BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

ĐỒ ÁN TỐT NGHIỆP

NGÀNH : CÔNG NGHỆ THÔNG TIN

Sinh viên : Đặng Thế Quang

Giảng viên hướng dẫn : Th.s Nguyễn Như Chiến

HẢI PHÒNG – 2022

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

TÌM HIỂU GIAO THỨC XÁC THỰC VÀ THỎA THUẬN KHÓA TRONG MẠNG DI ĐỘNG 5G

ĐỒ ÁN TỐT NGHIỆP ĐẠI HỌC HỆ CHÍNH QUY

NGÀNH: CÔNG NGHỆ THÔNG TIN

Sinh viên : Đặng Thế Quang

Giảng viên hướng dẫn : Ths. Nguyễn Như Chiến

HẢI PHÒNG – 2022

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC QUẢN LÝ VÀ CÔNG NGHỆ HẢI PHÒNG

NHIỆM VỤ ĐỀ TÀI TỐT NGHIỆP

Sinh viên: Đặng Thế Quang **Mã SV**: 1812112003

Lớp : CT2201M

Ngành : Quản trị mạng

Tên đề tài: Tìm hiểu giao thức xác thực và thỏa thuận khóa trong mạng di động 5G

NHIỆM VỤ ĐỀ TÀI

1. Nội dung và các yêu cầu cần giải quyết trong nhiệm vụ đề tài tốt nghiệp

a. Nội dung

- Tổng quan mạng di động 5G
- Nghiên cứu các giao thức xác thực và thỏa thuận khóa trong mạng di động 5G
- Phân tích an toàn của giao thức xác thực và thỏa thuận khóa trong mạng di động 5G so với các phiên bản trước

b. Các yêu cầu cần giải quyết

- Hiểu được vai trò của giao thức xác thực và thỏa thuận khóa trong mạng di động 5G
- Phân tích độ an toàn tin cậy giao thức xác thực và thỏa thuận khóa 5G AKA với EPS- AKA so các phiên bản trước

2. Các tài liệu, số liệu cần thiết

- Tài liệu tham khảo về các thế hệ mạng di động.
- Tài liệu về mạng di động 5G.
- Tài liệu Kiến trúc và quy trình bảo mật cho hệ thống 5G; (Bản phát hành 16). Năm 2020.
- Jingjing Zhang, Lin Yang, Weipeng Cao và Qiang Wang, “Phân tích chính thức về giao thức xác thực 5G EAP-TLS sử dụng Proverif”.
- Adrien Koutsos, “Quyền riêng tư của giao thức xác thực 5G-AKA”, Hội nghị chuyên đề về bảo mật và quyền riêng tư của IEEE Châu Âu (EuroS & P), 2019.

- An Braeken, Madhusanka Liyanage, Pardeep Kumar và John Murphy, “Giao thức xác thực 5G mới để cải thiện khả năng chống lại các cuộc tấn công chủ động và mạng phục vụ độc hại”, IEEE Aceess, tập 7, 2019.

- Tài liệu giới thiệu về so sánh xác thực giữa 4G và 5G.

- Ashraf Elbayoumy, “Tăng cường bảo mật cho Giao thức xác thực LTE (EPS-AKA)”, tháng 5 năm 2015.

3. Địa điểm thực tập tốt nghiệp

- Công ty TNHH Công Nghệ Và Dịch Vụ Viễn Thông Nam Việt.

CÁN BỘ HƯỚNG DẪN ĐỀ TÀI TỐT NGHIỆP

Họ và tên : Nguyễn Như Chiến

Học hàm, học vị : Thạc sĩ

Cơ quan công tác : Học Viện Kỹ Thuật Mật Mã

Nội dung hướng dẫn :

Nội dung dự kiến

- Tổng quan mạng di động 5G
- Nghiên cứu các giao thức xác thực và thỏa thuận khóa trong mạng di động 5G
- Phân tích an toàn của giao thức xác thực và thỏa thuận khóa trong mạng di động 5G so với các phiên bản trước

Đề tài tốt nghiệp được giao ngày 12 tháng 8 năm 2022

Yêu cầu phải hoàn thành xong trước ngày 22 tháng 10 năm 2022

Đã nhận nhiệm vụ ĐTTN	**Đã giao nhiệm vụ ĐTTN**
Sinh viên	*Giảng viên hướng dẫn*
Đặng Thế Quang	**ThS. Nguyễn Như Chiến**

Hải Phòng, ngày ..... tháng..... năm 2022

TRƯỞNG KHOA

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN TỐT NGHIỆP

Họ và tên giảng viên: Nguyễn Như Chiến

Đơn vị công tác: Học Viện Kỹ Thuật Mật Mã

Họ và tên sinh viên: Đặng Thế Quang Ngành: Công nghệ thông tin

Đề tài tốt nghiệp: **Tìm hiểu giao thức xác thực và thỏa thuận khóa trong mạng di động 5G**.

1. Tinh thần thái độ của sinh viên trong quá trình làm đề tài tốt nghiệp

Trong thời gian thực hiện đồ án tốt nghiệp, sinh viên Đặng Thế Quang đã có nhiều cố gắng, chủ dộng, có thái độ làm việc nghiêm túc. Mặc dù có những hạn chế nhất định về trình độ chuyên môn nghiệp vụ và đặc biệt là khoảng cách địa lý giữa sinh viên và thầy hướng dẫn nhưng học viên luôn tự tìm tòi, nghiên cứu, khảo sát thu thập tài liệu và khắc phục khó khăn để hoàn thành đồ án đầy đủ các nội dung đăng ký trong đề cương và đúng tiến độ đề ra.

2. Đánh giá chất lượng của đồ án/khóa luận(so với nội dung yêu cầu đã đề ra trong nhiệm vụ Đ.T. T.N trên các lý luận, thực tiễn, tính toán số liệu…)

Đồ án được trình bày rõ ràng trong 76 trang A4 bao gồm các ký hiệu chữ viết tắt, danh mục bảng biểu, danh mục hình vẽ, mục lục, lời nói đầu, nội dung 3 chương đồ án, kết luận và các tài liệu tham khảo. Nội dung đồ án đảm bảo tính khoa học, chặt chẽ và logic đối với đề tài nghiên cứu. Đồ án phân tích giao thức xác thực và thỏa thuận khóa, đánh giá được mô hình phân cấp khóa trong mạng 5G, phân tích được các lỗ hổng của giao thức xác thực và thỏa thuận ESP-AKA trong mạng 4G để so sánh với 5G-AKA. Từ đó phân tích được một số lỗ hổng của giao thức xác thực và thỏa thuận khóa.

3. Ý kiến của giảng viên chấm phản biện

Được bảo vệ ☐ Không được bảo vệ ☐ Điểm:…….

Hải Phòng, ngày 25 tháng 10 năm 2022

Giảng viên chấm phản biện

(Ký và ghi rõ họ tên)

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHIẾU NHẬN XÉT CỦA GIẢNG VIÊN CHẤM PHẢN BIỆN

Họ và tên giảng viên: Phùng Anh Tuấn

Đơn vị công tác: Trường Đại Học Quản Lý và Công Nghệ Hải Phòng

Họ và tên sinh viên: Đặng Thế Quang Ngành: Công nghệ thông tin

Đề tài tốt nghiệp: **Tìm hiểu giao thức xác thực và thỏa thuận khóa trong mạng di động 5G**.

1. Phần nhận xét của giảng viên chấm phản biện

- Tìm hiểu được tổng quan về mạng di động 5G

- Tìm hiểu được giao thức xác thực và thỏa thuận khóa trong mạng di động 5G

- Phân tích được an toàn của giao thức xác thực và thỏa thuận khóa trong mạng di động 5G so với các phiên bản trước

- Đáp ứng được yêu cầu cơ bản của đồ án tốt nghiệp ngành CNTT

2. Những mặt còn hạn chế

- Đề tài mới chỉ dừng lại tìm hiểu lý thuyết về:

+ Tổng quan về mạng di động 5G

+ Giao thức xác thực và thỏa thuận khóa trong mạng di động 5G

+ Phân tích an toàn của giao thức xác thực và thỏa thuận khóa trong mạng di động 5G

- Chưa trình bầy nhược điểm của giao thức xác thực và thỏa thuận khóa trong mạng di động 5G

- Chưa có minh họa thực tế cho việc an toàn của giao thức xác thực và thỏa thuận khóa trong mạng di động 5G

3. Ý kiến của giảng viên chấm phản biện

Được bảo vệ ☐ Không được bảo vệ ☐ Điểm:…….

Hải Phòng, ngày 25 tháng 10 năm 2022

Giảng viên chấm phản biện

(Ký và ghi rõ họ tên)

LỜI CẢM ƠN

Để hoàn thành tốt được Đồ án tốt nghiệp, em xin gửi lời cảm ơn chân thành đến các thầy cô trong Khoa Công Nghệ Thông tin của Trường ĐH Quản Lý và Công Nghệ Hải Phòng đã tạo điều kiện tốt nhất cho em để em hoàn thành đề tài đúng như dự kiến. Đặc biệt em xin gửi lời cảm ơn sâu săc đến Cô Nguyễn Thị Xuân Hương – Lãnh đạo Khoa Công Nghệ Thông Tin và Thầy Nguyễn Như Chiến – Giảng viên hướng dẫn đồ án đã trực tiếp hướng dẫn và tận tình giúp đỡ em để em có thể hoàn thành tốt đồ án tốt nghiệp của mình.

Em xin chân thành cảm ơn các lãnh đạo của Trường ĐH Quản Lý và Công Nghệ, các Thầy,Cô trong khoa Công Nghệ Thông Tin đã tạo cho em điều kiện tốt nhất từ khi còn ngồi trên ghế nhà trường cho đến khi hoàn thành đồ án tốt nghiệp quan trọng nhất trong cuộc đời sinh viên.

Trong quá trình thực tập, cũng như là trong quá trình làm đồ án tốt nghiệp em không tránh khỏi những sai sót, em rất mong các Thầy, Cô bỏ qua. Đồng thời do trình độ lý luận cũng như trong kinh nghiệm thực tiễn của em còn nhiều hạn chế nên không tránh khỏi những thiếu sót. Vậy nên, em rất mong sự đóng góp ý kiến từ Thầy, Cô để em học thêm được nhiều kinh nghiệm và kiến thúc để có thể góp ích cho những công việc sau này.

Em xin chân thành cảm ơn!

Hải Phòng, ngày 20 tháng 10 năm 2022

Sinh viên

(Ký và ghi rõ họ tên)

LỜI CAM ĐOAN

Em xin cam đoan rằng đề tài này được tiến hành một cách minh bạch, công khai. Mọi thứ được dựa trên sự cố gắng cũng như sự nỗ lực của bản thân cùng với sự giúp đỡ của thầy Nguyễn Như Chiến.

Các số liệu và kết quả nghiên cứu được đưa ra trong đồ án là trung thực và không sao chép hay sử dụng kết quả của bất kỳ đề tài nghiên cứu nào tương tự. Nếu như phát hiện rằng có sự sao chép kết quả nghiên cứu đề những đề tài khác bản thân em xin chịu hoàn toàn trách nhiệm.

Hải Phòng, ngày 20 tháng 10 năm 2022

Sinh viên

(Ký và ghi rõ họ tên)

MỤC LỤC

MỤC LỤC **1**

DANH MỤC TỪ VIẾT TẮT **3**

DANH MỤC HÌNH VẼ **7**

DANH MỤC BẢNG BIỂU **8**

LỜI NÓI ĐẦU **9**

CHƯƠNG 1: TỔNG QUAN VỀ MẠNG DI ĐỘNG 5G **10**

1.1. Giới thiệu mạng di động 5G **10**

1.1.1. Giới thiệu các thế hệ mạng di động 10

1.1.2. Giới thiệu mạng di động 5G 14

1.1.3. Lợi ích của mạng 5G 15

1.2. Kiến trúc mạng 5G **17**

1.2.1. Hệ thống thông tin mạng di động 5G 17

1.2.2. Kiến trúc mạng di động 5G 17

1.3. Vấn đề an ninh mạng 5G **18**

1.3.1. Kiến trúc an ninh mạng di động 5G 18

1.3.2. Các thách thức an ninh trong mạng 5G 20

A. Thách thức an toàn cho mạng truy cập (Access Networks) **20**

B. Những thách thức an toàn cho mạng lõi: **21**

1.4. Kết luận chương **22**

CHƯƠNG 2: NGHIÊN CỨU GIAO THỨC XÁC THỰC VÀ THỎA THUẬN KHÓA TRONG MẠNG DI ĐỘNG 5G **23**

2.1. Giới thiệu chung xác thực và thỏa thuận khóa **23**

2.1.1. Mục đích của xác thực và thỏa thuận khóa 25

2.1.2. Khung xác thực 25

2.1.3. Khởi tạo và lựa chọn phương pháp xác thực 27

2.2. Phân tích giao thức xác thực và thỏa thuận khóa trong mạng 5G 29
2.2.1. Giao thức xác thực và thỏa thuận khóa 5G AKA 29
2.2.1. Giao thức xác thực và thỏa thuận khóa EAP-AKA' 32
2.2.2 Giao thức xác thực và thỏa thuận khóa EAP-TLS 36
2.3. Mô hình phân cấp khóa trong mạng di động 5G 38
2.3.1. Hệ thống phân cấp khóa 38
2.3.2. Lược đồ dẫn xuất và phân phối khoá 41
2.3.3. Xử lý khóa liên quan đến người dùng 47
2.4. Kết luận chương 50
CHƯƠNG 3: PHÂN TÍCH AN TOÀN CỦA GIAO THỨC XÁC THỰC VÀ THỎA THUẬN KHÓA TRONG MẠNG 5G SO VỚI THẾ HỆ TRƯỚC 51
3.1. Phân tích các lỗ hổng của giao thức xác thực và thỏa thuận khóa EPS-AKA trong mạng 4G. 51
3.1.1. Xác thực trong mạng 4G 51
3.1.2. Thủ tục xác thực 4G EPS-AKA 51
3.1.3. Các lỗ hổng của giao thức xác thực và thỏa thuận khóa EPS-AKA trong mạng 4G. 53
3.2. So sánh an toàn của giao thức xác thực và thỏa thuận khóa 5G-AKA so với EPS-AKA..... 55
3.3. Phân tích một số lỗ hổng của giao thức xác thực và thỏa thuận khóa 5G 57
3.3.1. Kịch bản tấn công chi tiết..... 59
3.3.2. Thiết lập cho cuộc tấn công..... 60
3.3.3. Giai đoạn chính của cuộc tấn công..... 60
3.4. Kết luận chương 62
KẾT LUẬN……63
TÀI LIỆU THAM KHẢO 64

DANH MỤC TỪ VIẾT TẮT

TỪ VIẾT TẮT	TIẾNG ANH	TIẾNG VIỆT
5GC	5G Core Network	Mạng lõi 5G
5G-AN	5G Acess Network	Mạng truy cập 5G
NG-RAN	NG-Radio access network	Mạng truy cập vô tuyến 5G
5G AV	5G Home Environment Authentication Vector	Véc tơ xác thực môi trường thường trú 5G
5G SE AV	5G Serving Environment Authentication Vector	Véctơ xác thực môi trường dịch vụ 5G
ABBA	ABBA	Tham số ABBA
AKA	Authentication and key Agreement	Xác thực và Thỏa thuận khóa
AMF	Access Mobility Funcition	Chức năng quản lý truy cập và di động
ARPF	Authentication credential repository and processing function	Chức năng lưu trữ và xử lý thông tin xác thực
AUSF	Authentication Sever Funtion	Chức năng máy chủ xác thực
AUTN	Authentication TokenN	Xác thực Token
AV	Authentication Vector	Véctơ xác thực
AV'	Authentication Vector Control	Véctơ xác thực chuyển đổi
CP	Plane	Mặt phẳng điều khiển

EAP	Extensible Authentication Protocol	Giao thức xác thực mở rộng
EMSK	Extended Master Session Key	Khóa phiên chủ mở rộng
EPS	Evolved Packet System	Hệ thống gói phát triển
gNB	NR Node B	NR nút B
GUTI	Globally Unique Temporary UE Identity	Nhận dạng định danh tạm thời UE
HRES	Hash RESponse	Phản hồi của Hash
HXRES	Hash eXpected RESponse	Phản hồi mong đợi Hash
IKE	Internet Key Exchange	Trao đổi khóa Internet
MSK	Master Session Key	Khóa phiên Chủ
N3IWF	Non-3GPP access InterWorking Function	Chức năng InterWorking truy cập không phải 3GPP
NAI	Network Access Identifier	Mã định danh truy cập mạng
NAS	Non Access Stratum	Tầng không truy cập
NDS	Network Domain Security	Bảo mật miền mạng
NF	Network Function	Chức năng mạng
NG	Next Generation	Thế hệ tiếp theo
ng-eNB	Next Generation Evolved Node-B	Nút phát triển thế hệ tiếp theo – B
ngKSI	Key Set Identifier in 5G	Mã định danh bộ khóa trong 5G

N5GC	Non-5G-Capable	Không có khả năng 5G
NSSAI	Network Slice Selection Assistance Information	Thông tin hỗ trợ lựa chọn lớp mạng
RES	RESponse	Phản hồi
XRES	eXpected RESponse	Phản hồi của eXpect
SEAF	Security Anchor Function	Chức năng bảo mật khóa Anchor
SIDF	Subscription Identifier Deconcealing Function	Chức năng giải mã định danh thuê bao
SMC	Security Mode Command	Lệnh chế độ bảo mật
SMF	Session Management Function	Chức năng quản lý phiên
SN	Secondary Node	Nút phụ
SN Id	Serving Network Identifier	Mã định danh mạng dịch vụ
SUCI	Subscription Concealed Identifier	Định danh thuê bao tạm thời
SUPI	Subscription Permanent Identifier	Định danh thuê bao cố định
TLS	Transport Layer Security	Bảo mật lớp truyền tải
UE	User Equipment	Thiết bị người dùng
UEA	User Equipment	Thiết bị người dùng
UEA	UMTS Encryption Algorithm	Thuật toán mã hóa UMTS

UDM	Unified Data Management	Quản lý dữ liệu hợp nhất
UDR	Unified Data Repository	Kho lưu trữ dữ liệu hợp nhất
UP	User Plane	Mặt phẳng người dùng
UPF	User Plane Function	Chức năng mặt phẳng người dùng
URLLC	Ultra Reliable Low Latency Communication	Giao tiếp độ trễ siêu thấp đáng tin cậy
USIM	Universal Subscriber Identity Module	Mô đun nhận dạng thuê bao

DANH MỤC HÌNH VẼ

Hình 1.1: Quá trình phát triển hệ thống thông tin mạng di động 5G ***10***

Hình 1.2: Mô hình tổng thể hệ thống thông tin mạng 5G ***17***

Hình 1.3: Các thành phần chính trong mạng di động 5G ***17***

Hình 1.4: Kiến trúc an ninh của mạng 5G ***19***

Hình 2.1: Khung xác thực của 5G ***25***

Hình 2.2: Khởi tạo và lựa chọn phương pháp xác thực ***28***

Hình 2.3: Thủ tục xác thực cho 5G AKA ***29***

Hình 2.4: Thủ tục xác thực EAP-AKA' ***33***

Hình 2.5: Thủ tục xác thực cho EAP-TLS 5G ***36***

Hình 2.6: Hệ thống phân cấp khóa trong 5GS ***39***

Hình 2.7: Lược đồ phân phối khóa và dẫn xuất khóa cho các nút mạng ***44***

Hình 2.8: Lược đồ phân phối khóa và dẫn xuất khóa cho UE ***45***

Hình 3.1: Kiến trúc tổng quát mạng 4G ***51***

Hình 3.2: Thủ tục xác thực 4G/LTE ***52***

Hình 3.3: Điểm yếu tiết lộ danh tính người dùng ***53***

Hình 3.4: Tấn công Man In The Middle ***54***

Hình 3.5: Tấn công DoS ***54***

Hình 3.6: Hệ thống phân cấp khóa trong 4G và 5G ***56***

Hình 3.7: Các luồng tấn công của giao thức 5G-AKA ***59***

DANH MỤC BẢNG BIỂU

Bảng 3.1 : So sánh giao thức 5G-AKA và 4G-AKA **57**

Bảng 3.2 : So sánh giao thức xác thực 4G và 5G **57**

LỜI NÓI ĐẦU

Với đà phát triển trong lĩnh vực công nghệ thông tin và truyền thông, trong tiến trình đó, mỗi một kỷ nguyên mạng di động đều có những đột phá riêng, mạng di động đã được sử dụng rộng rãi trong nhiều lĩnh vực khác nhau mang lại nhiều tiện ích cho con người. Bên cạnh đó các vấn đề như sự an toàn của hệ thống mạng di động đã được đưa ra và được quan tâm ngày càng nhiều hơn. So với mạng cố định, hệ thống mạng di động dễ bị tổn thương bởi các tấn công hơn.

Để có được an toàn đáng tin cậy cho hệ thống mạng di động, phải có các biện pháp đảm bảo an ninh nhất định, ví dụ như tính bảo mật, tính xác thực và tính nặc danh. Người dùng và hệ thống máy chủ cần phải xác thực lẫn nhau và thiết lập các khóa phiên để tiếp tục liên lạc.

Đã có nhiều giao thức xác thực được đề xuất cho hệ thống mạng di động, trong số đó có các giao thức cung cấp xác thực lẫn nhau và thỏa thuận khóa giữa người dùng và máy chủ với chi phí tính toán thấp. Việc này rất quan trọng vì các thiết bị liên lạc trong mạng di động thường có nguồn năng lượng và khả năng xử lý bị hạn chế. Ngoài đòi hỏi ít tính toán và tốn ít năng lượng, các giao thức cần phải có độ an toàn cao, có khả năng chống lại các tấn công thường gặp trong mạng di động.

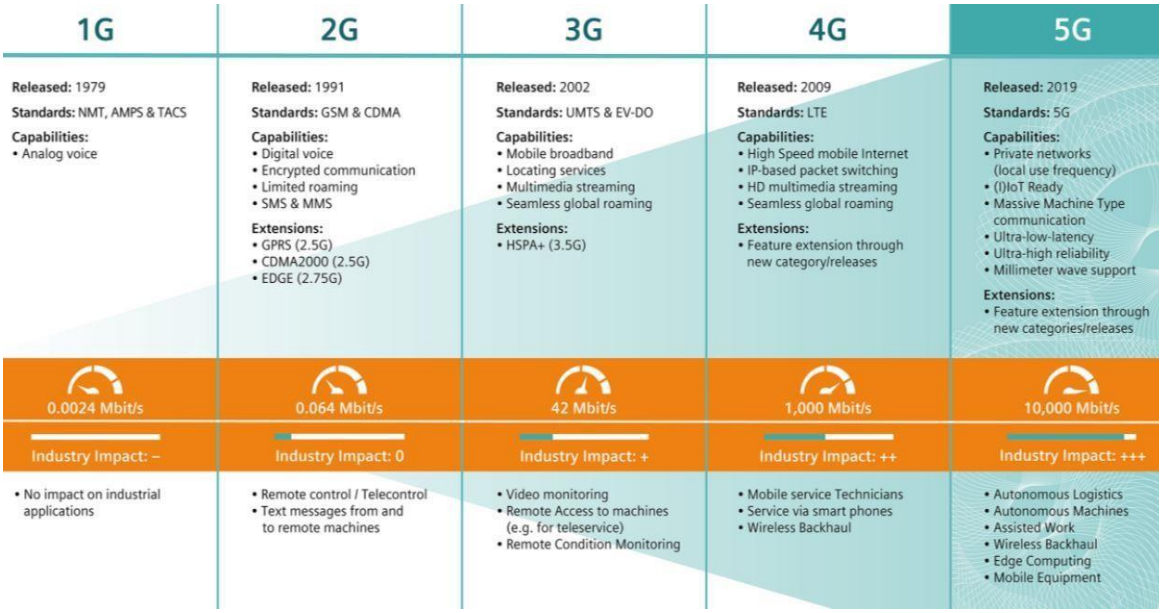
Vì vậy em chọn đề tài "**Tìm hiểu giao thức xác thực và thỏa thuận khóa trọng mạng 5G**" để nghiên cứu, tìm hiểu vấn đề về giao thức xác thực và thoả thuận khoá trong mạng di động 5G.

