering eavesdroppers will be very high. The communication between the UxNB and the UE or the communication between the UAVs used as a UE and the core network is always open to attacks by eavesdroppers. Secure, fast and lightweight AKA protocols are required to ensure the security of these communications.

In addition to the benefits of active use of UAVs, there are many challenges. One of the problems in the field of security is the authentication of several UAVs at the same time by core network or terrestrial BSs. Due to flying time limitations, it may be necessary to send more than one UAV to the area or to make continuous relocation for the continuity of the service to be provided with the UAV. For this reason, authentication will be required for each new arriving UAV by core network. In this scenario, a continuous authentication process will occur.

Public safety networks are a suitable model of the use-case of non-terrestrial networks via wireless channels. The nations are attempting to construct public safety networks that ultimately depend on cellular networks. The usage of terrestrial BS may be out of service in some places or disasters. The UAVs can be equipped with affiliated hardware and operated as BS to support public safety networks. The drone-mounted BS can have diverse links to provide service. The UAV can connect the core network through a satellite or a terrestrial BS [39]. Between UAV and satellite or terrestrial BS, there should be authentication and key agreement phases since the links are predominantly wireless links. The authentication and group handover solutions in the third chapter are presented to cover the AKA issues in the public safety networks. The solutions are assumed that the UAVs and UEs are utilizing the group authentication solution in this chapter. The security complexity is increased in the public safety networks when the UAVs are used as a swarm to accomplish intensive tasks. The authentication and handover methods are also presented in the fourth chapter for the drone swarms

The primary objective of service providers for cellular networks is to deliver coverage of 100 percent. Nevertheless, it is not practicable to install a new terrestrial BS in rural areas, public events causing temporary network demand, or disasters [40]. The drone base stations are the promising solution for these scenarios. Despite the advantages of drone base stations, aerial devices cannot perform heavy cryptographic solutions and are vulnerable to attacks on wireless channels. In addition, the aerial and terrestrial BSs should communicate with each other on a secure channel. Lightweight group authentication and handover schemes are presented in this and the following chapters.

2.4 Secret Sharing Schemes

A secret sharing scheme splits a secret into several shares and only authorized parties can recover the secret together. The first secret sharing schemes were developed by Shamir [1] and Blakley [2] in 1979 based on a threshold value. Several studies concerning threshold cryptography and multi-party computation are built on the threshold secret sharing schemes. Since the publication of the first secret sharing schemes, the type of schemes is generated by the researchers. The use of secret sharing schemes for quantum computation developed the quantum secret sharing scheme [41]. An image can be recovered only by the authorized parties with the use of secret sharing in visual secret sharing schemes [42]. The researchers also proposed studies concerning the verification of the secret recovery process by the public, which is called a publicly verifiable secret sharing scheme [43].

Most of the studies for group authentication schemes (GAS) are inspired by secret sharing schemes. In a group G of n parties, a secret s should be distributed in a way that at least $t < n$ parties' shares are needed to reveal the group secret s. This problem, in general, is solved with a secret sharing scheme or in other words a threshold scheme.

A classical approximation method, which is called polynomial interpolation, is utilized for the purpose of secret sharing. The idea of the method is based on the following theorem.

Theorem 1 *Let $(x_0, y_0), \ldots, (x_t, y_t)$ be points on the graph of a function $f(x)$. There exists a unique polynomial $p(x)$ of degree $\leq t$ such that $f(x_i) = p(x_i)$ for $i = 0, \ldots, t$ [44].*

Consider the group's secret s and assume that s is a real number. Theorem 1 suggests embedding s in a random polynomial $p(x)$ of degree $t-1$. In practice, the secret key s is assigned to be the constant term of a polynomial $p(x)$, where other coefficients are randomly selected. Each member of the group receives a point on the graph of $p(x)$. The secret s can be revealed if and only if t or more members disclose their shares and this method is known as the Shamir Secret Sharing (SSS) [1] scheme. Note that it is not feasible to recover the polynomial, even if $t-1$ points are known [1]. In fact, in SSS, a polynomial

$$p(x) = s + a_1 x + \ldots + a_{t-1} x^{t-1} \tag{2.1}$$

with degree $t-1$ is selected and first coefficient s is the secret value. x_i and the corresponding $p(x_i)$ for $i = 1, \ldots, t$ are the shares for secret sharing scheme. Anyone who has $t-1$ distinct $(x_i, f(x_i))$ pairs cannot have knowledge about the secret, but with knowledge of t or more pairs the secret value s can be recovered by Lagrange interpolation formula which is

$$secret = s = \sum_{i=1}^{t} p(x_i) \prod_{r=1, r \neq i}^{t} \frac{-x_r}{x_i - x_r}. \tag{2.2}$$

2.4.1 The threshold value for secret sharing

The secret sharing schemes depend on a threshold value (t). It is not feasible to recover a secret with the knowledge of $t-1$ shares. Anyone with shares up to the threshold value can generate the selected polynomial and ultimately the secret value. The degree of a polynomial for the secret sharing must be selected $t-1$. The more significant the selected degree is, the more challenging the intruders can generate the polynomial. However, the computational cost is increased proportionally with the degree of the polynomial. The balance between security and computational cost should be determined by the protocol developers. The minimum value for the threshold may be 2 since it is not possible to generate shares if the threshold value is 1. The computational cost is less for the polynomial of degree 2, but the intruders can recover the secret value with 2 shares.

The decision for the threshold value for group authentication schemes is different than the secret sharing schemes. In the secret sharing schemes, t users share their tokens with each other as plaintext and retrieve the polynomial and the secret value. However, the number of group members is greater than the threshold value in the group authentication. Also, the tokens for the group members are not transmitted as plaintext. There is a masking phase for the tokens before the transferring. The authors conduct cryptanalysis for the secret sharing schemes employed for group authentication in their study [45]. According to their results, intruders with masked tokens approximately two times the threshold value can obtain the secret key. Therefore, it is secure to select a threshold value greater than half of the group members.

2.5 Elliptic Curve for Group Authentication

Definition 1 *Let K be a field of characteristics different from 2 and 3. An elliptic curve E over K is an algebraic smooth curve defined by an equation of the form $y^2 = x^3 + Ax + B$ where $A, B \in K$.*

Let E be an elliptic curve over K. The set of all points (x, y) on the curve along with a point at infinity form an abelian group $E(K)$.

Definition 2 *Let $E(K)$ be an elliptic curve group for the elliptic curve E over K. Let P, Q be points in the group $E(K)$ such that $Q = aP$. For a given such points P, Q the problem of finding a is called discrete logarithm problem.*

The use of elliptic curves in secure communication is based on the hardness assumption of the discrete logarithm problem on elliptic curve groups [46]. We should note here that computing in an elliptic curve group requires addition, multiplication in a field K if one uses projective coordinates [47].

Elliptic curve Diffie-Hellman (ECDH) key exchange protocol is also used in our presented solution for the group key agreement phase. In the method, two parties want to have the same key. One party has a private integer a, and the other party has a private integer b. Their public keys are the multiplication of private integers with a public point P in an elliptic curve group. Each party sends its public value to the other party in order to compute the same key. Once the first party has public key bP of the second party, it computes a times the public information of bP. The second party performs b times aP. Finally, each party has the same value abP without releasing their secrets a and b.

2.6 Group Authentication Schemes

Group authentication is a solution for the time and resource-consuming authentication process. In an IoT environment, the IoT nodes have limited resources, which is the reason not to handle by traditional cryptographic computations. Lightweight algorithms are widely exploited in IoT scenarios. A lightweight group authentication scheme is one of the best solutions to authenticate parties in a communication environment with several IoT nodes.

Harn [3] and Chien [4] proposed lightweight group authentication schemes to authenticate a group of nodes at the same time. Their schemes decrease the computational load on the nodes. The method presented in this section addresses the shortcomings of these two studies. Below, we compare the authentication time and energy consumption in order to observe the resource consumption of IoT nodes.

Both works are a solution for group authentication, and in general, there are one group manager (GM) and multiple group users forming a group. GM determines initial parameters and keys. Each group user has one private key and one public key.

2.6.1 Harn's group authentication schemes

Harn proposed three group authentication solutions in his study [3]. The foremost solution can be utilized if the members in the group share their private keys with each other and validate each other at the same time. If there is a span for the authentication, an intruder can compute an useful private key and participate in the authentication.

In the first scheme, the GM selects a polynomial $f(x)$ of degree $t-1$. The secret key (s) is the first coefficient of the polynomial. For each group member U_i, the GM determines one unique public key (x_i) and computes corresponding private key $f(x_i)$. The keys are shared with the related group members. The public values for the scheme are the public keys of group members and the hash of the secret key $(H(s))$.

While performing group authentication, each member transfers its private key $f(x_i)$ with all group members up to m (m denotes the number of the group members). Each group member computes

$$secretkey = s' = \sum_{i=1}^{m} f(x_i) \prod_{r=1, r \neq i}^{m} \frac{-x_r}{x_i - x_r}. \tag{2.3}$$

If the hash of s' is equal to $H(s)$, all the group members are legitimate.

The second scheme can be employed while the group members disseminate their keys asynchronously. The scheme provides protection to recover the polynomial as described in the first scheme. The GM selects a random integer k such that $kt > n-1$ and random polynomials $f_l(x), l = 1,2,...,k$ of degree $t-1$. The random integers w_j and $d_j, j = 1,2,...,k$ are selected and a secret key s is computed as

$$secretkey = s' = \sum_{j=1}^{k} d_j f_j(w_j) \tag{2.4}$$

where each integer w is unique. Each group member U_i has private keys $f_l(x_i)$. The integers w_j and d_j and the hash of secret key $(H(s))$ are public.

While performing the group authentication, each group member computes one Lagrange interpolation

$$c_i = \sum_{j=1}^{k} d_j f_l(x_i) \prod_{r=1, r \neq i}^{m} \frac{w_j - x_r}{x_i - x_r}. \tag{2.5}$$

and shares the result c_i with all group members. Once each group member obtains interpolation results up to m, the group members can compute the secret key

$$secretkey = s' = \sum_{r=1}^{m} c_r. \tag{2.6}$$

If the hash of s' is equal to $H(s)$, all the group members are legitimate.

The last scheme can also be utilized for asynchronous transmission. The difference between the second and third schemes is that the last scheme generates a secret key for each session. In the initialization phase for the Harn's scheme:

The GM selects two prime numbers q and p, such that q divides $p-1$, and a generator g_i in Field F_q [3]. Two different polynomials $f_1(x)$ and $f_2(x)$ with degree $t-1$ are chosed (t is the threshold value for the group authentication). Two private keys $f_1(x_i)$ and $f_2(x_i)$ are generated for each user U_i.

The GM has several secret value s_i and for each s_i, two different integers $w_{i,j}$ and $d_{i,j}$, $j = 1,2$ are selected. The secret value s_i is equal to

$$s_i = g_i^{\sum_{j=1}^{2} d_{i,j} f_j(w_{i,j}) mod q}. \tag{2.7}$$

The integer values $w_{i,j}$ and $d_{i,j}$, the generator g_i, and the $H(s_i)$ are publicly known by everyone.

In the group authentication phase, each user computes

$$c_i = \sum_{j=1}^{2} d_{i,j} f_j(x_i) \prod_{r=1, r\neq i}^{m} \frac{w_{i,j} - x_r}{x_i - x_r}, \tag{2.8}$$

and $e_i = g_i^{c_i}$ in Harn's scheme [3]. Then, each user shares e_i.

To verify other users, each user computes

$$s_i' = \prod_{i=1}^{m} e_i. \tag{2.9}$$

in [3].

In total, one user should make $(45m + 1418)T_{mul,q}$ operations as depicted in [4] (m is the number of users in the group and $T_{mul,q}$ denotes the time for one multiplication).

2.6.2 Chien's group authentication schemes

Chien described in his paper [4] the weaknesses in Harn's second and third asynchronous schemes. In addition, a group authentication solution is presented based on the elliptic curve groups. The time breakdown of the schemes is given in the study. In the initialization phase for the Chien's scheme:

The GM selects two elliptic curve additive groups G_1, G_2, and one multiplicative elliptic curve group G_3 with order prime q [4]. One generator P is selected on G_2. A secret polynomial $f(x)$ with degree t is chosen and the first coefficient of the polynomial is secret value s.

For each user U_i, an unique private key $f(x_i)$ is created and shared with user privately. A public point Q is computed with the multiplication of s and P. A random point R_v in G_1 is selected for each authentication.

In Chien's scheme [4] each user computes

$$c_i = f(x_i) \prod_{r=1, r\neq i}^{m} \frac{-x_r}{x_i - x_r}, \tag{2.10}$$

and $c_i R_v$ in the group authentication phase. Then each user shares $c_i R_v$.

In the verification phase, each user computes

$$e\left(\sum_{i=1}^{m} c_i \times R_v, P\right) \stackrel{?}{=} e(R_v, Q) \tag{2.11}$$

in [4].

In total, one user should make $(7m + 6785)T_{mul,q}$ operations as depicted in [4].

2.6.3 Our proposed group authentication scheme

The GM is assumed to be infrastructure-based and has relatively more computational power. In addition to the GM, each group has several other members with the resource or computational constraints. Note that in IoT environments, the GM is basically the gateway with specific capabilities. Sensor nodes or radio frequency identification (RFID) tags can be considered to be the other members of a group. The capabilities of these nodes are at a certain restricted rate.

The proposed method has two stages. The first stage involves the authentication process, which is based on elliptic curves and secret sharing scheme. This first stage consists of two phases, which are called the initialization and confirmation phases. The second stage, which is the key agreement stage, provides a solution to construct a group key for further communications. The details of each phase are presented below.

The Initialization Phase:

1. GM selects a cyclic group G and a generator P for G.

2. GM selects $E = Encryption(\cdot)$ and $D = Decryption(\cdot)$ algorithms and a hashing function $H(\cdot)$.

3. A polynomial with degree $t-1$ is chosen by GM and the constant term is determined as group key s.

4. GM selects one public key x_i and one private key $f(x_i)$ for each user in the group U where each user is denoted by U_i for $i = 1,\ldots,n$.

5. GM computes $Q = s \times P$.

6. GM makes $P, Q, E, D, H(s), H(\cdot), x_i$ public and shares $f(x_i)$ with only user U_i for $i = 1,\ldots,n$.

The confirmation phase is executed after the GM shares the values with the related users. There are two different options in the confirmation phase. One is that the GM is responsible for confirming the group members (*the centralized approach*). The other is that any member of the group is responsible for confirming the other members (*the decentralized approach*). The member selection can be made on the basis of the instantaneous resource availability of each node, such as their battery levels.

The Confirmation Phase:

1. Each user computes $f(x_i) \times P$ and sends x_i and $f(x_i) \times P \| ID_i$ to the GM and other users (ID_i is the identification number of the user and $\|$ symbol shows the concatenation of two values).

2. If the GM verifies the authentication, the GM computes $f(x_i)$ for each user from x_i value.

3. The GM performs addition operations separately for $\sum[f(x_i)]$ and $\sum[f(x_i) \times P]$.

4. Once the GM has all public values from group members, computes $\sum[f(x_i)] \times P$.

5. If $\sum[f(x_i)] \times P$ is equal to $\sum[f(x_i) \times P]$, the group is authenticated.

6. If the GM is not included in the verification process, any user in the group computes

$$C_i = \left(\prod_{r=1, r \neq i}^{m} \frac{-x_r}{x_i - x_r}) \right) f(x_i) \times P \tag{2.12}$$

for each user (m denotes the number of the users in the group and m must be equal or larger than t).

7. User verifies whether

$$\sum_{i=1}^{m} C_i \overset{?}{=} Q \tag{2.13}$$

holds.

8. If it holds, authentication is done. Otherwise, the process will be repeated from the initialization phase.

It is clear that group members should only compute one elliptic curve multiplication operation. The users should send their identification numbers by concatenating with public shares in order to avoid confusion for further communications. This is because these public shares will be used by other users in further communications and in the group key agreement stage, and all members should know which public share belongs to which user.

After the authentication has been performed, users will communicate with each other by using symmetric key encryption. The key for symmetric key encryption will be calculated by senders and receivers.

ECDH key exchange protocol is used in order to compute the key between the group members. Let us set the key, K as

$$K = (y_i y_j P) \tag{2.14}$$

where $y_t = f(x_t)$, i.e., y_t is the private of the user U_t. The sender will use their own private key (y_i) and the value sent by the receiver $(y_j P)$. The receiver will obtain the same key with a similar operation, i.e., combining its own key y_j with the received data $y_i P$.

The Group Key Agreement Stage:

After this stage, group members can communicate with each other by symmetric key encryption method. However, using different keys for different users will cost computational and memory usage. Therefore, instead of using different keys for each user, the group key that was selected by the GM can be used as the group key. The problem is how the users will recover the group key. The secret sharing scheme and symmetric key encryption method to share the group key in the group key agreement stage.

1. Each user shares their own private key $f(x_i)$ with other users using symmetric key encryption.

2. Each user decrypts the values and obtains m different $f(x_i)$.

3. Each user computes

$$s' = \sum_{i=1}^{m} f(x_i) \prod_{r=1, r\neq i}^{m} \frac{-x_r}{x_i - x_r}. \tag{2.15}$$

4. Each user verifies whether

$$H(s') \overset{?}{=} H(s) \text{ holds.} \tag{2.16}$$

After the group key agreement process, the members of the group will be able to communicate with each other using the group key. In addition, the GM can update x_i and $f(x_i)$ values remotely using the group key in order to avoid replay attacks.

