5G Security

Alessandro Castelli
ID:147073
E-mail: castelli.alessandro@spes.uniud.it

October 25, 2024

Abstract

Negli ultimi decenni, le comunicazioni wireless hanno subito una rapida evoluzione, alimentata dalla crescente domanda degli utenti per connessioni sempre più veloci, affidabili e performanti. Tra le innovazioni tecnologiche più rilevanti, la tecnologia 5G si è affermata come la nuova frontiera delle telecomunicazioni mobili, promettendo una capacità di banda superiore, latenze ridotte e una enorme densità di connessioni per dispositivi intelligenti e IoT. Tuttavia, insieme a queste straordinarie capacità, emergono anche nuove sfide in termini di sicurezza. Il 5G introduce una infrastruttura di rete più complessa e decentralizzata, aumentando il rischio di vulnerabilità e attacchi informatici. Questo articolo esamina i principali aspetti della sicurezza del 5G, evidenziando le vulnerabilità della rete e discutendo le soluzioni tecnologiche avanzate sviluppate per mitigare i rischi.

Contents

1 Introduzione

La storia della comunicazione mobile è un viaggio di innovazione continua. Tutto inizia con il 1G [2], negli anni '70 e '80, quando la trasmissione dei dati era analogica. Era l'inizio, ma con grandi limiti: la qualità era bassa, la sicurezza inesistente e le chiamate potevano essere facilmente intercettate. Tuttavia, consentiva qualcosa di rivoluzionario per l'epoca: la connettività mobile e i primi servizi vocali, anche se in modo rudimentale.

Con l'arrivo del 2G nel 1991, la situazione cambiò drasticamente. La comunicazione diventò digitale, affrontando molti dei problemi del 1G. Ora c'era più sicurezza, efficienza e una maggiore larghezza di banda. Si aprirono così le porte a nuovi servizi come i messaggi di testo, rendendo la comunicazione mobile più sofisticata.

Successivamente, il 3G introdusse il concetto di banda larga mobile. Non era più solo una questione di chiamate o messaggi, ma anche di videochiamate, navigazione su Internet e una trasmissione dati molto più veloce. Il 3G rappresentava una svolta, anche se soffriva ancora di problemi legati allo spettro e alla latenza, dimostrando che la tecnologia aveva ancora margini di miglioramento.

Quando arrivò il 4G, tra il 2009 e il 2010, il mondo della comunicazione mobile fece un enorme balzo in avanti. Grazie a tecnologie come LTE, la velocità dei dati aumentò significativamente, portando il mobile streaming, i giochi online e i video in alta definizione a portata di mano ovunque. Le velocità di download teoriche potevano raggiungere i 100 Mbps, sebbene nella pratica fossero spesso inferiori.

Infine, con l'avvento del 5G, si entrò in una nuova era. Non si parlava più solo di miglioramenti incrementali, ma di una rivoluzione. Il 5G promette velocità fino a 20 Gbps [4], una latenza ultra bassa e la capacità di connettere miliardi di dispositivi contemporaneamente. È una tecnologia pensata per un mondo interconnesso, dove non ci sono solo smartphone, ma anche automobili, dispositivi IoT, smart cities e sistemi industriali automatizzati. Il 5G è il fondamento di quella che sarà l'Internet of Everything, dove ogni aspetto della vita quotidiana è connesso e integrato in una rete globale.

Il **5G** rappresenta quindi l'ultima evoluzione nella tecnologia di comunicazione mobile, portando miglioramenti significativi come *larghezza di banda elevata* e *latenza estremamente bassa*. Questa tecnologia supporta applicazioni avanzate come la realtà aumentata (AR), la realtà virtuale (VR) e le comunicazioni ultra-affidabili a bassa latenza (URLLC). Nel marzo 2018, il 3GPP ha rilasciato la 15ª release degli standard di comunicazione mobile, stabilendo le basi per il **5G**. La velocità di trasmissione di questa nuova tecnologia consente agli utenti di usufruire di trasferimenti dati notevolmente superiori, in particolare per applicazioni che richiedono un alto throughput, come lo streaming video in alta definizione [4].

La riduzione della latenza è un altro obiettivo chiave, con la previsione di una latenza inferiore a 1 millisecondo, aprendo la strada all'uso in tempo reale di applicazioni critiche come la telemedicina e la guida autonoma. Inoltre, il 5G permette la connessione simultanea di un numero molto maggiore di dispositivi

rispetto alle generazioni precedenti, una caratteristica fondamentale vista la continua crescita del mercato IoT.

Grazie a tutto questo, il 5G diventerà una base per una rete che connette non solo persone, ma anche oggetti, dispositivi e macchine. Si sta parlando, quindi, di un sistema che sta rivoluzionando il modo in cui immaginiamo internet, non più solo come uno scambio di dati tra persone, ma come un'integrazione massiccia tra esseri umani e macchine, e tra macchine stesse.

E qui entrano in gioco i tre scenari fondamentali del 5G: **eMBB, mMTC e uRLLC**. Ognuno di questi rappresenta una sfaccettatura dell'intera visione del 5G [5]: **eMBB** è pensato per una banda larga mobile potenziata, consentendo download rapidissimi e streaming ad altissima qualità; **mMTC** è rivolto alla comunicazione massiva tra macchine, essenziale per supportare l'IoT (Internet of Things); **uRLLC** invece è cruciale per applicazioni che richiedono una latenza minima e un'affidabilità estrema, come la telechirurgia o i veicoli autonomi. Ma quali sono le tecnologie che effettivamente rendono possibile tutto questo?
Il 3GPP ha definito più di 70 tipi di file 5G SA1 necessari a questo scopo, e le tecnologie chiave sviluppate per il 5G includono: *Massive MIMO*, *filter bank based multicarrier (FBMC)*, *Full Duplex*, *Ultra Dense networking (UDN)*, *software-defined networking (SDN)* e *network function virtualization (NFV)* [5].
In questo articolo verrà presentato uno studio approfondito sulla sicurezza all'interno delle reti 5G. Nella Sezione 2 si esamineranno gli asset, gli attaccanti e i rischi associati a una rete 5G. La Sezione 3 illustrerà gli obiettivi di sicurezza che si intendono raggiungere per gli asset identificati. Nella Sezione 4 verranno analizzati i servizi di sicurezza implementati all'interno di questa tecnologia. Infine, nella Sezione 5 si discuteranno le potenziali vulnerabilità presenti. Per mantenere il testo chiaro e conciso, evitando complicazioni eccessive e approfondimenti frequenti sulle diverse tecnologie e vulnerabilità, alla fine del documento è stato inserito un glossario. Questo glossario fornisce spiegazioni sui protocolli, sulle sigle e su altri termini pertinenti, facilitando così la comprensione del contenuto.

2 Threat model

In letteratura sono state identificate numerose sfide legate alla sicurezza del 5G. Gli asset principali coinvolti includono i dati sensibili degli utenti, come informazioni personali e dati di navigazione, che transitano attraverso la rete 5G. A questo si aggiungono l'infrastruttura di rete stessa, composta da stazioni base, server e dispositivi di rete, nonché i dispositivi degli utenti finali, tra cui smartphone, tablet e dispositivi IoT, che rappresentano una parte essenziale del sistema. È importante notare che, oltre ai dispositivi finali, i sistemi di controllo della rete, incaricati della gestione del traffico e dell'autenticazione, necessitano di una protezione adeguata per garantire l'integrità e la disponibilità della rete.

Le reti 5G introducono diverse tecnologie innovative, come il *software-defined networking (SDN)* e il *network function virtualization (NFV)*, che offrono vantaggi significativi in termini di flessibilità e scalabilità. Tuttavia, queste tecnolo-

gie espongono anche la rete a nuovi rischi di sicurezza, come l'esaurimento delle risorse e vulnerabilità nelle interfacce di programmazione, che possono diventare obiettivi per attacchi mirati. Inoltre, il *Massive Multiple-Input Multiple-Output (MIMO)* e le *comunicazioni a onde millimetriche (mmWave)* aumentano la capacità delle reti, ma devono affrontare problemi di sicurezza legati alla gestione delle risorse e alla segretezza delle informazioni. Anche il *cloud computing* e il *Multi-access Edge Computing* (MEC) possono contribuire a migliorare l'efficienza della rete, ma l'archiviazione e l'elaborazione dei dati nel cloud aumentano il rischio di attacchi ai dati sensibili [1].