CHƯƠNG 1: TỔNG QUAN VỀ MẠNG DI ĐỘNG 5G

1.1. Giới thiệu mạng di động 5G

1.1.1. Giới thiệu các thế hệ mạng di động

Trong những năm qua, hệ thống mạng không dây nói chung và mạng di động nói riêng đã có sự phát triển không ngừng và đã khá phổ biến trên toàn thế giới. Sự phát triển ấy đã mang lại những lợi ích to lớn khi được ứng dụng vào thực tế. Công nghệ mạng di động phát triển từ các thế hệ mạng đầu tiên là 1G đến các thế hệ mạng tiếp theo 2G, 3G, 4G và hiện nay thế hệ mạng 5G đang được hoàn thiện và đưa vào khai thác sử dụng.



Hình 1.1: Quá trình phát triển hệ thống thông tin mạng di động 5G

Thế hệ mạng di động 1G là mạng thông tin di động không dây sơ khai đầu tiên trên thế giới. Nó là hệ thống giao tiếp thông tin qua kết nối tín hiệu analog được giới thiệu lần đầu tiên vào những năm đầu thập niên 1980. Nó sử dụng các ăng-ten thu phát sóng gắn ngoài, kết nối theo tín hiệu analog tới các trạm thu phát sóng và nhận tín hiệu xử lý thoại thông qua các module gắn trong máy di động. Chính vì thế mà các thế hệ máy di động đầu tiên trên thế giới có kích thước khá to và cồng kềnh do tích hợp cùng lúc 2 module thu tín hiện và phát tín hiệu. Mặc dù là thế hệ mạng di động đầu tiên với tần số chỉ từ 150MHz nhưng mạng 1G cũng phân ra khá nhiều chuẩn kết nối theo từng phân vùng riêng trên thế giới: NMT (Nordic Mobile Telephone) là chuẩn dành cho các nước Bắc Âu và Nga; AMPS (Advanced Mobile Phone System) tại Hoa Kỳ; TACS (Total Access Communications System) tại Anh; JTAGS tại Nhật; C-Netz tại Tây Đức; Radiocom 2000 tại Pháp; RTMI tại Ý.

Mạng di động 2G đây chính là thế hệ mạng di động thứ 2 với tên gọi đầy đủ là: "**hệ thống thông tin di động toàn cầu**". Mạng **2G** có tên tiếng anh là **Global System for Mobile Communications** hay còn gọi là **GSM**. Mạng **2G** có khả năng phủ sóng rộng khắp, làm cho những chiếc điện thoại có thể được sử dụng ở nhiều nơi trên thế giới. GSM gồm nhiều các trạm thu phát sóng để những điện thoại di động có thể kết nối mạng qua việc tìm kiếm các trạm thu phát gần nhất. Các tính năng vượt trội của mạng 2G so với 2 công nghệ tiền nhiệm là 0G và 1G là: Gọi thoại với tín hiệu được mã hóa dưới dạng tín hiệu kĩ thuật số (digital encrypted); Sử dụng hiệu quả hơn phổ tần số vô tuyến cho phép nhiều người dùng hơn trên mỗi dải tần; Cung cấp dịch vụ dữ liệu cho di động, bắt đầu với tin nhắn văn bản SMS. Khi mạng 2G xuất hiện, chất lượng cuộc gọi được cải thiện đáng kể, tín hiệu và tốc độ cũng tốt hơn rất nhiều so với thế hệ trước đó. Thời gian và chi phí được tiết kiệm khi mã hóa dữ liệu theo dạng kĩ thuật số. Những thiết bị được thiết kế nhỏ gọn và nhẹ hơn, ngoài ra chúng còn có thể thực hiện tin nhắn dạng SMS.

Mạng 2G chia làm 2 nhánh chính: nền TDMA (Time Division Multiple Access) và nền CDMA cùng nhiều dạng kết nối mạng tuỳ theo yêu cầu sử dụng từ thiết bị cũng như hạ tầng từng phân vùng quốc gia:

GSM (TDMA-based), khởi nguồn áp dụng tại Phần Lan và sau đó trở thành chuẩn phổ biến trên toàn 6 Châu lục. Sau đó được sử dụng bởi hơn 80% nhà cung cấp mạng di động toàn cầu.

CDMA2000 – tần số 450 MHZ cũng là nền tảng di động tương tự GSM nói trên nhưng nó lại dựa trên nền CDMA và hiện cũng đang được cung cấp bởi 60 nhà mạng GSM trên toàn thế giới.

IS-95 hay còn gọi là CDMAOne, (nền tảng CDMA) được sử dụng rộng rãi tại Hoa Kỳ và một số nước Châu Á và chiếm gần 17% các mạng toàn cầu. Tuy nhiên, tính đến thời điểm này thì có khoảng 12 nhà mạng đang chuyển dịch dần từ chuẩn mạng này sang GSM (tương tự như HT Mobile tại Việt Nam vừa qua) tại: Mexico, Ấn Độ, Úc và Hàn Quốc.

PDC (nền tảng TDMA) tại Nhật

IDEN (nền tảng TDMA) sử dụng bởi Nextel tại Hoa Kỳ và Telus Mobility tại Canada.

IS-136 hay còn gọi là D-AMPS, (nền tảng TDMA) là chuẩn kết nối phổ biến nhất tính đến thời điểm này và được cung cấp hầu hết tại các nước trên thế giới cũng như Hoa Kỳ.

Mạng di động Thế hệ thứ 3 của chuẩn công nghệ điện thoại di động chính là mạng **3G Third-generation technology**, cho phép truyền cả dữ liệu thoại như nghe gọi, nhắn tin và dữ liệu ngoài thoại như gửi mail, tải dữ liệu, hình ảnh. Nhờ có mạng **3G** ta có thể truy cập Internet cho cả thuê bao cố định hay di chuyển ở các tốc độ khác nhau. Hầu hết các smartphone hiện nay đều hỗ trợ **công nghệ 3G.** Hiện nay công nghệ **3G** được xây dựng với 4 chuẩn chính: **W-CDMA, CDMA2000, TD-CDMA, TD-SCDMA.**

Mạng 3G cải thiện chất lượng cuộc gọi, tín hiệu, tốc độ cao hơn hẳn so với mạng 2G. người dùng có thể truy cập Internet tốc độ cao ngay khi đang di chuyển, truy cập thế giới nội dung đa phương tiện: nhạc, phim, hình ảnh chất lượng cao. Người dùng có thể trò chuyện mọi nơi với chi phí rẻ hơn rất nhiều qua các ứng dụng hỗ trợ như: zalo, Viber, Line,…

Công nghệ 3G cũng được nhắc đến như là một chuẩn IMT-2000 của Tổ chức Viễn thông Thế giới (ITU). Ban đầu 3G được dự kiến là một chuẩn thống nhất trên thế giới, nhưng trên thực tế, thế giới 3G đã bị chia thành 4 phần riêng biệt:

W-CDMA**:** Tiêu chuẩn W-CDMA là nền tảng của chuẩn UMTS (Universal Mobile Telecommunication System), dựa trên kỹ thuật CDMA trải phổ dãy trực tiếp, trước đây gọi là UTRA FDD, được xem như là giải pháp thích hợp với các nhà khai thác dịch vụ di động (Mobile network operator) sử dụng GSM, tập trung chủ yếu ở châu Âu và một phần châu Á (trong đó có Việt Nam). UMTS được tiêu chuẩn hóa bởi tổ chức 3GPP, cũng là tổ chức chịu trách nhiệm định nghĩa chuẩn cho GSM, GPRS và EDGE.

CDMA**:** Một chuẩn 3G quan trọng khác là CDMA2000, là thế hệ kế tiếp của các chuẩn 2G CDMA và IS-95. Các đề xuất của CDMA2000 nằm bên ngoài khuôn khổ GSM tại Mỹ, Nhật Bản và Hàn Quốc. CDMA2000 được quản lý bởi 3GPP2, là tổ chức độc lập với 3GPP. Có nhiều công nghệ truyền thông khác nhau được sử dụng trong CDMA2000 bao gồm 1xRTT, CDMA2000-1xEV-DO và 1xEV-DV. CDMA 2000 cung cấp tốc độ dữ liêu từ 144 kbit/s tới trên 3 Mbit/s. Chuẩn này đã được chấp nhận bởi ITU.

TD-CDMA**:** Chuẩn TD-CDMA, viết tắt từ Time-division-CDMA, trước đây gọi là UTRA TDD, là một chuẩn dựa trên kỹ thuật song công phân chia theo thời gian (Time-division duplex). Đây là một chuẩn thương mại áp dụng hỗn hợp của TDMA và CDMA nhằm cung cấp chất lượng dịch vụ tốt hơn cho truyền thông đa phương tiện trong cả truyền dữ liệu lẫn âm thanh, hình ảnh. Chuẩn TD-CDMA và W-CMDA đều là những nền tảng của UMTS, tiêu chuẩn hóa bởi 3GPP, vì vậy chúng có thể cung cấp cùng loại của các kênh khi có thể. Các giao thức của UMTS là HSDPA/HSUPA cải tiến cũng được thực hiện theo chuẩn TD-CDMA.

TD-SCDMA**:** Chuẩn được ít biết đến hơn là TD-SCDMA (Time Division Synchronous Code Division Multiple Access) đang được phát triển tại Trung Quốc bởi các công ty Datang và Siemens, nhằm mục đích như là một giải pháp thay thế cho W-CDMA. Nó thường xuyên bị nhầm lẫn với chuẩn TD-CDMA. Cũng giống như TD-CDMA, chuẩn này dựa trên nền tảng UMTS-TDD hoặc IMT 2000 Time-Division (IMT-TD). Tuy nhiên, nếu như TD-CDMA hình thành từ giao thức mang cũng mang tên TD-CDMA, thì TD- SCDMA phát triển dựa trên giao thức của S-CDMA.

Mạng di động 3.5G: là hệ thống mạng di động truyền tải tốc độ cao HSDPA (High Speed Downlink Packet Access), phát triển từ 3G và hiện đang được 166 nhà mạng tại 75 nước đưa vào cung cấp cho người dùng. Nó được kết hợp từ 2 công nghệ kết nối không dây hiện đại HSPA và HSUPA, cho phép tốc độ truyền dẫn lên đến 7.2Mbp/s.

Mạng thông tin di động 4G**,** là công nghệ truyền thông không dây thế hệ thứ tư, cho phép truyền tải dữ liệu với tốc độ tối đa trong điều kiện lý tưởng lên tới 1 – 1,5 Gbit/s. Mạng 4G hiện đang được sử dụng phổ biến và hội tụ rất nhiều ưu điểm. Dưới đây là những ưu điểm nổi bật nhất của mạng di động 4G.

Tốc độ mạng 4G đạt mức rất ấn tượng khi trong điều kiện lý tưởng, tốc độ tải của công nghệ mạng này khi di chuyển lên đến 100 Mbps và đạt xấp xỉ 1Gbps nếu đứng yên.

Công suất và hiệu suất hoạt động của mạng di động 4G cực kỳ cao khi một trạm phát 4G có thể phục vụ cùng lúc khoảng 300-400 người dùng. Mạng 4G hỗ trợ các chương trình mã hóa nhanh hơn, nén được nhiều dữ liệu bit hơn so với mạng 3G.

Nhờ tốc độ truyền dữ liệu cao nên mạng 4G hỗ trợ các phần mềm chạy mượt mà hơn, người dùng được xem video chất lượng cao Full HD và 4K.

Tuy nhiên công nghệ mạng 4G vẫn chưa đủ đáp ứng nhu cầu thông tin giải trí với chất lượng ngày càng cao của người dùng. Chất lượng tín hiệu bị suy giảm rõ rệt, thậm chí mất kết nối tại những khu vực có mật độ cao người sử dụng (sân vận động, lễ hội, bến xe,...) hay di chuyển trên các phương tiện giao thông tốc độ cao (tàu điện, tàu hỏa). Hơn nữa, mạng 4G không hỗ trợ các công nghệ truy nhập vô tuyến đa dạng để có thể đáp ứng yêu cầu IoT. Do đó, Liên minh viễn thông quốc tế ITU đã định nghĩa mạng thông tin di động thế hệ kế tiếp với tên gọi IMT-2020 (hay ngắn gọn là 5G), dự kiến sẽ được tiêu chuẩn hóa và là thế hệ mạng tiếp theo.

1.1.2. Giới thiệu mạng di động 5G

Mạng 5G (5th Generation), là thế hệ thứ 5 của mạng di động tiếp theo sau công nghệ di động 4G. 5G có tốc độ kết nối, truyền tải dữ liệu cao, độ trễ gói tin nhỏ. Với tốc độ kết nối 4G hiện tại độ trễ có thể kéo dài khoảng 20ms, với mạng 5G độ trễ ước tính sẽ giảm xuống chỉ còn 1ms tương đương với thời gian nháy sáng của đèn flash máy ảnh. Độ trễ nhỏ giúp tiết kiệm năng lượng, nâng cao chất lượng dịch vụ. Cơ quan Liên minh Viễn thông Quốc tế ITU đưa ra tiêu chuẩn của mạng 5G hỗ trợ một triệu thiết bị kết nối với nhau trên 1km2. Theo tính toán, tốc độ 5G nhanh hơn 4G từ 40 đến 100 lần. 5G là công nghệ quan trọng của ngành viễn thông, 40% dân số thế giới sẽ sử dụng 5G vào năm 2025.

Mạng 5G sử dụng sóng milimét (Millimetre wave) đại diện cho phổ tín hiệu RF giữa các tần số từ 20GHz đến 300GHz với bước sóng từ 1~15mm. Hiện tại các dải tần được sử dụng gồm 24GHz, 38GHz, 60GHz, 70GHz, 80 GHz. Một số quốc gia tiên phong triển khai mạng 5G dùng dải tần 73 GHz. Việc sử dụng tần số cao giúp cải thiện tốc độ truyền, nhận dữ liệu, cho phép các kênh băng thông rộng hỗ trợ tốc độ truy cập lên tới 10 Gbit/s. Tuy nhiên, điểm yếu là khoảng cách truyền dữ liệu sẽ bị thu hẹp, đồng nghĩa với việc phải có rất nhiều trạm phát sóng 5G được xây dựng.

Trong công nghệ mạng 2G, 3G và 4G chỉ sử dụng các trạm thu phát đặt trên mặt đất. Mạng 5G sử dụng các trạm thu phát trên không - HAPS (High Altitude Stratospheric Platform Stations). Các trạm HAPS là những chiếc

máy bay treo lơ lửng ở một vị trí cố định trong khoảng cách từ 7km đến 22km so với mặt đất và hoạt động như một vệ tinh, cách này giúp đường tín hiệu được truyền thẳng hơn và giảm tình trạng bị cản trở bởi những kiến trúc cao tầng. Ngoài ra, nhờ độ cao, trạm cơ sở có khả năng bao phủ diện tích rộng lớn, tăng diện tích vùng phủ sóng, thậm chí cả trên biển, nơi các trạm phát sóng trên đất liền không thể tới vẫn có tín hiệu mạng 5G.

Ăng-ten thu phát tín hiệu trong mạng 5G được cải tiến bằng cách sử dụng ăng-ten MIMO (Multiple Input, Multiple Output). Về bản chất, kích thước vật lý tổng thể của ăng ten MIMO 5G tương tự như 4G, đây là loại ăng ten tích hợp nhiều ăng-ten thu, phát sóng gồm các phần tử ăng ten nhỏ kết nối 4 mặt x 4 mặt để gửi và nhận nhiều dữ liệu cùng lúc, duy trì băng thông cao ở mọi thời điểm và đạt tốc độ tối đa khi truy cập mạng. Tất cả các thiết bị 5G bao gồm cả điện thoại di động sẽ được tích hợp công nghệ ăng ten MIMO.

Ngoài những cải tiến về tốc độ, dung lượng và độ trễ, 5G còn cung cấp các tính năng quản lý mạng, trong đó có tính năng chia mạng cho phép các nhà khai thác di động tạo nhiều mạng ảo trong một mạng 5G vật lý. Khả năng này sẽ cho phép các kết nối mạng không dây hỗ trợ các nhu cầu hoặc mô hình kinh doanh cụ thể và có thể được bán trên cơ sở dịch vụ. Chẳng hạn, một chiếc xe tự lái sẽ yêu cầu một lớp mạng cung cấp các kết nối cực nhanh, độ trễ thấp để một chiếc xe có thể điều hướng trong thời gian thực. Tuy nhiên, một thiết bị gia dụng có thể được kết nối thông qua kết nối mạng chậm hơn, tiêu thụ ít năng lượng hơn vì vấn đề hiệu suất cao không quan trọng. Với IoT (Internet of Things), có thể chỉ cần sử dụng các kết nối an toàn và chỉ có dữ liệu.

1.1.3. Lợi ích của mạng 5G

5G sẽ cung cấp tốc độ, độ trễ thấp và khả năng kết nối để tạo ra thế hệ ứng dụng, dịch vụ và cơ hội kinh doanh mới chưa từng thấy trước đây.

Có ba loại trường hợp sử dụng chính cho 5G:

Truyền thông từ máy đến máy khổng lồ - còn được gọi là Internet of Things (IoT) liên quan đến việc kết nối hàng tỷ thiết bị mà không có sự can thiệp của con người ở quy mô chưa từng thấy trước đây. Điều này có tiềm năng cách mạng hóa các quy trình và ứng dụng công nghiệp hiện đại bao gồm nông nghiệp, sản xuất và truyền thông kinh doanh.

Thông tin liên lạc có độ trễ thấp đáng tin cậy - nhiệm vụ quan trọng bao gồm kiểm soát thời gian thực các thiết bị, rô bốt công nghiệp, hệ thống an toàn và liên lạc từ phương tiện đến phương tiện, lái xe tự động và mạng lưới giao thông an toàn hơn. Thông tin liên lạc có độ trễ thấp cũng mở ra một thế giới mới nơi tất cả đều có thể chăm sóc y tế, thủ tục và điều trị từ xa.

Băng thông di động nâng cao - cung cấp tốc độ dữ liệu nhanh hơn đáng kể và dung lượng lớn hơn giúp thế giới luôn kết nối. Các ứng dụng mới sẽ bao gồm truy cập internet không dây cố định cho gia đình, các ứng dụng phát sóng ngoài trời mà không cần xe truyền hình và kết nối tốt hơn cho những người đang di chuyển.

Đối với cộng đồng, 5G sẽ cho phép kết nối hàng tỷ thiết bị cho các thành phố thông minh, trường học thông minh và ngôi nhà thông minh của chúng ta, các phương tiện thông minh và an toàn hơn, tăng cường chăm sóc sức khỏe và giáo dục cũng như cung cấp một nơi an toàn và hiệu quả hơn để sống.

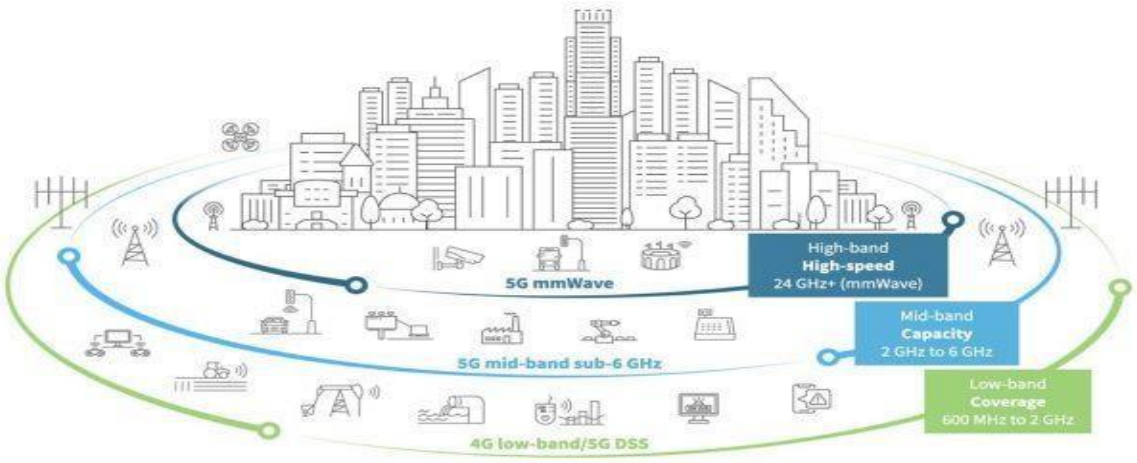
Đối với các doanh nghiệp và ngành công nghiệp, 5G và IoT sẽ cung cấp vô số dữ liệu cho phép họ hiểu sâu hơn về hoạt động của mình hơn bao giờ hết. Các doanh nghiệp sẽ vận hành và đưa ra các quyết định quan trọng do dữ liệu thúc đẩy, đổi mới trong nông nghiệp, trang trại thông minh và sản xuất, mở đường cho việc tiết kiệm chi phí, trải nghiệm khách hàng tốt hơn và tăng trưởng dài hạn.

Tất cả mọi người đều có thể tiếp cận các công nghệ mới và đang nổi như thực tế ảo và thực tế tăng cường. Thực tế ảo cung cấp những trải nghiệm kết nối mà trước đây không thể thực hiện được. Với 5G và VR, bạn sẽ có thể đi đến thành phố yêu thích của mình, xem một trận bóng đá trực tiếp với cảm giác như đang ở trên sân bóng, hoặc thậm chí có thể kiểm tra bất động sản và đi bộ qua một ngôi nhà mới từ sự thoải mái trên chiếc ghế dài của bạn.

5G sẽ giúp chúng ta kết nối trong các thành phố thông minh, ngôi nhà thông minh và trường học thông minh của ngày mai, đồng thời tạo ra những cơ hội mà chúng ta thậm chí chưa nghĩ đến.