2.6.4 De-centralized group authentication

The proposed scheme is a solution for both centralized and decentralized scenarios. There may not always be a trusted central authority, such as GM in the distributed and crowded IoT scenarios. The IoT nodes perform the same steps when a GM is not present. Initial parameters can be selected in the production time of IoT nodes and they can be embedded in the nodes. The group key agreement stage is the same for both centralized and decentralized scenarios. The key phase in the de-centralized scenario is the confirmation phase. If there exists a GM in the group, the GM can confirm the credentials sent by the group members. Otherwise, if there is no GM, a multi-party computational method is required to establish a secure group. After having $f(x_i)P$ public keys up to m, each group member can compute

$$c_i = \left(\prod_{r=1, r\neq i}^{m} \frac{-x_r}{x_i - x_r}) \right) f(x_i) \times P. \tag{2.17}$$

Afterward, each group member can compare

$$\sum_{i=1}^{m} c_i \overset{?}{=} Q. \tag{2.18}$$

If the confirmation is done, the group members can continue with the group key agreement stage.

2.6.5 Comparison of group authentication schemes

Group authentication is a novel method to increase the performance of the authentication system and to decrease the computational load on the group members. Additionally, the number of communications between GM and group members is kept to a minimum in group authentication.

The comparison of Harn's and Chien's GAS is given in [4]. Chien used a theoretical approach for the comparison. The author unveiled the required time to complete the group authentication for both studies. $T_{mul,q}$ value, (which is the time for one multiplication in the fields F_q where q is 160 bits), is used as the base factor. According to [4], $(7m+6785)T_{mul,q}$ is required to complete Chien's algorithm and $(45m+1418)T_{mul,q}$ is required to complete Harn's algorithm (m is the number of users in the group).

In our proposed approach, the group members should only compute one elliptic curve point multiplication (TEM). According to Chien [4], TEM is roughly equal to $29T_{mul,p}$ ($T_{mul,p}$ denotes the time for one multiplication in field p where p is 1024 bits). The security of ECC with a 160-bit key is roughly equal to that of RSA with a 1024-bit key or DH algorithm with a 1024-bit key [48]. Therefore, $T_{mul,p}$ is roughly equal to $41T_{mul,q}$ [4]. In our authentication algorithm, group members compute $29T_{mul,p}$, which is 1189 (29x41)$T_{mul,q}$. Due to this theoretical analysis, the simulation results are shown that our scheme costs a shorter authentication time and consumes less energy than the approaches proposed by Harn and Chien.

We implemented two most relevant schemes [3,4] and our scheme in order to compare the energy consumption by IoT nodes. Omnet++ simulation environment [49], which is widely used to simulate wireless schemes, was exploited for the implementation of algorithms. The simulation results are given in Figure 2.3 and Figure 2.4 for the groups with ten IoT nodes and fifty IoT nodes.

Initial parameters of simulation were selected according to the basics in the related papers. For Harn's scheme, the prime numbers p and q are two primes such that $p-1=2q$. w_i and d_i values are random integers that are used for each user and each secret calculation. Generator g_i of field q is 7, and coefficients of two polynomials are in the field of q.

Table 2.2 : Simulation Parameters.

Radio Medium	UnitDiskRadioMedium
IoT Node Range	500 m
Wlan Type	AckingWirelessInterface
Energy Storage Type	IdealEpEnergyStorage
Energy Consumer Type	SensorStateBasedEpEnergyConsumer
Wlan Mac Type	CsmaCaMac
BitRate	1 Mbps
Ack Usage	False

For Chien's and our proposed simulation, the same parameters were selected. Elliptic curve is $y^2 = x^3 + 6x + 36 \mod 2017$ selected in order to have fast computation. Coefficients of polynomial $f(x)$ are in the field of q.

Omnet++ simulation application offers various different configurations, and the configuration we used for our simulation can be seen in Table 2.2. IoT nodes were selected sensor node as in the omnetpp inet library. Sensors use the default options for energy storage and consumption.

It can easily be observed from the graphics that Harn's scheme takes more time than other schemes to complete the group authentication. Time is directly proportional to the number of IoT nodes. Our proposed method and Chien's scheme are almost consuming the same amount of time, which is 1.3 seconds for ten nodes and 6.9 seconds for fifty nodes. Harn's scheme consumes 10 seconds for ten nodes and 50 seconds for fifty nodes, as seen in Table 2.3.

Table 2.3 : Authentication Time.

Time (s)	Harn [3]	Chien [4]	Proposed Approach
10 Nodes	10 seconds	1.3 seconds	1.3 seconds
50 Nodes	50 seconds	6.9 seconds	6.9 seconds

In terms of energy consumption, our scheme costs the least energy both for the groups with ten nodes and fifty nodes. Harn's and Chien's schemes consume almost the same energy if the group is with ten nodes. Our scheme consumes 0.014 joules of energy, whereas other schemes consume 0.05 joules. If the number of group nodes increases, Harn's scheme consumes the most energy to complete group authentication. For groups with fifty nodes, Chien's scheme consumes 0.37 joules and Harn's scheme consumes 1.1 joules. The nodes consume only 0.062 joules in our proposed method for the group authentication if the group is with fifty nodes.

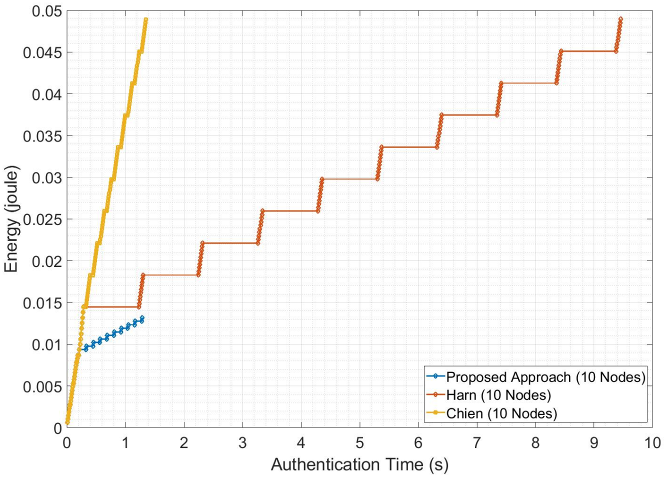

Figure 2.3 : Energy Consumption of one IoT Node in a group with 10 IoT Nodes.

In respect to algorithmic details, IoT nodes exploit modulo exponential operations for group authentication in Harn's algorithm. The operations consume too much time and energy, which can be observed in Figure 2.3 and Figure 2.4. If the number of IoT nodes increases, one IoT node consumes more time and energy. Chien's algorithm yields better results than Harn's algorithm. This is observed since the nodes only compute one elliptic curve multiplication operation and $m-1$ modulo multiplication and inverse operations (m is the number of group nodes). The difference between our algorithm and Chien's algorithm is that IoT nodes compute only one elliptic curve multiplication operation for group authentication. As seen in Figure 2.3 and Figure 2.4, our proposed method consumes less time and energy than Chien's scheme.

2.6.6 Comparison of 5G AKA and proposed group authentication scheme

The total authentication time is analyzed in the earlier section while defining the details of UE authentication in 5G NR AKA. The time is 33ms to authenticate one UE by an authentication server in the core network. In this section, a time breakdown of the proposed group authentication scheme is provided.

The centralized group authentication scheme demands one elliptic curve multiplication for each group member, one elliptic curve addition for each private key, and one elliptic curve multiplication to verify the group members. According to the results in [34, 35], one elliptic curve multiplication is required $612m\mu$s, on elliptic curve addition is

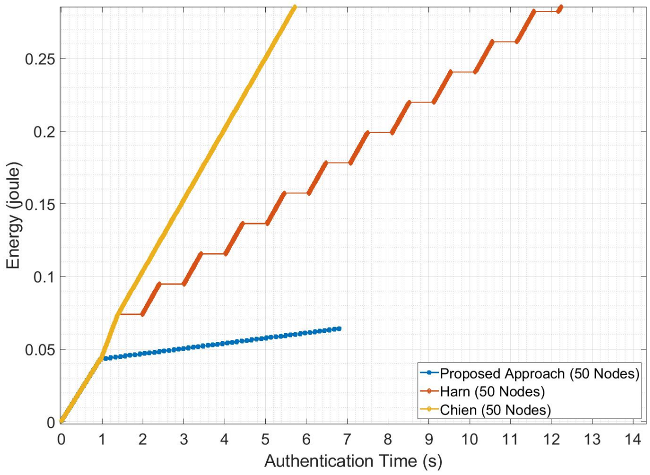

Figure 2.4 : Energy Consumption of one IoT Node in a group with 50 IoT Nodes.

$125m\mu$s, and total authentication in the proposed scheme is $1337m + 612\mu$s (m denotes the number of group members). If the group has 10 members, 5G AKA requires 330ms to authenticate all the group, while 14ms is enough for the proposed scheme.

2.7 Conclusion and Discussion

This chapter summarizes the authentication solutions for resource-limited devices such as IoT. Traditional one-to-one authentication schemes have always one claimer and one verifier. The claimer shares a predetermined value with the verifier according to the decided protocol and the verifier approves the shared value.

Table 2.4 : Time analysis for the proposed group authentication scheme.

Operation	Entity	Time
Elliptic Curve Multiplication	Each Group Member	$612m$ μs
Public Key Share with GM	Each Group Member	$600m$ μs
Elliptic Curve Addition for Each Private Key	GM	$125m$ μs
Elliptic Curve Multiplication	GM	612 μs
Total Authentication Time	Total	$(1337m + 612)$ μs

The traditional authentication schemes work appropriately in a centralized server-client infrastructure. If the number of end devices is more than a server can handle, the scalability and latency issues may take place. The authentication of each IoT device one by one is resource and time-consuming for a central authority. The many-to-many authentication solutions such as group authentication are promising schemes for future authentication requirements.

Symmetric key encryption is preferred more than public-key encryption for resource-limited devices due to the energy-consuming computations. The main issue for symmetric key encryption is that each party in the communication must know or agree on a key that is exploited to encrypt and decrypt the messages. Most of the traditional authentication solutions merely deal with the phase to verify the claimer. However, a key agreement phase is required in an authentication solution for the encryption of further communication between parties. Key agreement for the scenarios with several distributed IoT devices is a challenge for the researchers. Group authentication which can generate a group key that is known only by group members is a promising lightweight authentication solution for crowded groups.

In this thesis, the time breakdown of 5G NR AKA and proposed group authentication method are presented by a review of each step and transmission in the scheme. According to the time complexity, the group authentication scheme provides a more reasonable time than 5G AKA, and when the number of members in the group increase, the time differences between methods are more significant.

Another outcome of this chapter is the comparison of the group authentication solutions in the literature. The time and energy use of Harn's, Chien's, and proposed schemes are compared by utilizing the omnet++ simulation environment. The proposed group authentication solution provides more reasonable time complexity than Harn's scheme and less energy usage than Chien's scheme.

UE authentication in 5G AKA has several stages to confirm the end device and agree on the security keys between g-Nb and UE. The UEs may be mobile and switch from one g-Nb to another. It is not feasible to repeat the 5G AKA as explained in this chapter for each handover. Particularly in dense areas, the g-Nb is too busy delivering service to the UEs. The handover schemes between g-Nbs should be secure and time-saving. By exploiting the group authentication solution in this chapter, a group-based handover scheme is proposed in the next chapter. In addition, the current 5G handover solution does not have an authentication step between the g-Nbs since the connection between g-Nbs is not open to the outside world. However, the use of aerial devices as BS creates a wireless channel between terrestrial and aerial BSs. An authentication scheme is proposed in the next chapter based on the group authentication method in this chapter.

3. CAPACITY INJECTION AND GROUP HANDOVER

3.1 Introduction

In this chapter, the details about the handover solutions in LTE and 5G NR are presented. The reconstruction of the security keys from a single key by the servers in the core network, g-Nb, and UE is explained at the beginning of the chapter. In addition, there exists a section to describe the process for the sharing and creating security keys concerning the handover in 5G NR.

This chapter describes the scenarios requiring a capacity injection for the terrestrial BSs. The reason for the necessity of the authentication between the terrestrial BS and the aerial BS is explained in the chapter. Authentication and handover schemes are proposed based on the group authentication solution in the first chapter.

Simulations are conducted for the 5G NR handover scheme and proposed handover solution in the wireless simulation omnet++ environment. In addition, the comparisons concerning the time and the number of the communications in the proposed scheme and 5G NR solution are given. The chapter is concluded with a summary of the comparison results of the proposed scheme.

A substantial surge in the number of user equipments (UE) utilizing mobile services is expected in the near future. As the number of UEs connected to a terrestrial base station (BS) increases, the quality of service (QoS) per user tends to reduce. It is highly probable that the BS will even be out of service, and therefore, UEs will not be able to access to their mobile services. The current solution for such situations is applying to capacity injection, such as a mobile BS [50]. The service provider deploys mobile BSs in a crowded area, which eventually increases the mobile network's average QoS.

A radio access node on-board of unmanned aerial vehicle (UxNB) is a radio access node providing service to the UEs deployed on an unmanned aerial vehicle (UAV) according to 3GPP TS 22-125 [51]. The UxNB can connect to the core network as terrestrial base station, which is next generation NodeB (gNB) in 5G new radio (NR). The research community already has an interest in UxNB in order to enhance the mobile network coverage. The UxNB can be exploited in several scenarios, such as emergencies, and high-density areas. UxNB can be deployed to an area without terrain constraints [52].

Providing uninterrupted service to many different types of UEs is one of the main focus areas of 6G research activities [53]. The traffic requirements expected from mobile networks may vary depending on the usage scenario. Mobile networks will need to be reinforced towards scenarios such as unforeseen natural disasters, traffic congestion, high-density concerts, or football games.

Public safety communication systems are indispensable for rescue teams in case of disasters. However, this infrastructure is also affected by a disaster [54]. In order to ensure the continuity of communication, current mobile network infrastructure should be rearranged in accordance of such situations. Thanks to their assets and deployment advantages, UxNB is the main candidate to close these gaps in the current mobile networks. UxNBs can be exploited in high demand situations or public safety and disaster management operations. The main advantage of UxNB is the deployment capability to any area without an operating pilot. For high-density areas, a better QoS can be provided by UxNBs via capacity injection [55].

In the 5G handover, the security key for each UE is shared from the serving BS to the target BS. If two BSs are terrestrial, the media between them is a wired channel. The speed of sharing information may take nano seconds, which is acceptable. However, if one of the BS is aerial BS, the channel will be a wireless channel and the speed of transmission should be taken into consideration.

The interruptions for the services provided by a terrestrial base station can be faced in some circumstances. Consider a football game where there is a steady increase in the number of users in a particular area (stadium) in a specific period (90 min.). During the game, only one terrestrial BS may provide service to all UEs. It will be more beneficial to use UxNB to increase the BS's capacity, as shown in Figure 3.1. The security aspect of the capacity injection with UxNB is the trust between UxNB and terrestrial BS. Before transferring data to UxNB, the terrestrial BS should authenticate the UxNB.

After the confirmation of identity for the UxNB, a key agreement between BSs should be performed to prevent the eavesdroppers to capture the traffic. The symmetric key encryption may be preferred to encrypt the traffic once a key is agreed upon.

While capacity injection is the first issue in such dense deployment scenarios, the handover among the overlay cells after capacity injection is the second issue. The use of several BSs within a particular area will result in overlay cells. Terrestrial BS providing service to all UEs in the stadium will delegate some UEs to UxNB to reduce the traffic load. In the meantime, there will be many handover operations.

In the currently used LTE [56], and 5G standards [26], these handover operations should be done sequentially, i.e. one by one. Yet, due to the limitations of the UxNBs such as weight and battery life, their flying time will be a maximum of one hour [52]. Considering that a football game is at least 90 minutes, a new UxNB will take over from ex-UxNB at least once. This will cause an increase in the number of handover operations to be performed. UEs should be transferred from terrestrial to UxNB not individually but as a group in order to make this handover process more efficiently.

3.2 UAVs in 3GPP

According to 3GPP TS 22-261 [57], it is predicted that UAVs are going to be used in several applications by governments and commercial sectors. Latency and reliability will be one of the first concerns for the next generation 6G networks. UAVs will need more certain location information and security against theft and fraud.

An unmanned aerial system consists of UAVs and UAV controller [58]. The data traffic between these two components must be well-protected. Next generation mobile network providing service to the UAVs must be resistant to spoofing and non-repudation attacks.

Identification, tracking, and authorization of UAV and controllers are controlled by a central system, which is the Unmanned Aerial System Traffic Management (UTM) [58]. UTM stores all identity and meta information of UAVs and UAV controllers. The authentication and authorization of UAVs in the area have taken place by the information sharing procedures between UTM and mobile core network, especially access and mobility management function (AMF). It is clear that including of UAVs to the mobile network introduces a higher computational burden for the AMF.

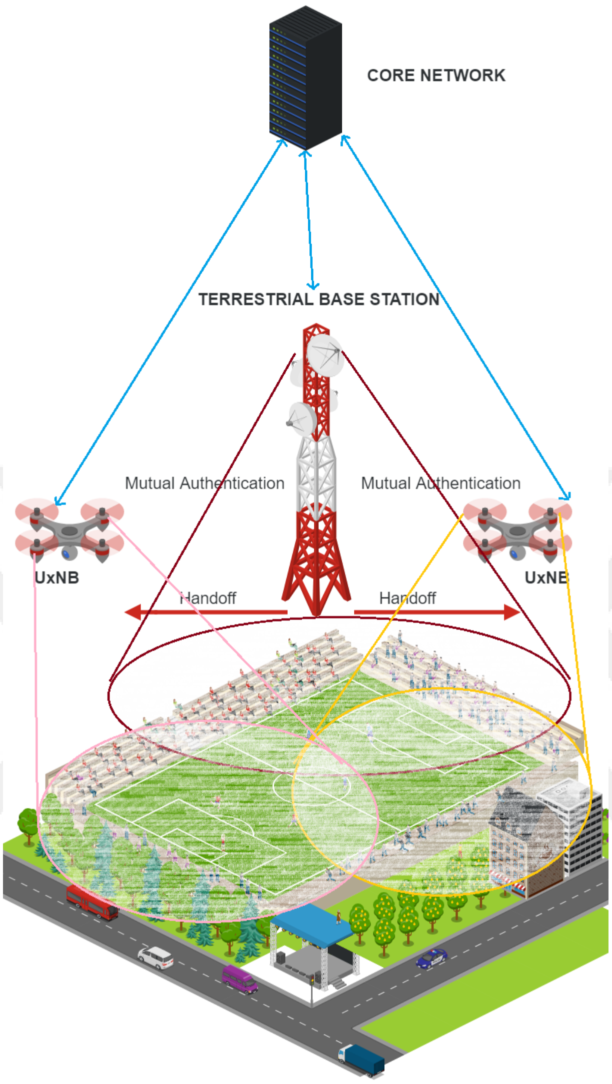

Figure 3.1 : An examplary use case for capacity injection and group handover.