I potenziali attaccanti in questo contesto possono variare notevolmente. Da una parte, ci sono hacker individuali che cercano di intercettare o manipolare i dati per scopi illeciti. Dall'altra, vi sono gruppi di cyber-criminali organizzati, e in alcuni casi anche attori sponsorizzati da stati, il cui obiettivo potrebbe essere ottenere accesso non autorizzato a informazioni sensibili o causare danni alla rete per ragioni economiche o geopolitiche. A rendere più complesso il quadro ci sono anche malintenzionati interni, ovvero personale con accesso legittimo alla rete, che potrebbe abusare delle proprie autorizzazioni. In questo contesto, è cruciale riconoscere che le vulnerabilità non provengono solo dall'esterno, ma anche da configurazioni errate e pratiche di sicurezza inadeguate da parte del personale autorizzato. I vettori di attacco attraverso cui questi attori possono colpire sono molteplici. La sicurezza delle interfacce radio, potrebbe essere compromessa se tali protocolli non vengono implementati correttamente o se si sfruttano vulnerabilità complesse. Questo apre la strada ad attacchi come l'intercettazione delle comunicazioni o i classici man-in-the-middle. Anche l'integrità del piano utente rappresenta un punto critico: nonostante l'introduzione di crittografia avanzata nel 5G, attacchi mirati potrebbero sfruttare eventuali falle nel processo di protezione dei dati, compromettendo così l'integrità dei dati trasmessi senza essere rilevati.

Durante il roaming, un altro momento delicato per la sicurezza, i parametri di protezione degli utenti potrebbero non essere aggiornati correttamente al passaggio tra reti diverse, esponendo gli utenti a potenziali attacchi di intercettazione o manipolazione dei dati. Questa problematica evidenzia la necessità di un'adeguata sincronizzazione e aggiornamento delle misure di sicurezza tra diverse reti, al fine di garantire una protezione continua e coerente.

L'infrastruttura del 5G, inoltre, non è immune da attacchi DoS (Denial of Service). Nonostante i progressi nelle misure di protezione, i sistemi di controllo della rete rimangono visibili e possono essere vulnerabili a interruzioni del servizio, soprattutto se i canali di controllo non sono crittografati adeguatamente. Qui, la gestione delle credenziali e delle configurazioni diventa fondamentale per prevenire accessi non autorizzati.

Infine, un importante vettore di attacco è rappresentato dai dispositivi degli utenti finali. Spesso, questi dispositivi non sono dotati di misure di sicurezza sufficienti a livello di sistema operativo e applicazioni, rendendoli vulnerabili a malware, attacchi DoS o manipolazioni dei dati di configurazione, compromettendo così l'intera rete. Questa vulnerabilità è accentuata dalla crescente diffusione dei dispositivi IoT, che possono presentare vulnerabilità intrinseche

dovute a progettazioni inadeguate o a una mancanza di aggiornamenti regolari.

In conclusione, il panorama delle minacce nella rete 5G è complesso e variegato, richiedendo un approccio multifattoriale per la protezione degli asset e la mitigazione dei rischi. Un'attenzione particolare deve essere dedicata non solo alle tecnologie e ai protocolli di sicurezza, ma anche alla formazione continua del personale e alla consapevolezza degli utenti finali riguardo ai rischi e alle migliori pratiche per la sicurezza.

3 Security goals

Ogni sistema di comunicazione affinchè sia considerato sicuro ha bisogno di protocolli e tecnolgie di protezione che proteggano le risorse usate la comunizazione in modo tale da garantire che i dati rispettino le proprietà di: **Riservatezza**, **Integrità**, **Disponibilità**, **Autenticità, Accountability** [8].
Questi obiettivi sono essenziali per garantire che le reti 5G possano operare in modo sicuro e affidabile, proteggendo i dati e le comunicazioni degli utenti.
Iniziamo con la Riservatezza. Questo obiettivo mira a garantire che solo gli utenti autorizzati possano accedere alle informazioni sensibili. Nelle reti 5G, dove la quantità di dati trasmessi è enorme e include informazioni personali e aziendali, è cruciale implementare misure di crittografia e autenticazione robusta. La riservatezza non è solo una questione di protezione dei dati, ma anche di fiducia degli utenti nel sistema. Se gli utenti percepiscono che i loro dati non sono al sicuro, potrebbero essere riluttanti a utilizzare i servizi offerti.
Passando all'Integrità, questo obiettivo si concentra sulla protezione dei dati da modifiche non autorizzate. In un ambiente 5G, dove i dispositivi IoT e le applicazioni critiche sono sempre più interconnessi, è fondamentale garantire che le informazioni rimangano accurate e non vengano alterate durante la trasmissione.
La Disponibilità è un altro obiettivo chiave. Le reti 5G devono essere sempre disponibili per garantire che gli utenti possano accedere ai servizi in qualsiasi momento. Questo è particolarmente importante per applicazioni critiche come quelle nel settore sanitario o nei trasporti. Per raggiungere questo obiettivo, è necessario implementare soluzioni di ridondanza e resilienza, in modo da mitigare gli effetti di attacchi come i Distributed Denial of Service (DDoS), che possono compromettere la disponibilità dei servizi.
L'Autenticità è fondamentale per garantire che le entità coinvolte nelle comunicazioni siano chi dichiarano di essere. In un contesto 5G, dove le interazioni avvengono tra una varietà di dispositivi e utenti, è essenziale implementare meccanismi di autenticazione robusti. Ciò non solo protegge gli asset da accessi non autorizzati, ma contribuisce anche a costruire un ecosistema di fiducia tra i vari attori coinvolti.
Infine, la Accountability è cruciale per garantire che tutte le azioni e le transazioni all'interno della rete possano essere tracciate e verificate. Questo obiettivo è particolarmente importante per la conformità alle normative e per la gestione delle responsabilità. Implementare sistemi di logging e monitoraggio

consente di rilevare attività sospette e di rispondere rapidamente a potenziali incidenti di sicurezza.
In sintesi, il modello CIAAA fornisce un framework completo per affrontare le sfide di sicurezza nelle reti 5G. Ogni obiettivo è interconnesso e contribuisce a creare un ambiente sicuro e affidabile per gli utenti e le applicazioni. La protezione degli asset in un contesto 5G richiede un approccio olistico che integri tecnologie avanzate, politiche di sicurezza rigorose e una continua vigilanza per affrontare le minacce emergenti.

4 Security service and implementation

L'architettura del 5G è organizzata attraverso 3 strati: uno strato applicatvo, uno strato di servizio e uno strato di trasporto [6]. Ogni strato è progettato con specifiche funzionalità di sicurezza che, combinate tra loro, creano un sistema sicuro e resistente alle minacce. I principali elementi di sicurezza nel 5G includono:

- **Sicurezza dell'accesso alla rete**: Meccanismi che permettono a un dispositivo utente (UE) di autenticarsi e accedere in modo sicuro ai servizi di rete. L'UE scambia messaggi di protocollo attraverso la rete di accesso con la rete di servizio (SN). Le chiavi crittografiche sono memorizzate nel modulo `USIM` del dispositivo e nell'ambiente dell'operatore. Questo garantisce la sicurezza dei dati e delle comunicazioni, impedendo accessi non autorizzati.

- **Sicurezza del dominio di rete**: Un insieme di caratteristiche che permettono ai nodi della rete di scambiarsi in modo sicuro i dati del piano di controllo e del piano utente all'interno delle reti 3GPP e tra reti diverse. Le tecniche di protezione includono crittografia e integrità per evitare intercettazioni e manomissioni.