1.2. Kiến trúc mạng 5G

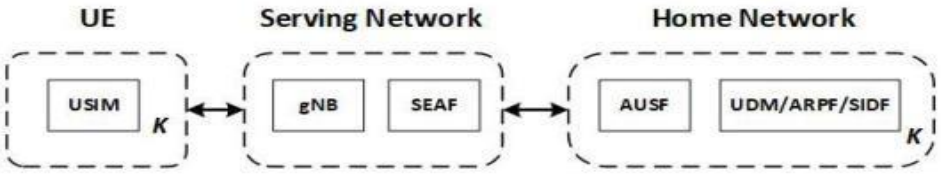
1.2.1. Hệ thống thông tin mạng di động 5G



Hình 1.2: Mô hình tổng thể hệ thống thông tin mạng 5G

1.2.2. Kiến trúc mạng di động 5G

Từ ngữ cảnh xác thực, mạng di động 5G bao gồm 3 thành phần cơ bản: Thiết bị người dùng UE (User Equipment), mạng dịch vụ SN (Serving Network), và mạng thường trú HN (Home Network) như trong hình 1.3.



Hình 1.3: Các thành phần chính trong mạng di động 5G

UE là thiết bị di động kết nối với mạng thường trú thông qua giao diện vô tuyến. Mỗi UE có một thẻ mạch tích hợp chung UICC (Universal Integrated Cicuit Card), lưu trữ ít nhất một USIM (Universal Subscriber Identity Module), USIM là nơi lưu trữ:

- Định danh cố định của thuê bao SUPI (Subscription Permanent Identifier).
- Khóa mật mã được chia sẻ trước giữa thuê bao và mạng thường trú.
- Khóa công khai của mạng thường trú.

Mạng dịch vụ gồm 2 phần tử: gNB là trạm gốc thay thế cho eNodeB của mạng 4G [1], chức năng kết nối an ninh SEAF (Security Anchor Function) giữ vai trò là trung gian kết nối giữa UE và mạng thường trú. SEAF có thể từ chối xác thực từ UE, nhưng nó cũng phụ thuộc vào mạng thường trú để chấp nhận xác thực UE.

Mạng thường trú gồm các thành phần sau:

Chức năng máy chủ xác thực AUSF (Authentication Server Function) là một thành phần của mạng thường trú. AUSF thực thi quyết định việc xác thực UE.

Quản lý dữ liệu hợp nhất UDM (Unified Data Management) là thực thể lưu trữ các chức năng liên quan đến quản lý dữ liệu, chẳng hạn ARPF và SIDF.

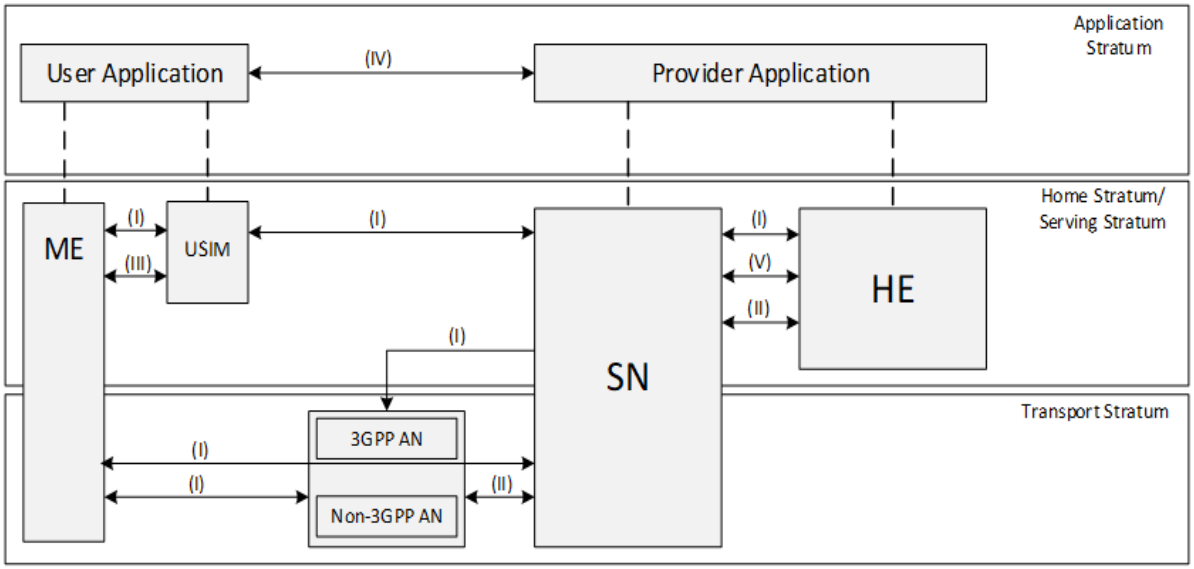
Chức năng lưu trữ và xử lý thông tin xác thực ARPF (Authentication Credential Repository and Processing Function), lựa chọn một trong 3 phương pháp xác thực dựa vào danh tính của thuê bao và chính sách đã cấu hình. Đồng thời, tính toán dữ liệu xác thực và dẫn xuất khóa cho AUSF (nếu cần).

Chức năng trích xuất định danh của thuê bao SIDF (Subscription Identifier De-concealing Function) chịu trách nhiệm giải mã định danh ẩn của thuê bao SUCI (Subscription Concealed Identifier) để có được định danh cố định của thuê bao (SUPI).

1.3. Vấn đề an ninh mạng 5G

1.3.1. Kiến trúc an ninh mạng di động 5G

Kiến trúc an ninh được tổ chức thành 3 tầng gồm: tầng ứng dụng, tầng dịch vụ và tầng vận chuyển. Hình 1.4 cho thấy một sơ đồ đơn giản của tầng dịch vụ và tầng vận chuyển.



Hình 1.4: Kiến trúc an ninh của mạng 5G

Bảo mật truy cập mạng (I): Một tập hợp các tính năng và cơ chế cho phép một UE xác thực và truy cập an toàn các dịch vụ mạng. Do đó, các UE trao đổi thông điệp giao thức thông qua mạng truy cập với mạng phục vụ (serving network -SN) và tận dụng PKI, nơi các khóa được lưu trữ trong USIM và môi trường mạng thường trú HE (Home Environment).

Bảo mật miền mạng (II): Một tập hợp các tính năng và cơ chế cho phép các nút mạng trao đổi an toàn dữ liệu luồng báo hiệu và luồng dữ liệu trong mạng 3GPP và giữa các mạng.

Bảo mật miền người dùng (III): Một tập hợp các tính năng và cơ chế tại UE nhằm đảm bảo quyền truy cập vào thiết bị di động và các dịch vụ di động. Nó thiết lập các cơ chế bảo mật phần cứng để ngăn các thiết bị đầu cuối di động và USIM bị thay đổi.

Bảo mật miền kiến trúc nền dịch vụ (SBA) (IV): Một tập hợp các tính năng và cơ chế mạng để đăng ký, phát hiện và ủy quyền phần tử mạng, cũng như để bảo vệ các giao diện dựa trên dịch vụ. Nó cho phép các chức năng 5GC mới, có thể được triển khai như các chức năng mạng ảo, được tích hợp một cách an toàn. Nó cũng cho phép chuyển vùng an toàn, liên quan đến SN cũng như mạng thường trú (HN/HE).

Khả năng hiển thị và khả năng cấu hình của bảo mật: Một tập hợp các tính năng và cơ chế cho phép thông báo cho người dùng liệu tính năng bảo mật có đang hoạt động hay không. Nó cũng có thể được sử dụng để cấu hình các tính

năng bảo mật. Các thông số kỹ thuật bảo mật 3GPP cho 5G chính thức thiết lập các tính năng bảo mật tùy chọn và mức độ tự do để triển khai và vận hành mạng an toàn. Điều này có nghĩa là người dùng 5G có thể sẽ gặp phải bối cảnh bảo mật khác nhau.

1.3.2. Các thách thức an ninh trong mạng 5G

Để hiểu đúng về việc đảm bảo an toàn kiến trúc của mạng một cách có hệ thống, thì đảm bảo an toàn theo kiến trúc mạng được mô tả theo ba cấp.

- Mạng truy cập

- Mạng Backhaul

- Mạng lõi

Để rõ ràng hơn, phần dưới sẽ nêu cụ thể hơn những thách thức về an toàn kiến trúc mạng di động 5G.

A. Thách thức an toàn cho mạng truy cập (Access Networks)

Tốc độ: Yêu cầu chính của mạng 5G là tốc độ dữ liệu cao với tính khả dụng phổ biến và độ trễ cực thấp. Các trường hợp sử dụng mới của MTC, IoT và V2X, Vv… sẽ đặt ra các yêu cầu rất đa dạng đối với mạng. Ví dụ: V2X và các ứng dụng MTC quan trọng sẽ cần độ trễ theo thứ từ 1 giây trở xuống, Ngoài những yêu cầu như vậy, độ tin cậy và tính sẵn sàng của các dịch vụ sẽ có yêu cầu cao hơn so với các mạng hiện tại. Tuy nhiên, các mạng hiện tại đã có xu hướng gặp rất nhiều mối đe dọa trên internet có thể nhắm mục tiêu đến các nút truy cập như eNB (E-UTRAN Node B) trong LTE và các nút truy cập được cung cấp năng lượng thấp. Với sự kết hợp của các thiết bị IP đa dạng trong 5G, các mối đe dọa bảo mật sẽ ra tăng hơn nữa.

Số lượng: Với sự gia tăng nhanh chóng của một số lượng lớn các thiết bị dịch vụ mới, nhu cầu về dung lượng mạng đang tăng nhanh hơn bao giờ hết bên cạnh việc cải thiện ngân sách liên kết và phạm vi phủ sóng. HetNets sẽ chia các nút với các đặc điểm khác nhau như công suất truyền, tần số vô tuyến,

***Không đồng nhất (HetNets)*:** Việc chuyển giao giữa các công nghệ truy cập khác nhau, như 3GPP và non-3GPP là một thách thức lớn. Ví dụ: các cuộc tấn công phát lại phiên thông qua khôi phục khóa phiên và khả năng điểm truy cập độc hại không được bảo mật trong 3GPP là những thách thức chính. Tuy nhiên, khi mạng 5G càng có số lượng điểm truy cập tăng lên và có nhiều

hơn các công nghệ truy cập khác nhau trong Hetnets 5G thì các vấn đề bảo mật liên quan còn mở rộng thêm rất nhiều. Vấn đề thiết kế các giao thức quản lý khóa an toàn vẫn là một thách thức còn bỏ ngỏ trong mạng 5G.

Các mạng 3GPP hiện tại yêu cầu UE cung cấp IMSI của nó qua mạng ở dạng không được mã hóa trong giai đoạn đính kèm ban đầu. Điều này cho phép những kẻ tấn công thụ động xác định được người dùng từ IMSI bằng cách quan sát lưu lượng truy cập. Điều này cũng khiến kẻ tấn công dễ dàng theo dõi người dùng trong quá trình chuyển vùng từ mạng này sang mạng khác.

B. Những thách thức an toàn cho mạng lõi:

Mạng lõi của LTE hoặc 4G, được gọi là EPC, bao gồm các thực thể khác nhau như MME, cổng phục vụ, cổng PDN và HSS. Trong 5G, các phần tử mạng lõi được thể hiện bằng chức năng mạng. Kiến trúc chi tiết của mạng lõi 5G với mô tả từ các chức năng mạng được mô tả ở phần 1.2.2 GPP Realese mới nhất. Mạng lõi dựa trên IP và đảm bảo cung cấp dịch vụ đầu cuối, bảo mật QoS, cũng như duy trì thông tin thuê bao. Mạng 5G linh động hơn so với các thế hệ trước đó nhờ sử dụng công nghệ NFV, SDN và đám mây. Tuy nhiên sự nâng cấp cải tiến cũng là mục tiêu chính của các mối đe dọa bảo mật và dễ có lỗ hổng bảo mật.

Trong 5G, khi hoạt động kết nối một số lượng lớn các thiết bị IoT có thể sẽ làm quá tải signaling plane như bị một cuộc tấn công DoS: Hàng tỷ các thiết bị IoT hạn chế tài nguyên, sẽ yêu cầu tài nguyên trong các đám mây để thực hiện xử lý, lữu trữ hoặc chia sẻ thông tin. Khả năng hạn chế của chúng cũng làm cho các thiết bị này trở thành mục tiêu dễ dàng để giả mạo hoặc trở thành môi trường cho các cuộc tấn công mạng dưới dạng tấn công DoS. Do đó, IoT sẽ mang lại nhiều thách thức cho vấn đề về tín hiệu hoặc mạng lõi.

Một số tấn công vào mạng 5G:

Tấn công bảo mật có thể chia làm 2 loại chính đó là tấn công thụ động và tấn công chủ động. Tấn công chủ động, kẻ tấn công cố gắng hoặc sử dụng thông tin những người dùng hợp pháp nhưng không làm ảnh hưởng đến trạng thái của thông tin. Những tấn công thụ động phổ biến trong mạng là tấn công nghe lén và phân tích lưu lượng đường truyền. Tấn công thụ động hướng đến những dữ liệu bảo mật riêng tư và quyền riêng tư của người dùng. Khác với tấn công thụ

động, tấn công chủ động có thể thay đổi dữ liệu hoặc gián đoạn liên lạc hợp pháp. Các tấn công chủ động như tấn công *Man - in - The maddle* (MITM), tấn công Relay, từ chối dịch vụ (DOS), phân tích tấn công từ chối dịch vụ (DDoS), những cơ chế được sử dụng để giải quyết các tấn công bảo mật có thể hầu hết được chia thành hai loại: Phương pháp tiếp cận mật mã với những giao thức mạng mới và phương pháp bảo mật lớp vật lý. Những kỹ thuật mật mã hầu hết được sử dụng cơ chế bảo mật mà thông thường được triển khai ở những lớp phía trên của mạng không dây 5G với những giao thức mạng mới. Mã hóa hiện đại bao gồm mã hóa đối xứng và mã hóa khóa công khai. Mã hóa khóa đối xứng nhằm vào những phương pháp mã hóa khóa bí mật chỉ được chia sẻ giữa người gửi và người nhận.

Trong khi đó, mã hóa khóa công khai hoặc còn gọi là mã hóa khóa bất đối xứng sử dụng 2 dạng khóa khác nhau, khóa công khai sử dụng cho mã hóa và khóa bí mật cho giải mã. Hiệu suất của một dịch vụ bảo mật phụ thuộc vào độ dài khóa và độ phức tạp tính toán của thuật toán. Quản lý và phân phối của những khóa đối xứng hoạt động bảo vệ tốt trong truyền thông. Do những giao thức phức tạp hơn và kiến trúc mạng bất đối xứng trong 5G, việc quản lý và phân phối của những khóa đối xứng có thể gặp những thách thức mới.

1.4. Kết luận chương

Chương này tìm hiểu tổng quan về mạng 5G với việc giới thiệu các thế hệ mạng di động từ 1G đến 5G. Đặc biệt trình bày các đặc điểm của mạng di động 5G, lợi ích của mạng 5G, kiến trúc và vấn đề an ninh của mạng di động 5G.

CHƯƠNG 2: NGHIÊN CỨU GIAO THỨC XÁC THỰC VÀ THỎA THUẬN KHÓA TRONG MẠNG DI ĐỘNG 5G

2.1. Giới thiệu chung xác thực và thỏa thuận khóa

Phân phối khóa là một cơ chế mà một bên (thường là *TA*) chọn khóa bí mật và sau đó truyền các khóa này cho bên kia. Việc truyền khóa bí mật được thực hiện bằng một kênh an toàn. Sau khi truyền xong khóa bí mật thì hai bên liên quan sẽ có thể liên lạc an toàn với nhau trên kênh không an toàn.

Thỏa thuận khóa là một giao thức mà hai hay nhiều bên liên kết với nhau để thiết lập một khóa bí mật bằng cách giao tiếp trên một kênh công khai. Trong một lược đồ thỏa thuận khóa, giá trị của khóa được xác định là một hàm của những đầu vào do các bên đã cung cấp và thông tin bí mật của hai bên liên lạc.

Bảo mật là một trong những chủ đề đã được thực hiện từ 2G lên 5G. Ngày nay, 5G là mạng di động an toàn và đáng tin cậy nhất. Nền tảng bảo mật của nó nằm trong mật mã, đặc biệt là hai quy trình cơ bản, đó là xác thực và thỏa thuận khóa.

Xác thực: Người dùng cần có đăng ký với nhà vận hành mạng di động MNO (Mobile Network Operator) để có thể truy cập mạng của MNO. Người dùng có đăng ký MNO được phép sử dụng các dịch vụ do mạng của MNO cung cấp, chẳng hạn như SMS, cuộc gọi thoại và truy cập Internet. Các MNO lần lượt lập hóa đơn hoặc tính phí người dùng cho các dịch vụ mà họ đã sử dụng. Để mô hình kinh doanh này hoạt động, mạng cần số nhận dạng đăng ký dài hạn duy nhất của người dùng được gọi là nhận dạng thuê bao di động quốc tế (IMSI) ở 2G, 3G và 4G hoặc mã nhận dạng vĩnh viễn của người dùng (SUPI) trong 5G. UE cung cấp số nhận dạng này được lưu trữ trong thẻ SIM cho mạng, do đó, xác định được người dùng. Tuy nhiên, để đảm bảo rằng người dùng không thể từ chối hóa đơn hoặc để ngăn người dùng gian lận mạo danh giá trị nhận dạng của người khác, mạng phải xác nhận rằng người dùng chính là người dùng hợp pháp. Xác thực cung cấp chức năng như vậy.

Trong 3GPP, xác thực là một quá trình bảo mật xác thực bằng mật mã hoặc chứng minh rằng số định danh thuê bao di động quốc tế IMSI thuộc về một người dùng cụ thể. Ngoài ra còn có một mặt khác của xác thực trong đó UE khẳng định rằng mạng đúng là nhà mạng cần liên lạc. Khi cả mạng và UE xác thực lẫn nhau, xác thực lẫn nhau sẽ đạt được.

Thỏa thuận khóa: Mặc dù không thể thiếu, nhưng chỉ xác thực là không đủ vì tính bảo mật của mạng di động cũng đòi hỏi lưu lượng truy cập an toàn. Các khả năng bảo mật khác, chủ yếu là bảo mật/mật mã, bảo vệ tính toàn vẹn và bảo vệ phát lại lưu lượng truy cập cũng cần thiết. Bảo mật/mật mã có nghĩa là mã hóa lưu lượng truy cập để người nhận trái phép không thể giải mã và đọc tin nhắn gốc. Bảo vệ tính toàn vẹn có nghĩa là thêm mã xác thực tin nhắn vào lưu lượng truy cập để các bên trái phép không thể giả mạo tin nhắn gốc khi người nhận phát hiện ra sự giả mạo. Bảo vệ phát lại có nghĩa là theo dõi lưu lượng để các bên trái phép không thể gửi lại lưu lượng hợp lệ trước đó mà người nhận không phát hiện được phát lại. Các phương tiện mật mã để đạt được các khả năng bảo mật này cần có các khóa bảo mật. Thỏa thuận khóa là những gì cung cấp các khóa bảo mật được yêu cầu.

Trong 3GPP, thỏa thuận khóa là một quy trình bảo mật cho phép UE và mạng thiết lập một hoặc nhiều khóa bảo mật dùng chung để bảo vệ các phiên liên lạc.

Xác thực và thỏa thuận khóa (AKA): Sự kết hợp của hai quy trình nêu trên được gọi trực quan là Xác thực và Thỏa thuận khóa. Nó là một giao thức bảo mật ở dạng giao thức phản hồi thách thức (challenge-response) trong đó mạng cung cấp thách thức (challenge) mật mã và UE cung cấp phản hồi mật mã.

3GPP luôn sửa đổi AKA để cải tiến khi phát triển các mạng di động thế hệ mới. Một ví dụ về cải tiến về mặt xác thực là trong khi chỉ có mạng xác thực UE trong 2G (xác thực một phía), nhưng trong các mạng di động thế hệ sau UE cũng xác thực (xác thực lẫn nhau). Ví dụ tương tự về các cải tiến thỏa thuận khóa vì trong 2G chỉ có khóa mã hóa được thiết lập, nhưng các mạng thế hệ sau đã bổ sung khóa để bảo vệ tính toàn vẹn sau thủ tục thỏa thuận khóa.

Có tám phiên bản chính của AKA trong 3GPP từ 2G đến 5G. Điểm chung của chúng là chúng dựa trên mật mã đối xứng, một khóa đối xứng được chia sẻ trước (K) được chia sẻ giữa mạng di động và thẻ SIM. Từ khóa K này, các khóa bảo mật được dẫn xuất từ ME và mạng di động. Tuy nhiên, khóa K không bao giờ nằm ngoài chức năng mạng lõi trong mạng di động và thẻ SIM. Lưu ý rằng cả SIM (2G) và UICC (3G, 4G, 5G) đều được coi là thành phần phần cứng an toàn chống giả mạo.

2.1.1. Mục đích của xác thực và thỏa thuận khóa

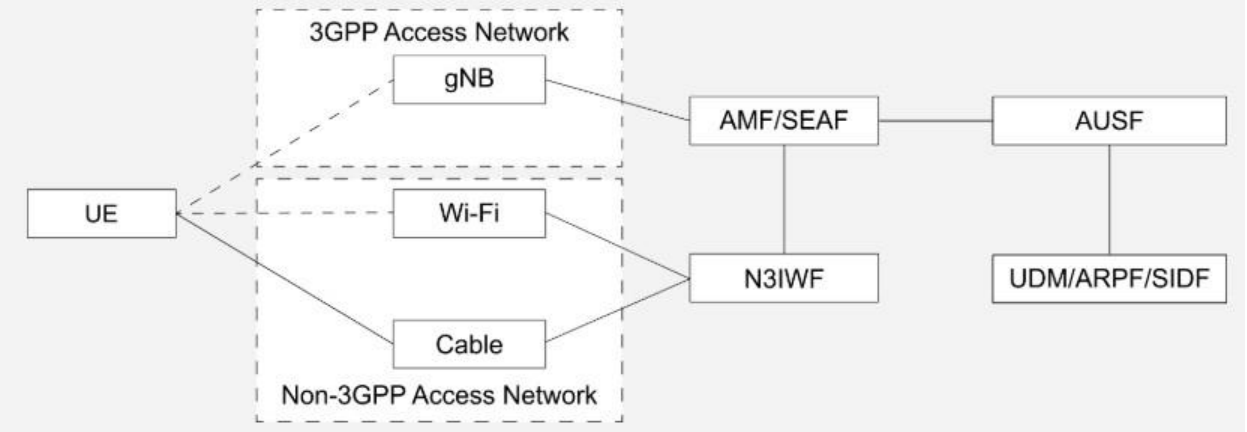
Mục đích của xác thực và thỏa thuận khóa là cho phép xác thực lẫn nhau giữa UE và mạng. Cung cấp khóa có thể được sử dụng giữa UE và mạng phục vụ trong các thủ tục bảo mật tiếp theo. Kết thúc giao thức xác thực và thỏa thuận khóa, AUSF tạo ra khóa K_{SEAF} cho SEAF của mạng phục vụ.

Các khóa cho nhiều hơn một ngữ cảnh bảo mật có thể được lấy từ K_{SEAF} mà không cần chạy xác thực mới. Một ví dụ cụ thể về điều này là xác thực qua mạng truy cập 3GPP cũng có thể cung cấp các khóa để thiết lập bảo mật giữa UE và N3IWF được sử dụng trong Non-3GPP.

Khóa K_{SEAF} có nguồn gốc từ một khóa trung gian gọi là K_{AUSF}. K_{AUSF} được thành lập giữa UE và HN do quá trình xác thực và thỏa thuận khóa. K_{AUSF} có thể được lưu trữ an toàn trong AUSF dựa trên chính sách sử dụng của nhà điều hành mạng thường trú.