The use of UxNB to increase the coverage area is specified in 3GPP standards. A UxNB can connect to 5G core network as a terrestrial BS via wireless backhaul link [52]. A UxNB can be used in various scenarios such as emergencies, temporary coverage for UEs, hots-spot events, due to their fast deployment and broad coverage capabilities [52]. UxNBs should be authenticated by the core network before operating as a BS. One of the requirements for using a BS on UAV is to keep the energy usage at the lowest level because UAV has limited power.

The use of UAVs alone is limited due to their airborne time and energy constraints. For example, using a single drone in delivery services results in waiting for that vehicle to come back to the base. For this reason, UAVs should be used as a swarm. The essential requirement for a swarm of UAVs is group management [52]. Group management requires group authentication and secure communication inside a group, as given in the following sections.

3.3 Handover Management in Long Term Evolution

There are two types of handover scenario in long term evolution (LTE) based on the existing of the mobility management entity (MME) change [59]. Inter-BS with intra-MME is described in this section step by step. The user equipment (UE) disconnects from serving BS (*s-BS*) and connects to the target (*t-BS*) without changing MME.

The handover steps are shown in Figure 3.2 and also listed below.

1. The UE measurement procedure is configured by the *s-BS*.
2. The UE sends a measurement report (MR) to the *s-BS*.
3. According to the report, the *s-BS* makes a handover decision.
4. The *s-BS* sends a handover request to the the *t-BS*.
5. The *t-BS* sends an acknowledgment to the *s-BS* according to its resources.
6. The *t-BS* informs the UE for handover with necessary information.
7. The UE attaches to the target cell.
8. The *t-BS* sends uplink allocation and timing information to the UE.
9. The *t-BS* informs the MME for UE cell change.
10. MME informs the serving gateway (SGW) for UE.
11. SGW updates the path for UE.
12. MME informs the *t-BS* for path update.

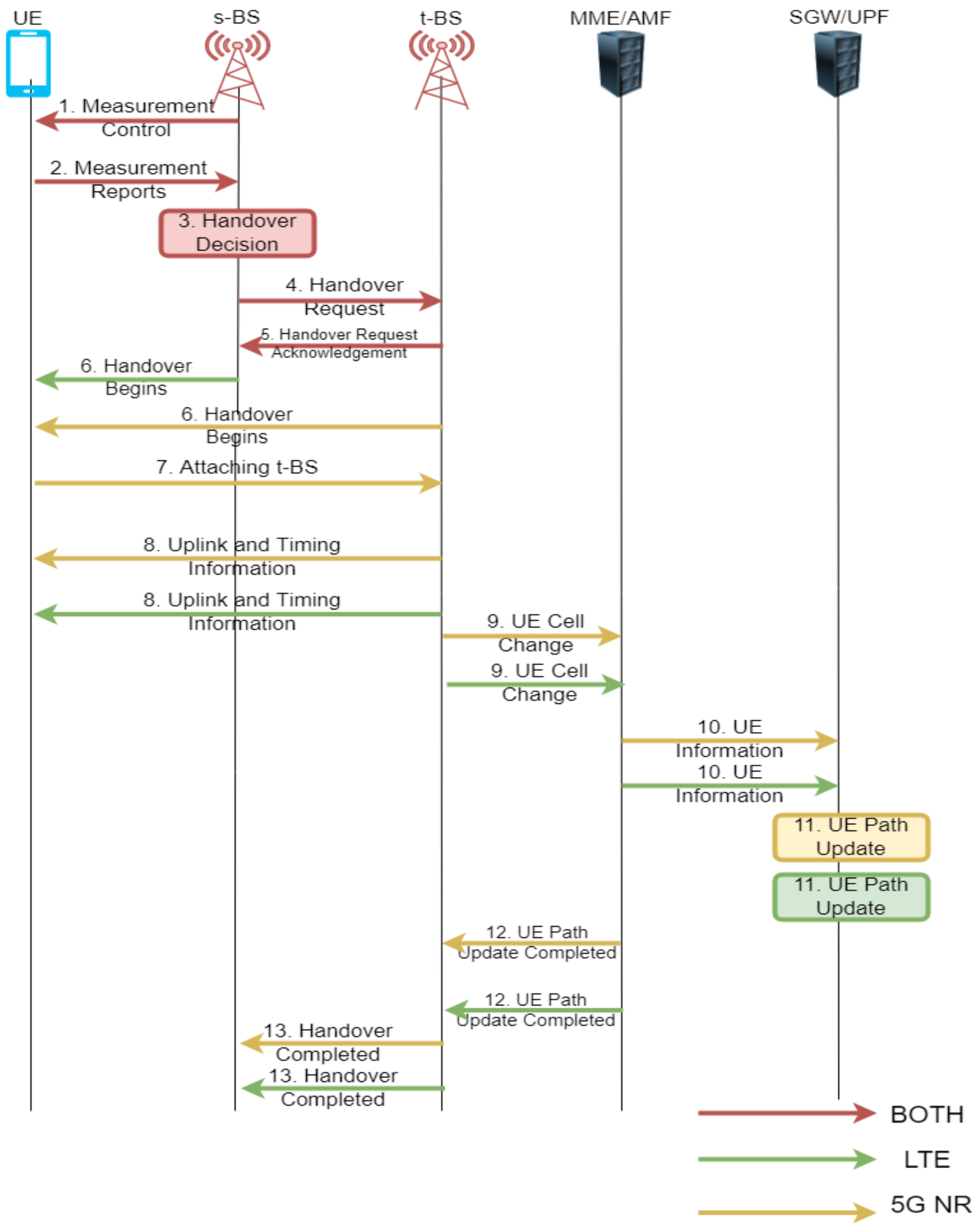

Figure 3.2 : Handover in LTE and 5G NR.

13. The *t-BS* informs the *s-BS* for the completion of the handover.

3.4 Handover Management in 5G New Radio

The handover procedure for 5G NR is almost the same with LTE with little changes. Access and mobility management function (AMF) executes the duties of MME, while the user plane function (UPF) is the same as SGW.

The handover steps are listed as:

1. The UE measurement procedure is configured by the *s-BS*.
2. The UE sends MR to the *s-BS*.
3. According to the report, the *s-BS* makes a handover decision.
4. The *s-BS* sends a handover request to the *t-BS*.
5. The *t-BS* sends an acknowledgment to the *s-BS* according to its resources.
6. The *s-BS* sends a handover command to the UE.
7. The UE attaches to the target cell.
8. The *t-BS* sends uplink allocation and timing information to the UE.
9. The *t-BS* informs the AMF for UE cell change.
10. AMF informs UPF for UE.
11. UPF updates the path for UE.
12. AMF informs the *t-BS* for path update.
13. The *t-BS* informs the *s-BS* for the completion of the handover.

3.5 Key Hierarchy and Key Exchange for Handover in 5G NR

It is crucial to understand the key generation process in 5G NR in order to explain the key exchange between the base stations in the handover phase. The key generation steps are depicted in Figure 3.3. In the second chapter, it is presented that the UDM computes an encryption key (CK) and integrity key (IK) from 128 bit long term key and a random value. In addition, the UDM generates a security key K_{AuSF} for AuSF by computing HMACSHA256 key derivation function. The key is the concatenation of CK and IK and the message is the concatenation of the serving name and sequence number for the HMACSHA256 algorithm.

The K_{AuSF} is shared with AuSF to derive other keys from it [26, 60]. The AuSF generates a security key K_{SEAF} for the security anchor function (SEAF) by computing

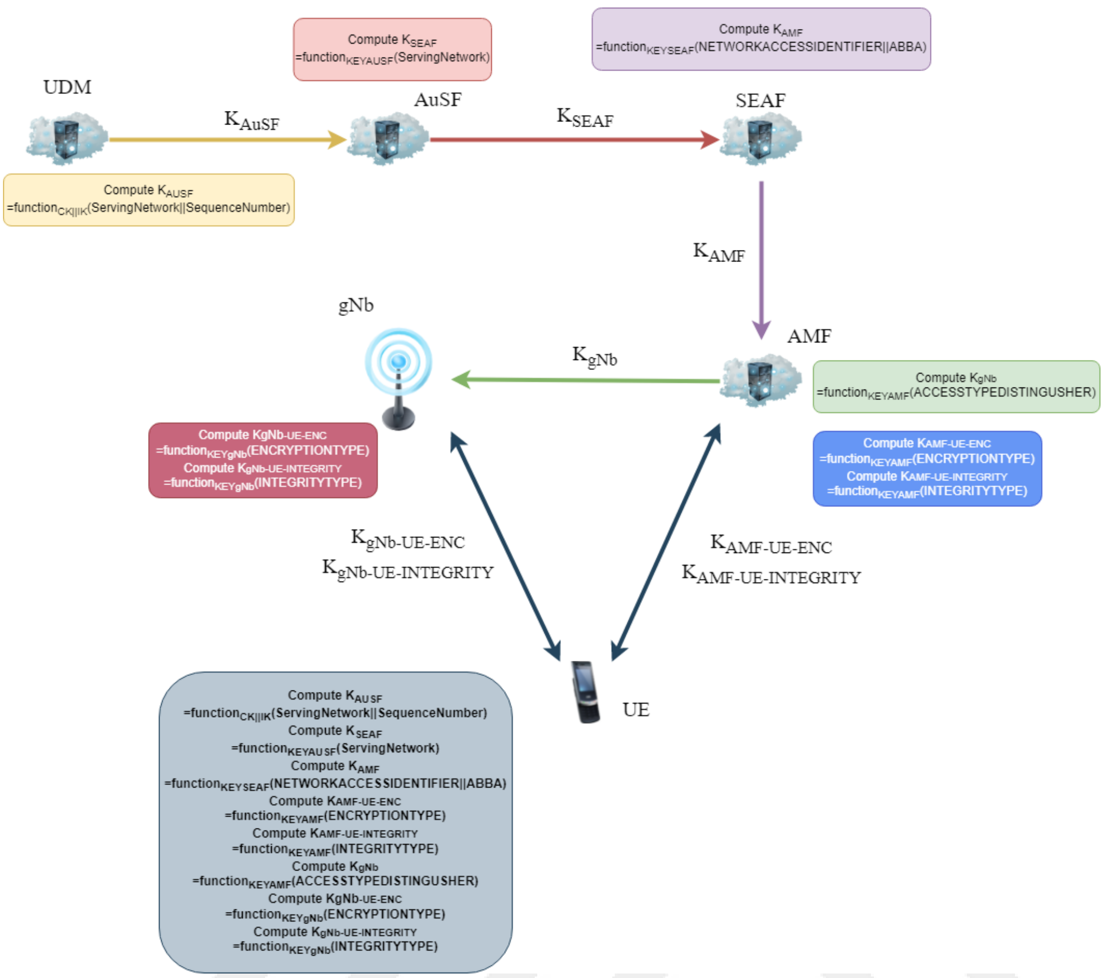
Compute K_{SEAF}
$=\text{function}_{KEYAUSF}$(ServingNetwork)
Compute K_{AMF}
$=\text{function}_{KEYSEAF}$(NETWORKACCESSIDENTIFIER||ABBA)
UDM
K_{AuSF}
AuSF
K_{SEAF}
SEAF
Compute K_{AUSF}
$=\text{function}_{CK|||K}$(ServingNetwork||SequenceNumber)
K_{AMF}
gNb
AMF
K_{gNb}
Compute K_{gNb}
$=\text{function}_{KEYAMF}$(ACCESSTYPEDISTINGUSHER)
Compute KgNb-UE-ENC
$=\text{function}_{KEYgNb}$(ENCRYPTIONTYPE)
Compute $K_{gNb\text{-}UE\text{-}INTEGRITY}$
$=\text{function}_{KEYgNb}$(INTEGRITYTYPE)
Compute KAMF-UE-ENC
$=\text{function}_{KEYAMF}$(ENCRYPTIONTYPE)
Compute KAMF-UE-INTEGRITY
$=\text{function}_{KEYAMF}$(INTEGRITYTYPE)
$K_{gNb\text{-}UE\text{-}ENC}$
$K_{gNb\text{-}UE\text{-}INTEGRITY}$
$K_{AMF\text{-}UE\text{-}ENC}$
$K_{AMF\text{-}UE\text{-}INTEGRITY}$
Compute K_{AUSF}
$=\text{function}_{CK|||K}$(ServingNetwork||SequenceNumber)
Compute K_{SEAF}
$=\text{function}_{KEYAUSF}$(ServingNetwork)
Compute K_{AMF}
$=\text{function}_{KEYSEAF}$(NETWORKACCESSIDENTIFIER||ABBA)
Compute KAMF-UE-ENC
$=\text{function}_{KEYAMF}$(ENCRYPTIONTYPE)
Compute KAMF-UE-INTEGRITY
$=\text{function}_{KEYAMF}$(INTEGRITYTYPE)
Compute K_{gNb}
$=\text{function}_{KEYAMF}$(ACCESSTYPEDISTINGUSHER)
Compute KgNb-UE-ENC
$=\text{function}_{KEYgNb}$(ENCRYPTIONTYPE)
Compute $K_{gNb\text{-}UE\text{-}INTEGRITY}$
$=\text{function}_{KEYgNb}$(INTEGRITYTYPE)
UE

Figure 3.3 : Key Generation in 5G NR.

HMACSHA256 key derivation function. The key is the K_{AuSF} and the message is the serving network for the HMACSHA256 algorithm.

The K_{SEAF} is shared with SEAF to derive other keys from it. The SEAF generates a security key K_{AMF} for the AMF by computing HMACSHA256 key derivation function. The key is the K_{SEAF} and the message is the concatenation of predetermined network access identifier and ABBA parameter for the HMACSHA256 algorithm. These parameters to derive the K_{AMF} are known by SEAF and UE.

The K_{AMF} is shared with AMF to derive other keys from it. The UE may generate the security keys CK, IK, K_{AuSF}, K_{SEAF}, K_{AMF} since the UE has random value and 128 bit long term key. The following step for the key hierarchy is to derive the encryption and integrity keys between AMF and UE in order to build a secure channel. The AMF and UE generate encryption and integrity key by computing a HMACSHA256 key derivation function whose key is the K_{AMF} and input is algorithm type distinguisher. The algorithm type distinguisher is different to generate encryption and integrity keys.

The security key for gNb K_{gNb} is generated by UE and AMF. The key is the K_{AMF} and the input is the access type distinguisher for the HMACSHA256 key derivation function. The K_{gNb} is shared with gNb. The gNb and UE generate encryption and integrity key by computing a HMACSHA256 key derivation function whose key is the K_{gNb} and input is algorithm type distinguisher. The algorithm type distinguisher is different to generate encryption and integrity keys. The key derivation process is achieved for 5G NR and the UE has a secure channel with gNb.

Once the handover decision is taken by the *s-BS*, *t-BS* and UE don't perform the same key derivation steps from the beginning. The *s-BS* computes the next BS key value K_{gNB*} by using K_{gNB} as a key and the target physical cell id of *t-BS* as input for HMACSHA256 key derivation function. The new integrity and encryption keys for secure communication between UE and the *t-BS* are derived from K_{gNB*}. The UE also can compute K_{gNB*}, since the UE has K_{gNB} and the target physical cell id of *t-BS*. Then, the UE can compute the new encryption keys and message authentication codes (MAC) for further communications with *t-BS*.

3.6 An Authentication and Handover Scheme for Capacity Injection

An UxNB, which is responsible for capacity injection, should be authenticated by the closest terrestrial BS in order to assume the emerging UxNB is legitimate. After succeeding authentication, the handover of UEs, which are in the range of UxNB, must be fulfilled from terrestrial to UxNB. Before authentication of UxNB, we assume that terrestrial BS with UEs in certain range formed a group and a group authentication was carried out as in the second chapter. Consequently, the terrestrial BS has a polynomisl $p(x)$, which is private and only known by the terrestrial BS, and UDM. The UDM must have a table which stores the identity of terrestrial BSs with their corresponding private function. In addition, after a successful group authentication, each UE in the range of terrestrial BS has a private value $p(x_i)$ and public values $(x_i, p(x_i)P)$. The i is the identity of UE, and P is the generator in the elliptic group, which is used to keep $p(x_i)$ private by powering operation in the elliptic curve group. The UDM stores the private values of UEs in the database as well. To authenticate the new emerging UxNB, the work sequence at below should be followed.

3.6.1 Authentication of emerging UxNB for capacity injection and group handover

The drone control station assigns private key $p(x_{UxNB})$ and public key pairs $(x_{UxNB}, p(x_{UxNB})P)$ which did not designate any other UE to the UxNB by coordination with UDM. Once UxNB is the range of terrestrial BS, UxNB transmit x_{UxNB} and $p(x_{UxNB})P$ pairs to terrestrial BS. Afterward, terrestrial BS verifies the pairs by using the private polynomial $p(x)$. Finally, if the UxNB is legitimate, $p(x)$ is shared with UxNB. Both terrestrial BS and UxNB have the private key $p(x_{UxNB})$ of UxNB. By a symmetric key encryption method, the polynomial $p(x)$ can be encrypted and sent securely to the UxNB by terrestrial BS.