- **Sicurezza del dominio utente**: Si concentra sulla protezione del dispositivo dell'utente e dei dati contenuti, impedendo l'accesso non autorizzato al terminale mobile. Sono implementati meccanismi hardware per proteggere il modulo `USIM` e prevenire la manomissione dei terminali, garantendo l'autenticità dell'utente.

- **Sicurezza del dominio dell'architettura basata su servizi**: Protegge la registrazione, la scoperta e l'autorizzazione degli elementi di rete, nonché le interfacce basate su servizi. Consente l'integrazione sicura delle nuove funzioni di rete virtuali del 5G, e supporta il roaming sicuro, coinvolgendo la rete di servizio e la rete domestica.

- **Visibilità e configurabilità della sicurezza**: Consente agli utenti di essere informati sulla presenza di funzioni di sicurezza e offre la possibilità di configurare le caratteristiche di sicurezza in base alle esigenze. Le specifiche di sicurezza del 5G, definite dal 3GPP, stabiliscono funzionalità

opzionali, fornendo gradi di libertà per l'implementazione e il funzionamento sicuro della rete.

Le procedure di sicurezza del 5G si basano su un framework a derivazione gerarchica. La chiave a lungo termine `K` è conservata dalla `Authentication Credential Repository and Processing Function` (ARPF) mentre la USIM conserva la copia corrispondente di tale chiave simmetrica dell'utente [6]. Tutte le altre chiavi sono derivate da essa (per vedere come vengono generate le chiavi guarda 13).

Il 3GPP ha introdotto l'`Extensible Authentication Protocol (EAP)` per l'Autenticazione e l'Accordo delle Chiavi, definendo l'`EAP-AKA` e il `5G AKA` come metodi obbligatori di autenticazione per i dispositivi (UE) e la rete. Questi protocolli garantiscono un'autenticazione reciproca tra il dispositivo e la rete, oltre a proteggere la sicurezza e la cifratura dei servizi. Durante la registrazione, un dispositivo 5G invia il SUCI per avviare il processo di autenticazione basato sul protocollo selezionato.

Le specifiche di sicurezza del 5G definiscono vari contesti di sicurezza per diverse situazioni: per una singola rete di servizio 5G (SN), tra più SN e tra reti 5G e 4G. Quando un dispositivo è connesso a due SN, ciascuna rete deve gestire e utilizzare autonomamente un proprio contesto di sicurezza. Nel caso in cui il dispositivo sia registrato su due SN all'interno della stessa rete pubblica mobile terrestre (PLMN), che siano 3GPP o non-3GPP, il dispositivo stabilisce due connessioni NAS (Non-Access Stratum) separate per ciascuna rete, ma condivide un contesto di sicurezza NAS comune, che include un unico insieme di chiavi e algoritmi di sicurezza.

Le procedure per mantenere o scartare un contesto di sicurezza durante la transizione di stato dicano che la configurazione della tipologia di handover è a discrezione dell'operatore, basandosi sui requisiti di sicurezza individuali. Di conseguenza, la sicurezza durante l'handover diventa una funzione opzionale e non obbligatoria, il che potrebbe portare alcuni operatori a implementare procedure di handover potenzialmente non sicure.

La separazione crittografica e la protezione contro attacchi di replay per due connessioni NAS attive vengono garantite attraverso un contesto di sicurezza NAS condiviso, con parametri distinti per ciascuna connessione. Il NAS impiega algoritmi di cifratura a 128 bit per garantire l'integrità e la riservatezza dei dati. È importante notare, tuttavia, che sono previste anche opzioni di cifratura e protezione dell'integrità nulle. Inoltre, se il dispositivo non dispone di un contesto di sicurezza NAS, il messaggio NAS iniziale viene trasmesso in chiaro, includendo l'identificatore dell'abbonato e le capacità di sicurezza del dispositivo stesso.

Nel controllo delle risorse radio, l'integrità e la riservatezza vengono garantite dal livello PDCP (Packet Data Convergence Protocol) che opera tra il dispositivo e il gNB. È importante notare che nessun livello al di sotto del PDCP è soggetto a protezione dell'integrità. La protezione contro gli attacchi di replay è attivata quando la protezione dell'integrità è in funzione, tranne nel caso in cui sia selezionata la protezione dell'integrità nulla. I controlli di integrità RRC

vengono effettuati sia sul dispositivo che sul gNB, e se un controllo di integrità fallisce dopo che la protezione è stata attivata, il messaggio corrispondente viene immediatamente scartato.

Passando al piano utente, la funzione di gestione delle sessioni (SMF) si occupa di fornire la politica di sicurezza per una sessione PDU (Protocol Data Unit) al gNB durante la fase di stabilimento della sessione. Se la protezione dell'integrità non è attivata per i portatori radio di dati (DRB), né il gNB né il dispositivo saranno in grado di proteggere l'integrità del traffico di tali DRB. Allo stesso modo, se la cifratura del piano utente non è attivata per i DRB, il traffico non verrà cifrato. La SMF locale ha la possibilità di sovrascrivere l'opzione di riservatezza presente nella politica di sicurezza del piano utente ricevuta dalla SMF della rete di origine (HN).

Infine, per quanto riguarda la privacy dello ID di abbonamento, il SUCI rappresenta la versione nascosta dell'identificatore di abbonamento permanente del 5G (SUPI). Questo viene trasmesso via etere per evitare l'esposizione dell'identità dell'utente in chiaro. Il SUCI è generato dal SUPI utilizzando la chiave pubblica dell'operatore e un metodo di crittografia asimmetrica probabilistica, il quale aiuta a prevenire il tracciamento dell'identità. Tuttavia, il sistema di protezione nulla del SUPI è utilizzato durante sessioni d'emergenza non autenticate, se configurato dalla rete di origine (HN), oppure quando la chiave pubblica dell'operatore non è stata fornita. Le specifiche del 5G definiscono anche un identificatore temporaneo, il 5G Globally Unique Temporary Identifier (5G-GUTI), per ridurre l'esposizione del SUPI e del SUCI. Il 5G-GUTI deve essere riassegnato in base ai trigger del dispositivo, ma la frequenza di tale riassegnazione è lasciata alla discrezione dell'implementazione della rete.

5 Attacks and Vulnerabilities

In questa sezione, verranno analizzate le vulnerabilità presenti nelle reti 5G, tenendo conto delle differenze legate alle architetture utilizzate. Le reti 5G possono essere suddivise in due categorie principali: il 5G Non-Standalone (NSA), un'architettura transitoria che si basa sull'infrastruttura 4G LTE per la gestione della segnalazione e del controllo, e il 5G Standalone (SA), che rappresenta una rete completamente autonoma. È fondamentale comprendere che le vulnerabilità possono manifestarsi in entrambe le architetture; tuttavia, alcune di esse possono risultare più comuni o rilevanti in una rispetto all'altra, in base alle specifiche implementazioni e tecnologie utilizzate. Di seguito, saranno illustrate alcune delle principali vulnerabilità facilmente sfruttabili in contesti di attacco, applicabili sia alle reti NSA che SA. Inizierò esaminando le debolezze che è più facile che si verifichino nelle architetture NSA, per poi trattare vulnerabilità più generali.

5.1 Minacce al Radio Access Network

Le minacce alla sicurezza del Radio Access Network (RAN) si concentrano sulle vulnerabilità della parte radio della rete, che include le stazioni base e i dispositivi mobili.

Fuga di informazioni: La perdita di informazioni può comprendere minacce come l'intercettazione del paging e il cracking dell'`IMSI`. L'intercettazione del paging è una tecnica di scansione passiva che sfrutta i messaggi di paging inviati dalle stazioni base ai terminali mobili. Un attaccante, utilizzando un `dispositivo SDR` (software-defined radio), può captare i segnali RF nelle vicinanze della vittima e rilevare l'identità temporanea del sottoscrittore mobile (S-TMSI) o il ciclo di paging. Sfruttando queste informazioni, l'attaccante può calcolare l'indice del frame di paging (PFI), limitando a soli 8 i possibili candidati IMSI della vittima. Successivamente, invia un paging IMSI con questi 8 candidati e osserva le risposte per individuare l'IMSI reale della vittima.