2.1.2. Khung xác thực

Khung xác thực được định nghĩa để thực thi xác thực 5G cho cả mạng truy cập 3GPP và mạng phi truy cập 3GPP (Non-3GPP) (xem hình 2.1)



Hình 2.1: Khung xác thực của 5G

Một khi giao thức xác thực mở rộng được sử dụng (EAP-AKA‟ hoặc EAP-TLS), thì SEAF đóng vai trò chuyển tiếp giữa UE và AUSF.

Khi UE kết nối với mạng Wifi hoặc mạng dây gọi là mạng phi truy cập 3GPP (Non-3GPP), thì thực thể mới cụ thể là chức năng liên kết N3IWF (Non-3GPP Interworking Function), được yêu cầu hoạt động như một máy chủ VPN để cho phép UE truy cập vào mạng lõi 5G qua mạng phi truy cập thông qua các đường hầm IPsec (bảo mật IP).

Một số bối cảnh an ninh có thể được thiết lập với một lần thực thi xác thực, cho phép UE di chuyển từ mạng truy cập 3GPP tới mạng non-3GPP mà không cần phải xác thực lại.

2.1.2.1. Khung EAP

Khung EAP được giới thiệu chi tiết trong RFC 3748. Nó xác định các vai trò sau: máy chủ xác thực ngang hàng, máy chủ chuyển tiếp và máy chủ xác thực phụ trợ. Máy chủ xác thực phụ trợ hoạt động như máy chủ EAP, máy chủ này kết thúc phương thức xác thực EAP với máy ngang hàng. Trong hệ thống 5G, khung EAP được hỗ trợ theo cách sau:

- UE giữ vai trò điểm ngang hàng.

- SEAF giữ vai trò là thực thể xác thực thông tin.

- AUSF giữ vai trò của máy chủ xác thực phụ trợ.

2.1.2.2. Các thành phần của dẫn xuất khóa liên kết khóa với mạng dịch vụ

Các thủ tục xác thực và thỏa thuận khóa có liên quan đến khóa K_{SEAF} của mạng dịch vụ. Liên kết với mạng dịch vụ ngăn một mạng dịch vụ tự nhận là mạng dịch vụ khác và do đó cung cấp xác thực mạng dịch vụ ngầm cho UE.

Xác thực mạng dịch vụ ngầm này sẽ được cung cấp cho UE bất kể là công nghệ mạng truy cập 3GPP hay mạng truy cập non-3GPP.

Hơn nữa, khóa dẫn xuất được cung cấp cho mạng dịch vụ cũng phải cụ thể cho xác thực đã diễn ra giữa UE và mạng lõi 5G, tức là K_{SEAF} sẽ được tách bằng mật mã từ khóa K_{ASME} được phân phối từ mạng thường trú đến mạng dịch vụ trong các thế hệ mạng di động trước đó.

Liên kết khóa phải đạt được bằng cách bao gồm một tham số được gọi là "tên mạng phục vụ" Các khóa dẫn xuất từ khóa dài hạn của thuê bao đến khóa K_{SEAF}.

2.1.2.3. Tên mạng dịch vụ

Tên mạng dịch vụ được sử dụng trong dẫn xuất khóa. Nó phục vụ một mục đích kép, cụ thể là:

- Nó liên kết khóa với mạng dịch vụ bằng cách bao gồm mã định danh mạng dịch vụ (SN Id).

- Nó đảm bảo rằng khóa là cụ thể để xác thực giữa mạng lõi 5G và UE bằng cách bao gồm mã dịch vụ được đặt thành "5G".

- Trong 5G AKA, tên mạng dịch vụ có mục đích tương tự với liên kết RES* và XRES* của mạng dịch vụ.

- Tên mạng dịch vụ ghép với mã dịch vụ và SNid với ký tự phân tách ":" sao cho mã dịch vụ thêm vào SNid.

- SNid xác định PLMN phục vụ và ngoại trừ các mạng ngoài độc lập, được định nghĩa là mã định danh mạng SNN trong TS 24.501.

Xây dựng tên mạng dịch vụ của UE

UE xây dựng tên mạng dịch vụ như sau:

- Quy định đặt mã dịch vụ thành "5G".

- Nó sẽ đặt mã định danh mạng vào SNid của mạng mà nó đang xác thực.

- Kết hợp mã dịch vụ và SNid với ký tự tách ":".

Xây dựng tên mạng dịch vụ của SEAF

SEAF sẽ xây dựng tên mạng dịch vụ như sau:

- Quy định đặt mã dịch vụ thành "5G".

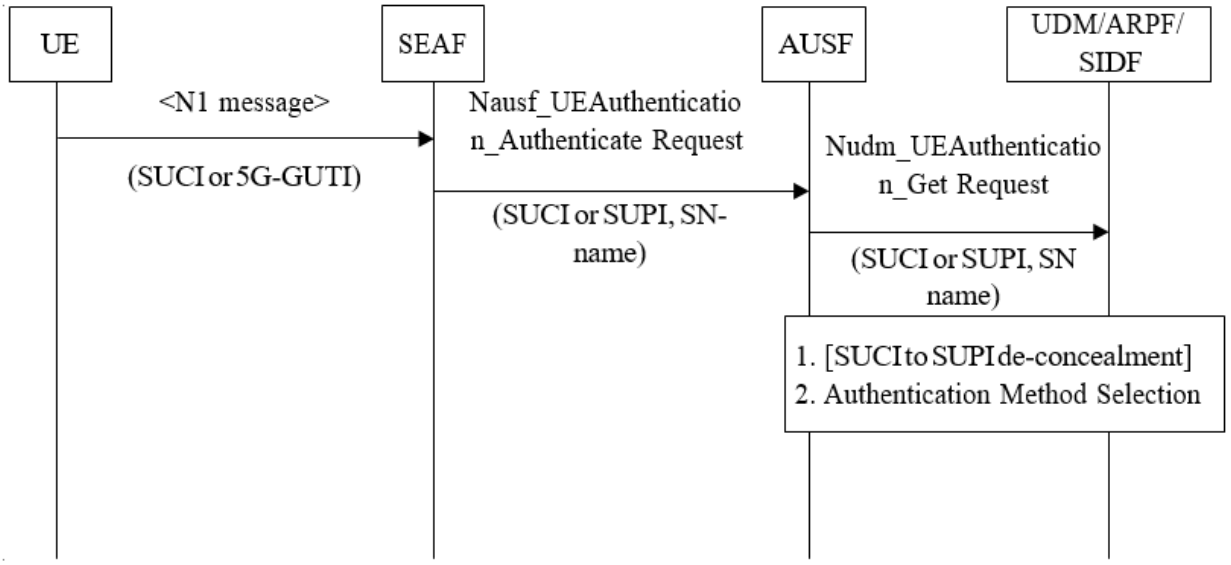
- Nó sẽ đặt mã định danh mạng vào SNid của mạng dịch vụ mà AUSF gửi dữ liệu xác thực.

- Nó sẽ kết hợp mã dịch vụ và chứng minh SN với ký tự tách ":".

*Lưu ý: AUSF nhận được tên mạng dịch vụ từ SEAF. Trước khi sử dụng tên mạng dịch vụ, AUSF kiểm tra xem SEAF có được phép sử dụng không.

2.1.3. Khởi tạo và lựa chọn phương pháp xác thực

SEAF có thể khởi tạo thủ tục xác thực sau khi nhận được thông báo từ UE. Thông báo này chứa định danh tạm thời 5G-GUTI hoặc định danh ẩn của thuê bao SUCI. Nếu 5G-GUTI chưa được phân bổ từ mạng dịch vụ cho UE thì SUCI được sử dụng. Khi đó, SUCI sử dụng khóa công khai của mạng thường trú để mã hóa SUPI.



Hình 2.2: Khởi tạo và lựa chọn phương pháp xác thực

SEAF chuyển tiếp yêu cầu xác thực *Nausf_UEAuthentication Request,* chứa SUCI hoặc SUPI cùng với định danh của mạng dịch vụ SN- name tới AUSF.

Khi nhận được thông báo,*Nausf_UEAuthentication_AuthenticateRequets, AUSF* sẽ kiểm tra xem yêu cầu SEAF trong mạng dịch vụ có quyền sử dụng tên mạng dịch vụ trong Nausf_UEAuthentication_Authenticate Request bằng cách so sánh tên mạng dịch vụ với tên mạng dịch vụ dự kiến. AUSF sẽ lưu trữ tạm thời tên mạng dịch vụ nhận được. Nếu mạng dịch vụ không được phép sử dụng tên mạng dịch vụ, AUSF sẽ trả lời bằng "mạng dịch vụ không được phép" trong *Nausf_UEAuthentication_Authenticate Response.*

Nudm_UEAuthentication_Get Request được gửi từ AUSF đến UDM bao gồm các thông tin sau:

- SUCI hoặc SUPI;

- Tên mạng dịch vụ;

- Sau khi nhận được *Nudm_UEAuthentication_Get Request,* UDM sẽ gọi SIDF nếu nhận được SUCI. SIDF sẽ giải mã SUCI để được SUPI trước khi UDM có thể xử lý yêu cầu.

Dựa trên SUPI, UDM/ARPF sẽ chọn phương thức xác thực.

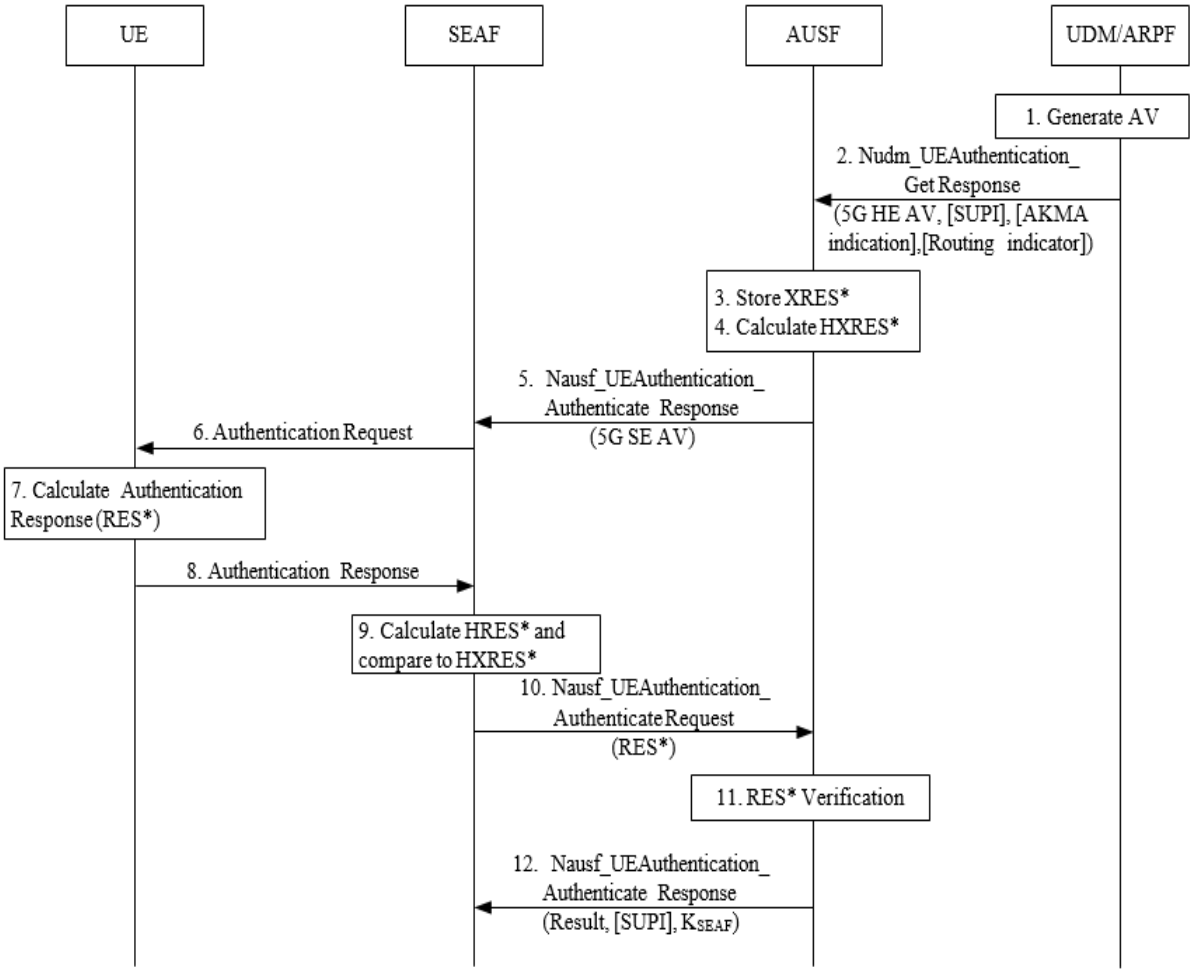
*Lưu ý: *Nudm_UEAuthentication_Get Response* để trả lời *Nudm_UEAuthentication_Get Request* và thông báo *Nausf_UEAuthentication_Authenticate Response* để trả lời thông báo *Nausf_UEAuthentication_Authenticate Request.*

2.2. Phân tích giao thức xác thực và thỏa thuận khóa trong mạng 5G

Xác thực và thỏa thuận khóa đạt được bằng việc thực thi giao thức xác thực giữa người dùng và mạng. Mỗi thế hệ mạng di động có các giao thức xác thực riêng, 3GPP đã chỉ định 3 phương pháp xác thực trong mạng 5G gồm: 5G-AKA, EAP-AKA‟ và EAP-TLS. Mạng thường trú lựa chọn một phương pháp xác thực phù hợp dựa vào định danh của UE.

2.2.1. Giao thức xác thực và thỏa thuận khóa 5G AKA

Sau khi thực hiện mục 2.1.3 thì UDM/ARPF lựa chọn phương pháp xác thực là 5G AKA. 5G AKA là phiên bản cải tiến của giao thức AKA hiện đang được sử dụng trong 4G (EPS-AKA) [1]. Quy trình giao thức 5G AKA hoạt động như sau [2,3]:



Hình 2.3: Thủ tục xác thực cho 5G AKA

1. Đối với mỗi Nudm_Authenticate_Get Respone, UDM/ARPF sẽ tạo ra 5G HE AV. UDM/ARPF thực hiện điều này bằng cách tạo ra một AV với bit tách trường quản lý xác thực (AMF) được đặt thành "1". UDM/ARPF sau đó sẽ dẫn xuất K_{AUSF} như mục 2.3.1 của tài liệu và tính XRES*. Cuối cùng, UDM/ARPF sẽ tạo ra 5G HE AV từ RAND, AUTN, XRES* và K_{AUSF}.

2. UDM sau đó sẽ trả lại 5G HE AV cho AUSF cùng với một dấu hiệu cho thấy 5G HE AV sẽ được sử dụng cho 5G AKA trong thông báo phản hồi *Nudm_UEAuthentication_Get Response*.

3. AUSF sẽ lưu trữ XRES* tạm thời cùng với SUCI hoặc SUPI đã nhận được. AUSF có thể lưu K_{AUSF}.

4. AUSF sau đó sẽ tạo ra AV 5G từ 5G HE AV nhận được từ UDM/ARPF bằng cách tính toán HXRES* từ XRES* và K_{SEAF} từ K_{AUSF}, và thay thế XRES* bằng HXRES* và K_{AUSF} bằng K_{SEAF} trong 5G HE AV.

5. AUSF sau đó sẽ xóa K_{SEAF} và gửi lại 5G SE AV (RAND, AUTN, HXRES*) cho SEAF trong thông báo phản hồi

Nausf_UEAuthentication_Authenticate Response.

6. SEAF sẽ gửi RAND, AUTN đến UE trong yêu cầu xác thực tin nhắn NAS. Thông báo này cũng sẽ bao gồm ngKSI sẽ được UE và AMF sử dụng để xác định K_{AMF} và bối cảnh bảo mật gốc một phần được tạo ra nếu xác thực thành công. Thông báo này cũng sẽ bao gồm tham số ABBA. SEAF sẽ thiết lập tham số ABBA. ME sẽ chuyển tiếp RAND và AUTN nhận được trong yêu cầu xác thực tin nhắn NAS đến USIM.

*Lưu ý: Tham số ABBA được bao gồm để cho phép giảm hóa đơn để bảo vệ các tính năng bảo mật có thể được giới thiệu sau này.

7. Khi nhận được RAND và AUTN, USIM sẽ kiểm tra tính mới của vectơ xác thực 5G AV bằng cách kiểm tra xem AUTN có được chấp nhận như mô tả trong TS 33.102 hay không. Nếu đúng, USIM tính toán RES phản hồi. USIM sẽ trả lại RES, CK, IK cho ME. Nếu USIM tính toán K_C (tức là GPRS K_C) từ CK và IK sử dụng chức năng chuyển đổi C3 (trong TS 33.102) và gửi nó đến ME, sau đó ME sẽ xóa K_C GPRS và không lưu trữ GPRS K_C trên USIM hoặc trong ME. Sau đó, ME sẽ tính RES* từ RES theo phụ lục A3. ME sẽ

tính K_{AUSF} từ CK//IK theo phụ lục A2. ME tính K_{SEAF} từ K_{AUSF} theo phụ lục A5. ME đang truy cập 5G sẽ kiểm tra việc xác thực bằng "bit tách trường" trong trường AMF của AUTN được đặt thành 1. "bit phân tách" là 0 của trường AMF của AUTN

8. UE sẽ trả lại RES* cho SEAF trong thông báo phản hồi xác thực NAS.

9. SEAF sau đó sẽ tính HRES* từ RES* theo phụ lục A.4 và SEAF sẽ so sánh HRES* và HXRES*. Nếu trùng nhau, SEAF sẽ quyết định xác thực thành công UE từ mạng dịch vụ. Nếu không, SEAF tiến hành như mục a) dưới đây. Nếu UE không tương tác và SEAF chưa từng nhận được RES*, SEAF sẽ coi việc xác thực UE là thất bại và gửi thông báo xác thực thất bại cho AUSF.

10. SEAF sẽ gửi RES*, như đã nhận được từ UE, trong thông báo phản hồi *Nausf_UEAuthentication_Authenticate Request* cho AUSF.

11.Khi AUSF nhận được thông báo yêu cầu xác thực *Nausf_UEAuthentication_Authenticate Request* bao gồm RES* nó có thể kiểm tra xem 5G AV đã hết hạn hay chưa. Nếu 5G AV đã hết hạn, AUSF có thể coi việc xác thực là không thành công. Ngược lại, AUSF sẽ so sánh RES* đã nhận được với XRES* được lưu trữ. Nếu RES* và XRES* bằng nhau, AUSF xem như xác thực thành công. AUSF sẽ thông báo cho UDM về kết quả xác thực.

12. AUSF sẽ chỉ ra cho SEAF trong *Nausf_UEAuthentication_Authenticate Response* cho dù việc xác thực có thành công hay không. Nếu xác thực thành công,K_{SEAF} sẽ được gửi đến SEAF trong thông báo *Nausf_UEAuthentication_Authenticate Response*. Trong trường hợp AUSF nhận được SUCI từ SEAF trong yêu cầu xác thực và nếu xác thực thành công, thì AUSF cũng sẽ đưa SUPI vào thông báo *Nausf_UEAuthentication_Authenticate Response*.

Nếu xác thực thành công, khóa K_{SEAF} nhận được trong thông báo Nausf_UEAuthentication_Authenticate Response sẽ trở thành khóa chủ trong phân cấp khóa (xem mục 2.3.1 của tài liệu này). Sau đó, SEAF sẽ dẫn xuất khóa K_{AMF} từ K_{SEAF}, tham số ABBA và SUPI. SEAF sẽ cung cấp ngKSI và K_{AMF} cho AMF. Nếu AUSF chỉ ra rằng việc xác thực đã thành công, thì AMF sẽ bắt đầu quy trình chế độ bảo mật NAS với UE, để sử dụng ngữ cảnh bảo mật NAS 5G gốc một phần mới được tạo ra. Sau khi nhận được thông báo chế độ bảo mật NAS hợp lệ từ AMF, UE sẽ xem xét xác thực chính được thực hiện là thành công.

Nếu SUCI được sử dụng cho việc xác thực này, thì SEAF sẽ chỉ cung cấp ngKSI và K_{AMF} cho AMF sau khi nó đã nhận được thông báo Nausf_UEAuthentication_Authenticate Response có chứa K_{SEAF} và SUPI; không có dịch vụ truyền thông nào được cung cấp cho UE cho đến khi SUPI được mạng dịch vụ biết đến.

Lỗi xác minh RES* trong SEAF hoặc AUSF hoặc cả hai:

Trong bước 9 ở phần trên, SEAF sẽ tính toán HRES* từ RES* và SEAF sẽ so sánh HRES* và HXRES*. Nếu chúng không trùng nhau, thì SEAF sẽ coi việc xác thực là không thành công.

SEAF sẽ tiếp tục với bước 10 trong quy trình và sau khi nhận được thông báo phản *hồi Nausf_UEAuthentication_Authenticate Response* từ AUSF ở bước 12, tiến trình được mô tả như dưới đây:

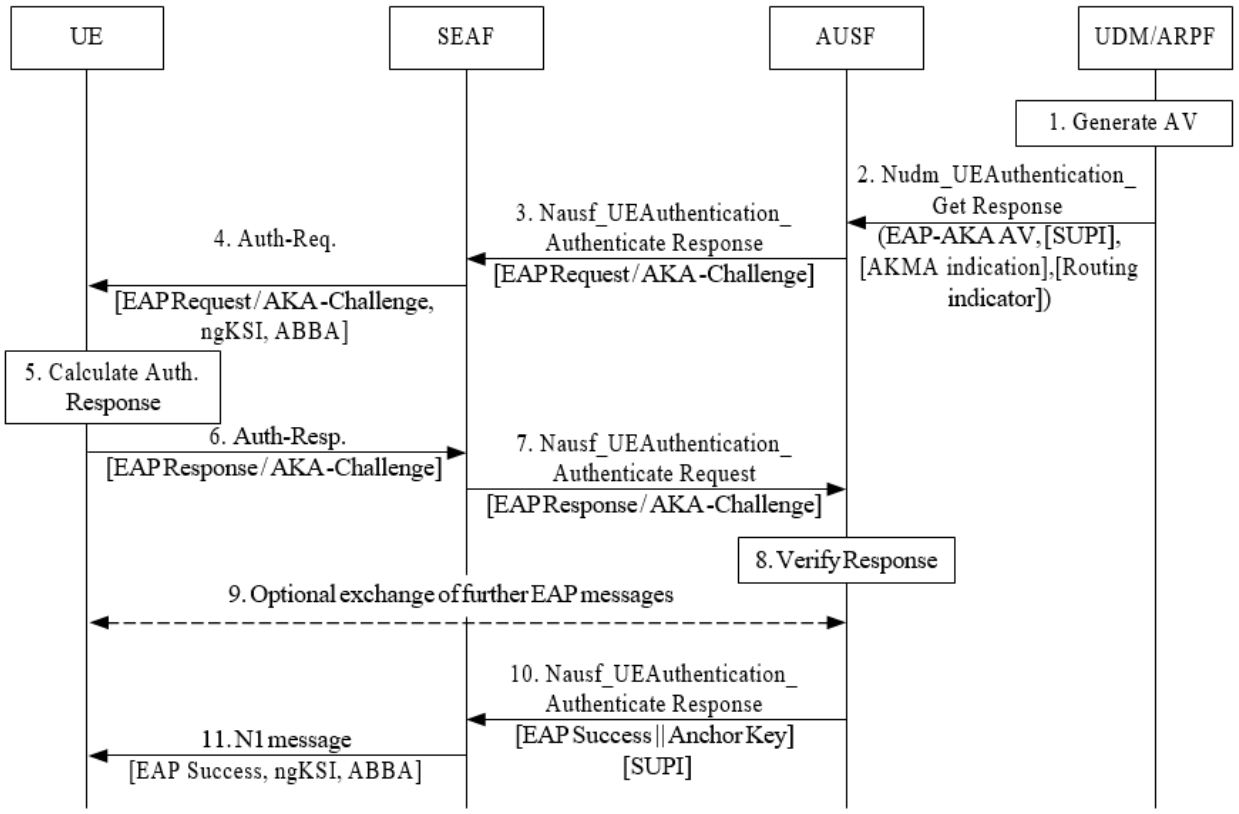
Nếu AUSF đã chỉ ra trong thông báo phản hồi *Nausf_UEAuthentication_Authenticate Response* cho SEAF rằng việc xác minh RES* không thành công ở AUSF.