After accomplishing of authentication of UxNB, BSs can communicate with each other confidently by a symmetric key encryption. After successful authentication of UxNB, group handover can be performed anytime needed. UEs send their public values $(x_{UxNB}, p(x_{UxNB})P)$ to UxNB and UxNB confirms UEs. The work sequence for group handover should be followed, as detailed below:

Each UE sends its public value $(x_i, p(x_i)P)$ to the UxNB. UxNB performs addition operation for each $p(x_i)$ and $p(x_i)P$ separately. At the end of the additional computation, the total $p(x_i)$ value is multiplied by the generator P. If the result is equal to the total $p(x_i)P$ value, all UEs are valid. Otherwise, the UEs are verified one by one. After successful control, UxNB begins to provide service for UEs. All requests from UE to UxNB are going to be encrypted by the private key $p(x_i)$ of UE, and also x_i value should be appended to all data.

3.6.2 Computational and communication complexity

The proposed scheme consists of two stages. In the first stage, the UxNB authentication stage, UxNB sends the public key pair $(x_{UxNB}, p(x_{UxNB})P)$ to the terrestrial BS in the first transmission. In the second transmission, the terrestrial BS sends acknowledgment to the UxNB for each UxNB. Therefore the communication complexity of the first stage is proportional to the number of emerging UxNB (x). The terrestrial BS performs one powering operation in the elliptic curve group $(p(x_{UxNB})P)$ for each UxNB in order to compare the value sent by UxNB.

Table 3.1 : Computational and Communication Complexity.

Stage	**Computational Complexity**	**Communication Complexity**
UxNB Authentication	x ECP	$2x$
Group Handover	y A, y ECA , 1 ECP	$1y$

In the second stage, the group handover stage, UE sends its public key pair $(x_i, p(x_i)P)$ to the UxNB. Communication complexity is proportional to the number of UEs (y). UxNB performs one addition operation $(TotalX + p(x_i))$ and one elliptic curve addition operation $(TotalPoint + p(x_i)P)$ for each UE, and one powering operation in the elliptic curve group to compare the end result as reported in Table 3.1.

3.6.3 Comparison of LTE and proposed handover solutions

The main objectives in this section are to show the importance of capacity injection for QoS and compare the handover time and the number of control packet transmissions in group handover. The Simu5G [61] library built on top of the Omnet++ package version 5.5.1 and INET framework are used to simulate handover operations. The most complex LTE scenarios can be simulated in SimuLTE in accordance with the 3GPP Release 16 [56]. The simulation framework exploits the layer base structured environment, and the handover process is accomplished mostly by the physical layer. Further, the X_2 link between BSs and protocols are well-designed and implemented by SimuLTE.

The main difference between the proposed scheme and LTE handover solution is that there is no data sharing between BSs in proposed scheme . Therefore, the X_2 interface parameters should be taken into consideration carefully while performing simulation. Ethernet connection is used for the X_2 interface in SimuLTE simulation environment. Ethernet connection capacity is selected as 10 Gbps for the simulations. With this connection capacity, data transfer between base stations is completed in 100 ns. Different configuration settings can be seen in Table 3.2. Other simulation parameters are selected as default parameters provided by SimuLTE.

Table 3.2 : Data Transfer Time between BSs.

X_2 **Ethernet Type**	**Data Transfer Time**
10 Gbps	100 ns
1 Gbps	522 ns
100 Mbps	14170 ns
10 Mbps	57250 ns

In the simulations, there are two BSs, core network and the UEs whose number can be changed to figure out handover time and the number of transmissions. UEs are placed at a point between BSs where the handover operation will begin in order to figure out the actual handover time. In the ready-made LTE handover simulations on SimuLTE, the UE sends the handover begining warning to the *s-BS* and the *s-BS* sends the UE information to the *t-BS*. The *t-BS* responds with acknowledgment. After the *t-BS* informs the core network about path switching, the handover process is completed. In the presented scheme, the UE starts the handover process with the *t-BS*. The *t-BS* informs the core network and *s-BS* after authentication control. The distance between the BSs is the same for both environments, and the transmission power for BSs and UEs are left at the SimuLTE default values. The time for the UE to initiate the handover operation with the *t-BS* and the *t-BS* to inform the core network is the same for both simulations. Data transfer time between BSs is the main difference between the two simulations.

According to the simulated scenario, a terrestrial BS provides service to UEs inside a high capacity football stadium. Due to the excessive number of UEs, the BS cannot provide the desired QoS. More than one UxNB is sent to the zone throughout the game for capacity injection. According to the scenario, it is necessary to authenticate UxNBs and to handover UEs from terrestrial BS to the nearest UxNB.

In parallel with the technological advancements in mobile networks, the peak data rates of downlink and uplink increase. While the average downlink value provided today in LTE technology is 100 megabits per second (Mbps), the uplink value has been 50 Mbps [62]. A BS that encounters a request above this uplink and downlink threshold values will start dropping packets. As a result, there will be a decrease in the QoS values, which are determined by the service provider.

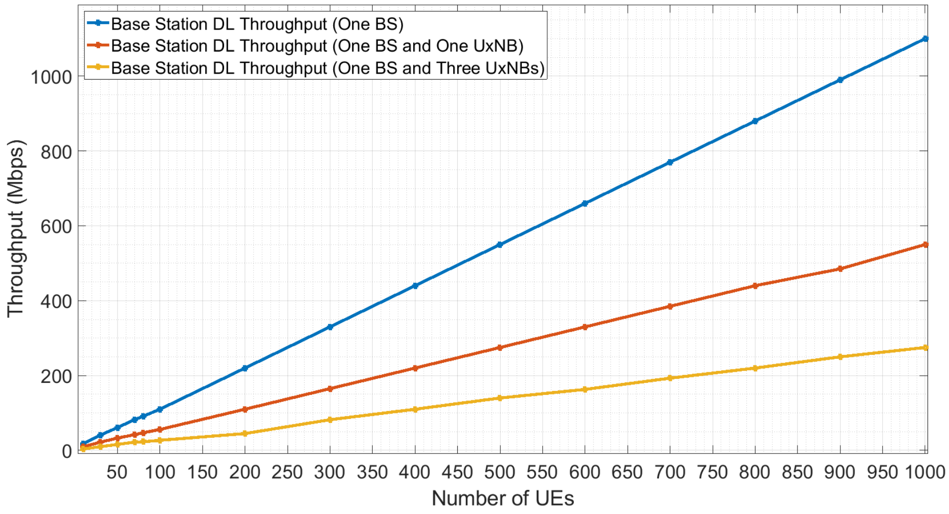

Figure 3.4 : Base station throughput per UE.

It is expected that the number of IoT devices connected to the network will reach 60 billion in 2022 [63]. The increase in the number of end devices will also cause increase in the number of groups. Therefore, high-density areas will be encountered more frequently. In high-density areas, such as stadiums, the downlink value will typically be high. In the simulations, it is simulated that UEs request service to watch a video simultaneously. According to the simulations implemented by SimuLTE, as the number of UEs increases, the required downlink value also increases, as shown in Figure 3.4. For example, the request created by 100 UEs at the same time creates an downlink value of 110 Mbps for the BS. Only 100 UEs can consume all the downlink limit for one terrestrial BS if they all watch video simultaneously.

As can be seen, it is not possible to provide service with only one BS in crowded environments. The use of UxNB emerges as a promising solution. Another question at this point is how many UxNBs on average can be sufficient to cover a stadium. According to the study [64], the downlink value for UxNB is 160 Mbps, a typical flight height of 150 m. The solution will need one UxNB for approximately 10 UE. Using too much UxNBs will cause several handover processes. Therefore, a group handover is a promising solution for presented scenario.

The latency is one of the main issues in the handover schemes. If the latency is high in the communications, the quality of service dedicated by providers will be low. The time used up in the handover process, and the number of control packet transmissions

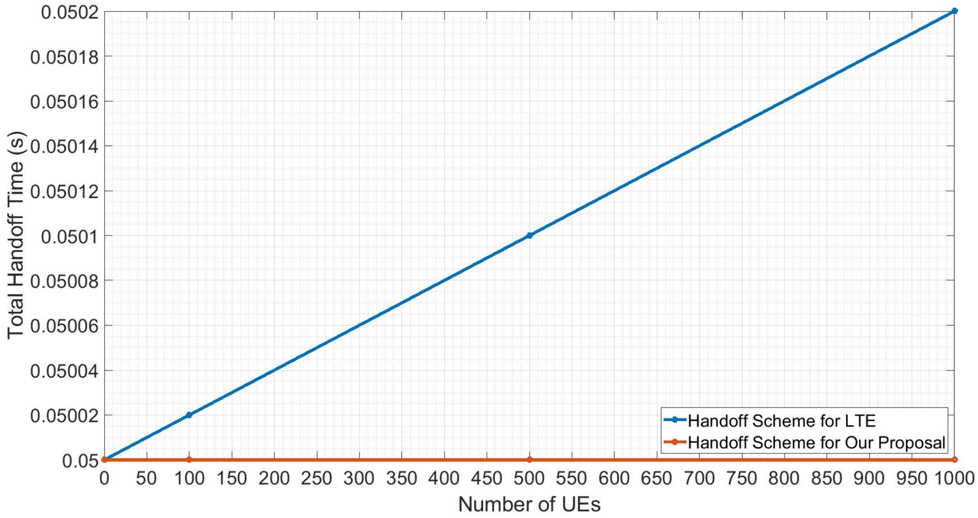

Figure 3.5 : The comparison of handover time.

between UEs and BS bring along the latency for handover. Recall that in presented scenario several UEs in a football stadium will switch their access network from a terrestrial BS to an UxNB. The pre-designed scheme in SimuLTE, in accordance with standards are exploited to simulate the LTE handover scheme. Some of the codes are reconfigured in the LTE scheme in order to attain statistical information about total handover time and the number of control packet transmissions created by BS and UEs.

As given in Figure 3.5, the total handover time is increasing in the LTE scheme when the number of UEs surges. The *s-BS* should send user-related data for each UE to the *t-BS* according to the standards. Hence, the communication between BSs is proportional to the number of UEs, as in Figure 3.6. Each UE is linked with the core network to update handover parameters, and six transmissions from UE to the core network is a fixed value in both standards and proposed scheme. The most energy-consuming transmissions occurs between BSs.

As seen in Figure 3.5, the number of UEs is not affecting the total handover time of proposed handover solution. Because a group handover scheme is performed by the *t-BS*. The *t-BS* collects public values of UEs and compares the received values with values produced by the private function. The number of control packet transmissions for proposed scheme is in Figure 3.6. The control packet transmissions per UE is still six as in standards. Because the UE must update handover parameters with the core network. The advantage of proposed scheme on the LTE is the communication between BSs being zero. The *t-BS* can handle authentication of UEs by confirming their public keys without the requirement of communication with the *s-BS*.

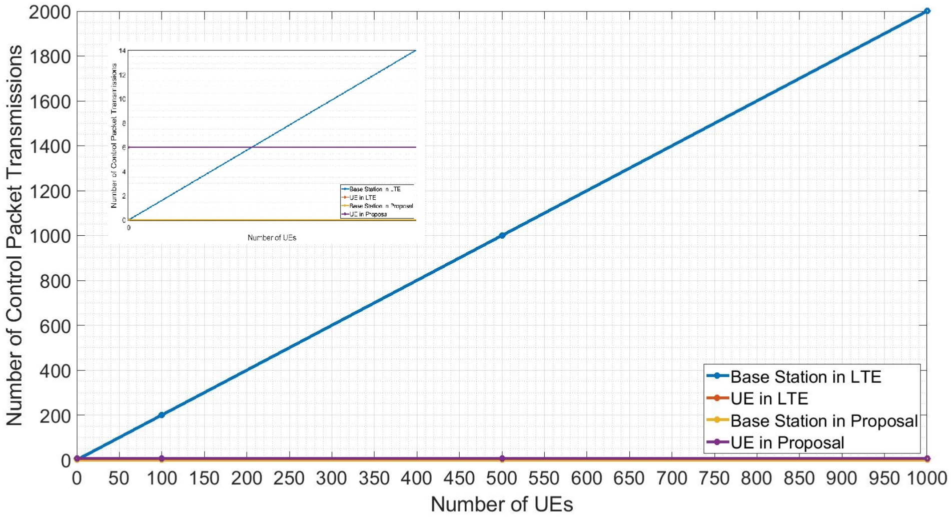

Figure 3.6 : Total number of control packet transmissions.

Both in TS 36.300 [56] and proposed scheme, the number of control packet transmissions for path switching per UE is six. The reason behind that is the UE contacts with the core network six times to transfer the new connection parameters for the *t-BS*.

In release-16 [56], the *s-BS* sends the connection information for related UE to the *t-BS*. Each connection between the *s-BS* and the *t-BS* has an acknowledgment message to endorse the receiving of the data. At the end of the handover process, the *t-BS* informs the *s-BS* for completing the handover. Hence, the total number of control packet transmissions by the *s-BS* or the *t-BS* is twice the number of UEs.

In proposed scheme, the communication between the *s-BS* and the *t-BS* is not performed. The *t-BS* gets the secret $p(x)$ function, which the key factor for the confirmation, when the *t-BS* becomes active. The *s-BS* (terrestrial) authenticates the *t-BS* (UxNB) when the *t-BS* become active at the football stadium. Once authentication is confirmed, the *s-BS* shares the secret function with the *t-BS*. In the handover process, the *t-BS* performs the confirmation by using the private function. The relevant UE sends the public keys $(x_i, p(x_i)P)$ to the *t-BS*. The *t-BS* performs addition for each x_i value and elliptic curve addition for each $p(x_i)P$ value. Once all the UEs in the group send public values, the *t-BS* compares the total x_i and total $p(x_i)P$.

The total handover time for LTE and proposed scheme is compared, the surge of the number of UEs does not change the total handover time in proposed scheme. However, the handover time is proportional to the number of UEs in standards. The reason for that is the communication between the *s-BS* and the *t-BS* getting increased if the number of UEs is too much.

According to the simulation results, the time for one control packet transmission between BSs is approximately 100 nanoseconds. The *s-BS* sends one packet to the *t-BS* for indicating information and receives one packet from the *t-BS* for the acknowledgment. The total time to send one UE data from the *s-BS* to the *t-BS* is 200 nanoseconds. 0.05 seconds is the standard time for both proposed scheme and LTE standard. This time slot is required to start the handover process by UE and to update the core network about cell change. The reason for the change in handover time in LTE is data sharing between BSs. The data sharing process for one UE is 200 nanoseconds, it is 0.2 milliseconds for 1000 UEs, and this value increases linearly as the number of UEs increases, as shown in Figure 3.5.

3.6.4 Time analysis of 5G NR and proposed UxNB authentication solutions

The time analysis for the algorithmic operations and data transmissions both in 5G NR and proposed UxNB authentication solutions is presented in this subsection. The time to authenticate a UE with the 5G NR authentication solution is 33 ms as described in the second chapter.

Table 3.3 : Time Analysis for The Proposed UxNB Authentication Scheme.

Operation	Entity	Time
Public Key Sharing with Terrestrial BS	UxNB	600 μs
Elliptic Curve Multiplication	Terrestrial BS	612 μs
Symmetric Key Encryption	Terrestrial BS	161 μs
Encrypted Secret Polynomial Sharing with UxNB	Terrestrial BS	600 μs
Symmetric Key Encryption	UxNB	161 μs
Total Handover Time	Total	2.2 ms

In the proposed scheme, the UxNB consumes one transmission to transfer the public key to the terrestrial BS. The terrestrial BS computes one elliptic curve multiplication to verify the public key. If the key is valid, the terrestrial BS consumes one symmetric key encryption to encrypt the secret polynomial. The encrypted polynomial is sent to the UxNB. The UxNB performs decryption to complete the authentication. In total, 2.2 ms is required for the authentication of UxNB as seen in Table 3.3, which is a more reasonable time than 5G NR.

3.6.5 Time analysis of 5G NR and proposed handover solutions

The time analysis for the algorithmic operations and data transmissions both in 5G NR and proposed handover solutions is presented in this subsection. The *s-BS* computes one HMACSHA256 key derivation function to generate the new security key. The new security key is shipped to the *t-BS* and the *t-BS* sends back an acknowledgment message. The *t-BS* and UE compute the encryption and integrity keys to set a secure communication channel between them. Two key derivation functions are needed to create new keys. In total, three HMACSHA256 and two transmissions between BSs, whose time complexiy is a total of $(202m)$ μs (m denotes the number of UEs), is needed to complete handover for 5G NR as shown in Table 3.4.

Table 3.4 : Time Analysis for The 5G NR Handover Scheme.

Operation	Entity	Time
Security Key Derivation Function	*s-BS*	$67m$ μs
Security Key Sharing	*s-BS*	$0.1m$ μs
Acknowledgment Response	*t-BS*	$0.1m$ μs
Encryption Key Derivation Function	*t-BS*, UE	$67m$ μs
Integrity Key Derivation Function	*t-BS*, UE	$67m$ μs
Total Handover Time	Total	$(202m)$ μs

The *t-BS* computes one elliptic curve addition for each public key of UE and at the end of obtaining all public keys, one elliptic curve multiplication operation is required to compare the result for the handover. In total, $(125m+612)$ μs is needed to complete the handover as seen in Table 3.5.

Table 3.5 : Time Analysis for The Proposed Group Handover Scheme.