Denial of Service (DoS) per l'utente: Questo tipo di attacco include varie forme, come il DoS alla connessione `RRC` (Radio Resource Control), il DoS di rifiuto `RRC` e il DoS di rilascio `RRC`. Il DoS alla connessione `RRC` è particolarmente grave, poiché sfrutta l'`S-TMSI` (SAE-Temporary Mobile Subscriber Identity) della vittima, precedentemente ottenuto attraverso una fuga di informazioni. Le stazioni base non implementano procedure di autenticazione per i terminali, consentendo agli attaccanti di interferire con l'accesso wireless della vittima. L'attaccante può inviare un messaggio di richiesta di connessione `RRC` utilizzando il valore `S-TMSI` della vittima, portando alla disconnessione della connessione `RRC` della vittima e stabilendo una connessione con l'attaccante, che può poi continuare a inviare richieste per impedire l'accesso legittimo al servizio.

DoS della stazione base: Un attacco DoS può anche mirare a esaurire le risorse della stazione base, rendendo difficile per gli utenti legittimi connettersi. Quando un terminale cerca di stabilire una connessione, utilizza il protocollo `RRC`, che prevede un processo di accesso casuale. Gli attaccanti possono sfruttare questo processo per inviare richieste non autorizzate, aumentando il numero di connessioni `RRC` attive e sovraccaricando la stazione base, causando ritardi o interruzioni nei servizi.

Eavesdropping: In teoria, l'intercettazione delle reti wireless dovrebbe essere impossibile grazie alle impostazioni di sicurezza tra terminali e stazioni base. Tuttavia, esistono casi in cui è possibile estrarre il flusso di chiavi di sicurezza e decifrare le comunicazioni. Il traffico vocale nelle comunicazioni mobili utilizza il protocollo RTP (Real-time Transport Protocol) ed è trasmesso tramite un bearer vocale, distinto dal bearer dati. Per garantire la qualità del servizio (QoS), il bearer vocale è dedicato, con un identificatore di classe QoS (QCI) separato. Durante la creazione del flusso di chiavi per la cifratura nella procedura di sicurezza AS, sono utilizzati quattro parametri: `conteggio, direzione, lunghezza e ID del bearer`. Di questi, solo l'ID del bearer (ID DRB) rappresenta una variabile critica. L'ID DRB viene assegnato quando la stazione base

crea un bearer vocale, ma alcune stazioni base di determinati produttori possono assegnare lo stesso ID DRB all'interno della stessa connessione RRC, creando una vulnerabilità. Un attaccante può sfruttare questa falla intercettando la comunicazione vocale cifrata della vittima tramite uno sniffer. Dopo che la chiamata è terminata, l'attaccante può effettuare una chiamata vocale verso la vittima, intercettando sia la chiamata in chiaro che quella cifrata. Applicando l'operazione XOR tra il testo in chiaro e quello cifrato della seconda chiamata, l'attaccante è in grado di estrarre il flusso di chiavi, che può essere utilizzato per decifrare la prima chiamata, poiché entrambe hanno utilizzato lo stesso ID DRB e si sono svolte nella stessa connessione RRC. Per evitare questo tipo di attacco, lo standard 3GPP TS 33.401 raccomanda di utilizzare ID DRB diversi per i vari bearer, prevenendo così il riutilizzo dello stesso ID DRB nella stazione base.

Utilizzo non autorizzato dei dati: Nelle reti mobili esistono bearer predefiniti e dedicati, progettati per comunicazioni legittime. Un attaccante può sfruttare questi bearer per accedere ai dati in modo non autorizzato, ad esempio stabilendo comunicazioni senza costi. Inoltre, il masquerading del chiamante, noto anche come caller spoofing, è un attacco in cui l'attaccante falsifica l'identità del chiamante, ingannando la vittima.

5.2 Core Network Security Threats

Fuga di informazioni: Le informazioni relative alle reti core 5G NSA possono essere essenzialmente classificate in due categorie: quelle riguardanti l'equipaggiamento EPC (Evolved Packet Core), dedicato all'elaborazione dei dati, e quelle concernenti l'equipaggiamento IMS (IP Multimedia Subsystem), che fornisce vari servizi. Poiché l'equipaggiamento EPC utilizza il protocollo GTP per le comunicazioni, mentre l'equipaggiamento IMS si basa sul protocollo SIP (Session Initiation Protocol), un attaccante ha la possibilità di scegliere il protocollo più appropriato per accedere alle informazioni desiderate. Il protocollo GTP si distingue in due componenti: GTP-C, impiegato per la comunicazione tra le attrezzature della rete core, e GTP-U, responsabile del trasporto del traffico dati dal terminale utente attraverso un tunnel tra la stazione base e il PGW (Packet Gateway). Per estrarre informazioni sull'indirizzo IP dell'equipaggiamento EPC, l'attaccante può ricorrere a un metodo di iniezione di pacchetti, caricando nel payload dei dati una richiesta di eco (echo request) insieme a un messaggio GTP-C per il controllo dello stato di salute delle attrezzature di rete. Utilizzando un programma denominato Packit, è possibile eseguire il comando Android Debug Bridge (ADB) nel terminale Android, generando così un pacchetto. Inviando questo pacchetto all'indirizzo IP ottenuto tramite il comando Tracert in modalità tethering, il pacchetto GTP-C viene iniettato e trasmesso alla rete di comunicazione mobile. Il PGW, una volta ricevuto il pacchetto, lo verifica e invia una risposta di eco, consentendo all'attaccante di identificare l'IP sorgente di quel messaggio come PGWIP.

Esaurimento degli indirizzi IP: Utilizzando la tecnica GTP-in-GTP, un

attaccante può esaurire il pool di indirizzi IP della rete inviando richieste di sessione con numeri di terminale incrementati, impedendo così ai terminali legittimi di connettersi. Questa tecnica sfrutta la vulnerabilità del protocollo GTP (GPRS Tunneling Protocol), utilizzato per il trasporto di dati nelle reti mobili. GTP-in-GTP implica l'incapsulamento di pacchetti GTP all'interno di altri pacchetti GTP, consentendo all'attaccante di inviare richieste multiple in una singola connessione. L'attaccante crea delle sessioni GTP all'interno di altre sessioni GTP, amplificando l'attacco e aumentando il numero di richieste generate, rendendo ancora più rapido l'esaurimento delle risorse di rete. Questa tecnica si rivela particolarmente efficace perché sfrutta l'overhead di gestione delle sessioni GTP, causando un sovraccarico del sistema di allocazione degli indirizzi IP.

Denial of Service (DoS): Un attacco DoS può essere eseguito inviando ripetutamente messaggi di richiesta di connessione alla rete 5G NSA, sovraccaricando il core di rete e causando l'interruzione del servizio.

Manipolazione del NAS: I messaggi del protocollo NAS, utilizzati per la segnalazione tra terminali e core di rete, non sempre sono protetti da cifratura. Un attaccante può sfruttare questa vulnerabilità installando una stazione base malevola per manipolare i messaggi e alterare i parametri critici per la cifratura e l'integrità dei dati.

Intercettazione: La comunicazione vocale su una rete 5G sfrutta la rete IMS e avvia le sessioni tramite il protocollo SIP, seguendo le direttive stabilite dallo standard 3GPP. Di conseguenza, la sicurezza del protocollo SIP è cruciale e viene principalmente garantita attraverso le associazioni di sicurezza (SA) dell'IPSec. Tuttavia, l'implementazione di IPSec SA è gestita in modo selettivo dagli operatori delle reti 5G, e il supporto per il VoLTE (Voice over LTE) non implica necessariamente una copertura totale dell'IPSec, a causa dell'impatto significativo che potrebbe avere sulle prestazioni del terminale. Prendiamo ad esempio il Samsung Galaxy S10, che supporta IPSec, ma presenta un problema: l'impostazione relativa può essere disattivata tramite un menu nascosto. Se un attaccante riesce a ottenere l'accesso remoto a questo menu nascosto e modifica l'impostazione di IPSec, le comunicazioni vocali della vittima avverranno senza cifratura. Inoltre, se il campo EEA viene alterato mediante una manipolazione del NAS (Non-Access Stratum) e non viene utilizzato un algoritmo di cifratura NAS, anche la comunicazione wireless nella sezione AS (Access Stratum) risulterà non cifrata. In tale scenario, l'attaccante può intercettare il traffico wireless utilizzando un attacco man-in-the-middle (MitM), permettendogli di ascoltare il traffico vocale della vittima privo di cifratura.