Nếu kiểm tra RES* không thành công trong SEAF. SEAF sẽ từ chối xác thực bằng cách gửi từ chối xác thực đến UE nếu SUCI được UE sử dụng trong tin nhắn NAS ban đầu hoặc SEAF/AMF sẽ bắt đầu quy trình nhận dạng với UE nếu UE 5G-GUTI được UE sử dụng trong tin nhắn NAS ban đầu để lấy SUCI và bổ sung xác thực bổ sung có thể được bắt đầu.

Ngoài ra, nếu SEAF không nhận được bất kỳ thông báo phản hồi *Nausf_UEAuthentication_Authenticate Response* nào từ AUSF như mong đợi, thì SEAF sẽ từ chối xác thực cho UE hoặc bắt đầu lại thủ tục nhận dạng với UE.

2.2.1. Giao thức xác thực và thỏa thuận khóa EAP-AKA'

EAP-AKA‟ là phương pháp xác thực khác được hỗ trợ trong 5G. Nó cũng là giao thức dựa vào cơ chế hỏi - đáp sử dụng khóa mật đã được chia sẻ trước giữa UE và mạng thường trú. EAP-AKA' đạt được mức các thuộc tính bảo mật như 5G-AKA, ví dụ, việc xác thực lẫn nhau giữa UE và mạng. Vì nó dựa vào EAP, các luồng thông báo của nó khác với các luồng của 5G-AKA. Sau khi thực hiện mục 2.1.3 thì UDM/ARPF lựa chọn phương pháp xác thực là EAP-AKA'.



Hình 2.4: Thủ tục xác thực EAP-AKA'

Quy trình xác thực cho EAP-AKA hoạt động như sau:

1. UDM/ARPF trước tiên sẽ tạo ra một vector xác thực với bit tách trường quản lý xác thực (AMF) = 1. UDM/ARPF sau đó sẽ tính toán CK' và IK' để thay thế CK và IK theo phụ lục A1.

2. UDM sau đó sẽ gửi vector xác thực chuyển đổi AV' (RAND, AUTN, XRES, CK', IK') đến AUSF khi nó nhận được thông báo yêu cầu *Nudm_UEAuthentication_Get Request* cùng với chỉ định rằng AV' sẽ sử dụng cho EAP-AKA‟ bằng cách sử dụng thông báo phản hồi *Nudm_UEAuthentication_Get Response*.

Trong trường hợp SUCI được đưa vào thông báo yêu cầu *Nudm_UEAuthentication_Get Request,* UDM sẽ đưa SUPI vào thông báo phản hồi *Nudm_UEAuthentication_Get Response*. AUSF và UE sau đó sẽ tiến hành như được mô tả trong RFC 5448, cho đến khi AUSF sẵn sàng gửi EAP-Success.

Nếu thuê bao có đăng ký AKMA, UDM sẽ bao gồm chỉ dẫn AKMA trong thông báo phản hồi *Nudm_UEAuthentication_Get Response.*

3. AUSF sẽ gửi thông báo EAP-Request/AKA'-Challenge đến SEAF trong một thông báo phản hồi *Nausf_UEAuthentication_Authenticate Response.*

4. SEAF sẽ chuyển tiếp thông báo EAP-Request/AKA'-Challenge đến UE trong thông báo yêu cầu xác thực tin nhắn NAS. ME sẽ chuyển tiếp RAND và AUTN nhận được trong thông báo EAP-Request/AKA'- Challenge đến USIM. Thông báo này sẽ bao gồm tham số ngKSI và ABBA. Trên thực tế, SEAF sẽ bao gồm tham số ngKSI và ABBA trong tất cả các thông báo yêu cầu xác thực EAP. ngKSI sẽ được UE và AMF sử dụng để xác định trường hợp bảo mật gốc, một phần được tạo ra nếu xác thực thành công. SEAF sẽ thiết lập tham số ABBA. Trong quá trình xác thực EAP, giá trị của tham số ngKSI và ABBA do SEAF gửi đến UE sẽ không được thay đổi.

*Lưu ý: SEAF cần hiểu rằng phương pháp xác thực được sử dụng là phương pháp EAP bằng cách đánh giá loại phương thức xác thực dựa trên thông báo *Nausf_UEAuthentication_Authenticate Response*.

5. Khi nhận được RAND và AUTN, USIM sẽ kiểm tra tính mới của AV‟ bằng cách kiểm tra AUTN có thể được chấp nhận hay không. Nếu vậy, USIM tính toán RES phản hồi. USIM sẽ trả lại RES, CK, IK cho ME. Nếu USIM tính toán Kc (tức là GPRS Kc) từ CK và IK sử dụng chức năng chuyển đổi C3 [TS 33.102] và gửi nó đến ME, thì ME sẽ xóa bỏ GPRS Kc đó và không lưu trữ GPRS Kc trên USIM hoặc trong ME.

ME sẽ lấy CK‟ và IK' theo phụ lục A.3. Nếu việc xác minh AUTN thất bại trên USIM, thì USIM và ME sẽ tiến hành như được trình bày trong [3,mục 6.1.3.3].

6. UE sẽ gửi thông báo EAP-Response/AKA'-Challenge đến SEAF trong thông báo Auth-Resp của NAS.

7. SEAF sẽ chuyển tiếp thông báo EAP-Response/AKA'-Challenge đến AUSF trong thông báo *Nausf_UEAuthentication_Authenticate Reques*t.

8. AUSF sẽ xác minh thông báo bằng cách so sánh XRES và RES, nếu AUSF đã xác minh thành công thông báo này, nó sẽ tiếp tục như sau, nếu không sẽ trả lại lỗi cho SEAF. AUSF sẽ thông báo cho UDM về kết quả xác thực.

9. AUSF và UE có thể trao đổi EAP-Request/AKA'- Notification và EAP-Response/AKA'- Notification thông qua SEAF. SEAF sẽ chuyển tiếp các thông báo này.

10. AUSF có nguồn gốc EMSK từ CK' và IK'. AUSF sử dụng 256-bit đầu tiên của EMSK làm KAUSF và sau đó tính KSEAF từ KAUSF. AUSF sẽ gửi một thông báo thành công EAP đến SEAF trong thông báo phản hồi *Nausf_UEAuthentication_Authenticate Response*, SEAF sẽ chuyển nó cho UE. Thông báo *Nausf_UEAuthentication_Authenticate Response* có chứa KSEAF. Nếu AUSF nhận được SUCI từ SEAF khi khởi tạo xác thực, thì AUSF cũng sẽ đưa SUPI vào thông báo *Nausf_UEAuthentication_Authenticate Response*. AUSF lưu trữ KAUSF dựa trên chính sách của nhà điều hành mạng cục bộ. Để ngăn chặn hợp pháp, việc AUSF gửi SUPI đến SEAF là cần thiết nhưng không đủ. Bằng cách bao gồm SUPI làm tham số đầu vào cho nguồn gốc khóa của KAMF từ KSEAF, đảm bảo bổ sung về tính chính xác của SUPI đạt được bởi mạng phục vụ từ cả hai, mạng cục bộ và phía UE.

11. SEAF sẽ gửi thông báo EAP Success đến UE trong thông báo N1. Thông báo này cũng sẽ bao gồm thông số ngKSI và ABBA. SEAF sẽ thiết lập tham số ABBA. Bước 11 có thể là lệnh chế độ bảo mật NAS hoặc kết quả xác thực.

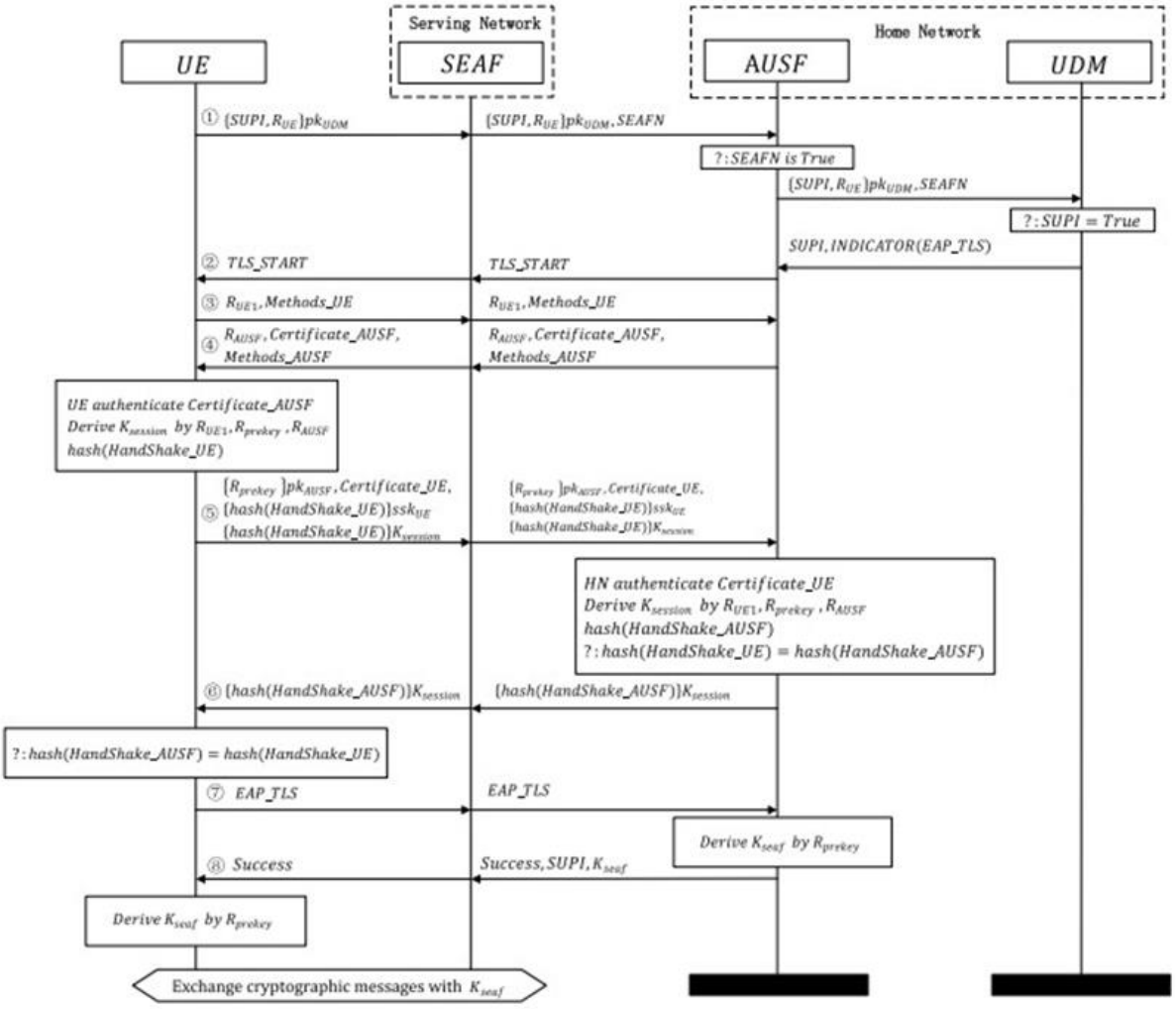
Khóa KSEAF nhận được trong thông báo phản hồi từ AUSF *Nausf_UEAuthentication_Authenticate Response*. SEAF sau đó sẽ tính KAMF từ KSEAF, tham số ABBA và SUPI được gửi đến AMF. Khi nhận được thông báo EAP-Success, UE lấy EMSK từ CK‟ và IK'. ME sử dụng 256-bit đầu tiên của EMSK như KAUSF và sau đó tính toán KSEAF theo cách tương tự như AUSF. UE sẽ tính KAMF từ KSEAF, tham số ABBA và SUPI.

Lưu ý: UE tạo bối cảnh bảo mật tạm thời như được mô tả trong bước 11 sau khi nhận được thông báo EAP cho phép EMSK được tính toán. UE biến bối cảnh bảo mật tạm thời này thành bối cảnh bảo mật một phần khi nhận được EAP Success. UE sẽ loại bỏ ngữ cảnh bảo mật tạm thời nếu xác thực EAP không thành công.

Các bước tiếp theo được thực hiện bởi AUSF khi nhận được thông báo EAP-Response/AKA'-Challenge được xác minh thành công. Nếu thông báo EAP-Response/AKA'-Challenge không được xác minh thành công, hành động tiếp theo của AUSF được xác định theo chính sách của mạng cục bộ. Nếu AUSF và SEAF xác định rằng việc xác thực đã thành công, thì SEAF cung cấp ngKSI và KAMF cho AMF.

2.2.2 Giao thức xác thực và thỏa thuận khóa EAP-TLS

EAP-TLS được đưa ra trong mạng 5G để xác thực thuê bao trong các trường hợp sử dụng hạn chế như mạng riêng và môi trường IoT. EAP-TLS là được thực hiện giữa UE và AUSF thông qua SEAF, SEAF hoạt động như một trình xác thực bằng cách chuyển tiếp các thông điệp EAP-TLS qua lại giữa UE và AUSF. Để thực hiện việc xác thực lẫn nhau, cả UE và AUSF có thể xác minh chứng chỉ của nhau hoặc khóa chia sẻ trước (PSK) nếu nó đã được thiết lập trong quá trình bắt tay bảo mật tầng vận tải (TLS) hoặc ngoài băng tần. Chi tiết các bước của giao thức xác thực 5G EAP-TLS được mô tả như trong hình 2.3.[4]



Hình 2.5: Thủ tục xác thực cho EAP-TLS 5G

1. Đầu tiên, thiết bị người dùng khởi tạo yêu cầu kết nối và chuyển tiếp thông báo chứa SUPI và RUE được mã hóa bởi khóa công khaicủa mạng thường trú {SUPI, RUE} pkUDM tới mạng dịch vụ. Thông báo sau khi mã hóa ký hiệu là SUCI.

2. Mạng dịch vụ sẽ bắt đầu thủ tục xác thực khi nhận được thông báo SUCI, và chuyển tiếp SUCI cùng với tên SEAFN tới mạng thường trú.

3. Module AUSF của mạng thường trú sẽ kiểm tra tên SEAFN là tên mạng dịch vụ hợp lệ. Nếu thông qua việc kiểm tra, thì AUSF gửi thông báo đến UDM, ở đây chức năng SIDF yêu cầu giải mã SUCI chứa nhận dạng thuê bao cố định SUPI. UDM sau đó kiểm tra nếu đã bao gồm SUPI là định danh hợp lệ của thuê bao.

4. Nếu thông qua được kiểm tra trên, module UDM gửi đáp trả chứa SUPI và lựa chọn phương pháp xác thực (được ký hiệu bằng INDICATIOR (EAP-TLS)) tới AUSF. Trong trường hợp này, AUSF sẽ khởi tạo giao thức 5G EAP-TLS.

5. Khi đó AUSF gửi thông báo TLS_START tới thiết bị người dùng thông qua mạng dịch vụ tới tín hiệu khởi động của thủ tục xác thực EAP- TLS.

6. Thiết bị người dùng sinh một số RUE1 và gửi nó tới SEAF với thông tin về thuật toán đã hỗ trợ phương pháp Methods_UE. SEAF sẽ chuyển tiếp trực tiếp thông báo này tới AUSF.

7. AUSF đáp trả thông báo tới thiết bị người dùng thông qua SEAF, SEAF chứa số ngẫu nhiên RAUSF, chứng chỉ mạng thường trú Certificate_AUSF và thông tin về thuật toán nó hỗ trợ Methods_AUSF.

8. Khi nhận được thông báo Certificate_AUSF, thiết bị người dùng đầu tiên kiểm tra giá trị của chứng chỉ này. Trong trường hợp kiểm tra thành công, thiết bị người dùng sinh một nonce mới Rprekey, Rprekey gọi là khóa chủ trước, và dẫn xuất khóa phiên sử dụng Ksession bằng khóa Rprekey, RUE1 và RAUSF.Vì vậy, thiết bị người dùng tính toán hàm băm hash (HandShake_UE) của thông báo bắt tay trước (tức là thông báo trong bước 2,3 và 4. Thiết bị người dùng chuyển tiếp tới mạng dịch vụ SEAF theo thông báo sau: việc mã hóa {Rprekey}pkAUSF khóa chủ gốc sử dụng khóa công khai của AUSF, việc mã hóa {hash(HandShake_UE}Ksession hàm băm sử dụng khóa phiên đã dẫn xuất và chữ ký số {hash(HandShake_UE)}sskUE với khóa ký riêng của nó sskUE. Khi đó SEAF chuyển tiếp thông báo trên tới AUSF trực tiếp.

9. AUSF sau khi kiểm tra chứng chỉ của thiết bị người dùng. Nếu nó hợp lệ, AUSF giải mã {Rprekey}pkAUSF chứa khóa chủ gốc, và tính khóa phiên Ksession cùng với giá trị nonces trước đó RUE1 và RAUSF. Khi đó nó chứa hàm băm {hash (HandShake_UE} Ksession, và so sánh với giá trị trong chữ ký số

{hash(HandShake_UE)}sskUE bằng việc sử dụng khóa ký công khai của UE spkUE. AUSF cũng tính hàm băm hash(HandShake_AUSF) của thông báo bắt tay trước đó, và so sánh với giá trị băm nhận được từ thiết bị người dùng hash(HandShake_UE). Nếu chúng bằng nhau, AUSF sau đó mã hóa hàm băm này với khóa phiên Ksession và gửi nó trở lại thiết bị người dùng.

10. Thiết bị người dùng giải mã thông báo và nhận hàm băm hash(HandShake_AUSF), và so sánh hàm băm của chính nó hash(HandShake_UE). Nếu chúng bằng nhau, thiết bị người dùng đưa ra yêu cầu việc xác thực thành công, và gửi thông báo EAP_TLS tới SEAF, SEAF sau đó chuyển thẳng tới AUSF.

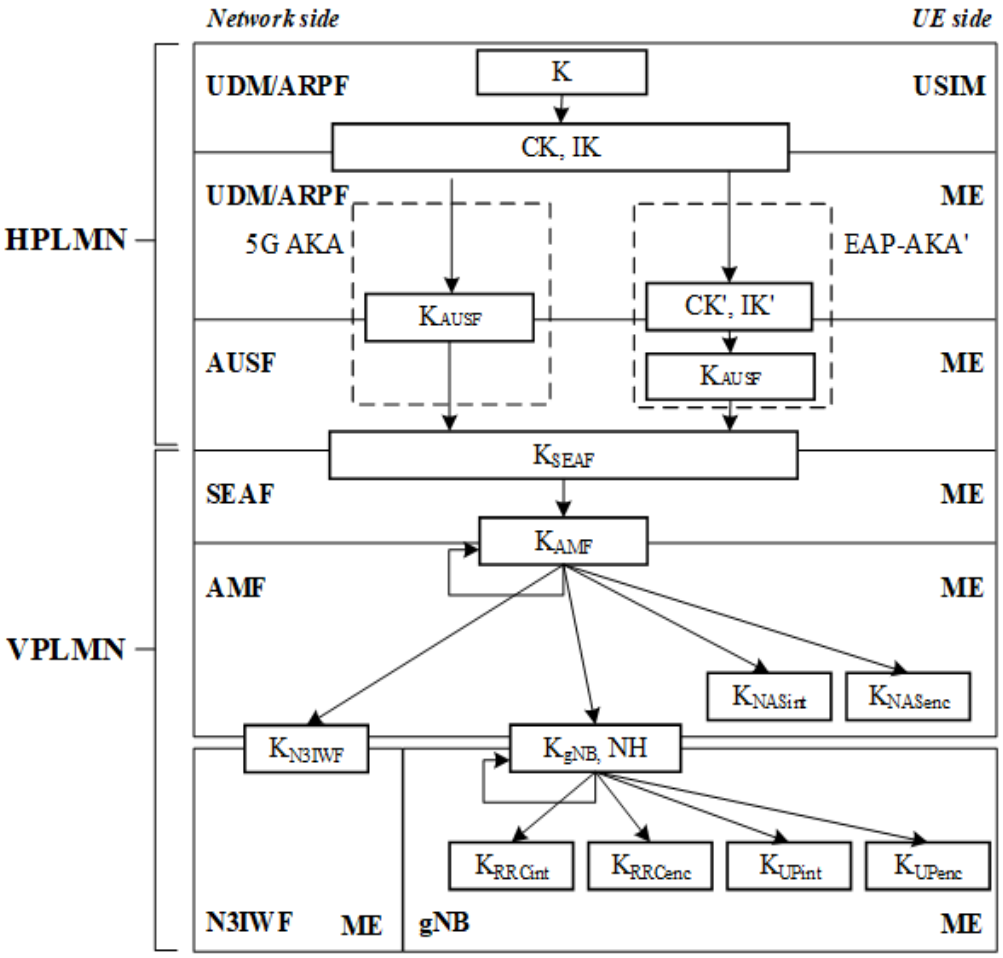
11. Khi AUSF nhận được thông báo EAP_TLS, AUSF sinh khóa Kseaf mới dựa vào khóa chủ gốc Rprekey[2] và gửi nó tới SEAF cùng với định danh của thiết bị người dùng SUPI và thông báo Success.

12. SEAF chuyển tiếp thông báo Success tới thiết bị người dùng, bao gồm thủ tục xác thực trên mặt phẳng máy chủ. Khi nhận được thông báo này, thiết bị người dùng sinh khóa KSEAF theo cách tương tự AUSF. Khóa KSEAF khi đó được sử dụng để bảo mật liên lạc giữa thiết bị người dùng và mạng.

2.3. Mô hình phân cấp khóa trong mạng di động 5G

2.3.1. Hệ thống phân cấp khóa

Yêu cầu về 5GC và NG-RAN liên quan đến khóa. Phần sau mô tả chi tiết các khóa của hệ thống phân cấp khóa trong 5GS [3]:



Hình 2.6: Hệ thống phân cấp khóa trong 5GS

Các khóa liên quan đến xác thực bao gồm các khóa sau: K, CK/IK. Trong trường hợp EAP-AKA', các khóa CK', IK' có nguồn gốc từ CK, IK.