Operation	Entity	Time
Elliptic Curve Addition Operation	*t-BS*	$125m$ μs
Elliptic Curve Multiplication Operation	*t-BS*	612 μs
Total Handover Time	Total	$(125m+612)$ μs

When the results are compared, the 5G NR handover solution provides more reasonable time complexity than the proposed scheme as long as the number of UEs requesting handover is less than 7. Once the number of UEs reaches 7, the proposed scheme begins to provide better time complexity.

3.7 Conclusion and Discussion

The limitations of using one terrestrial BS in an extremely-dense area are examined in the chapter. The QoS requirements may not be met by the service provider to the customers due to the considerable requests. The use of UxNB for the capacity injection is a solution for the cellular networks to decrease the burden on the terrestrial BS.

The consumption of bandwidth of a terrestrial BS in a dense area is simulated in this chapter. Approximately, one hundred UEs may devour all the bandwidth provided by BS if the UEs request to download a video from the internet. Each UxNB raises the bandwidth proportionally. The link between two terrestrial BS is currently using a wired channel, which has better transmission time than wireless channel. However, the link between a terrestrial BS and UxNB will be wireless and the transmission of security keys will take more time. A handover solution is presented in this chapter without sharing the security keys between BSs. Although capacity injection via UxNBs provides a promising solution to increase the bandwidth of a terrestrial BS, the handover between terrestrial BS and UxNB or between new and ex-UxNB may cost latency if the handover solution in 5G NR is used.

The main cause for the latency in 5G NR is the security key sharing for each UE between terrestrial BS and UxNB. The UxNB and UEs perform group authentication in the proposed handover method to eliminate the data sharing phase. Therefore, the handover time for 5G NR is increasing if the number of UEs requesting for handover is rising. The group authentication solution in the second chapter is utilized to present an authentication scheme between terrestrial and aerial BSs and a group handover method from terrestrial to aerial BS in this chapter. The next chapter contains also authentication and handover solutions based on the group authentication scheme in the second chapter. The schemes are used to cover security issues in drone swarms.

4. AUTHENTICATION AND HANDOVER FOR DRONE SWARMS

4.1 Introduction

The fourth chapter mainly concentrates on the authentication and handover necessities of the drone swarms. The requirements are given in the chapter with sample scenarios in order to describe the authentication and handover sufficiently.

The two-step UAV authentication in 5G NR is presented in detail before describing the proposed schemes. For each authentication and handover requirement, a novel group-based solution is proposed in the chapter. The 5G NR authentication and proposed authentication solution are simulated with the omnet++ to compare the authentication time. The chapter continues with the time analysis of the schemes. Overall results from the chapter and simulation are given in the conclusion section.

The use of drones for daily activities began with military purposes and now they are everywhere from border security to cargo delivery or visual shows. The more surface of the use of drones increases, the more intensity of the tasks becomes high. The tasks with limited time and a larger area can not be carried out with a single drone.

The drone swarms are the new solutions for completing the dense tasks. A group of drones may perform the tasks in a short period. In this chapter, the drone swarms are presented from the security point of view. The security aspects of the drone swarms are aligned under titles of five requirements.

The first requirement is the authentication of the drones requesting to join the swarm as shown in Figure 4.1. The number of a drone swarm may change according to the duration of the task. If the duration is more than the flying time of a drone, the drone reaching the end of the airtime should turn back to the base. Instead of the leaving drone, the new drones are sent to the swarm by the drone control station. The security issue at this point is the trust between the drones in the swarm and the new drone. The intruders may send an illegitimate drone to the swarm. The drone swarm may request

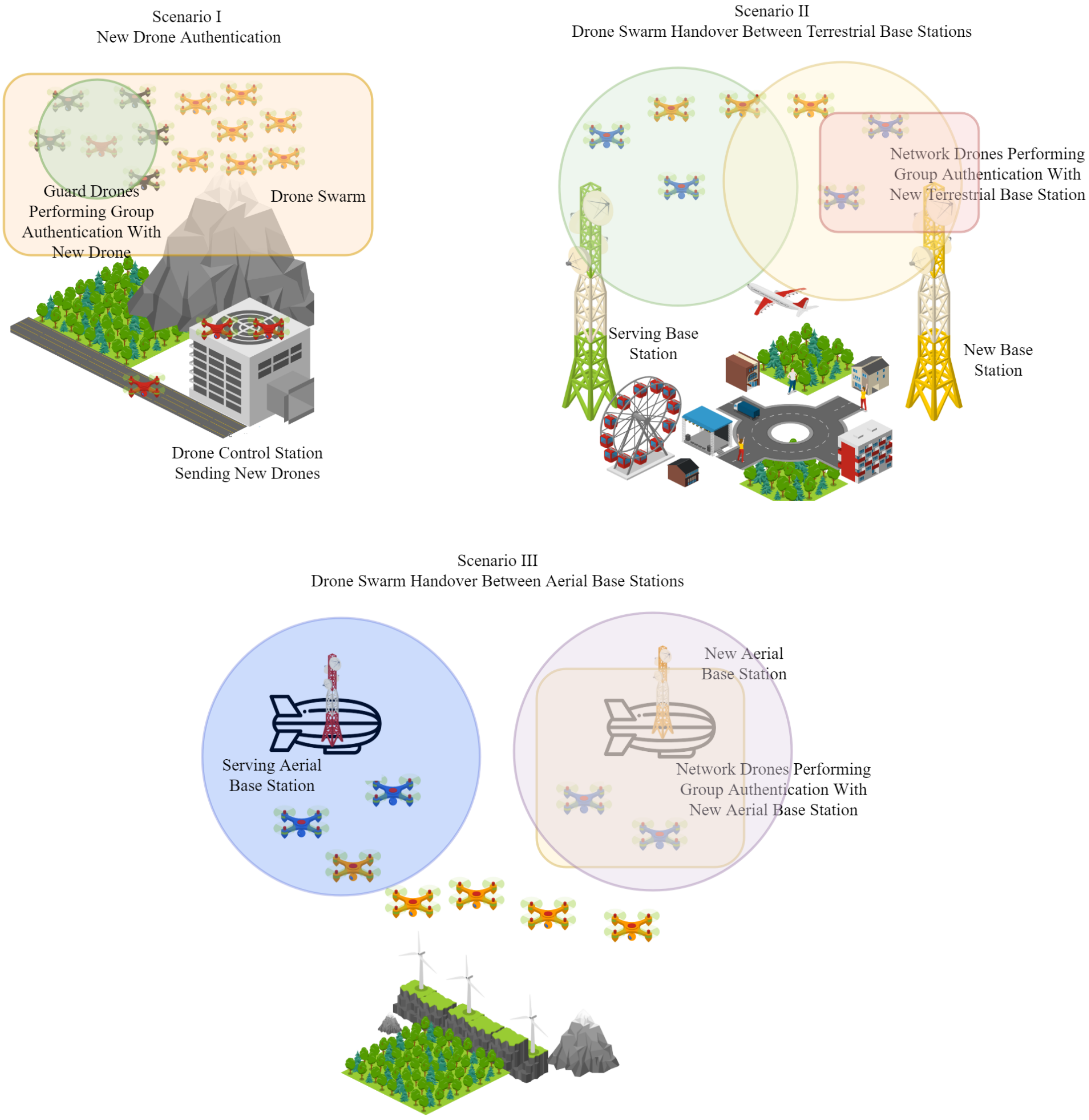
Scenario I
New Drone Authentication
Guard Drones Performing Group Authentication With New Drone
Drone Swarm
Drone Control Station Sending New Drones
Scenario II
Drone Swarm Handover Between Terrestrial Base Stations
Network Drones Performing Group Authentication With New Terrestrial Base Station
Serving Base Station
New Base Station
Scenario III
Drone Swarm Handover Between Aerial Base Stations
Serving Aerial Base Station
New Aerial Base Station
Network Drones Performing Group Authentication With New Aerial Base Station

Figure 4.1 : Authentication and Handover Scenarios for Drone Swarms.

authentication from the core network as explained in the second chapter for each drone joining the swarm. However, this solution costs time and resource for the swarms with limited time and resources. A lightweight authentication solution should be provided to the swarm.

The second security issue is the confidentiality of the messages between the drones in the swarm. The messages may contain sensitive information and be shared with the other drones in plaintext form. Due to the wireless nature of the channel between drones, the channel is vulnerable to sniffing attacks. The data within the swarm should be in ciphertext form. The encryption methods, which are symmetric and public-key encryption, change according to the structure of the key. Public key encryption is not the preferred one for resource-limited devices. Therefore, a key between parties should be agreed upon in order to encrypt and decrypt the messages. The best authentication solutions are the ones that establish a security key between parties after the authentication. A security group key should be agreed upon between the new drones and drones in the swarm after the authentication.

Another authentication requirement for the drone swarms is the authentication between the parties after the merger of two drone swarms. It is possible to combine two swarms to perform more intensive tasks. The issues are the scalability and the number of the permutation to complete the authentication process. If the primary authentication in 5G NR is used for each drone, the communications between parties and computations may be too much to complete the tasks. An authentication solution which save time and resources should be used for the merger of the two swarms.

Due to the mobility nature of the drones, the handover from one terrestrial BS to another is not inevitable for the drone swarms. The speed and scalability are the reasons not to use handover solution explained in the third chapter. A group of drones change their positions in a short time period. Sharing security keys between BSs and complete the steps required for the handover for each drone may not be possible. A new handover solution should be proposed for the drone swarms to overcome this issues.

The last security requirement for the drone swarms is the situation that the BS is also a UxNB. In some tasks especially rescue or disaster missions, the BS providing service for the drones may be a UxNB. Two handovers should be taken into consideration. The first one is the same handover issue for the terrestrial BSs. The second issue is the replacement of UxNB with a new one.

4.2 Challenges of Drone Swarms

Drone swarms have numerous advantages over a single drone. The first of these advantages is the reliability of the data transmitted to the ground control station. Instead of data from a single drone's sensor, the aggregation of data from more than one drone will provide more accurate results. Another reason to employ drone swarms is the network benefits. During a mission with a single drone, if the drone is stuck in a dead zone the connection between the drone and the control station will be lost. In a drone swarm structure, neighbor drones can deliver a network connection to the lost drone.

In addition to much innumerable usefulness, drone swarms also contain many challenges. The most significant issue among these challenges is drone authentication. Drones will frequently communicate with other drones in the swarm and ground control station. New drones will join the swarm and some drones will leave the swarm and return to the base [65]. Each of these phases requires independent identity verification. Security in drone swarms encompasses not only single drone security but also entire swarm security. While designing security solutions, it will not be practical to build solutions for only a single drone.

Another security challenge is the detection of fake drones in the swarm. In a dense swarm environment using a wireless channel, intrusion detection will be hard. The drones in the swarm will discover the intruders, not a central authority. Consequently, it will be essential to invent a distributed intrusion detection system to be employed by drone swarms. Group authentication scheme can contribute to the security of the entire swarm.

4.3 UAV Authentication in 3GPP

3GPP TR 33.854 study on security aspects of unmanned aerial system (UAS) [66] is the main document dealing with the security issues of UAVs. The key security issues for UAS are mentioned at the preliminary of the document and the corresponding solutions are given in the next section.

Authentication and authorization of the vehicles are the first security issue for the 3GPP Release-17. Two identification numbers are assigned to a UAV by the unmanned aerial system (UAS) service provider and the 3GPP core network. The civil aviation authority level identification number provides the ease of remote identification of a UAV in the air. UAVs utilize the 3GPP identification number when the services provided by the core network are accessed. The authentication of UAVs to provide 3GPP network services is accomplished with two phases. The usual new user equipment (UE) authentication process is performed between UAV and core network in the first

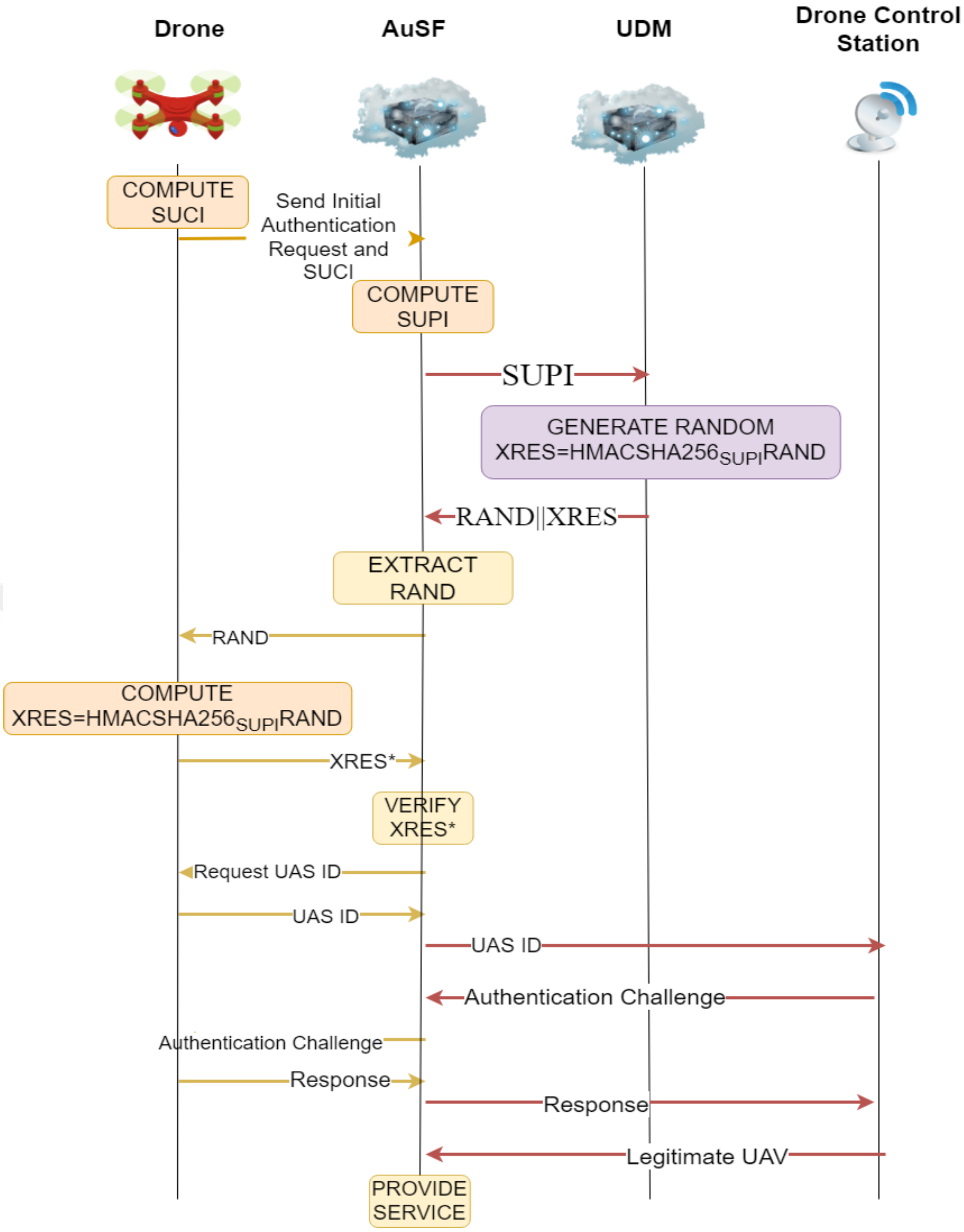

Figure 4.2 : UAV Authentication.

phase as shown in Figure 4.2. Once the UAV is authenticated by the core network, the UAV control station sends a challenge to the UAV to perform a second authentication. The end-to-end authentication solution between UAV and control station is not covered by the 3GPP standard. The solution is peculiar to the UAS service provider. The steps fo the authentication of a UAV are:

1. The UAV computes the subscription concealed identifier (SUCI) by encrypting the subscription permanent identifier (SUPI) with the base station (BS) public key.
2. The UAV sends the SUCI to BS.
3. The BS decrypts the SUCI and sends the SUPI to authentication server function (AuSF).
4. The AuSF shares the SUCI with unified data management (UDM).
5. The UDM generates a random value (RAND) and computes expected response (XRES) with SUCI and RAND.
6. The UDM sends back to AuSF the RAND and XRES.
7. The AuSF extracts the random value and shares it with the UAV.
8. The UAV computes XRES and sends it back to the AuSF.
9. If the AuSF confirms the identity of the UAV, UAS ID is requested from the UAV.
10. The UAV sends the UAS ID to AuSF.
11. The AuSF sends the ID to the control station.
12. The control station and UAV perform a second authentication.
13. After control station confirmation, the AuSF directs the BS to begin to provide 3GPP service to the UAV.

4.4 UAV Attacks

UAVs possess distinct use-cases spread from public safety operations to logistics. Commercial companies exploit the UAVs in agriculture, visual shows, and smart homes. Although the use-cases and technology of UAVs are developed, the security is not at the expected status.

Two UAVs are utilized for an assassination attempt on the President of Venezuela in 2018. The UAVs were loaded with explosives and guns. The event is an instance of the use of UAVs for terrorism purposes. The next terrorist action is the use of 10 UAVs to target oil facilities in Saudi Arabia. The UAVs initiated several fires in the facilities and the country shut down all their refineries, which cause the increase in oil prices all around the world. Without appropriate security preventions, the UAVs hold a huge amount of use-cases for the attacks.

There exist several types of attacks on UAVs. The jamming attacks contain the aim to interrupt the communication between the ground control station and UAV [67]. The attack is achieved by raising the noise in the UAV receiver. The attackers may assault the UAVs physically to seize the device. Once the device is captured, the forensics on the UAV may be performed to obtain security keys and to be utilized for the other type of attacks. Wireless communication between the ground control station and UAV is vulnerable to de-authentication attacks. The powerful signals are sent to the UAV to lock the connection to the ground control station in order to establish a new channel between the UAV and attacker.