Spoofing: Lo spoofing di IP è un attacco comune in cui l'attaccante invia pacchetti con indirizzi IP falsificati, causando problemi di fatturazione e potenziali attacchi DoS. Inoltre, lo spoofing del campo `from` nei pacchetti SIP o MMS può essere utilizzato per il voice phishing, presentando numeri falsificati sul terminale ricevente.

5.3 Contromisure

Possiamo considerare un approccio alle contromisure contro le minacce alla sicurezza del 5G su due livelli: la standardizzazione delle linee guida di sicurezza e il rilevamento tramite sistemi di rilevamento delle intrusioni o sistemi di prevenzione delle intrusioni.

Denial of Service (DoS) della connessione RRC.
La causa principale della minaccia di DoS sulla connessione RRC è che la richiesta di connessione RRC, un messaggio trasmesso quando un terminale utente accede alla rete, viene inviata in chiaro, e il messaggio include il TMSI, un'informazione di identificazione temporanea del terminale utente. Per rispondere a questo, è necessario verificare la contraffazione dei messaggi RRC a livello di stazione base, il che non è facile da definire nelle specifiche 3GPP. Inoltre, bloccare gli aggressori dal scoprire l'informazione di identificazione temporanea di un utente specifico può essere un modo per verificare, ma anche questo non è semplice, poiché esistono troppi metodi noti. L'utilizzo dell'informazione di identificazione temporanea nella richiesta di connessione RRC serve a prevenire l'invasione della privacy causata dalla fuga e dall'abuso dell'IMSI, che è l'informazione di identificazione dell'abbonato all'interno della USIM. Tuttavia, gli aggressori possono intercettare i messaggi di richiesta di connessione RRC inviati in chiaro e identificare facilmente il TMSI. Da ciò, l'aggressore può creare e inviare un messaggio di richiesta di connessione RRC modulato in modo che la stazione base confonda il messaggio con uno inviato dal terminale della vittima. Nella rete centrale, l'informazione di identificazione temporanea viene creata a intervalli di tempo secondo regole specifiche basate sull'IMSI, e anche se il TMSI viene cambiato, l'aggressore può identificare il TMSI cambiato e creare nuovamente un messaggio di attacco. Quando riceve la richiesta di connessione RRC modulata, le stazioni base annullano la connessione al terminale esistente della vittima senza verificare lo stato di modulazione e consentono l'accesso al terminale dell'aggressore. In tale situazione, se la stazione base non disconnette il terminale esistente della vittima o mantiene la connessione per un certo periodo di tempo, può ridurre la minaccia di DoS della vittima. Poiché il terminale dell'aggressore fallisce l'autenticazione dopo la connessione RRC, mantenere la connessione con il terminale esistente solo durante il periodo in cui il terminale dell'aggressore invia la richiesta di connessione RRC e l'autenticazione fallisce potrebbe non influenzare significativamente le prestazioni della stazione base.

Manipolazione NAS (spoofing della cifratura NAS).
Lo standard 5G della 3GPP supporta sia la verifica dell'integrità che la comunicazione cifrata per rafforzare la sicurezza del protocollo NAS tra i terminali e le reti centrali 5G. Tuttavia, poiché la comunicazione cifrata non è obbligatoria ma una funzione opzionale tra le funzioni di sicurezza del protocollo NAS, ci sono alcuni casi in cui le funzioni di sicurezza non vengono utilizzate a causa della politica del paese o dell'operatore mobile. Oltre alle chiamate di emergenza, alcuni paesi o operatori potrebbero non utilizzare le capacità di cifratura fornite dagli standard 5G in termini di sicurezza. Inoltre, lo standard 5G non

definisce l'autenticazione reciproca tra terminali (UE) e reti 5G né la funzione di verifica dell'integrità dei messaggi iniziali scambiati prima della cifratura, basandosi su un affidamento sottostante che presume che i messaggi iniziali non siano modulati. Questo problema deriva da una vulnerabilità che non conferma la contraffazione del primo messaggio di richiesta di accesso (richiesta di attacco) alla rete 5G inviato dall'UE. Un attaccante malintenzionato si infiltra tra l'UE della vittima e una stazione base, manipola un messaggio di richiesta di accesso che include una richiesta di cifratura e verifica dell'integrità normalmente inviato dal terminale in un messaggio di richiesta di accesso con cifratura disabilitata e integrità non verificata, e lo invia a una stazione base normale.

Le apparecchiature della rete centrale 5G (MME) formano un canale non cifrato con l'UE secondo la richiesta di disabilitazione della cifratura, un messaggio manipolato diverso dal messaggio originale inviato dall'UE, anche se l'attivazione della cifratura è predefinita. Questo problema si verifica perché lo standard 3GPP non incorpora una procedura di autenticazione dell'integrità per controllare la contraffazione del messaggio iniziale prima della fase di autenticazione reciproca, il che porta a una comunicazione non cifrata causata da messaggi UE manipolati non cifrati e non verificati per l'integrità.

Possono sorgere due minacce da questo, la prima è la manipolazione del contenuto del messaggio. Ci sono vulnerabilità o rischi in cui gli aggressori malintenzionati possono modulare i messaggi inviati dal terminale di una vittima a loro piacimento. Ciò è dovuto al fatto che lo standard non definisce alcuna procedura di verifica dell'integrità per controllare se i messaggi di richiesta di accesso inviati da un terminale durante il primo accesso alla rete di comunicazione siano stati manipolati o meno. La seconda minaccia è l'intercettazione delle comunicazioni. A causa di una richiesta di disabilitazione della cifratura all'interno del messaggio di accesso iniziale modulato, la comunicazione tra il terminale e la rete 5G sarà formata come un canale non cifrato, consentendo a un aggressore malintenzionato di intercettare tutte le comunicazioni wireless e di esporre le informazioni personali e di localizzazione contenute nei messaggi scambiati. Un aggressore può disabilitare le impostazioni di cifratura tra il terminale della vittima e la rete centrale utilizzando una stazione base falsa per utilizzare i dati della vittima o per intercettare il contenuto del messaggio. Abbiamo implementato un algoritmo per rilevare questo e condotto test di prestazione di rilevamento. Analizzando i campi di cifratura nei messaggi del protocollo NAS tra terminali e reti centrali, è possibile impostare canali di bypass della cifratura o determinare se si tratta di terminali non standard.

Intercettazione (spoofing SIP).
Poiché l'intercettazione causata dallo spoofing SIP è possibile quando l'IPSec è disattivato, è necessario guidare le impostazioni di cifratura della comunicazione vocale tra i terminali e la rete 5G per essere gestite dalla rete dell'operatore mobile, invece di essere elaborate secondo la funzione del terminale (è necessaria un'applicazione selettiva nella rete per i terminali non supportivi dell'IPSec). Se l'impostazione IPSec del servizio vocale 5G è determinata dalla funzione del terminale, gli utenti malintenzionati potrebbero tentare più attacchi sfruttando

le impostazioni del loro terminale. Inoltre, è necessario fare sforzi per sensibilizzare e pubblicizzare il rischio di fuga dei dettagli di comunicazione quando gli aggressori modulano maliziosamente i messaggi e si impegnano in comunicazioni non cifrate tra il terminale e la rete 5G. La sezione applicabile per l'IPSec è definita come politica locale nella 3GPP, ma è necessario esaminare se renderla obbligatoria a livello di standard 3GPP. Di conseguenza, abbiamo provato a presentare un rapporto di vulnerabilità sui problemi sopra descritti alla 3GPP e abbiamo discusso queste questioni attraverso una collaborazione con un gruppo di ricerca. Le linee guida per la corretta configurazione e attivazione del protocollo IPSec nella rete 5G potrebbero essere incorporate nella prossima revisione delle specifiche 3GPP.