Hệ thống phân cấp khóa bao gồm các khóa sau: K_{AUSF}, K_{SEAF}, K_{AMF}, K_{NASint}, K_{NASenc}, K_{N3IWF}, K_{gNB}, K_{RRCint}, K_{RRCenc}, K_{UPint} và K_{UPenc}.

Khóa cho AUSF trong mạng cục bộ:

- KAUSF là một khóa có nguồn gốc:

+ Từ ME và AUSF được dẫn xuất từ các khóa CK', IK' trong trường hợp EAP-AKA', CK' và IK' được AUSF tiếp nhận như một phần của AV‟ chuyển đổi từ ARPF;

+ Từ ME và ARPF được dẫn xuất từ các khóa CK, IK trong trường hợp 5G AKA, KAUSF được AUSF nhận như một phần của 5G HE AV từ ARPF.

- KSEAF là một khóa có nguồn gốc từ ME và AUSF từ KAUSF. KSEAF được AUSF cung cấp cho SEAF trong mạng dịch vụ.

- Khóa cho AMF trong mạng dịch vụ:

KAMF là một khóa được dẫn xuất từ KSEAF được thực hiện từ ME và SEAF. KAMF được dẫn xuất thêm bởi ME và nguồn AMF khi thực dẫn xuất khóa ngang.

- Các khóa cho tín hiệu NAS:

+ KNASint là một khóa được dẫn xuất từ KAMF do ME và AMF thực hiện, khóa này chỉ được sử dụng để bảo vệ tín hiệu NAS với một thuật toán toàn vẹn cụ thể.

+ KNASenc là một khóa được dẫn xuất từ KAMF do ME và AMF thực hiện, khóa này sẽ chỉ được sử dụng để bảo vệ tín hiệu NAS với một thuật toán mã hóa cụ thể.

- Khóa cho NG-RAN:

KgNB là một khóa được dẫn xuất từ khóa KAMF do ME và AMF. KgNB được dẫn xuất thêm bởi ME và nguồn gNB khi thực hiện dẫn xuất khóa ngang hoặc dọc. KgNB được sử dụng giống như KeNB giữa ME và ng-eNB.

- Các khóa cho lưu lượng UP (User Plane):

+ KUPenc là một khóa được dẫn xuất từ KgNB thực hiện bởi ME và gNB, Khóa này chỉ được sử dụng để bảo vệ lưu lượng mặt phẳng người dùng UP với một thuật toán mã hóa cụ thể.

+ KUPint là một khóa được dẫn xuất từ KgNB do ME và gNB, khóa này được sử dụng để bảo vệ lưu lượng mặt phẳng người dùng UP giữa ME và gNB với một thuật toán toàn vẹn cụ thể.

- Khóa cho tín hiệu RRC:

+ KRRCint là một khóa được dẫn xuất từ KgNB do ME và gNB thực hiện, khóa này chỉ được sử dụng để bảo vệ tín hiệu RRC với một thuật toán toàn vẹn cụ thể.

+ KRRCenc là một khóa được dẫn xuất từ KgNB do ME và gNB, khóa này chỉ được sử dụng để bảo vệ tín hiệu RRC với một thuật toán mã hóa cụ thể.

- Các khóa trung gian:

+ NH là một khóa có nguồn gốc từ ME và AMF để cung cấp bảo mật phía trước.

+ KNG-RAN* là một khóa có nguồn gốc từ ME và NG-RAN (tức là gNB hoặc ng-eNB) khi thực hiện dẫn xuất khóa ngang hoặc dọc sử dụng KDF.

+ K‟‟AMF là một khóa có thể được bắt nguồn từ ME và AMF khi UE di chuyển từ AMF này sang AMF khác trong quá trình di chuyển liên bằng cách sử dụng KDF.

- Khóa cho quyền truy cập non- 3GPP:

KN3IWF là một khóa được dẫn xuất từ KAMF do ME và AMF thực hiện để truy cập Non- 3GPP. KN3IWF không được chuyển tiếp giữa N3IWFs.

2.3.2. Lược đồ dẫn xuất và phân phối khoá

2.3.2.1. Các khóa trong các thực thể mạng

- Các khóa trong ARPF:

+ ARPF sẽ xử lý khóa K dài hạn và bất kỳ dữ liệu nhạy cảm nào khác chỉ trong môi trường an toàn của nó. Khóa K có thể có độ dài 128-bit hoặc 256- bit.

+ Trong quá trình xác thực và thỏa thuận khóa, ARPF sẽ lấy CK' và IK' từ K trong trường hợp EAP-AKA' được sử dụng và dẫn xuất KAUSF từ K trong trường hợp 5G AKA được sử dụng. ARPF sẽ chuyển tiếp các khóa dẫn xuất tới AUSF.

+ ARPF giữ khóa riêng của mạng thường trú, khóa này được SIDF sử dụng để giải mã SUCI và tái tạo lại SUPI. Việc tạo và lưu trữ khóa gốc không được đề cập trong tài liệu này.

- Các khóa trong AUSF

+ Trong trường hợp EAP-AKA' được sử dụng làm phương pháp xác thực, AUSF sẽ lấy KAUSF khóa từ CK' và IK' cho EAP-AKA'.

+ Trong trường hợp 5G AKA được sử dụng làm phương thức xác thực, UDM/ARPF sẽ tạo KAUSF.

+ KAUSF có thể được lưu trữ trong AUSF giữa hai thủ tục xác thực và thỏa thuận khóa tiếp theo.

+ Khi AUSF lưu trữ KAUSF, AUSF sẽ lưu trữ KAUSF mới nhất được tạo sau khi hoàn thành thành công xác thực chính mới nhất. Việc xác thực được coi là thành công và AUSF sẽ lưu trữ KAUSF mới nhất hoặc thay thế KAUSF cũ bằng KAUSF mới (nếu có) AMF kết thúc chọn cùng một phiên bản AUSF để xác thực (lại) UE):

Trong trường hợp 5G AKA được sử dụng làm phương pháp xác thực, khi RES* và XRES* bằng nhau (xem mục 2.2.1, Bước 11).

Trong trường hợp EAP-AKA' được sử dụng làm phương thức xác thực, khi AUSF gửi thông báo EAP-Success tới SEAF (xem mục 2.2.2, Bước 10).

AUSF sẽ tạo khóa dẫn xuất KSEAF, từ khóa xác thực gốc nhận được từ ARPF trong quá trình xác thực và thỏa thuận khóa.

- Các khóa trong SEAF:

+ SEAF nhận khóa KSEAF từ AUSF khi quá trình xác thực thành công trong mỗi mạng dịch vụ.

+ SEAF sẽ không chuyển giao KSEAF cho một tổ chức bên ngoài SEAF. Khi KAMF được dẫn xuất, KSEAF sẽ bị xóa.

+ SEAF sẽ tạo KAMF từ KSEAF ngay sau thủ tục xác thực và thỏa thuận khóa và chuyển giao KAMF cho AMF.

*Lưu ý 1: Điều này ngụ ý rằng mỗi lần chạy quy trình xác thực và thỏa thuận khóa một khóa KAMF mới, cùng với một khóa KSEAF mới được tạo.

*Lưu ý 2: SEAF nằm cùng với AMF.

- Các khóa trong AMF

+ AMF nhận KAMF từ SEAF hoặc từ một AMF khác.

+ AMF dựa trên chính sách sẽ dẫn xuất một khóa K‟‟AMF từ KAMF để chuyển cho một AMF khác trong tính di động giữa các AMF. Khi nhận được khóa K‟‟AMF từ AMF khác, AMF sẽ sử dụng K‟‟AMF như khóa chính của nó trong trường hợp chuyển vùng.

+ AMF sẽ tạo ra các khóa KNASint và KNASenc dành riêng để bảo vệ lớp

+ AMF sẽ tạo ra các khóa cụ thể của mạng truy nhập từ KAMF. Đặc biệt:

+ AMF sẽ tạo KgNB và chuyển nó đến gNB.

+ AMF sẽ tạo NH và chuyển nó đến gNB, cùng với giá trị NCC tương ứng.

+ AMF cũng có thể chuyển một khóa NH, cùng với giá trị NCC tương ứng, sang một AMF khác.

+ AMF sẽ tạo KN3IWF và chuyển nó đến N3IWF khi KAMF được nhận từ SEAF hoặc khi K‟‟AMF được nhận từ AMF khác.

- Các khóa trong NG-RAN

+ NG-RAN (tức là gNB hoặc ng-eNB) nhận KgNB và NH từ AMF. Ng-eNB sử dụng KgNB làm KeNB.

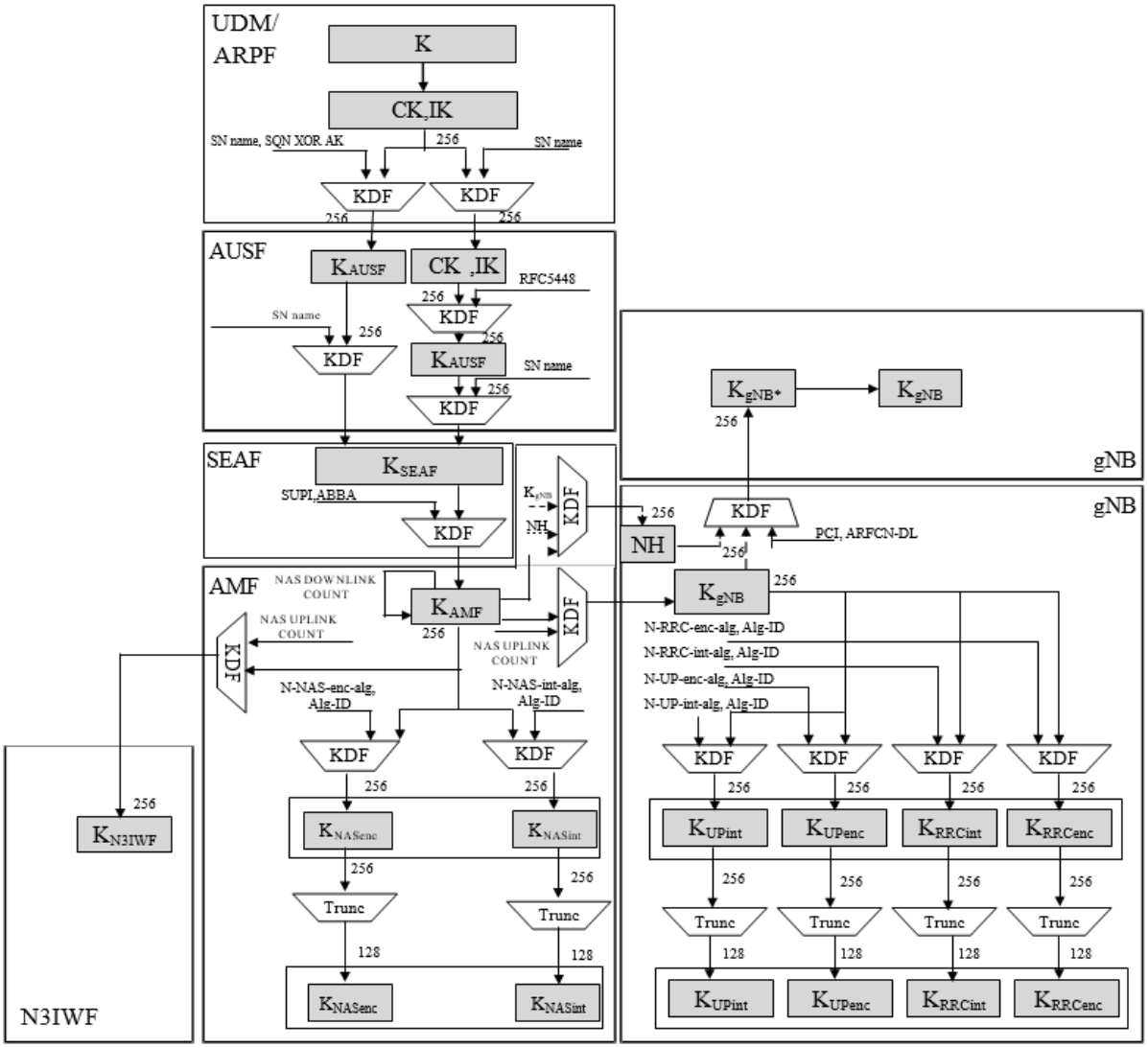
+ NG-RAN (tức là gNB hoặc ng-eNB) sẽ tạo ra tất cả các khóa tầng truy cập (AS) tiếp theo từ KgNB hoặc NH.

- Các khóa trong N3IWF

+ N3IWF nhận KN3IWF từ AMF.

+ N3IWF sẽ sử dụng KN3IWF làm MSK chính cho IKEv2 giữa UE và N3IWF trong các thủ tục truy cập non- 3GPP.

Hình dưới cho thấy sự phụ thuộc giữa các khóa khác nhau và cách chúng dẫn xuất từ quan điểm của các nút mạng.

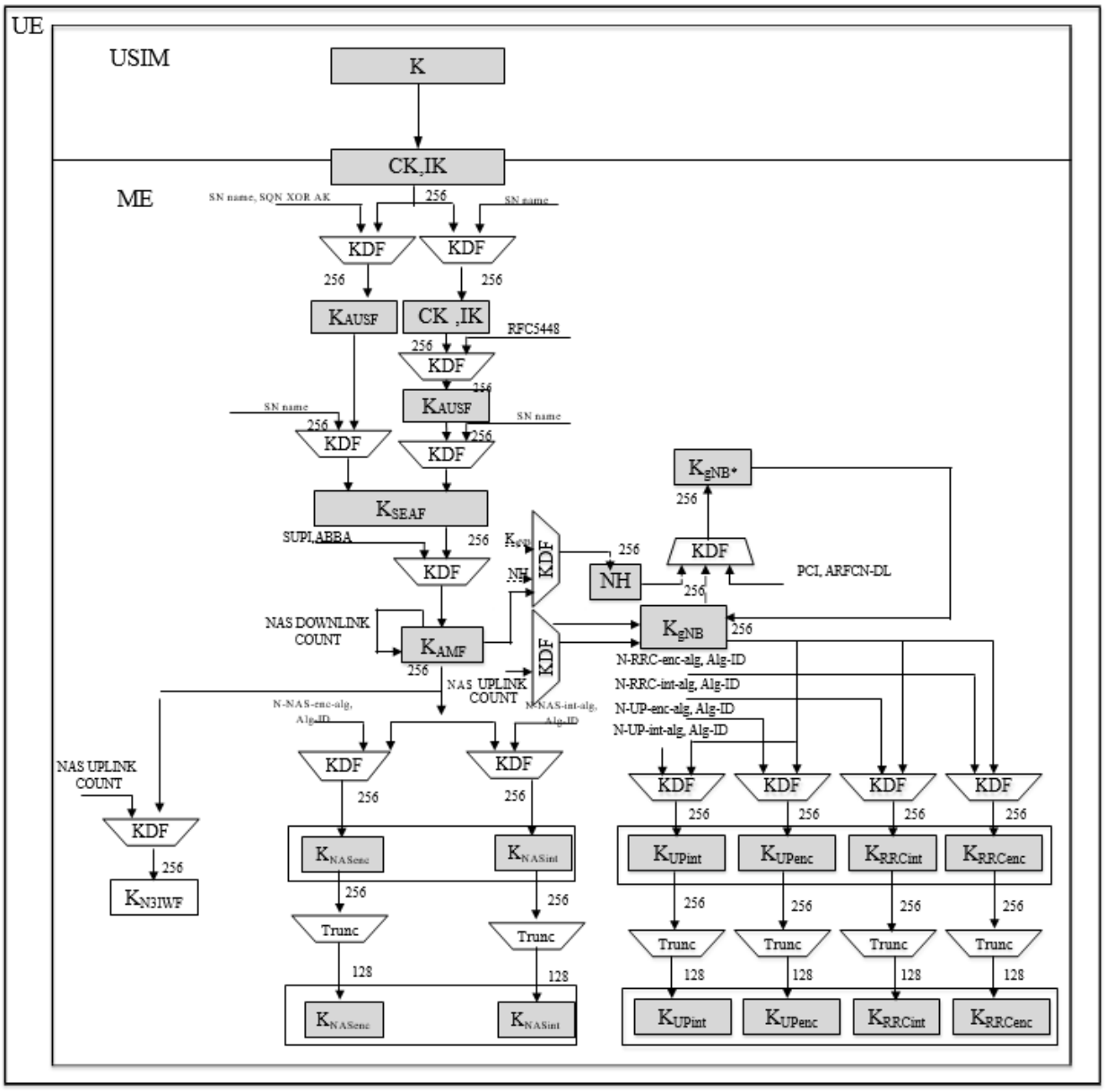


Hình 2.7: Lược đồ phân phối khóa và dẫn xuất khóa cho các nút mạng

2.3.2.2. Các khóa trong UE

Đối với mỗi khóa trong một thực thể mạng, có một khóa tương ứng trong UE.

Hình dưới cho thấy các mối liên quan và nguồn gốc tương ứng được thực hiện trong UE.



Hình 2.8: Lược đồ phân phối khóa và dẫn xuất khóa cho UE

Các khóa trong USIM

USIM sẽ lưu trữ một khóa dài hạn K, khóa này cũng được lưu trữ trong ARPF.

Trong quá trình xác thực và thỏa thuận quan trọng, USIM sẽ tạo khóa gốc từ K để chuyển tiếp cho ME.

Nếu được cung cấp bởi nhà khai thác mạng thường trú, USIM sẽ lưu trữ khóa công khai của mạng thường trú, khóa công khai này sẽ được sử dụng để mã hóa SUPI.

Các khóa trong ME

ME sẽ tạo K_{AUSF} từ CK, IK nhận được từ USIM. Việc tạo khóa này là cụ thể cho mỗi phương pháp xác thực.

- Khi sử dụng 5G AKA, ME sẽ thực hiện việc tạo RES* từ RES.

UE sẽ lưu trữ K_{AUSF} mới nhất hoặc thay thế K_{AUSF} cũ bằng K_{AUSF} mới nhất, sau khi hoàn tất thành công xác thực mới nhất. Nếu USIM hỗ trợ lưu trữ thông số 5G, K_{AUSF} sẽ được lưu trữ trong USIM. Nếu không, K_{AUSF} sẽ được lưu trữ trong bộ nhớ cố định của ME.

Trong trường hợp 5G AKA được sử dụng làm phương pháp xác thực, khi nhận được thông báo chế độ bảo mật NAS hợp lệ từ AMF (để sử dụng ngữ cảnh từng phần tương ứng bắt nguồn từ K_{AUSF} mới được tạo), UE sẽ coi xác thực được thực hiện là thành công và UE sẽ lưu trữ K_{AUSF} mới được tạo dưới dạng K_{AUSF} mới nhất hoặc thay thế K_{AUSF} cũ bằng K_{AUSF} mới nhất.

Trong trường hợp có bất kỳ phương pháp EAP tạo khóa nào được sử dụng làm phương pháp xác thực cho xác thực (lại) khóa, khi nhận được thông báo EAP- Success, xác thực khóa sẽ được coi là thành công và UE sẽ lưu trữ K_{AUSF} mới được tạo thành K_{AUSF} mới nhất hoặc thay thế K_{AUSF} cũ bằng K_{AUSF} mới nhất.

ME sẽ thực hiện việc tạo ra K_{SEAF} từ K_{AUSF}. Nếu USIM hỗ trợ lưu trữ thông số 5G, thì K_{SEAF} sẽ được lưu trữ trong USIM. Nếu không, K_{SEAF} sẽ được lưu trữ trong bộ nhớ cố định của ME.

ME sẽ thực hiện việc tạo ra K_{AMF}. Nếu USIM hỗ trợ lưu trữ thông số 5G, K_{AMF} sẽ được lưu trữ trong USIM. Nếu không, K_{AMF} sẽ được lưu trữ trong bộ nhớ cố định của ME.

ME sẽ thực hiện việc tạo tất cả các khóa tiếp theo khác có nguồn gốc từ K_{AMF}.

Mọi bối cảnh bảo mật 5G, K_{AUSF} và K_{SEAF} được lưu trữ tại ME sẽ bị xóa khỏi ME nếu:

a) USIM bị loại khỏi ME khi ME ở trạng thái mở (the ME is in power on state);

b) ME được cung cấp năng lượng và ME phát hiện ra rằng USIM khác với USIM đã được sử dụng để tạo bối cảnh bảo mật 5G;

c) ME được cung cấp năng lượng (powered up) và ME phát hiện ra rằng không có USIM nào hiện diện tại ME.

2.3.3. Xử lý khóa liên quan đến người dùng

2.3.3.1. Thiết lập khóa

Thiết lập khóa xảy ra khi kết thúc quy trình xác thực thành công. Việc xác thực và thiết lập khóa có thể được mạng bắt đầu thường xuyên như mong muốn của nhà điều hành mạng khi tồn tại một kết nối NAS đang hoạt động. Thiết lập khóa có thể xảy ra ngay khi AMF biết được danh tính của thuê bao di động (tức là 5G-GUTI hoặc SUPI). Việc chạy thành công 5G AKA hoặc EAP-AKA' dẫn đến một K_{AMF} mới được lưu trữ trong UE và AMF với bối cảnh bảo mật từng phần mới.

Các khóa NAS (tức là K_{NASint} và K_{NASenc}) và khóa AS (tức là K_{gNB}, K_{RRCenc}, K_{RRCint}, K_{UPenc}, K_{UPint}) được lấy từ K_{AMF} bằng cách sử dụng các KDF. Các khóa NAS bắt nguồn từ K_{AMF} mới được sử dụng trong AMF và UE bằng thủ tục chế độ bảo mật NAS. Các khóa AS được đưa vào sử dụng với quy trình lệnh của chế độ bảo mật AS hoặc với quy trình thay đổi khóa khi đang di chuyển.

Đối với truy cập Non-3GPP, khóa K_{N3IWF} được lấy từ K_{AMF}. K_{N3IWF} được lưu trữ trong UE và N3IWF. Khóa K_{N3IWF} này và các khóa mật mã IPsec SA được sử dụng với việc thành lập Hiệp hội Bảo mật IPsec (SA) giữa UE và N3IWF

2.3.3.2. Nhận dạng khóa

Khoá K_{AMF} sẽ được nhận dạng bằng mã định danh bộ khoá ngKSI. ngKSI có thể là kiểu riêng hoặc kiểu được ánh xạ. Một ngKSI sẽ được lưu trữ trong UE và AMF cùng với K_{AMF} và số nhận dạng tạm thời 5G-GUTI, nếu có.

Lưu ý: 5G-GUTI trỏ đến AMF nơi K_{AMF} được lưu trữ.

Một ngKSI riêng được liên kết với K_{SEAF} và K_{AMF} được tạo ra trong quá trình xác thực. Nó được cấp phát bởi SEAF và được gửi cùng với bản tin yêu cầu xác thực đến UE nơi nó được lưu trữ cùng với K_{AMF}. Mục đích của ngKSI

là làm cho UE và AMF có thể xác định bối cảnh bảo mật riêng mà không cần gọi thủ tục xác thực. Điều này được sử dụng để cho phép sử dụng lại ngữ cảnh bảo mật riêng trong quá trình thiết lập kết nối tiếp theo.