Maldrone and SkyJack are two software malware to control UAVs by attackers. The researchers conducted reverse engineering on the Parrot AR drone software in order to build the malware Maldrone. Maldrone interrupts the traffic between the ground station and the UAV and injects the malicious codes into the communication to create a backdoor to the UAV. The control commands can be transmitted to the UAV by using the backdoor.

Denial of service attacks can be conducted via a wireless channel to force the UAV to land. A Parrot UAV is tested by sending fake connection requests as a ground control station. After 1000 requests, the UAV closed and began to land. A buffer overflow attack is executed by transmitting a large amount of data to the UAV. Again, the attack was successful and the Parrot UAV crashed. A reverse engineering attack is performed to find vulnerabilities in the Digi XBee 868LP radio frequency module for UAVs. The researcher discovered an API interface to inject commands to the UAV. In addition, the module includes a broadcast response that contains addresses of the UAV.

UAVs can be utilized as a fake access point or base station [68]. The access point controlled by an attacker can be mounted on the drones and sent to a public area. The service set identifier (SSID) name of the real access point is replicated by the fake access point. The real access point is neutralized by transmitting jamming signals to it, as well. The victim computers or smartphones begin to have service from a fake access point. The attacker can monitor the entire traffic and capture the personal and security information from the wireless traffic. Actually, fake drones can control neighbor drones in the same way.

4.5 Group Authentication and Handover Solutions for Drone Swarm

Proposed solutions for the authentication of a new drone joining to the swarm, the merger of two drone swarms, group handover method for the terrestrial BS handover, and aerial BS handover and the organization of the drone swarm are explained in detail in the section.

4.5.1 Organization of drone swarms

The drone swarm is divided into three types of drones as shown in Figure 4.3 not to make busy entire drones for the authentication and handover process. The group authentication and handover solutions in the previous chapters depend on the threshold value. A sub-group with members up to the threshold value may perform group authentication. Therefore, the drone swarm is divided into three types.

The first sub-group is the guard drones which are responsible for tracking the drones joining and leaving the swarm. The guard drones authenticate the new drones approaching the swarm in the air with the proposed group authentication solution. The network drones are the ones that perform all kinds of work about networking. The connectivity with the 3GPP network and handover operations are executed by the network drones. The last group is the service drones which perform the real services for the drone swarm.

4.5.2 Authentication of new drones by drone swarm

Each drone in the swarm has the group key to encrypt the messages before transmitting them to the other drones. The guard drones should authenticate the new parties willing to be part of the swarm and share the group key with the new party. The guard drones blocks the new drone in the air as shown in Figure 4.4 before the service drones and follows the steps below for authentication:

- The control station assign a private key ($p(x_{new})$) and public key pairs $(x_{new}, p(x_{new})P)$ to the new drone.

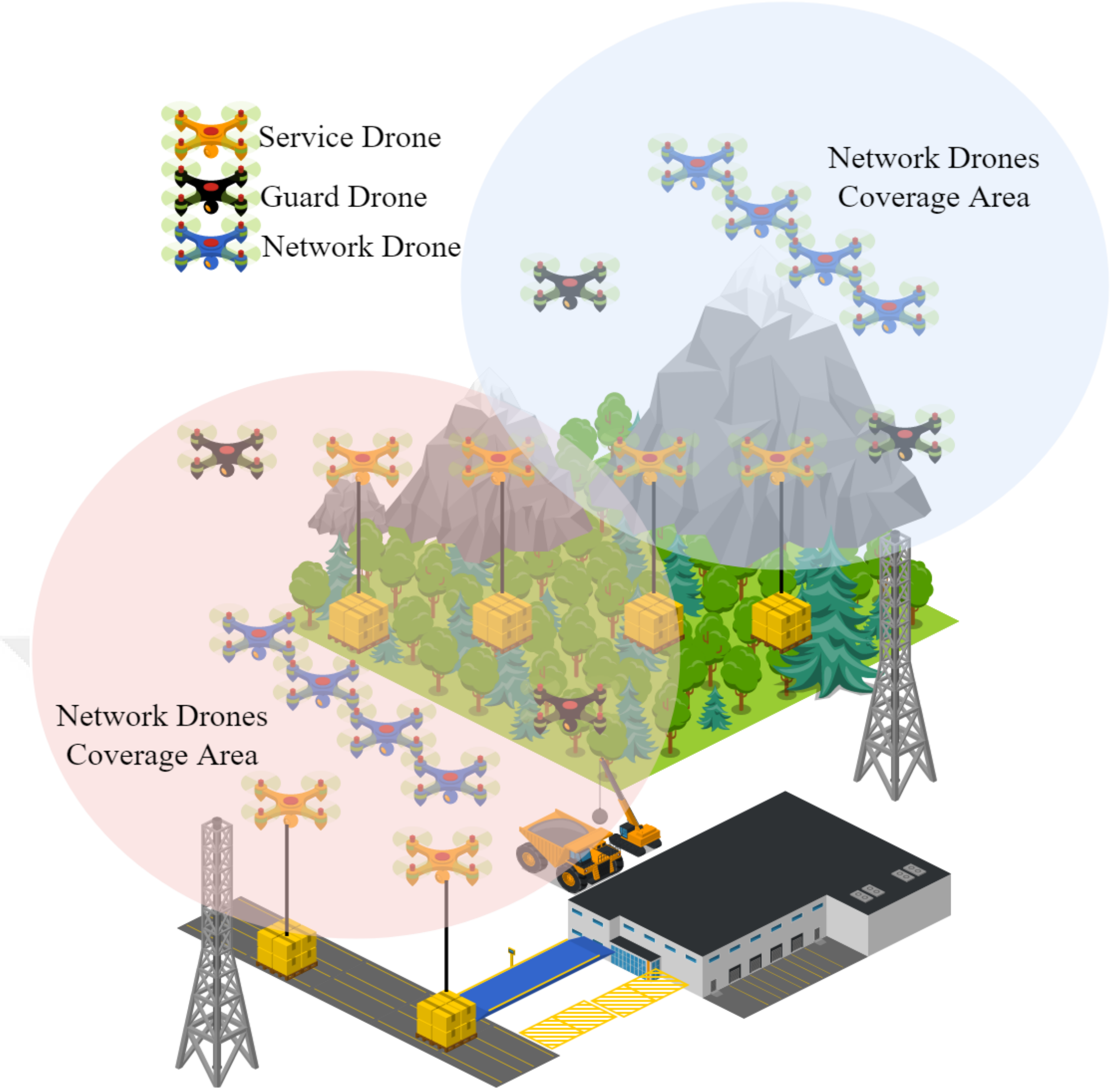

Figure 4.3 : Types of Drones in the Swarm.

- The keys are shared with the new drone and the new drone is sent to the drone swarm.
- The new drone shares the public key pairs with guard drones.
- The guard drones perform group authentication as in second chapter.
- If the authentication is valid, the pre-defined guard drone perform the key agreement step as in second chapter with the new drone.
- The group key is encrypted by the agreed key and sent to the new drone.
- If the authentication is not valid, the new drone is forced to leave the area by guard drones.

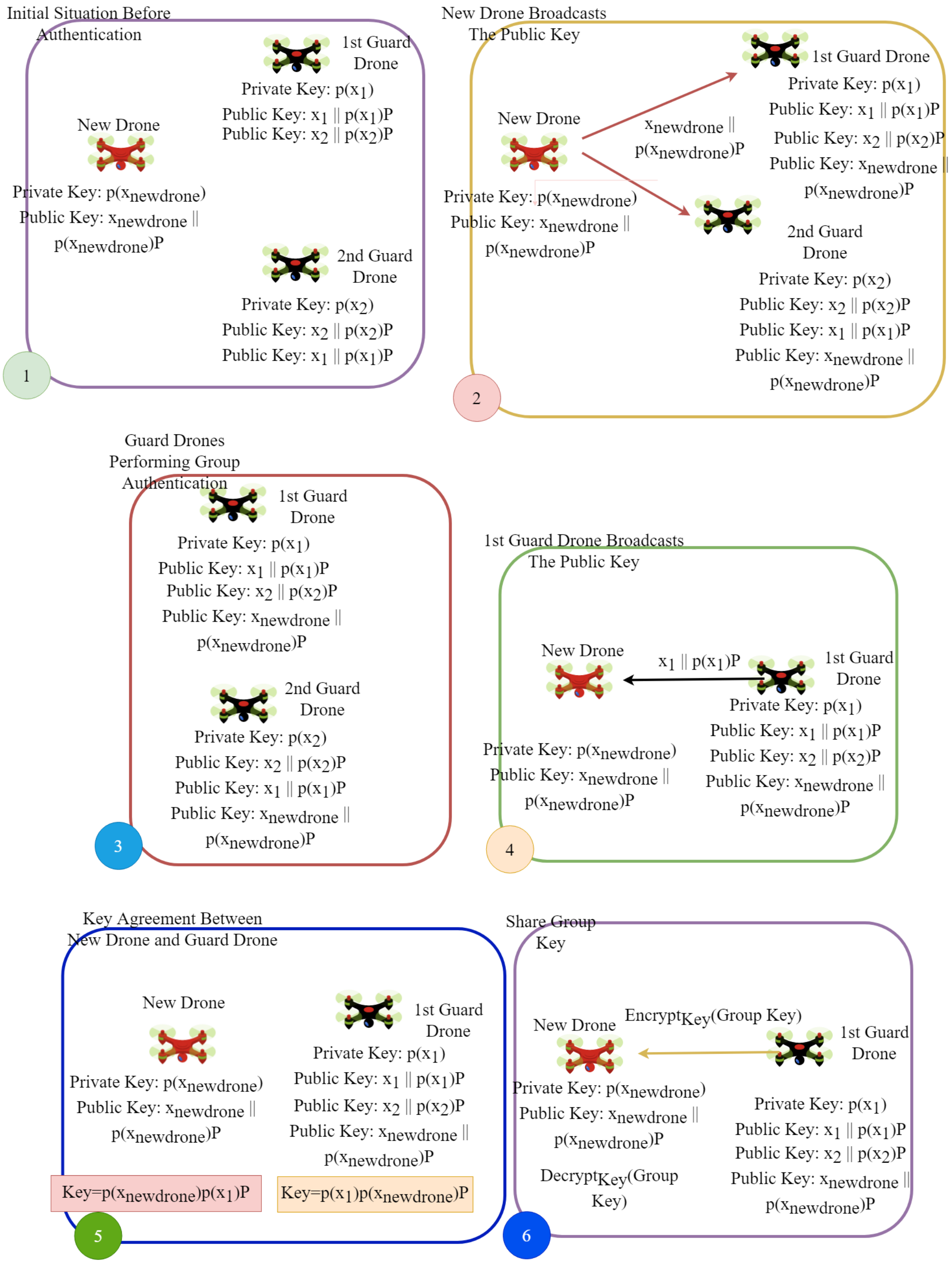
Initial Situation Before Authentication
1st Guard Drone
Private Key: $p(x_1)$
Public Key: $x_1 \| p(x_1)P$
Public Key: $x_2 \| p(x_2)P$
New Drone
Private Key: $p(x_{newdrone})$
Public Key: $x_{newdrone} \|$ $p(x_{newdrone})P$
2nd Guard Drone
Private Key: $p(x_2)$
Public Key: $x_2 \| p(x_2)P$
Public Key: $x_1 \| p(x_1)P$
1
New Drone Broadcasts The Public Key
1st Guard Drone
Private Key: $p(x_1)$
Public Key: $x_1 \| p(x_1)P$
Public Key: $x_2 \| p(x_2)P$
Public Key: $x_{newdrone} \|$ $p(x_{newdrone})P$
New Drone
$x_{newdrone} \|$ $p(x_{newdrone})P$
Private Key: $p(x_{newdrone})$
Public Key: $x_{newdrone} \|$ $p(x_{newdrone})P$
2nd Guard Drone
Private Key: $p(x_2)$
Public Key: $x_2 \| p(x_2)P$
Public Key: $x_1 \| p(x_1)P$
Public Key: $x_{newdrone} \|$ $p(x_{newdrone})P$
2
Guard Drones Performing Group Authentication
1st Guard Drone
Private Key: $p(x_1)$
Public Key: $x_1 \| p(x_1)P$
Public Key: $x_2 \| p(x_2)P$
Public Key: $x_{newdrone} \|$ $p(x_{newdrone})P$
2nd Guard Drone
Private Key: $p(x_2)$
Public Key: $x_2 \| p(x_2)P$
Public Key: $x_1 \| p(x_1)P$
Public Key: $x_{newdrone} \|$ $p(x_{newdrone})P$
3
1st Guard Drone Broadcasts The Public Key
New Drone
$x_1 \| p(x_1)P$
1st Guard Drone
Private Key: $p(x_1)$
Public Key: $x_1 \| p(x_1)P$
Public Key: $x_2 \| p(x_2)P$
Public Key: $x_{newdrone} \|$ $p(x_{newdrone})P$
Private Key: $p(x_{newdrone})$
Public Key: $x_{newdrone} \|$ $p(x_{newdrone})P$
4
Key Agreement Between New Drone and Guard Drone
New Drone
Private Key: $p(x_{newdrone})$
Public Key: $x_{newdrone} \|$ $p(x_{newdrone})P$
1st Guard Drone
Private Key: $p(x_1)$
Public Key: $x_1 \| p(x_1)P$
Public Key: $x_2 \| p(x_2)P$
Public Key: $x_{newdrone} \|$ $p(x_{newdrone})P$
Key=$p(x_{newdrone})p(x_1)P$
Key=$p(x_1)p(x_{newdrone})P$
5
Share Group Key
New Drone
$Encrypt_{Key}$(Group Key)
1st Guard Drone
Private Key: $p(x_{newdrone})$
Public Key: $x_{newdrone} \|$ $p(x_{newdrone})P$
$Decrypt_{Key}$(Group Key)
Private Key: $p(x_1)$
Public Key: $x_1 \| p(x_1)P$
Public Key: $x_2 \| p(x_2)P$
Public Key: $x_{newdrone} \|$ $p(x_{newdrone})P$
6

Figure 4.4 : New Drone Authentication.

4.5.3 The merger of two drone swarms

The two different drone swarms have different polynomials and keys. Each group performed group authentication as explained in the second chapter. Let us suppose the polynomial for the first swarm is $f(x)$ and for the second swarm is $g(x)$. Each parties in the first swarm has one unique private key $f(x_i)$ and public keys $(x_i, f(x_i)P)$. The private key for the second swarm is $g(x_i)$ and public key is $g(x_i)P$.

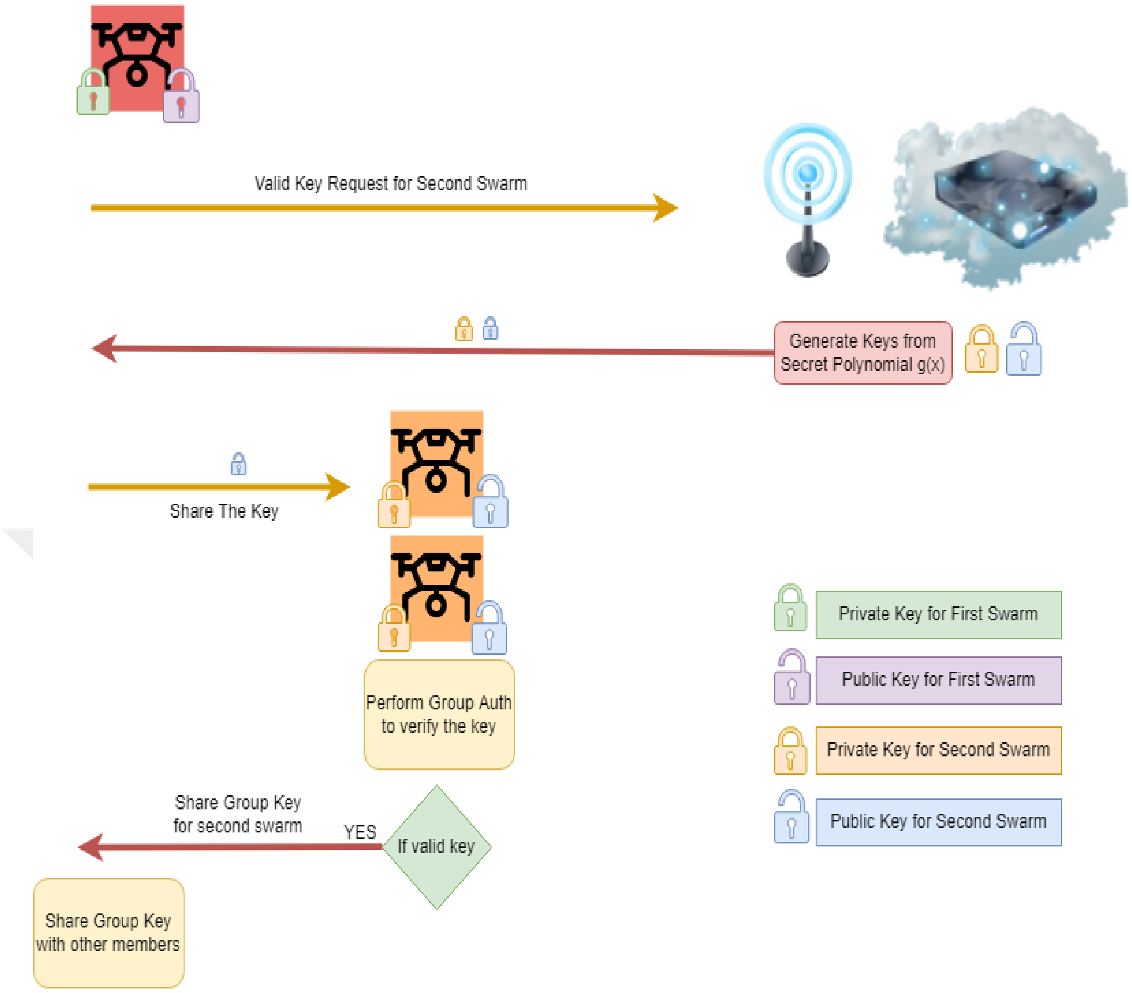
Valid Key Request for Second Swarm
Generate Keys from Secret Polynomial g(x)
Share The Key
Perform Group Auth to verify the key
Share Group Key for second swarm
YES
If valid key
Share Group Key with other members
Private Key for First Swarm
Public Key for First Swarm
Private Key for Second Swarm
Public Key for Second Swarm

Figure 4.5 : The Merger of Two Drone Swarms.