5.4 GUTI Reallocation Command Attack

Il 5G-GUTI (Globally Unique Temporary Identifier) è un identificatore temporaneo assegnato agli utenti per garantire la loro privacy. In alcune reti 5G SA (Standalone), questo identificatore viene riassegnato in modo casuale e non prevedibile. La vulnerabilità risiede nel fatto che il comando per la riassegnazione del GUTI viene inviato senza protezione di sicurezza, né in termini di integrità né di crittografia [3]. Gli attaccanti possono sfruttare questa vulnerabilità in diversi modi:

- **Man-in-the-Middle (MiTM)**: Un attaccante può intercettare il messaggio di aggiornamento della configurazione e modificarne il valore 5G-GUTI. Se l'UE cerca di ristabilire una connessione usando questo valore alterato, la rete non lo riconoscerà, portando a un attacco di Denial of Service (DoS).
- **GUTI Refreshment Neutralization**: Questo attacco sfrutta la mancanza di una richiesta di riconoscimento (ACK) nel messaggio di aggiornamento della configurazione. Se l'UE non invia un messaggio di completamento, l'attaccante può bloccare o alterare i comandi senza conseguenze.
- **Tracciamento della Vittima**: L'assenza di crittografia nel comando di riassegnazione GUTI consente agli attaccanti di tracciare la posizione degli utenti. Possono inviare messaggi silenziosi (che non attivano notifiche) e osservare le risposte della rete per determinare la presenza dell'UE in specifiche aree geografiche.

5.4.1 Difficoltà in Scenari di Rete Ampia

In una rete con molti dispositivi connessi, è complicato per l'attaccante isolare un singolo dispositivo a causa del numero di messaggi inviati. Tuttavia, possono migliorare l'accuratezza dell'attacco inviando messaggi a intervalli specifici o in orari di bassa attività.

5.4.2 Responsabilità degli Operatori e contromisura

Le vulnerabilità identificate derivano da errori di implementazione nelle reti 5G. In particolare, gli operatori non dovrebbero inviare messaggi NAS senza garantire l'integrità. Inoltre, la mancanza di crittografia è una scelta progettuale, secondo i documenti 3GPP, che rendono la crittografia facoltativa. In conclusione, per mitigare questo problema basterebbe da parte degli operatoi inviare questi messaggi garantendone l'integrità tramite crittografia.

5.5 Security Capabilities Bidding-Down Attack

Il Bidding-Down Attack è una vulnerabilità che può manifestarsi in alcune implementazioni delle reti 5G, in particolare nelle reti non standalone (NSA) e nelle reti standalone (SA) di operatori che non seguono correttamente le specifiche di sicurezza definite dalla 3GPP, cioè non eseguono adeguatamente la verifica delle capacità di sicurezza supportate dall'UE (non può comprendere la differenza tra le capacità di sicurezza supportate comunicate nella richiesta di registrazione iniziale e quelle ricevute nel messaggio NAS SMC). Questo attacco sfrutta le debolezze nel processo di negoziazione delle capacità di sicurezza tra il dispositivo utente (UE) e la rete, con potenziali conseguenze negative sulla riservatezza e l'integrità dei dati trasmessi [3].

Quando un UE invia una richiesta di registrazione alla rete, comunica le proprie capacità di sicurezza, specificando gli algoritmi di cifratura e di integrità supportati. Tuttavia, un attaccante attivo in modalità man-in-the-middle può intercettare questo messaggio e modificarlo, sostituendo gli algoritmi di sicurezza comunicati con quelli più deboli.

Successivamente, viene eseguita la procedura di autenticazione basata su 5G-AKA. Una volta completata l'autenticazione, la rete centrale (CN) invia un comando NAS Security Mode Command (SMC) al UE. Nelle implementazioni delle reti 5G NSA e SA, il comando NAS SMC non include un codice di autenticazione del messaggio (MAC), il che significa che il UE non è in grado di verificare l'integrità del messaggio ricevuto. Pertanto, l'attaccante può nuovamente alterare gli algoritmi di sicurezza, inducendo il dispositivo ad accettare quelli più deboli, portando a una completa compromissione della sicurezza.

Quindi, il Bidding-Down Attack rappresenta una seria minaccia nelle implementazioni di reti 5G che non implementano adeguatamente meccanismi di sicurezza, evidenziando l'importanza di seguire le linee guida stabilite per garantire la protezione delle comunicazioni.

Per evitare il Bidding-Down Attack, ci sono diverse misure che possono essere adottate. Innanzitutto, è fondamentale includere sempre un codice di autenticazione del messaggio (MAC). Un altro aspetto importante è l'implementazione di meccanismi di verifica robusti. È essenziale che la rete esegua controlli accurati sulle capacità di sicurezza comunicate dall'UE, confrontando ciò che il dispositivo dichiara di supportare con quello che la rete è in grado di gestire. In questo modo, si può rilevare e prevenire l'accettazione di algoritmi di sicurezza più deboli. In aggiunta, è fondamentale utilizzare algoritmi di sicurezza

avanzati. Le reti dovrebbero evitare l'uso di algoritmi obsoleti o meno sicuri, optando per quelli più recenti e robusti, che offrano una protezione adeguata contro attacchi di questo tipo.

6 Conclusions

La tecnologia 5G rappresenta una delle ultime frontiere nel campo delle comunicazioni senza fili. Essa ha il potenziale di rivoluzionare molte attività umane e il nostro modo di concepire le comunicazioni moderne, grazie a elevate velocità di trasmissione, bassa latenza e un alto throughput. Tuttavia, con l'avanzamento della tecnologia mobile, si sviluppano anche nuove minacce che possono compromettere la sicurezza di queste reti. In questo articolo, sono state analizzate le principali vulnerabilità associate al 5G. Molte di queste vulnerabilità sono ereditate dal 4G, mentre altre sono completamente nuove. La ricerca sulla sicurezza e l'identificazione di soluzioni innovative rappresentano un compito cruciale per tutti gli attori coinvolti, dai fornitori di servizi di rete a coloro che definiscono i protocolli di comunicazione. Questo diventa particolarmente necessario, considerando che il 5G è sempre più fondamentale per settori della vita quotidiana che possono diventare estremamente delicati se non gestiti correttamente, come la telemedicina e i veicoli a guida autonoma. L'evoluzione della cybersecurity nel contesto del 5G non è solo una risposta alle minacce esistenti, ma anche una sfida per prevedere e mitigare rischi futuri, considerando la crescente interconnessione globale. Tecnologie chiave come l'intelligenza artificiale e il machine learning offrono un potenziale significativo per migliorare la protezione delle reti, identificando in tempo reale minacce sofisticate e attacchi su larga scala. Inoltre, la crittografia deve evolversi per far fronte a nuove forme di attacco, inclusi quelli che potrebbero emergere dall'uso di computer quantistici. Guardando al futuro, è chiaro che la sicurezza del 5G diventerà un aspetto sempre più centrale, soprattutto con l'incremento dei dispositivi IoT connessi e l'utilizzo del 5G in infrastrutture critiche. Senza una protezione adeguata, le conseguenze potrebbero essere devastanti, mettendo a rischio non solo la privacy degli utenti, ma anche la stabilità dei sistemi economici e sociali. La cooperazione internazionale, lo sviluppo di nuove tecnologie e la definizione di standard sempre più stringenti saranno essenziali per garantire che il 5G sia non solo un motore di progresso, ma anche una piattaforma sicura per le generazioni future.