Một ngKSI được ánh xạ được liên kết với K_{AMF} bắt nguồn từ các khóa EPS trong quá trình làm việc với nhau. Nó được tạo ra trong cả UE và AMF tương ứng khi lấy K_{AMF} được ánh xạ khi chuyển từ EPS sang 5GS. ngKSI được ánh xạ được lưu trữ cùng với K_{AMF} được ánh xạ.

Mục đích của ngKSI được ánh xạ là để UE và AMF có thể chỉ ra việc sử dụng K_{AMF} được ánh xạ trong các thủ tục liên kết.

Định dạng của ngKSI sẽ cho phép người nhận tham số như vậy phân biệt được tham số là kiểu riêng hay kiểu được ánh xạ. Định dạng phải chứa một trường loại và một trường giá trị. Trường loại cho biết loại của bộ khóa. Trường giá trị bao gồm ba bit trong đó bảy giá trị, không bao gồm giá trị '111', được sử dụng để xác định bộ khóa. Giá trị '111' được dành riêng để UE sử dụng để chỉ ra rằng K_{AMF} hợp lệ là không có sẵn để sử dụng.

K_{NASenc} và K_{NASint} trong hệ thống phân cấp khóa được dẫn xuất từ K_{AMF}, có thể được xác định duy nhất bởi ngKSI cùng với các tham số đó từ tập hợp {bộ phân biệt thuật toán, bộ nhận dạng thuật toán}, được sử dụng để lấy các khóa này từ K_{AMF}.

K_{N3IWF} có thể được xác định duy nhất bởi ngKSI cùng với uplink NAS COUNT được sử dụng để dẫn xuất theo phụ lục A7.

Khởi tạo K_{gNB} có thể được xác định duy nhất bởi ngKSI, cùng với uplink NAS COUNT được sử dụng để theo phụ lục A7.

Khóa trung gian NH [3, mục 6.9.2.1.1] có thể được xác định duy nhất bởi ngKSI, cùng với khởi tạo K_{gNB} được dẫn xuất từ bối cảnh bảo mật NAS 5G hiện tại để sử dụng trong trạng thái CM-CONNECTED đang diễn ra và một bộ đếm đếm có bao nhiêu NH- các dẫn xuất đã được thực hiện từ K_{gNB}. Bộ đếm chuỗi bước nhảy tiếp theo, NCC, đại diện cho 3-bit cuối của bộ đếm này.

Khóa trung gian K_{NG-RAN}*, cũng như K_{gNB} không phải ban đầu [3, mục 6.9.2.1.1], có thể được xác định duy nhất bởi ngKSI cùng với các tham số đó từ tập hợp {K_{gNB} hoặc NH, chuỗi PCI và ARFCN-DLs}, được sử dụng để lấy các khóa này từ K_{gNB} hoặc NH.

K_{RRCint}, K_{RRCenc}, K_{UPint} và K_{UPenc} trong phân cấp khóa có thể được xác định duy nhất bởi ngKSI cùng với các tham số đó từ tập {bộ phân biệt thuật toán, bộ nhận dạng thuật toán}, được sử dụng để lấy các khóa này từ K_{gNB}.

2.3.3.3. Vòng đời khóa

K_{AUSF} và K_{SEAF} sẽ được tạo khi chạy xác thực khóa thành công. K_{AMF} sẽ được tạo trong các trường hợp sau:

1. Xác thực

2. Khóa lại khóa NAS.[3, mục 6.9.4.2]

3. Làm mới khóa NAS .[3, mục 6.9.4.3]

4. Quy trình tương tác với EPS

Trong trường hợp UE không có K_{AMF} hợp lệ, một ngKSI có giá trị "111" sẽ được UE gửi đến mạng, có thể bắt đầu (lại) thủ tục xác thực để nhận K_{AMF} mới dựa trên xác thực thành công.

K_{NASint} và K_{NASenc} được dẫn xuất dựa trên K_{AMF} khi chạy quy trình NAS SMC thành công.

K_{N3IWF} có nguồn gốc từ K_{AMF} và vẫn có giá trị miễn là UE được kết nối với 5GC qua quyền truy cập Non-3GPP hoặc cho đến khi UE được xác thực lại.

K_{gNB} và NH được tính dựa trên K_{AMF} hoặc K_{gNB} hoặc NH trong các trường hợp sau:

1. Chuyển giao giữa gNB-CU. [3, mục 6.9.2.3.1]

2. Chuyển đổi trạng thái [3, mục 6.8]

3. Khóa lại khóa AS. [3, mục 6.9.4.4]

4. Làm mới khóa AS. [3, mục 6.9.4.5]

K_{RRCint}, K_{RRCenc}, K_{UPint} và K_{UPenc} được dẫn xuất dựa trên K_{gNB} sau khi một K_{gNB} mới được dẫn xuất.

2.4. Kết luận chương

Chương 2 đã giới thiệu về xác thực và thỏa thuận khóa nói chung, với mục đích của quá trình xác thực và thỏa thuận khóa, khung xác thực, cách thức khởi tạo và lựa chọn phương pháp xác thực trong 5G nói riêng. Đồng thời, chương này cũng phân tích chi tiết các luồng thông báo trong mỗi giao thức xác thực và thỏa thuận khóa trong mạng 5G. Cuối chương, trình bày mô hình phân cấp khóa trong mạng 5G, chỉ ra các khóa trong các thực thể mạng và các khóa trong thiết bị người dùng UE. Từ đó, có thể nhận thấy ảnh hưởng lớn của giao thức xác thực và thỏa thuận khóa trong mạng 5G, bởi kết quả của giao thức ngoài việc xác thực lẫn nhau người dùng và mạng, nó sẽ thực hiện dẫn xuất các khóa để bảo vệ dữ liệu và tính toàn vẹn giữa người dùng và mạng ở các bước tiếp theo.

CHƯƠNG 3: PHÂN TÍCH AN TOÀN CỦA GIAO THỨC XÁC THỰC VÀ THỎA THUẬN KHÓA TRONG MẠNG 5G SO VỚI THẾ HỆ TRƯỚC

3.1. Phân tích các lỗ hổng của giao thức xác thực và thỏa thuận khóa EPS-AKA trong mạng 4G.

3.1.1. Xác thực trong mạng 4G

Từ ngữ cảnh xác thực có thể mô tả kiến trúc tổng quát của mạng 4G bao gồm 3 thành phần: Các UE, mạng dịch vụ (Service network- SN), và mạng thường trú (Home network - HN) (Hình 3.1). [1]

Hình 3.1: Kiến trúc tổng quát mạng 4G

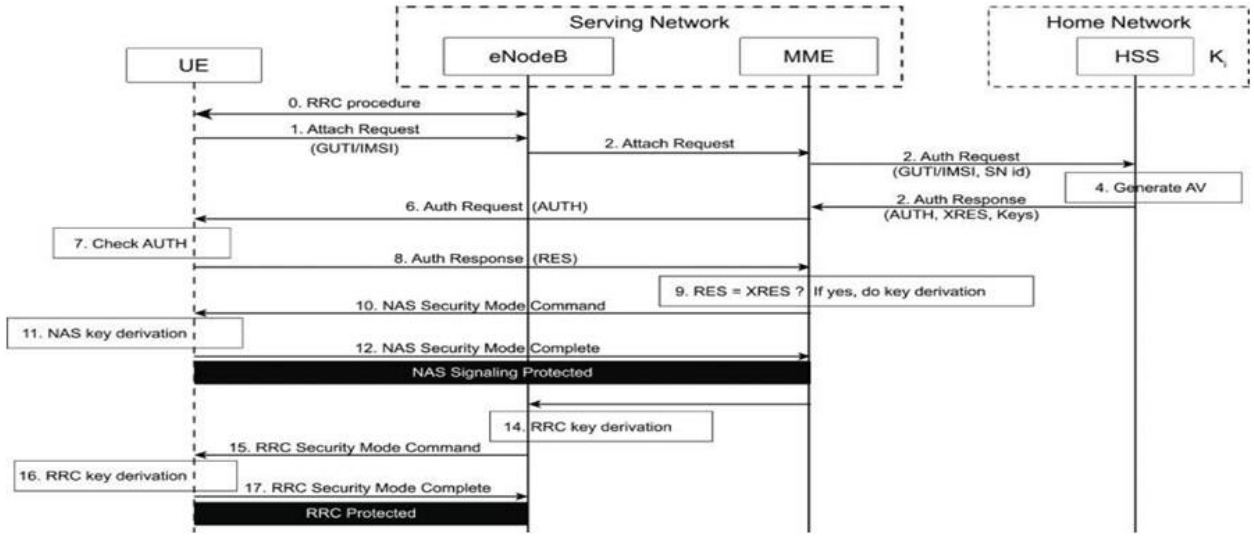
Mỗi UE có một thẻ mạch tích hợp chung (UICC), lưu trữ ít nhất một USIM. USIM là nơi lưu trữ khóa mật mã được chia sẻ trước với thuê bao của mạng thường trú.

Mạng dịch vụ trong 4G bao gồm thiết bị truy cập vô tuyến như trạm gốc (eNodeB), các thực thể quản lý di động (MME) và một số thiết bị khác. UE giao tiếp với mạng thường trú thông qua giao diện vô tuyến.

Mạng thường trú trong 4G bao gồm các máy chủ xác thực như máy chủ thuê bao thường trú (HSS), nơi lưu trữ thông tin đăng nhập và xác thực người dùng. Liên lạc giữa mạng dịch vụ và mạng thường trú là dựa vào IP. Các thực thể lõi được kết nối qua mạng IP được gọi chung là hệ thống lõi gói cải tiến (EPS).

3.1.2. Thủ tục xác thực 4G EPS-AKA

3GPP chọn giao thức EPS-AKA (Evolved Packet System - Authentication and Key Agreement) làm thủ tục xác thực cho người dùng di động 4G/ LTE. Phương pháp xác thực 4G/LTE (Hình 3.2) có thể được trình bày như dưới đây:



Hình 3.2: Thủ tục xác thực 4G/LTE

EPS-AKA kích hoạt sau khi UE hoàn thành quy trình kiểm soát tài nguyên vô tuyến (RRC) với eNodeB và gửi một bản tin đính kèm tới MME (Hình 3.2). MME gửi yêu cầu xác thực tới HSS nằm trong mạng thường trú, bao gồm nhận dạng UE (ví dụ., IMSI) và nhận dạng mạng dịch vụ. HSS thực hiện các hoạt động mật mã dựa trên khóa bí mật được chia sẻ trước, Ki (đã được chia sẻ với UE), để lấy một hoặc nhiều vecto xác thực (AVs), được gửi trở lại MME trong thông báo phản hồi xác thực. Vecto xác thực bao gồm mã xác thực thông báo (AUTH) và mã thông báo phản hồi xác thực (XAUTH), cùng với các dữ liệu khác.

Sau khi nhận được mã thông báo phản hồi xác thực từ HSS, MME gửi yêu cầu xác thực tới UE, bao gồm mã xác thực thông báo (AUTH). UE xác thực AUTH bằng cách so sánh nó với mã xác thực thông báo mà UE tạo ra dựa vào khóa K_i.

Nếu việc xác thực thành công, UE chắc chắn mạng đăng nhập là hợp lệ và gửi thông báo phản hồi xác thực trở lại MME, bao gồm giá trị RES, cùng với mã xác thực thông báo AUTH đã sinh ra dựa vào K_i.

Sau đó, MME so sánh giá trị RES với giá trị XRES. Nếu chúng bằng nhau, MME thực hiện việc dẫn xuất khóa và gửi thông báo thiết lập chế độ bảo mật tới UE, sau đó dẫn xuất các khóa liên quan để bảo vệ các thông báo báo hiệu NAS tiếp theo. MME cũng sẽ gửi eNodeB một khóa từ các khóa bảo vệ kênh RRC được tạo ra. Sau đó UE cũng nhận được các khóa tương ứng, liên lạc tiếp theo giữa UE và eNodeB sau đó được bảo vệ.

3.1.3. Các lỗ hổng của giao thức xác thực và thỏa thuận khóa EPS-AKA trong mạng 4G.

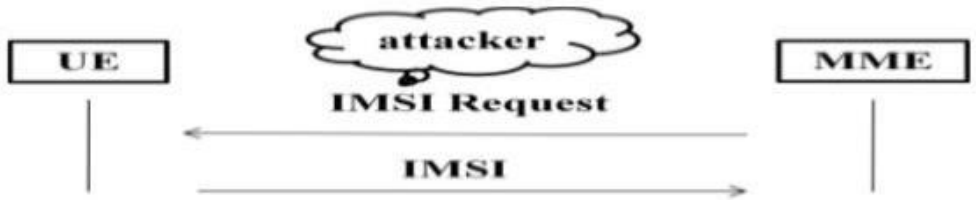
Có hai lỗ hổng trong 4G EPS-AKA [1]

Thứ nhất, định danh UE gửi trên mạng vô tuyến không được mã hóa. Mặc dù, định danh tạm thời GUTI có thể được sử dụng để ẩn định danh thuê bao cố định IMSI, nhiều nhà nghiên cứu chỉ ra rằng định danh tạm thời GUTI có điểm yếu: GUTI không được thay đổi thường xuyên khi cần thiết, và phân bố GUTI có thể dự đoán được (ví dụ, với các byte cố định). Quan trọng hơn, định danh cố định của UE được gửi dưới dạng văn bản rõ trong thông báo phản hồi xác thực tới mạng.

Thứ hai, mạng thường trú cung cấp các AV khi được mạng dịch vụ truy vấn trong quá trình xác thực UE, nhưng nó không phải là phần quyết định của xác thực. Quyết định xác thực chỉ được thực thi bởi mạng dịch vụ SN.

Trong giao thức EPS-AKA của mạng 4G có nhiều mối đe dọa và các điểm yếu, có thể ảnh hưởng tới tính riêng tư và tính bí mật của mạng và người dùng di động. Phần này sẽ phân tích làm rõ bên dưới một số hiểm họa và các cuộc tấn công có thể xảy ra đối với giao thức EPS-AKA.[1,8]

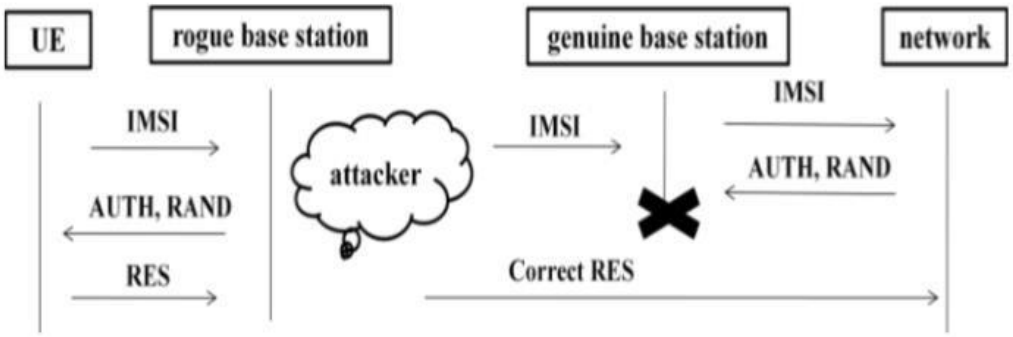
a) Tiết lộ danh tính người dùng



Hình 3.3: Điểm yếu tiết lộ danh tính người dùng

Điểm yếu tiết lộ danh tính người dùng gây ra khi UE đăng ký mạng lần đầu tiên, UE gửi IMSI trong bản rõ. Vì vậy, kẻ tấn công có thể chặn bắt IMSI như trong hình 3.3. Kẻ tấn công có thể mạo danh UE sau đó và gửi IMSI đến MME để có được một số thông tin. Khi đã có được IMSI, kẻ tấn công có thể có được thông tin thuê bao, thông tin vị trí và thậm chí thông tin cuộc trò chuyện, và sau đó giả mạo UE thực và khởi chạy các cuộc tấn công khác như tấn công DoS để phá hủy mạng.

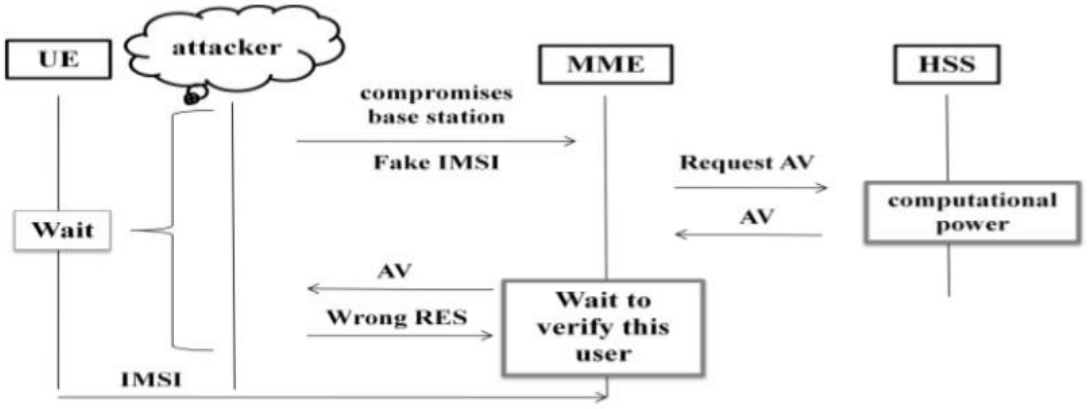
b) Tấn công Man In The Middle



Hình 3.4: Tấn công Man In The Middle

Cuộc tấn công xen giữa MITM (Man In The Middle) kẻ tấn công có được IMSI của UE, kẻ tấn công sử dụng số IMSI này để đăng nhập vào mạng, bằng việc yêu cầu mạng gửi các tham số vectơ xác thực và RAND. Khi nhận được các tham số này kẻ tấn công sẽ thực hiện ngắt kết nối. Sau đó, hướng UE thật đăng nhập vào trạm BS giả bằng việc gửi RAND và AUTH ban đầu để UE tính giá trị RES. Trạm gốc giả khởi tạo lại yêu cầu xác thực vào mạng. Lần này, trạm gốc giả Mạo có được số RES chính xác.

c) Tấn công từ chối dịch vụ



Hình 3.5: Tấn công DoS

Tấn công từ chối dịch vụ (DoS), vì MME quản lý nhiều eNodeB trong kiến trúc LTE, các trạm cơ sở trong mạng LTE dễ bị tấn công hơn so với những người trong kiến trúc UMTS-3G, nơi chỉ có mạng phục vụ trong UMTS quản lý một vài RNC theo cách phân cấp. Một khi một kẻ tấn công thỏa hiệp với trạm gốc, nó có thể gây nguy hiểm hơn nữa cho toàn bộ mạng do tính chất toàn IP của LTE.

Kẻ tấn công có thể khởi động các cuộc tấn công DoS đến HSS và MME. Kẻ tấn công có thể giả mạo một UE hợp pháp để liên tục gửi IMSI giả mạo để đánh lừa các HSS. Như vậy HSS phải tiêu thụ sức mạnh tính toán của nó để tạo ra các vector xác thực quá mức cho UE. Mặt khác, MME phải sử dụng bộ nhớ đệm của nó để chờ quá mức khoảng thời gian dài cho một phản hồi hợp pháp hoặc sai từ UE tương ứng.

3.2. So sánh an toàn của giao thức xác thực và thỏa thuận khóa 5G-AKA so với EPS-AKA

Để so sánh an toàn của giao thức xác thực và thỏa thuận khóa 5G-AKA so với các thế hệ di động thế hệ trước điển hình là giao thức và thỏa thuận khóa EPS-AKA của 4G. Trước tiên, sẽ xem xét sự khác nhau giữa giao thức 5G-AKA và EPS-AKA [2,7]

5G-AKA khác với 4G EPS-AKA ở các điểm sau:

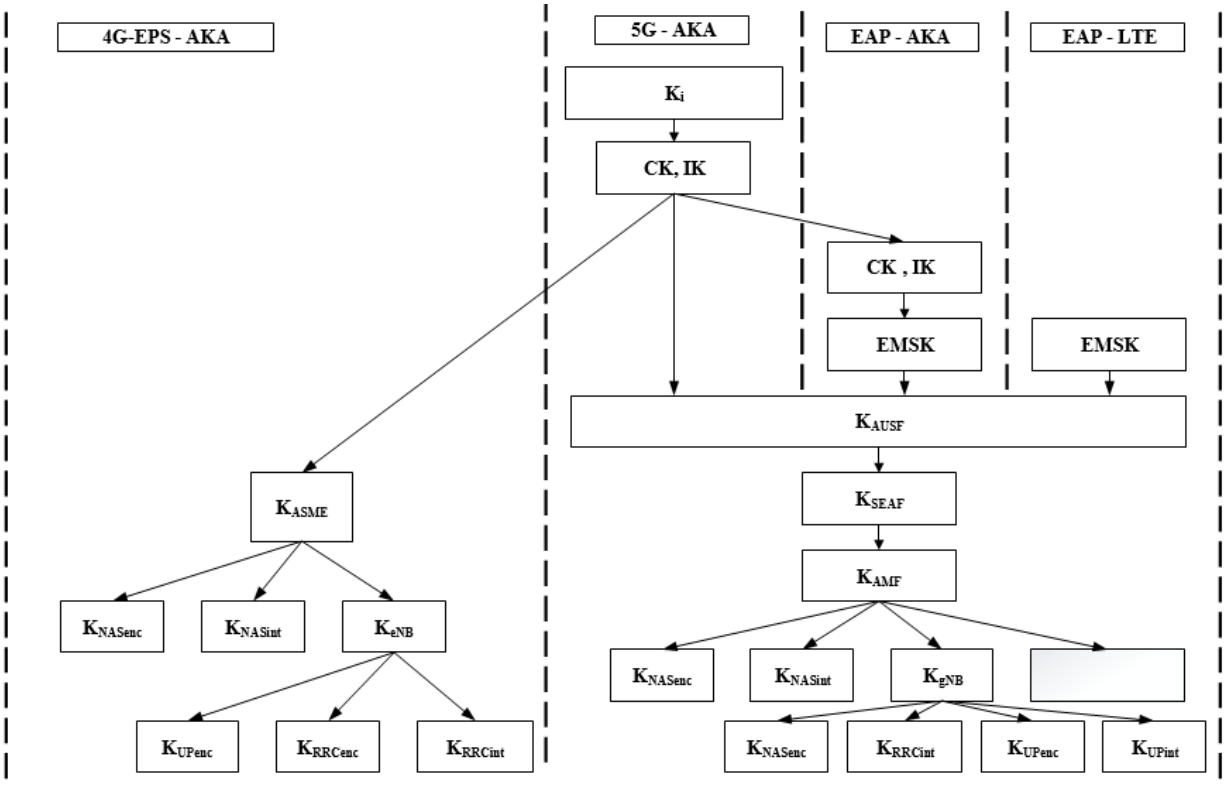
Các thực thể liên quan trong xác thực là khác nhau do kiến trúc dựa trên dịch vụ mới trong 5G. Đặc biệt SIDF là mới; nó không tồn tại trong 4G.