The merger of the swarms requires one group authentication operation. Let us suppose the threshold value is three. Three drones are enough to perform group authentication. Therefore, one guard drone from the first swarm and two guard drones from the second swarm may form a group to authenticate each other at the same time. The guard drones follow the steps in Figure 4.5.

- The guard drone from first swarm requests a new unique private key $g(x_i)$ and corresponding public key $(x_i, g(x_i)P)$ for the second swarm by sending the request to the 3GPP network.

- The authentication server in core network generate the keys from secret polynomial $g(x)$ for second swarm.

- The private and public keys are shared with the guard drone.
- The guard drone only shares the public key with the guard drones in the second swarm.
- Due to the fact that the threshold value is three, the guard drones may perform group authentication in the second swarm.
- If the group autehntication is valid, one guard drone from first swarm and one guard drone from second swarm may generate an encryption key by using their private keys $g(x_i), g(x_j)$.
- Once the encryption key is generated, the group key for the second swarm can be encrypted and shared with the guard drone from first swarm.
- The guard drone from first swarm may decrypt the group key and encrypt it again with the group key of first swarm.
- After encryption, the guard drone sends the new group key as broadcast message to the other group members.
- Once each group member obtains the new group key, two drone swarm may begin to communicate securely.

4.5.4 Terrestrial BS handover

The territory in which a drone swarm exists may change very speedily as shown in Figure 4.6. The movement of numerous drones taking service from one BS to the other area causes the handover loading on the s-BS and t-BS. In our proposed method, the network drones are responsible for the handover process. The number of network drones depends on the threshold value in second chapter. In order to perform the group authentication as in second chapter, the number of group members must be equal or greater than the threshold value. The network drones and BS create a group and perform group authentication. Therefore, the number of network drones must be one missing from the threshold value. The network drones and t-BS follow the steps below:

- The network drones share their public key pairs with the t-BS.

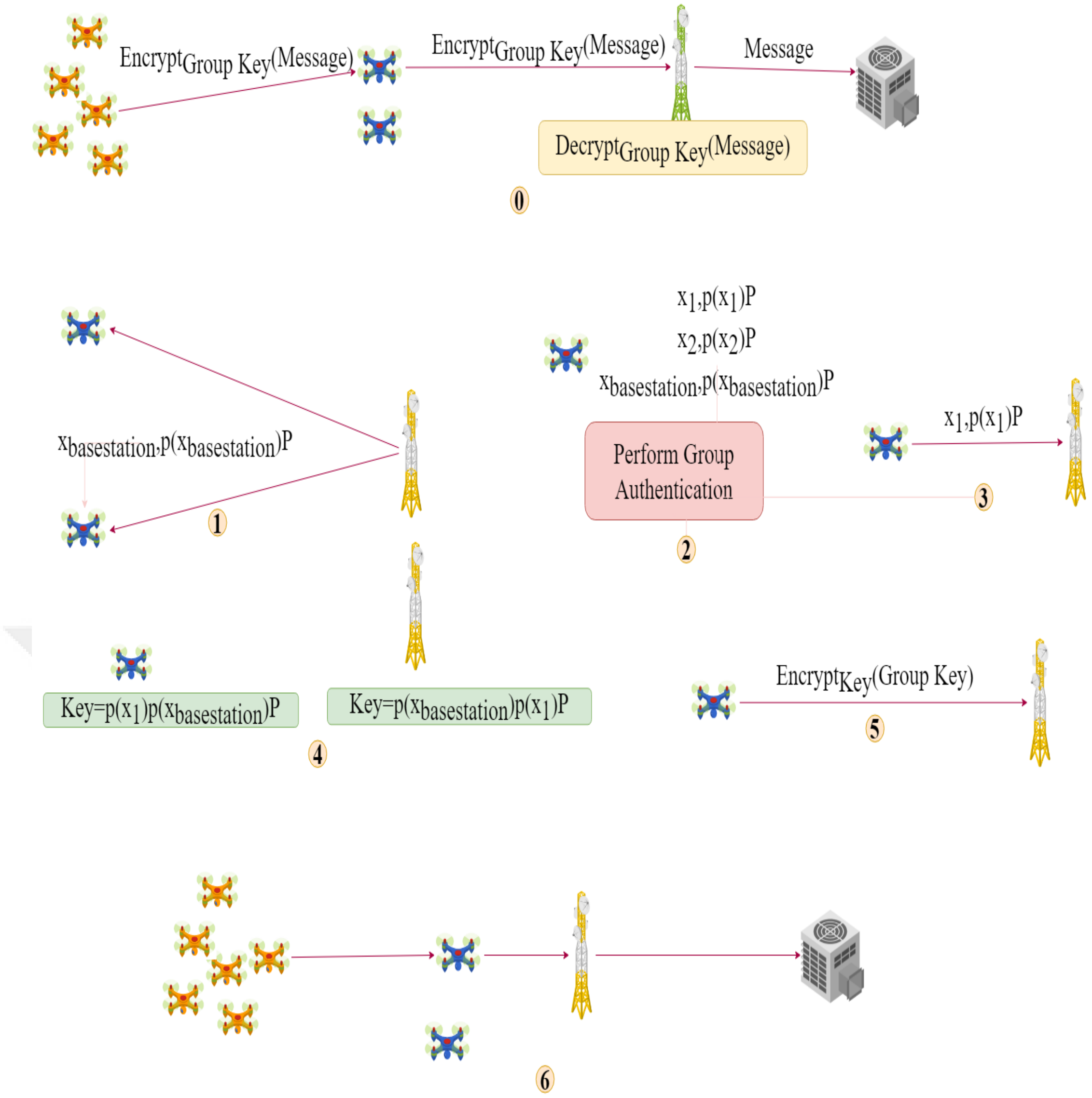
$\text{Encrypt}_{\text{Group Key}}(\text{Message})$
$\text{Encrypt}_{\text{Group Key}}(\text{Message})$
Message
$\text{Decrypt}_{\text{Group Key}}(\text{Message})$
0
$x_{1}, p(x_{1})P$
$x_{2}, p(x_{2})P$
$x_{basestation}, p(x_{basestation})P$
$x_{basestation}, p(x_{basestation})P$
1
Perform Group Authentication
2
$x_{1}, p(x_{1})P$
3
$\text{Key}=p(x_{1})p(x_{basestation})P$
$\text{Key}=p(x_{basestation})p(x_{1})P$
4
$\text{Encrypt}_{\text{Key}}(\text{Group Key})$
5
6

Figure 4.6 : Group Handover for Terrestrial BS.

- The t-BS performs the group authentication as in second chapter.
- If the authentication is valid, the t-BS begins to proivde service to the requests coming from drone swarm.

4.5.5 Aerial BS handover

The connectivity to the core network from the drone swarm may be provided not only by terrestrial BS but also by aerial BS as shown in Figure 4.7. Serving aerial BS may be altered by a new aerial BS due to the limitations of the UAV. Rather than authentication of each drone in the swarm by new aerial BS, a group authentication between network

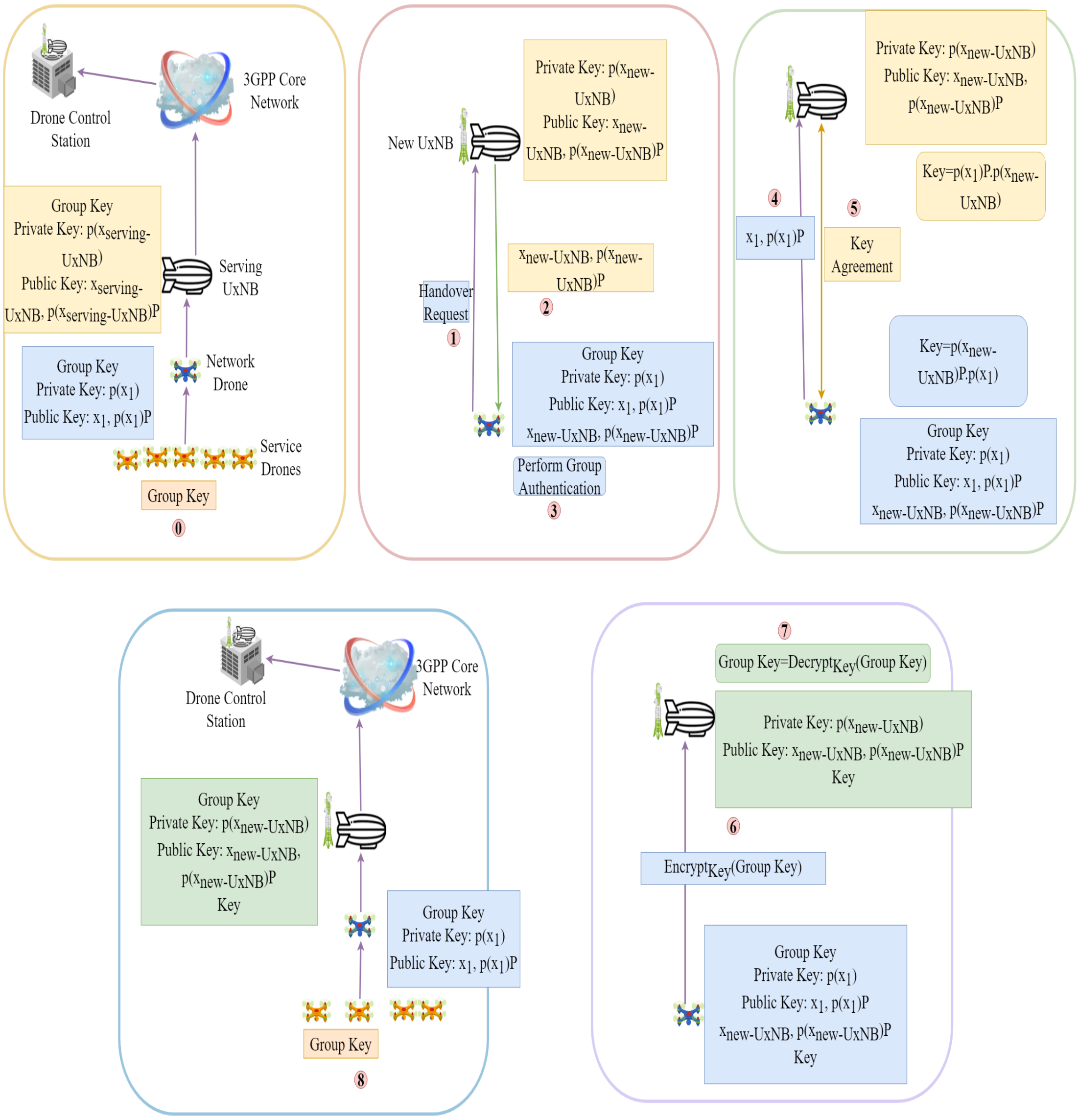

Figure 4.7 : Group Handover for Aerial BS.

drones and aerial BS can solve the scalability issues in the handover process. The steps for the group handover are mentioned at below:

- The new aerial BS shares its public key pairs $(x_{newBS}, p(x_{newBS})P)$ with the network drones.
- The network drones perform group authentication and verify the new aerial BS.

In order to get numerical results to compare the group-based authentication of a new drone joining to the swarm with the UAV authentication scheme in [66], both solutions are simulated in omnetpp [61].

4.6 Numerical Results

The total number of communication between UAV and authentication servers in the 3GPP network is eight to begin to provide service after authentication. It is observed from the simulation results that one communication from the UAV to servers costs 10 ms. The time for the authentication of one drone by the authentication servers is 80 ms.

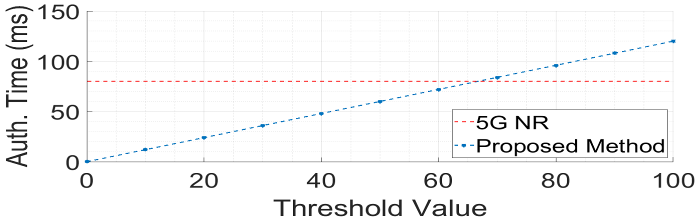

Figure 4.8 : The Authentication Time for New Drone.

The presented authentication scheme requires one data sharing over the wireless channel from the new drone to guard drones and one elliptic curve powering operation to verify the new drone. 600 μs is the time observed from the simulation needed to send data over a wireless channel and 612 μs is the time for the elliptic curve operation [35]. The number of the guard drones which should verify the new drone is determined with the threshold value t. One guard drone requires 1.2 ms to verify the new drone and total time for the authentication is 1.2t ms. Figure 4.8 shows that if the threshold value selected for the polynomial is less than 70, the presented authentication scheme for the new drone reduces the authentication time.

After comparing the results for the new drone authentication, the handover scenario for the drone swarm is simulated in omnetpp. According to the measurement reports from UE, serving-BS decides the handover. If a handover decision is taken, the serving-BS shares the relevant security keys with target-BS. After the data-sharing phase between BSs, the UE de-attaches from serving-BS and attaches to the target-BS. These handover steps as mentioned in 3GPP Rel-17 are simulated in omnetpp to observe the time for the handover in 5G NR. According to the simulation results, the total time for handover operations in 5G NR is 50 ms as explained in third chapter.

The network drones in the swarm and target-BS perform a group authentication to complete the handover for the drone swarm. The total time for authentication, which is 1.2t ms, depends on the predetermined threshold value. If the threshold value is less

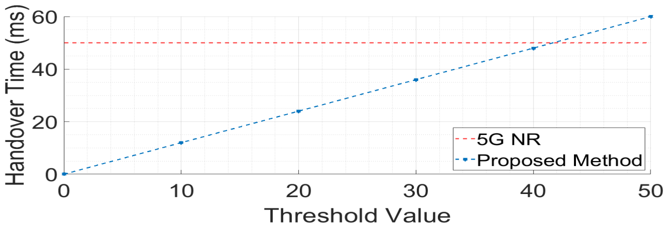

Figure 4.9 : Comparison of handover time in 5G NR and the proposed method.

than 40, the proposed handover solution costs less time than the 5G NR as shown in Figure 4.9.

4.7 Conclusion and Discussion

In this chapter of the thesis, the security issues for the drone swarms are analyzed and the authentication and handover solutions based on many-to-many authentication are presented for the five security requirements of the drone swarms. The separating of the responsibilities of drones decreases the interruptions for the service provided by drone swarm. The service drones are not busy with the security and network issues.The authentication of drones with group authentication and handover as a group via network drones reduce time and resource usage.

The authentication of a single drone by 3GPP UAV authentication solution requires two phases, which are the initial phase with the core network and the next phase with the drone control station. There are four transmissions between the core network and UAV, while four transmissions are conducted between the drone control station and UAV. The cryptographic operations are also accomplished by the UAV, drone control station, and core network. It is not scalable and also is time-consuming to authenticate each drone in a swarm with 3GPP solutions. In addition, there is not a key to be used after the authentication to create a secure channel between the new drone and the other drones in the swarm. The authentication solution in this chapter provides more reasonable time and communication complexity than 3GPP standards and a group key for establishing a secure channel for the swarm. Also, the group authentication solution to merge two drone swarms decreases the number of communication between swarms and the core network.

The 5G NR handover solution has a stage to transfer the security keys from serving-BS to the target-BS. The necessity of key sharing between BSs for the handover is a challenge for the drone swarms. The mobility nature of drones and their speeds require a time-saving handover scheme. In the proposed group handover scheme, just network drones are engaged with the handover operation. The service and guard drones resume their tasks. The network drones conduct group authentication with the target-BS, which eliminates the security key transmitting step.

5. CONCLUSIONS AND RECOMMENDATIONS

This thesis in general focuses on the authentication and handover requirements of the next-generation networks. The main objective of the thesis is to propose solutions consuming less time, resources, and communication than the 5G authentication and handover schemes. A flexible and lightweight group authentication scheme, which can be used in devices with limited resources such as IoT and UAVs, is presented in the thesis.

The UE and UAV authentication solutions in 5G NR are simulated in omnet++ to figure out the total time and number of the transmissions between the UE and the 3GPP network. In addition, the solution for the UE handover from serving-BS to a new BS is simulated and the results for time and communication complexities are obtained.

The 5G NR solution for the authentication of a UE requires three data transfers, eight key derivation functions, and public-key encryption and decryption operations. The time for the cryptographic operations and transmissions to complete the authentication is 33 ms. Furthermore, the handover procedure in 5G NR requires two transmissions between BSs and three key derivation functions. The total time for the handover is 202 μs according to the steps in 5G NR standards.

The obtained time results are reasonable for normal environments such as smartphone communication. However, the next-generation networks need time and resource-saving, lightweight authentication, and handover solutions due to their numerical density. If the 5G NR authentication and handover solutions are used for the crowded technologies, the service providing base stations or authentication servers may be encountered scalability issues.

In this thesis, authentication and handover operations are performed as a group to propose solutions for problems in the one-to-one authentication methods. The proposed group authentication and handover solution provide more reasonable time and communication complexity according to the simulation results and time analysis.

When the number of UEs requesting authentication and handover increases, the difference in the authentication time for the group between 5G NR and the proposed solutions rises.

The number of transmissions between UEs and the authentication server consumes more time than the time required for the computations in the key derivation functions. In addition, sharing the security key for each UE in the 5G NR handover scheme increases communications. The group authentication and handover solutions in this thesis decreases the number of communication and computation cost for cryptographic operations.