A Termini da ricordare

- **Massive MIMO**: I sistemi wireless Multiple Input Multiple Output sfruttano più antenne di trasmissione e ricezione per aumentare la capacità di rete, migliorando il throughput dei dati e servendo un maggior numero di utenti. MIMO suddivide il segnale in sottosegnali a bassa velocità, trasmessi su antenne spazialmente separate sullo stesso canale di frequenza. Grazie alla propagazione su percorsi multipli, il ricevitore separa i segnali in flussi paralleli per recuperare il segnale originale. MIMO aumenta la capacità del canale senza consumare ulteriore larghezza di banda o potenza e la velocità può crescere aggiungendo più antenne. Nel 5G, la tecnologia Massive MIMO va oltre la configurazione 2×2 del 4G, utilizzando numerosi flussi simultanei per aumentare la capacità di rete e l'efficienza spettrale. L'array di antenne più grande permette un'elaborazione coerente del segnale, adattandosi velocemente ai cambiamenti del canale di propagazione [7].

- **mmWave**: Le comunicazioni ad onde millimetriche si rifereiscono all'uso di onde elettromagnetiche molto elevate, tipicamente comprese tra *30 GHz e 300GHz*. Questo onde sono chiamate millimetriche perchè la loro lunghezza d'nda varia tra 1mm e 30mm, che sono molto più corte rispetto alle onde radio tradizionalmente usate. Esse permetono velocità molto elevate e basssa latenza, ma hanno una portata limitata e scarsa capacità di penetrazione, richiedendo infrastrutture dense come small cells e tecnologie avanzate come il beamforming. Utilizzate insieme a frequenze più basse per garantire una copertura completa, le mmWave sono cruciali per migliorare la capacità delle reti in aree ad alta densità di utenti.

- **EAP-AKA**: è un protocollo di autenticazione progettato per consentire l'autenticazione sicura tra un dispositivo mobile e una rete, basato sul concetto di chiavi simmetriche. Quando un dispositivo, desidera connettersi a una rete, invia una richiesta di autenticazione utilizzando un `SUCI`, una versione cifrata del suo identificatore permanente, il `SUPI`, consentendo alla rete di identificare il dispositivo senza rivelare l'identità reale dell'utente e garantendo la sua privacy. La rete, ricevuta la richiesta, utilizza il SUCI per accedere alle credenziali memorizzate nel database dell'`ARPF`, dove è custodita la chiave segreta `K`, condivisa tra il dispositivo e la rete; se viene scelto il protocollo `EAP-AKA`, la rete avvia il processo di autenticazione generando una `sfida` per il dispositivo composta da tre elementi: un numero casuale `(RAND)`, un messaggio di autenticazione `(AUTN)` e la risposta attesa `(XRES)`, che vengono inviati al dispositivo. Questo verifica il valore `AUTN` utilizzando la chiave `K` nella sua `USIM`, e, se l'`AUTN` è valido, calcola una risposta `(RES)` basata su `RAND` e la chiave `K`, quindi la invia alla rete, che confronta la `RES` ricevuta con la `XRES` generata in precedenza; se corrispondono, l'autenticazione ha successo e entrambe le parti hanno verificato l'identità reciproca. Successivamente, si genera la chiave di sessione, derivata dalla chiave `K` e dai materiali generati nella sfida, con

chiavi come CK (per la cifratura dei dati) e IK (per l'integrità dei messaggi), essenziali per proteggere le comunicazioni. Una volta completato il processo di autenticazione e derivate le chiavi di sessione, il dispositivo e la rete possono iniziare a scambiare dati in modo sicuro, sapendo che le comunicazioni sono protette da solide misure di sicurezza.

- **5G AKA**: Il processo 5G AKA inizia con l'invio, da parte del dispositivo, di una richiesta di autenticazione alla rete tramite il SUCI, una versione cifrata del SUPI, che protegge l'identità dell'utente durante la registrazione. La rete riceve questa richiesta e la invia al database delle credenziali, che contiene la chiave segreta K condivisa tra il dispositivo e la rete. Se viene scelto il protocollo 5G AKA, la rete genera una sfida composta da un numero casuale (RAND), un'autenticazione temporanea (AUTN) e una risposta attesa (XRES), che vengono inviati al dispositivo. Il dispositivo, usando la chiave K memorizzata nella USIM, verifica l'AUTN per confermare l'identità della rete; se la verifica è valida, calcola una risposta (RES) basata su RAND e K, che viene poi inviata alla rete. La rete confronta la RES con la XRES generata in precedenza, e se corrispondono, l'autenticazione ha successo. A questo punto, vengono generate le chiavi di sessione per la cifratura e l'integrità delle comunicazioni, garantendo la sicurezza dei dati trasmessi. Una caratteristica importante del 5G AKA è il rafforzamento della privacy dell'utente, grazie alla separazione delle chiavi di cifratura e integrità e a meccanismi più robusti per prevenire attacchi di tracciamento e correlazione delle identità, migliorando significativamente la sicurezza rispetto alle generazioni precedenti.

- **PLMN (Public Land Mobile Network)**: È una rete mobile pubblica terrestre. Un PLMN è una rete mobile che fornisce servizi di comunicazione mobile al pubblico. Ogni operatore mobile ha il proprio PLMN identificato da un codice univoco, che consente ai dispositivi di identificare e connettersi a quella rete.

- **FBMC**: Il Filter Bank Multicarrier (FBMC) è una tecnica di modulazione che divide un segnale in più sottocanali, applicando filtri per ridurre le interferenze tra questi, migliorando così l'efficienza spettrale rispetto all'OFDM.

- **FullDuplex**:Il full duplex è una modalità di comunicazione in cui i dati possono essere trasmessi e ricevuti contemporaneamente tra due dispositivi o punti. In altre parole, entrambe le parti possono inviare e ricevere informazioni allo stesso tempo, senza dover aspettare che una delle due abbia finito di trasmettere.

- **Ultra Dense Networking**:L'Ultra Dense Networking (UDN) è una architettura di rete progettata per migliorare la capacità e la copertura della rete in ambienti ad alta densità di utenti o dispositivi.DN si basa sull'idea di aumentare il numero di celle o piccole stazioni base (small cells) in un'area geografica, riducendo la distanza tra queste stazioni e i dispositivi

connessi. Questo riduce il carico su ogni singola stazione base, migliorando la capacità di banda e la qualità del segnale.

- **Software-Defined Networking**: Software-Defined Networking (SDN) è un approccio alla gestione delle reti che separa il piano di controllo (control plane) dal piano dati (data plane). Tradizionalmente, i router e gli switch svolgono sia il compito di instradare il traffico (piano dati) che di decidere come farlo (piano di controllo). SDN sposta il piano di controllo in un'entità software centrale chiamata `controller`, che ha una visione globale della rete e può programmare dinamicamente come i pacchetti devono essere gestiti dagli switch, semplificando la gestione della rete e migliorandone l'agilità.

- **Network Function Virtualization**: La Network Function Virtualization (NFV) è una tecnologia che virtualizza le funzioni di rete, come firewall, router, load balancer e altri dispositivi di rete, su server standard, eliminando la necessità di hardware specializzato. NFV consente di distribuire e gestire le funzioni di rete come software, migliorando la scalabilità, la velocità di implementazione e riducendo i costi.

- **S-TMSI**: è un identificatore temporaneo utilizzato nelle reti 4G LTE e 5G per rappresentare un abbonato senza rivelarne l'IMSI (International Mobile Subscriber Identity). Esso viene generato dalla rete e cambia periodicamente, riducendo il rischio di tracciamento e attacchi informatici.