UE luôn sử dụng khóa công khai của mạng thường trú để mã hóa định danh cố định của UE trước khi nó gửi tới mạng 5G. Trong 4G, UE luôn gửi định danh cố định của người dùng trong bản rõ tới mạng, điều này dẫn tới số định danh cố định dễ bị đánh cắp bởi mạng độc hại (ví dụ, trạm cơ sở giả) hoặc đối phương thụ động qua giao diện vô tuyến (nếu liên lạc qua giao diện vô tuyến không được bảo vệ).

Trong mạng 5G mạng thường trú (ví dụ, AUSF) đưa ra quyết định cuối cùng về xác thực UE. Ngoài ra, kết quả xác thực UE cũng gửi đến quản lý dữ liệu thống nhất UDM để ghi lại. Trong 4G, mạng thường trú tham chiếu trong quá trình xác thực chỉ để sinh ra vectơ xác thực, HSS không đưa ra quyết định về kết quả xác thực.

Hệ thống phân cấp khóa trong 5G dài hơn trong 4G vì 5G giới thiệu 2 khóa trung gian, K_{AUSF} và K_{AMF} (xem hình 3.6). Lưu ý: K_{SEAF} là khóa dẫn xuất trong 5G, tương ứng với khóa K_{ASME} trong 4G.

Trong điểm mới trong giao thức 5G AKA là giới thiệu mật mã khóa bất đối xứng, các phiên bản AKA của các thế hệ mạng trước chỉ sử dụng khóa đối xứng [5,6].



Hình 3.6: Hệ thống phân cấp khóa trong 4G và 5G

So sánh an toàn của 5G-AKA so với 4G EPS-AKA:

Trong 5G-AKA, SEAF có thể bắt đầu thủ tục xác thực sau khi nhận được bất kỳ thông báo tín hiệu nào từ UE. Lưu ý rằng UE phải gửi cho SEAF định danh tạm thời (5G-GUTI) hoặc định danh ẩn của thuê bao (SUCI) nếu 5G-GUTI chưa được phân bổ từ mạng phục vụ cho UE. SUCI là dạng mã hóa của SUPI sử dụng khóa công khai của mạng thường trú. Do đó, định danh cố định của UE (tương ứng với IMSI trong mạng 4G), không bao giờ được gửi trong bản tin rõ qua mạng vô tuyến trong 5G. Tính năng này được coi là cải tiến bảo mật lớn hơn so với các thế hệ trước như 4G [7].

Trong bảng 3.1 và 3.2 có thể thấy rằng các phương pháp xác thực của 5G đều có sự tham gia của mạng thường trú HN (AUSF). HN sẽ đưa ra quyết định về việc xác thực người dùng điều này dẫn đến việc mạng thường trú có thể xác thực được chính xác người dùng đang truy cập vào mạng có phải là người dùng hợp pháp hay không, còn trong 4G EPS-AKA việc quyết định xác thực người dùng là do MME của mạng dịch vụ chứ không phải mạng thường trú. Mạng thường trú chỉ được dùng để sinh vectơ xác thực, chứ không đưa ra quyết định đến việc xác thực người dùng UE. Do đó, dẫn tới các cuộc tấn công xen giữa.

Ngoài ra, như phân tích ở trên có thể thấy trong mạng di động 5G hỗ trợ nhiều phương pháp xác thực hơn (5G AKA, EAP-AKA‟, EAP-TLS). Mỗi phương pháp xác thực được sử dụng trong các trường hợp khác nhau thể hiện sự linh hoạt và cải tiến của mạng 5G so với mạng 4G tiền nhiệm.

Bảng 3.1: So sánh giao thức 5G-AKA và 4G-AKA

	5G-AKA	**4G-AKA**
Sending the UE identity in cipher text	✓	x
Masking a final decision of authentication by the HN	✓	x

Bảng 3.2: So sánh giao thức xác thực 4G và 5G

		4G Authentication	5G Authentication		
		EPS-AKA	5G-AKA	EAP-AKA'	EAP-TLS
ENTITIES (LOCATED IN)	USER EQUIPMENT (UE)	USIM	USIM		USIM/Non-USIM
	SERVING NETWORK (SN)	MME	SEAF		
	HOME NETWORK (HN)	HSS	AUSF UDM/ARPF/SIDF		
MESSAGE FORMAT	UE <-> SN	NAS	NAS	NAS|EAP	NAS|EAP
	SN <-> HN	Diameter	HTTP-based web APIs		
TRUST MODEL		Shared symmetric key	Shared symmetric key		Public key certificate
UE IDENTITY	UE -> SN	IMSI/GUTI	SUCI/5G-GUTI		
	SN -> HN	IMSI	SUCI/SUPI		
SN IDENTITY		SN id (MCC+MNC)	SN name (5G:MCC+MNC)		
AUTHENTICATION VECTOR GENERATED BY		HSS	UDM/ARPF	UDM/ARPF	N/A
AUTHENTICATION OF UE DECIDED BY		MME	SEAF & AUSF	AUSF	AUSF
HN INFORMED OF UE AUTHENTICATION?		No	Yes	Yes	Yes
ANCHOR KEY HIERARCHY		K_i -> CK+IK -> K_{ASME}	K_i -> CK+IK -> K_{ASME} -> K_{SEAF}	K_i -> CK+IK -> CK'+IK' -> EMSK -> K_{SEAF}	EMSK -> K_{AUSF} -> K_{SEAF}

3.3. Phân tích một số lỗ hổng của giao thức xác thực và thỏa thuận khóa 5G

Như đã trình bày ở trên, các giao thức xác thực và thỏa thuận khóa được đưa ra trong mạng 5G ít nhiều điều được cải tiến, với mục đích nâng cao khả năng xác thực giữa người dùng và mạng dịch vụ. So với giao thức xác thực và thỏa thuận khóa trong mạng 4G thì các giao thức trong mạng 5G có độ an toàn cao hơn như số định danh của người dùng luôn được mã hóa, chức năng của mạng thường trú được nâng cao, dẫn xuất khóa phức tạp hơn. Tuy nhiên bên cạnh đó, giao thức trong mạng 5G, cụ thể là giao thức 5G AKA tiêu chuẩn cũng còn tồn tại một số yếu điểm có thể tổng hợp như sau [6]:

Theo dõi thuê bao được nhắm mục tiêu, điều này vi phạm quyền riêng tư của người dùng do những bất cập khác nhau, như MAC or việc đồng bộ hóa. Rò rỉ thông tin từ tham số SQN, dẫn đến khả năng xảy ra các cuộc tấn công giám sát được thực hiện.

Mạo danh một SN hợp pháp bằng cách sử dụng một SN độc hại, nếu việc xác thực không được kiểm tra đầy đủ bởi UE. Về cơ bản, điều này bắt nguồn từ thực tế là giao thức AKA tiêu chuẩn không chỉ ra các vòng xác nhận khóa bổ sung, cũng không chỉ định rằng thuê bao phải chờ việc này. Lỗ hổng này có hai tình huống được chỉ ra trong giao thức tiêu chuẩn.

+ Đầu tiên, SN có thể khởi tạo các thay đổi khóa trên đường đi.

+ Thứ hai, SN có thể chuyển đổi bối cảnh bảo mật bao gồm các khóa và các thông số.

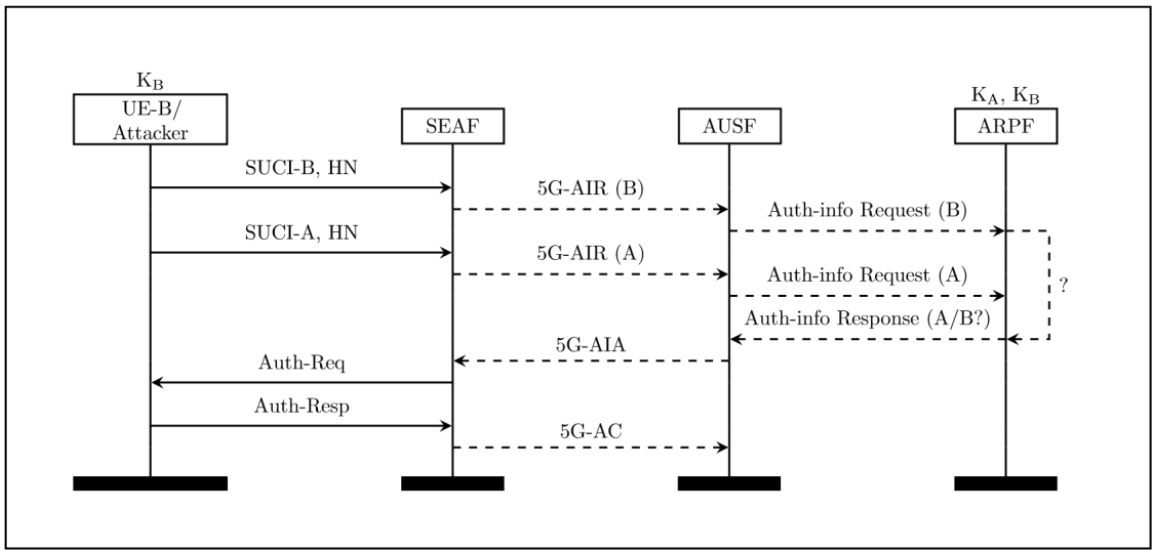
Một cuộc tấn công làm ảnh hưởng đến SN có thể dẫn đến một vi phạm quyền riêng tư của người dùng. Điều này cho phép SN độc hại thu thập các yêu cầu xác thực từ UE và sau đó chặn bắt tham số RES do UE gửi trên kênh không bảo mật ở giai đoạn sau. Kết hợp dữ liệu (SUCI, RES) và gửi nó đến HN, dựa vào kết quả nhận được HN sẽ tính toán và trả lại kết quả là SUPI cho SN độc hại.

Bên cạnh đó, trong tài liệu [10] cũng đưa ra bản dự thảo cuộc tấn công vào giao thức 5G AKA có thể được tài liệu trình bày thêm ở đây:

Một kẻ tấn công 'B' bắt đầu hai phiên 5G-AKA với mạng dịch vụ cục bộ gần như cùng một lúc. Một phiên được bắt đầu bằng cách phát lại SUCI chặn bắt được (của mục tiêu, người dùng 'A'), và phiên còn lại là với USIM và SUCI của kẻ tấn công (dành cho người dùng 'B').

Các phiên chạy song song và dẫn đến tình trạng race-condition; nếu điều này xảy ra, AUSF sẽ không thể phân biệt giữa hai phản hồi có chứa vector xác thực từ ARPF và có khả năng liên kết phản hồi sai (và khóa kết quả) với người dùng sai. Trong trường hợp điều này xảy ra, AUSF và SEAF sẽ tin rằng một tập hợp các vectơ xác thực và khóa được dành cho người dùng

A (và bắt nguồn từ K_A khóa dài hạn của người dùng A), trong khi chúng thực tế có nguồn gốc từ khóa dài hạn của người dùng B, K_B. Kết quả là, người dùng độc hại B bây giờ sẽ có thể lấy được khóa dẫn xuất và sử dụng nó để mạo danh người dùng A vào mạng. Xem hình 3.7 về luồng tấn công của giao thức 5G-AKA.



Hình 3.7: Các luồng tấn công của giao thức 5G-AKA

Cuộc tấn công phá vỡ giao thức như thế nào?

Thuộc tính cụ thể bị vi phạm là tính bảo mật của K_{SEAF} (và khóa dẫn xuất, K_{AUSF}), theo quan điểm của SEAF và AUSF. Đó là, khi kết thúc quá trình chạy giao thức 5G-AKA:

SEAF, AUSF và người dùng sẽ thỏa thuận và cùng sở hữu khóa mật mã (K_{SEAF}) để phục vụ cho liên lạc tiếp theo giữa người dùng và mạng phục vụ

SEAF và AUSF tin rằng khóa này dành cho người dùng thật và không bị xâm phạm (trong ví dụ người dùng 'A' với 'SUPI-A') và cả SEAF và AUSF đều tin rằng khóa này là bí mật với kẻ tấn công.

Do đó, dự thảo giao thức thiếu một thuộc tính ngăn chặn quan trọng đó là: kẻ tấn công có thể xâm phạm khóa dài hạn của người dùng (ví dụ: 'B') và có thể mạo danh bất kỳ người dùng nào (ví dụ: 'A') để truy cập vào SEAF và AUSF, bởi vì nó biết khóa K_{SEAF} của các phiên mà SEAF và AUSF giả định là từ người dùng 'A'.

3.3.1. Kịch bản tấn công chi tiết

Cuộc tấn công diễn ra trong hai giai đoạn riêng biệt (có thể là tạm thời và thậm chí về mặt địa lý). Trong giai đoạn đầu tiên, kẻ tấn công nghe lén và ghi lại một 'SUPI được mã hóa' hợp pháp, còn được gọi là SUCI. Trong giai đoạn thứ hai, tổ chức diễn ra cuộc tấn công.

3.3.2. Thiết lập cho cuộc tấn công

1. Người dùng hợp pháp 'A' có ID 'SUPI-A' được đăng ký với mạng thường trú (HN). Không quan tâm đến khóa K_A dài hạn của nó, vì cuộc tấn công không yêu cầu quyền truy cập vào nó. Người dùng thực này khởi tạo giao thức 5G-AKA, gửi SUCI-A (SUPI được mã hóa tương ứng của người dùng A) đến SEAF và HN. Sau đó, người dùng có thể hoàn thành giao thức như bình thường.

2. Kẻ tấn công nghe lén các tín hiệu vô tuyến công cộng từ bước trước và ghi lại tin nhắn có chứa SUCI-A, HN.

3. Kẻ tấn công mua một USIM hợp pháp từ cùng một mạng thường trú với nạn nhân dự định của mình; Nó có ID 'SUPI-B'. Kẻ tấn công, tấn công và thỏa hiệp USIM, và trích xuất Khóa K_B dài hạn của USIM này thuộc sở hữu của nó.

3.3.3. Giai đoạn chính của cuộc tấn công

Biểu đồ chuỗi tin nhắn của giai đoạn chính của cuộc tấn công có thể được tìm thấy trong Hình 3.7

1. Sau giai đoạn thiết lập, kẻ tấn công bắt đầu giao thức 5G-AKA bằng cách phát lại cho SEAF tin nhắn có chứa „SUCI-A“ (định danh ẩn của người dùng A được ghi lại trước) và tên mạng thường trú của người dùng ('HN') đến SEAF trong mạng dịch vụ (tên SNID). Thậm chí, kẻ tấn công không cần biết đó là ID của ai hoặc hình thức được giải mã của nó.

2. Giao thức này diễn ra bình thường: SEAF giao tiếp với AUSF trong mạng thường trú được chỉ định bằng cách gửi thông điệp "5G-AIR". Thông báo này chứa 'SUCI-A', và SNID (tức là ID của mạng dịch vụ đang được sử dụng).

3. Song song với phiên cho SUCI-A, kẻ tấn công bắt đầu phiên 5G-AKA cho USIM mà nó sở hữu (SUPI-B) với cùng mạng thường trú, thông qua cùng mạng dịch vụ (SEAF). Kẻ tấn công đã sở hữu khóa dài hạn của SUPI-B (K_B), vì nó đã làm tổn hại đến USIM trong giai đoạn thiết lập. Như thường lệ, nó bắt đầu phiên 5G-AKA bằng cách gửi ID ẩn của riêng mình ('SUCI-B') và tên của mạng thường trú (HN), đến cùng SEAF như trong phiên song song khác. SEAF xử lý điều này như một phiên riêng biệt.

4. Như trước đây, SEAF liên lạc với AUSF trong mạng thường trú bằng cách gửi thông điệp "5G-AIR", chứa 'SUCI-B' và SNID. AUSF sau đó gửi thông báo 'Yêu cầu Thông tin Auth' đến ARPF của mạng thường trú, theo giao thức.

5. SIDF (trong ARPF) giải mã SUCI-B được SUPI-B, và ARPF sau đó trả lời bằng cách gửi thông báo 'Phản hồi thông tin Auth-Thông tin' đến AUSF. Thông báo này chứa các thuật ngữ để dẫn xuất (K_B bị xâm phạm) và các tham số RAND, SQN và SNID, nhưng đáng chú ý là không có tham chiếu đến SUPI hoặc SUCI.

5. AUSF nhận được thông báo phản hồi thông tin Auth-Info Respone(A/B), nhưng vì thông điệp này không có SUPI hoặc SUCI kèm theo nó, AUSF không biết liệu thông báo này có dành cho phiên làm việc với 'SUCI- A/SUPI-A', hoặc dành cho phiên làm việc với 'SUCI-B/SUPI-B' hay không. AUSF có thể tiếp tục phiên làm việc của mình một cách hợp pháp dành cho 'SUCI-A/SUPI-A' với thông báo 'Phản hồi thông tin Auth-Info' đáng ra dành cho phiên với 'SUPI-B'.

6. AUSF sau đó tiến hành giao thức, bằng các gửi thông điệp 5G-AIA chứa 'SUPI-A' đến SEAF; thông báo này chứa khóa dẫn xuất K_{SEAF} mà ARPF tạo ra cho 'SUPI-B', nhưng bây giờ AUSF liên kết nó với 'SUPI-A' (và kết quả là SEAF cũng vậy). Vì kẻ tấn công đã xâm phạm khóa dài hạn K_B của SUPI-B (và RAND và SQN được truyền công khai trong giao thức), kẻ tấn công giờ đây có thể sinh khóa K_{SEAF} mà AUSF và SEAF hiện tin là khóa cho 'SUPI-A'. Đó là, kẻ tấn công có thể lấy được K_{SEAF} mà AUSF và SEAF tin là cho 'SUPI-A' thật (chứ không phải mà kẻ tấn công 'SUPI-B').

Chú ý:

Thứ nhất, cuộc tấn công này không thể hoạt động một cách tình cờ. Điều kiện race-condition xảy ra lành tính và các vector xác thực (AVs) sai vô tình được chuyển đến người dùng giả (thật) sẽ không gây ra vi phạm thuộc tính bảo mật. Một USIM thật nhận AVs sai sẽ tính toán một MAC khác với giá trị chứa trong AVs nhận được; tại thời điểm này, UE sẽ từ chối nỗ lực xác thực (vì lỗi này có thể chỉ ra cho người dùng rằng kẻ tấn công đã cố gắng sửa đổi các tin nhắn trên đường đi) và thử lại giao thức.

Thứ hai, các bộ đếm hoặc giá trị SQN không có bất kỳ ảnh hưởng nào đến cuộc tấn công này, vì chỉ có ARPF và UE lưu trữ giá trị 'chính xác' của SQN là gì. AUSF và SEAF không sử dụng SQN trực tiếp trong bất kỳ tính toán hoặc dẫn xuất nào, và do đó, cả AUSF và SEAF không thể kiểm tra xem nó có khớp (hoặc lớn hơn) giá trị được lưu trữ cho một người dùng cụ thể hay không.

Kẻ tấn công tất nhiên có thể chấp nhận Vector xác thực (dẫn đến khóa) được tạo ra với bất kỳ giá trị SQN nào và có thể suy ra trực tiếp giá trị SQN nào được sử dụng. Nói cách khác, trong khi các bộ đếm được sử dụng trong giao thức AKA để ngăn chặn một số hình thức phát lại với các mạng 3G trước đây, thì trong giao thức 5G-AKA tiêu chuẩn chúng được sử dụng theo hướng khác để thực hiện các cuộc tấn công.

3.4. Kết luận chương

Chương 3 đã trình bày thủ tục xác thực và thỏa thuận khóa trong mạng di động 4G EPS-AKA. Từ đó, phân tích các lỗ hổng trong giao thức, đặc biệt chỉ ra các tấn công từ những lỗ hổng của giao thức EPS-AKA. Trên cơ sở đó so sánh an toàn của giao thức 5G AKA với giao thức EPS-AKA. Nhận thấy rằng, giao thức xác thực và thỏa thuận khóa của 5G về cơ bản đã khắc phục những yếu điểm đã chỉ ra trong mạng 4G. Tuy nhiên, bên cạnh đó giao thức xác thực và thỏa thuận khóa trong mạng 5G tiêu chuẩn cũng còn tồn tại một số yếu điểm khác cần phải tiếp tục nghiên cứu và tìm hiểu trong các thời gian tiếp theo.

KẾT LUẬN

Để có được an toàn tin cậy cho hệ thống mạng di động, phải có các biện pháp đảm bảo an ninh nhất định, ví dụ như tính bảo mật, tính xác thực và tính nặc danh. Người dùng và hệ thống máy chủ cần phải xác thực lẫn nhau và thiết lập các khóa phiên để tiếp tục liên lạc.

Đã có nhiều giao thức xác thực được đề xuất cho hệ thống mạng di động , trong số đó có các giao thức cung cấp xác thực lẫn nhau và thỏa thuận khóa giữa người dùng và máy chủ với chi phí tính toán thấp. Việc này rất quan trọng vì các thiết bị liên lạc trong mạng di động thường có nguồn năng lượng và khả năng xử lý bị hạn chế.

Ngoài đòi hỏi ít tính toán và tốn ít năng lượng, các giao thức cần phải có độ an toàn cao, có khả năng chống lại các tấn công thường gặp trong mạng di động. Đồng thời, phân tích những ưu điểm của giao thức đề xuất với giao thức tiêu chuẩn nhằm có những cải tiến phù hợp để chống lại được các cuộc tấn công chủ động trong mạng 5G.

Trên đây là bài nghiên cứu tìm hiểu về giao thức xác thực và thỏa thuận khóa trong mạng 5G của em . Trong quá trình làm đồ án, em đã đạt được một số kết quả như sau :

- Tìm hiểu thêm được các thế hệ mạng di động từ 1G – 5G

- Hiểu được kiến trúc và các vấn đề an ninh mạng 5G

- Hiểu được vai trò của giao thức xác thực và thỏa thuận khóa trong mạng di động 5G

- Phân tích độ an toàn tin cậy giao thức xác thực và thỏa thuận khóa 5G AKA với EPS- AKA so các phiên bản trước

*Hạn chế :

Mặc dù đã rất cố gắng trong việc nghiên cứu và thực hiện đồ án, nhưng do thời gian và sự hiểu biết của em có hạn chế nên đồ án chỉ dừng lại ở tìm hiểu và phân tích các giao thức xác thực và thỏa thuận khóa trong mạng di động 5G so với các thế hệ trước. Đồng thời, đồ án chắc chắn cũng không tránh khỏi những thiếu xót, nên em rất mong nhận được ý kiến đóng góp từ thầy cô**.** Em xin chân thành cảm ơn các thầy cô !

TÀI LIỆU THAM KHẢO

[1]. 3GPP-Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system; (Release 16). 2020.

[2]. Jingjing Zhang, Lin Yang, Weipeng Cao And Qiang Wang, "*Formal Analysis of 5G EAP-TLS Authentication Protocol Using Proverif*"

[3]. Adrien Koutsos, "*The 5G-AKA Authentication Protocol Privacy*", IEEE European Symposium on Security and Privacy (EuroS&P), 2019.

[4]. An Braeken, Madhusanka Liyanage, Pardeep Kumar And John Murphy, "*Novel 5G Authentication Protocol to Improve the Resistance Against Active Attacks and Malicious Serving Networks*", IEEE Aceess, volume 7, 2019.

[5]. "*A Comparative Introduction to 4G and 5G Authentication*", https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication

[6]. Ashraf Elbayoumy, "*Security Enhancement for LTE Authentication Protocol (EPS-AKA)*", May 2015