5.1 Recommendation for Future Works

This thesis generally focuses on the authentication and handover concerns in IoT and low-altitude domains of the non-terrestrial networks. As future work, the authentication and handover necessities for the space and high-altitude domains of the non-terrestrial network may be investigated and group-based solutions can be suggested. In addition, the scenarios in which the high and low altitude domains of the non-terrestrial network are utilized concurrently should be taken into consideration. The aerial devices are going to be both service providers and service consumers in the next-generation networks. A drone in the service consumer role may switch the service from low altitude BS to high-altitude BS. There may be requirements for mutual authentication between low and high-altitude BSs. The handover and authentication requirements should be studied for the hybrid scenarios in future works.

The implementation of the 3GPP standard solutions and proposed authentication and handover schemes is conducted with the omnet++ environment. Although the simulation of the schemes is coded as explained in the documentation, it is more satisfactory to perform real-life experiments. Therefore, the proposed schemes may be implemented with real IoT devices and UAVs in order to have more satisfactory results in the future.

The distributed nature of devices is going to extend with 6G and the communication between machine to machine will boost. The rouge devices inside a group of legitimate devices are going to interrupt, eavesdrop, and steal essential information easier if security preventions are not taken into consideration. Authentication and handover schemes should deal with the distributed character of the next-generation devices without a central authority. Lightweight encryption schemes should be utilized to ensure confidentiality for the communication between the devices. Each authentication solution should construct a key between the parties for further communications.

Quantum computing and blockchain are going to be essential parts of the 6G cellular network. The cryptography solutions based on problems, which are hard to solve, will be in-danger since quantum computing is going to solve the problems. The authentication solutions for both a UE and a UAV contain traditional cryptography, which will not be used in the future [69]. Quantum cryptography and blockchain should be more included in the authentication and handover schemes for 6G.

REFERENCES

[1] **Shamir, A.** (1979). How to share a secret, *Communications of the ACM*, *22*(11), 612–613.

[2] **Blakley, G.R.** (1979). Safeguarding cryptographic keys, *Managing Requirements Knowledge, International Workshop on*, IEEE Computer Society, pp.313–313.

[3] **Harn, L.** (2012). Group authentication, *IEEE Transactions on computers*, *62*(9), 1893–1898.

[4] **Chien, H.Y.** (2017). Group authentication with multiple trials and multiple authentications, *Security and Communication Networks*, *2017*.

[5] **Hsu, C.F.**, **Harn, L.**, **Mu, Y.**, **Zhang, M. and Zhu, X.** (2017). Computation-efficient key establishment in wireless group communications, *Wireless Networks*, *23*(1), 289–297.

[6] **Park, Y. and Park, Y.** (2017). A selective group authentication scheme for IoT-based medical information system, *Journal of medical systems*, *41*(4), 48.

[7] **Asmuth, C. and Bloom, J.** (1983). A modular approach to key safeguarding, *IEEE transactions on information theory*, *29*(2), 208–210.

[8] **Mahalle, P.N.**, **Prasad, N.R. and Prasad, R.** (2014). Threshold cryptography-based group authentication (TCGA) scheme for the Internet of Things (IoT), *2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, IEEE, pp.1–5.

[9] **Gupta, S.**, **Parne, B.L. and Chaudhari, N.S.** (2018). DGBES: Dynamic group based efficient and secure authentication and key agreement protocol for MTC in LTE/LTE-A networks, *Wireless Personal Communications*, *98*(3), 2867–2899.

[10] **Chen, Y.W.**, **Wang, J.T.**, **Chi, K.H. and Tseng, C.C.** (2012). Group-based authentication and key agreement, *Wireless Personal Communications*, *62*(4), 965–979.

[11] **Li, J.**, **Wen, M. and Zhang, T.** (2015). Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks, *IEEE Internet of Things Journal*, *3*(3), 408–417.

[12] **Lai, C., Lu, R., Zheng, D., Li, H. and Shen, X.S.** (2016). GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications, *Computer Networks*, *99*, 66–81.

[13] **Cao, J., Yu, P., Ma, M. and Gao, W.** (2018). Fast authentication and data transfer scheme for massive NB-IoT devices in 3GPP 5G network, *IEEE Internet of Things Journal*, *6*(2), 1561–1575.

[14] **Yıldız, H., Cenk, M. and Onur, E.** (2021). PLGAKD: A PUF-Based Lightweight Group Authentication and Key Distribution Protocol, *IEEE Internet of Things Journal*, *8*(7), 5682–5696.

[15] **Xue, K., Meng, W., Zhou, H., Wei, D.S. and Guizani, M.** (2020). A lightweight and secure group key based handover authentication protocol for the software-defined space information network, *IEEE Transactions on Wireless Communications*, *19*(6), 3673–3684.

[16] **Fedrizzi, R., Goratti, L., Gomez, K. and Rasheed, T.** (2014). On the feasibility of handover over WiFi backhaul in LTE-based aerial-terrestrial networks, *2014 IEEE wireless communications and networking conference (WCNC)*, IEEE, pp.2196–2201.

[17] **Yang, H., Hu, B. and Wang, L.** (2017). A deep learning based handover mechanism for UAV networks, *2017 20th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, IEEE, pp.380–384.

[18] **Park, K.N., Kang, J.H., Cho, B.M., Park, K.J. and Kim, H.** (2016). Handover management of net-drones for future Internet platforms, *International Journal of Distributed Sensor Networks*, *12*(3), 5760245.

[19] **Alladi, T., Venkatesh, V., Chamola, V. and Chaturvedi, N.** (2021). Drone-MAP: A novel authentication scheme for drone-assisted 5G networks, *IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, pp.1–6.

[20] **Wang, G., Lim, K., Lee, B.S. and Ahn, J.Y.** (2017). Handover key management in an lte-based unmanned aerial vehicle control network, *2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, IEEE, pp.200–205.

[21] **Wang, G., Lee, B.S. and Ahn, J.Y.** (2016). Authentication and key management in an LTE-based unmanned aerial system control and non-payload communication network, *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, IEEE, pp.355–360.

[22] **Guo, H., Liu, T., Lui, K.S., Danilov, C. and Nahrstedt, K.** (2020). Secure broadcast protocol for unmanned aerial vehicle swarms, *2020 29th International Conference on Computer Communications and Networks (ICCCN)*, IEEE, pp.1–9.

[23] **Xiao, W.**, **Li, M.**, **Alzahrani, B.**, **Alotaibi, R.**, **Barnawi, A. and Ai, Q.** (2021). A Blockchain-Based Secure Crowd Monitoring System Using UAV Swarm, *IEEE Network*, *35*(1), 108–115.

[24] **Brust, M.R.**, **Danoy, G.**, **Bouvry, P.**, **Gashi, D.**, **Pathak, H. and Gonçalves, M.P.** (2017). Defending against intrusion of malicious uavs with networked uav defense swarms, *2017 IEEE 42nd conference on local computer networks workshops (LCN workshops)*, IEEE, pp.103–111.

[25] **Khanh, T.D.**, **Komarov, I.**, **Iureva, R.**, **Chuprov, S.** *et al.* (2020). TRA: Effective Authentication Mechanism for Swarms Of Unmanned Aerial Vehicles, *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*, IEEE, pp.1852–1858.

[26] **3GPP** (2021). 3GPP Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system, (33.501), version 17.3.0.

[27] **Cao, J.**, **Yan, Z.**, **Ma, R.**, **Zhang, Y.**, **Fu, Y. and Li, H.** (2020). LSAA: a lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks, *IEEE Internet of Things Journal*, *7*(6), 5329–5344.

[28] **Shafagh, H. and Hithnawi, A.** (2014). Security comes first, a public-key cryptography framework for the internet of things, *2014 IEEE International Conference on Distributed Computing in Sensor Systems*, IEEE, pp.135–136.

[29] **Series, M.** (2017). Minimum requirements related to technical performance for IMT-2020 radio interface (s), *Report*, 2410–0.

[30] **Li, J.**, **Zhang, Y.**, **Chen, J.**, **Li, H. and Zhang, W.** (2014). Group key agreement in multimedia service for machine type communication, *2014 Asia-Pacific Services Computing Conference*, IEEE, pp.141–146.

[31] **Lai, C.**, **Li, H.**, **Lu, R.**, **Jiang, R. and Shen, X.** (2013). LGTH: A lightweight group authentication protocol for machine-type communication in LTE networks, *2013 IEEE Global Communications Conference (GLOBECOM)*, IEEE, pp.832–837.

[32] **3GPP** (2020). 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses, (33.402), version 16.0.0.

[33] **3GPP** (2020). 3G Security; Security architecture, (33.102), version 16.0.0.

[34] **Saxena, N. and Chaudhari, N.S.** (2014). NS-AKA: An improved and efficient AKA protocol for 3G (UMTS) networks, *International conference on advances in computer science and electronics engineering (CSEE'14), Kuala Lampur, Malaysia*, pp.220–224.

[35] **Ouaissa, M. and Rhattoy, A.** (2019). A secure model for machine to machine device domain based group in a smart city architecture, *International Journal of Intelligent Engineering and Systems*, *12*(1), 151–164.

[36] **Tiloca, M.**, **Nikitin, K. and Raza, S.** (2017). Axiom: DTLS-based secure IoT group communication, *ACM Transactions on Embedded Computing Systems (TECS)*, *16*(3), 1–29.

[37] **Zeng, Y.**, **Wu, Q. and Zhang, R.** (2019). Accessing from the sky: A tutorial on UAV communications for 5G and beyond, *Proceedings of the IEEE*, *107*(12), 2327–2375.

[38] **Li, B.**, **Fei, Z.**, **Zhang, Y. and Guizani, M.** (2019). Secure UAV communication networks over 5G, *IEEE Wireless Communications*, *26*(5), 114–120.

[39] **He, D.**, **Chan, S. and Guizani, M.** (2017). Drone-assisted public safety networks: The security aspect, *IEEE Communications Magazine*, *55*(8), 218–223.

[40] **Hassija, V.**, **Saxena, V. and Chamola, V.** (2020). A blockchain-based framework for drone-mounted base stations in tactile internet environment, *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, IEEE, pp.261–266.

[41] **Gottesman, D.** (2000). Theory of quantum secret sharing, *Physical Review A*, *61*(4), 042311.

[42] **Yang, C.N. and Laih, C.S.** (2000). New colored visual secret sharing schemes, *Designs, Codes and cryptography*, *20*(3), 325–336.

[43] **Stadler, M.** (1996). Publicly verifiable secret sharing, *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, pp.190–199.

[44] **Jeffreys, H. and Jeffreys, B.** (1988). Lagrange's interpolation formula, *Methods of mathematical physics*, *3*, 260.

[45] **Xu, R.**, **Wang, X.**, **Morozov, K.**, **Cheng, C. and Ding, J.** (2022). Revisiting Group Oriented Secret Sharing Schemes, *Information Sciences*.

[46] **Koblitz, N.** (1987). Elliptic curve cryptosystems, *Mathematics of computation*, *48*(177), 203–209.

[47] **Cohen, H.**, **Frey, G.**, **Avanzi, R.**, **Doche, C.**, **Lange, T.**, **Nguyen, K. and Vercauteren, F.** (2005). *Handbook of elliptic and hyperelliptic curve cryptography*, CRC press.

[48] **Gura, N.**, **Patel, A.**, **Wander, A.**, **Eberle, H. and Shantz, S.C.** (2004). Comparing elliptic curve cryptography and RSA on 8-bit CPUs, *International workshop on cryptographic hardware and embedded systems*, Springer, pp.119–132.

[49] **Varga, A.**, (2010). OMNeT++, Modeling and tools for network simulation, Springer, pp.35–59.

[50] **Forstall, S.**, **Christie, G.N.**, **Borchers, R.E. and Tiene, K.**, (2013), Mobile device base station, uS Patent 8,463,238.

[51] **3GPP** (2021). 3GPP Technical Specification Group Services and System Aspects; Unmanned aerial system (UAS) support in 3GPP, (22.125), version 17.4.0.

[52] **3GPP** (2021). 3GPP Technical Specification Group Services and System Aspects; Enhancement for unmanned aerial vehicles, (22.829), version 17.1.0.

[53] **Bor-Yaliniz, I. and Yanikomeroglu, H.** (2016). The new frontier in RAN heterogeneity: Multi-tier drone-cells, *IEEE Communications Magazine*, *54*(11), 48–55.

[54] **Ali, K.**, **Nguyen, H.X.**, **Vien, Q.T.**, **Shah, P. and Raza, M.** (2020). Deployment of drone-based small cells for public safety communication system, *IEEE Systems Journal*, *14*(2), 2882–2891.

[55] **Zhou, X.**, **Durrani, S.**, **Guo, J. and Yanikomeroglu, H.** (2018). Underlay drone cell for temporary events: Impact of drone height and aerial channel environments, *IEEE Internet of Things Journal*, *6*(2), 1704–1718.

[56] **3GPP** (2021). 3GPP Technical Specification Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2, (36.300), version 16.6.0.

[57] **3GPP** (2021). 3GPP Technical Specification Group Services and System Aspects; Service Requirements for the 5G System, (22.261), version 18.4.0.

[58] **3GPP** (2021). 3GPP Technical Specification Group Services and System Aspects; Study on supporting Unmanned Aerial Systems (UAS) connectivity, Identification and tracking, (23.754), version 17.1.0.

[59] **Tayyab, M.**, **Gelabert, X. and Jäntti, R.** (2019). A survey on handover management: From LTE to NR, *IEEE Access*, *7*, 118907–118930.

[60] **Gupta, S.**, **Parne, B.L. and Chaudhari, N.S.** (2018). Security vulnerabilities in handover authentication mechanism of 5G network, *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, IEEE, pp.369–374.

[61] **Virdis, A.**, **Stea, G. and Nardini, G.**, (2015). Simulating lte/lte-advanced networks with simulte, Simulation and Modeling Methodologies, Technologies and Applications, Springer, pp.83–105.

[62] **Al-Hilfi, H.M.T. and Abbas, M.J.** (2020). LTE Capacity Estimation with Changing Different Planning Parameters., *J. Commun.*, *15*(9), 687–692.

[63] **Gurunath, R.**, **Agarwal, M.**, **Nandi, A. and Samanta, D.** (2018). An overview: security issue in IoT network, *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on*, IEEE, pp.104–107.

[64] **Hayat, S.**, **Bettstetter, C.**, **Fakhreddine, A.**, **Muzaffar, R. and Emini, D.** (2019). An experimental evaluation of LTE-A throughput for drones, *Proceedings of the 5th Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*, pp.3–8.

[65] **Akram, R.N.**, **Markantonakis, K.**, **Mayes, K.**, **Habachi, O.**, **Sauveron, D.**, **Steyven, A. and Chaumette, S.** (2017). Security, privacy and safety evaluation of dynamic and static fleets of drones, *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, IEEE, pp.1–12.

[66] **3GPP** (2021). 3GPP Technical Specification Group Services and System Aspects; Study on security aspects of Unmanned Aerial Systems (UAS), (33.854), version 17.0.0.

[67] **Chamola, V.**, **Kotesh, P.**, **Agarwal, A.**, **Gupta, N.**, **Guizani, M.** *et al.* (2021). A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques, *Ad hoc networks*, *111*, 102324.

[68] **Yaacoub, J.P.**, **Noura, H.**, **Salman, O. and Chehab, A.** (2020). Security analysis of drones systems: Attacks, limitations, and recommendations, *Internet of Things*, *11*, 100218.

[69] **Wang, M.**, **Zhu, T.**, **Zhang, T.**, **Zhang, J.**, **Yu, S. and Zhou, W.** (2020). Security and privacy in 6G networks: New areas and new challenges, *Digital Communications and Networks*, *6*(3), 281–291.

CURRICULUM VITAE

Name Surname : Yücel AYDIN

EDUCATION :

- **B.Sc.** : 2007, Ankara Military Academy, Faculty of Engineering, Department of Electrical and Electronics Engineering
- **B.Sc.** : 2021, Erzurum Atatürk University, Faculty of Engineering, Department of Electrical and Electronics Engineering
- **M.Sc.** : 2017, Istanbul Technical University, Informatics Institute, Cybersecurity Engineering and Cryptography Programme

PROFESSIONAL EXPERIENCE AND REWARDS:

- 2018-2020 Cyber Security Specialist in Ankara Land Forces
- 2020-2021 Cyber Security Specialist in caniasERP
- 2021-2022 Network and Security Specialist in mayaICT

PUBLICATIONS, PRESENTATIONS AND PATENTS ON THE THESIS:

- International Journals
  - **Aydin, Y.**, Kurt, G. K., Ozdemir, E., Yanikomeroglu, H. (2022). Authentication and Handover Challenges and Methods for Drone Swarms, *IEEE Journal of RFID*, under review.
  - **Aydin, Y.**, Kurt, G. K., Ozdemir, E., Yanikomeroglu, H. (2021). Group Handover for Drone Base Stations, *IEEE Internet of Things Journal*, 8(18), 13876–13887.
  - **Aydin, Y.**, Kurt, G. K., Ozdemir, E., Yanikomeroglu, H. (2020). A Flexible and Lightweight Group Authentication Scheme, *IEEE Internet of Things Journal*, 7(10), 10277–10287.
- International Conferences
  - **Aydin, Y.**, Kurt, G. K., Ozdemir, E., Yanikomeroglu, H. (2021). Group Authentication for Drone Swarms, *2021 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE)*, October 12–14, 2021 Cleveland, Ohio, USA. (The best paper award)

- Patent Applications
  - **Aydin, Y.**, Kurt, G. K., Ozdemir, E., Yanikomeroglu, H., Authenticated Handover Algorithm for Group Communications, TR2019/10780.