- **RRC**: Il protocollo RRC è una parte fondamentale dell'architettura delle reti mobili, utilizzato per gestire la comunicazione tra il terminale utente (UE) e la rete radio nel contesto delle tecnologie mobili. RRC si occupa della gestione delle risorse radio, garantendo che il terminale possa accedere e utilizzare le risorse di rete in modo efficiente. Il protocollo svolge diverse funzioni chiave, tra cui: la configurazione e la gestione delle connessioni radio, il monitoraggio delle condizioni della rete, la gestione delle transizioni tra le diverse modalità operative (ad esempio, da stato di idle a stato connesso), e l'assegnazione delle risorse necessarie per la trasmissione dei dati. Durante il processo di handover, RRC garantisce la continuità del servizio, trasferendo il controllo delle risorse radio da una cella all'altra quando l'utente si sposta. RRC si divide in diverse modalità di funzionamento: RRC_IDLE, in cui il terminale non è connesso attivamente alla rete, e RRC_CONNECTED, dove il terminale è in comunicazione attiva con la rete. Il protocollo svolge anche un ruolo importante nel garantire la sicurezza delle comunicazioni, gestendo le chiavi di cifratura e autenticazione.

- **eNB**: Rappresenta il nodo di accesso radio delle reti `4G LTE`. eNB è responsabile della trasmissione e ricezione dei segnali radio tra l'utente finale e la rete core `LTE` e ha funzioni di gestione delle risorse radio, codifica e decodifica, controllo di potenza, gestione della mobilità e dellos cheduling dei dati.

- **gNB**: Il gNB è la stazione base utilizzata nelle reti 5G e rappresenta l'evoluzione dell'eNB delle reti LTE. Svolge un ruolo fondamentale nel fornire connettività radio ai terminali utente (UE) e gestisce le comunicazioni tra il dispositivo mobile e il core network 5G. Il gNB è progettato per supportare una maggiore capacità e una latenza ridotta, consentendo così servizi avanzati come il massive IoT (Internet delle Cose), la realtà aumentata e le comunicazioni critiche. A differenza dell'eNB, il gNB può gestire simultaneamente diverse modalità di accesso radio, inclusa la NR (New Radio), e supporta configurazioni sia standalone (SA) che non standalone (NSA). Il gNB comunica con il core network tramite il protocollo NG, che include interfacce per la segnalazione e il trasporto dei dati. Una delle caratteristiche distintive del gNB è la sua capacità di coordinazione con altri gNB per implementare tecniche avanzate come il Coordinated Multi-Point (CoMP), migliorando la copertura e l'efficienza spettrale. Inoltre, il gNB implementa meccanismi di sicurezza avanzati, come l'autenticazione e la cifratura, per garantire comunicazioni sicure e protette.

- **IMSI**: International Mobile Subscriber Identity è un numero identificativo univoco, composto da 15 cifre associato a ciascun abbonato nella rete mobili. Questo numero è utilizzato per identificare e autenticare un utente all'interno di una rete mobile. `IMSI` è memorizzato nella scheda SIM e include il codice del paese `(MCC)`, il codice dell'operatore `(MNC)` e un numero identificativo dell'abbbonato `(MSIN)`.

- SDR: Un dispositivo SDR (Software-Defined Radio) è una radio in cui gran parte delle operazioni di elaborazione del segnale, come modulazione e demodulazione, viene eseguita tramite software anziché hardware fisso. Questo permette di adattare il dispositivo a diverse frequenze e protocolli radio semplicemente aggiornando il software, rendendolo estremamente flessibile e versatile per applicazioni come telecomunicazioni, ricerca e analisi di sicurezza.

- **RTP**: Il protocollo RTP è utilizzato per il trasporto di dati multimediali in tempo reale, come audio e video, su reti IP, ed è fondamentale per applicazioni come la telefonia VoIP e le videoconferenze. RTP fornisce funzionalità per sincronizzare il flusso multimediale e garantire la corretta sequenza dei pacchetti, anche se viaggiano attraverso percorsi di rete diversi. Durante la trasmissione, i dati multimediali vengono incapsulati in pacchetti RTP che includono informazioni essenziali come il timestamp (per la sincronizzazione del flusso) e il numero di sequenza (per l'ordinamento dei pacchetti). Il protocollo è spesso utilizzato insieme a RTCP (RTP Control Protocol), che monitora la qualità del servizio, fornendo feedback sul ritardo, jitter e perdita di pacchetti. RTP non fornisce nativamente funzionalità di sicurezza, quindi per garantire la protezione delle comunicazioni, può essere usato in combinazione con protocolli come SRTP (Secure RTP), che offre cifratura e autenticazione. RTP è partico-

larmente adatto per trasmissioni in tempo reale poiché è ottimizzato per minimizzare i ritardi e mantenere una qualità costante anche su reti non affidabili.

- **GTP**: Il GTP è un protocollo utilizzato nelle reti mobili per il trasporto dei dati e la segnalazione tra nodi della rete. Si divide in due componenti principali: il **GTP-C** (Control Plane), che gestisce la segnalazione e il controllo delle sessioni, e il **GTP-U** (User Plane), che si occupa del trasporto effettivo dei dati dell'utente. Quando un utente si connette alla rete, il GTP-C crea un tunnel per la segnalazione tra i nodi della rete core. Una volta stabilito il tunnel, il GTP-U trasporta i pacchetti dati dell'utente incapsulandoli e inviandoli attraverso la rete. Se l'utente cambia cella o la connessione deve essere aggiornata, il GTP-C interviene per modificare la sessione, garantendo la continuità della trasmissione dei dati. Al termine della sessione, il GTP-C chiude il tunnel e termina la connessione. Anche se il GTP è essenziale per il trasporto efficiente dei dati, può presentare vulnerabilità che potrebbero essere sfruttate da attacchi, rendendo necessaria l'adozione di misure di sicurezza appropriate.

- **NAS**: Gestisce la comunicazione tra il dispositivo dell'utente e il core network, occupandosi di autenticazione e registrazione, assicurando che solo i dispositivi autorizzati accedano alla rete. Inoltre, si occupa della mobilità, consentendo agli utenti di passare da una cella all'altra senza interruzioni. Gestisce anche le sessioni di dati, stabilendo e terminando le connessioni e mantenendo la qualità del servizio.

- **MME**: L'Mobility Management Entity (MME) è un componente software nel core network delle reti mobili 4G e 5G, responsabile della gestione della mobilità degli utenti e della segnalazione. Svolge funzioni chiave come l'autenticazione degli utenti, la gestione delle sessioni, il monitoraggio della posizione e l'instradamento delle richieste di servizio verso altre entità di rete. L'MME comunica con dispositivi terminali e altri elementi della rete utilizzando protocolli come NAS (Non Access Stratum) e GTP (GPRS Tunneling Protocol).

References

[1] Ijaz Ahmad et al. "Security for 5G and Beyond". In: *IEEE Communications Surveys & Tutorials* 21 (2019), pp. 3682–3722. DOI: 10.1109/COMST.2019.2916180.

[2] Ramraj Dangi et al. "Study and investigation on 5G technology: A systematic review". In: *Sensors* 22.1 (2021).

[3] Stavros Eleftherakis et al. "Demystifying Privacy in 5G Stand Alone Networks". In: *arXiv preprint arXiv:2409.17700* (2024).

[4] Iqra Javid and Sibaram Khara. "5G Network: Architecture, Protocols, Challenges and Opportunities". In: *2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. IEEE. 2022, pp. 1–5.

[5] Xinsheng Ji et al. "Overview of 5G security technology". In: *Science China Information Sciences* 61 (2018). DOI: 10.1007/s11432-017-9426-4.

[6] Roger Piqueras Jover and V. Marojevic. "Security and Protocol Exploit Analysis of the 5G Specifications". In: *IEEE Access* 7 (2018), pp. 24956–24963. DOI: 10.1109/ACCESS.2019.2899254.

[7] Akash R. Kathavate et al. "Critical Aspects of 5G Technology- A Study on the Drivers, Technology Enhancement, Performance, and Spectrum Usage". In: *Asian Journal of Advanced Research and Reports* (2021). DOI: 10.9734/ajarr/2021/v15i530396.

[8] Jaya Preethi Mohan, Niroop Sugunaraj, and Prakash Ranganathan. "Cyber security threats for 5G networks". In: *2022 IEEE international conference on electro information technology (eIT)*. IEEE. 2022, pp. 446–454.