UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA TRIENNALE IN INGEGNERIA INFORMATICA

"TECNOLOGIA 5G: STUDIO E ANALISI DELLE VULNERABILITÀ"

Laureanda: Segalin Elena, 1225243

Relatore: Prof. Mauro Migliardi

ANNO ACCADEMICO 2021 – 2022

Data di laurea: 21 Settembre 2022

Indice

Sommario

Questo elaborato ha lo scopo di analizzare e confrontare le varie tecnologie di reti mobili, con una particolare attenzione all'ultima: il 5G.
Si fornisce una descrizione delle principali caratteristiche delle diverse tecnologie e delle architetture che le costituiscono. Si passa poi ad analizzare la nuova rete mobile 5G, molto più veloce del 4G, con una più bassa latenza, con un supporto di molti più dispositivi rispetto a quelle precedenti.
Questa nuova tecnologia porta con sé anche una serie di vulnerabilità e problematiche legate alla sicurezza della rete, ereditate dalla tecnologia precedente. Vengono infine illustrati alcuni dei più comuni attacchi informatici della suddetta rete e proposte alcune possibili mitigazione al problema.

Introduzione

La tecnologia svolge un ruolo fondamentale nelle nostre vite e nella nostra società. In particolare le comunicazioni mobili hanno sconvolto il modo di interagire con le altre persone. Pochi decenni fa non esistevano i telefoni cellulari, mentre oggi ogni persona può comunicare con il mondo da qualsiasi posto e in qualsiasi momento, tramite chiamate, videochiamate, messaggi, social network.
I cellulari, che inizialmente servivano solo per telefonare, si sono gradualmente evoluti, diventando sempre più dei veri e propri dispositivi complessi, essenziali per moltissimi aspetti quotidiani.
Oggi tramite un cellulare è possibile scattare fotografie e girare video ad alta risoluzione, navigare su internet, usufruire di una moltitudine di servizi grazie ad applicazioni e siti web, effettuare pagamenti e transizioni bancarie tramite un click.
Questa evoluzione ha avuto inizio con la prima generazione della tecnologia cellulare wireless, la cosidetta tecnologia 1G, fino ad arrivare all'attuale 5G.
Nel *Capitolo 1* di questo elaborato vengono presentate le tecnologie pregresse al 5G. Viene fornita una panoramica delle principali caratteristiche e un'analisi dell'architettura che le costituisce.
All'interno del *Capitolo 2* vengono esposti nel dettaglio le motivazioni che stanno alla base della nascita della nuova tecnologia 5G e gli obiettivi che questa si pone.
Viene poi svolta una descrizione della nuova architettura, evidenziandone gli aspetti innovativi, e vengono illustrate e confrontate le sue modalità d'installazione.
Nel *Capitolo 3* vengono analizzati gli aspetti di sicurezza delle varie tecnologie di rete mobile precedenti al 5G. Di seguito viene fatta un'analisi più specifica delle problematiche che la tecnologia 5G eredita dal 4G e che la rendono vulnerabile. In alcuni casi viene fornita anche qualche soluzione o mitigazione al problema in questione.

Capitolo 1

Storia delle tecnologie precedenti

1.1 1G

Negli anni '80, periodo in cui nasce la tecnologia 1G, tutte le comunicazioni wireless sono voice-centric, ovvero incentrate sulla conversazione vocale e sono basate su sistemi analogici. Si fa questa scelta a causa degli eccessivi costi di produzione di quelli digitali.
Lo standard inerente a questa tecnologia viene chiamato AMPS (Advanced Mobile Phone Service), in seguito identificato come 1G. Questo prevede l'utilizzo di frequenze separate per ogni conversazione. È molto dispendioso in termini di potenza computazionale selezionare le frequenze e serve una quantità di banda considerevole per far conversare molti utenti. Da questo momento in poi vengono lanciate nuove generazioni di reti mobili all'incirca ogni dieci anni.

1.2 2G/2.5G

All'inizio degli anni '90 si sviluppa lo standard di telefonia mobile di seconda generazione, il 2G. La novità principale sta nello spostamento a un sistema di comunicazione digitale, che permette la trasmissione di voce e dati.
Lo standard GSM (Global System for Mobile Communications) è un sistema digitale che usa come interfaccia aerea il sistema TDMA (Time Division Multiple Access) multiplexing.
L'interfaccia aerea è la più importante per tutti i sistemi mobile, perchè è l'unica a cui l'utente iscritto è esposto.
La TDMA permette agli utenti la trasmissione sulla stessa frequenza, applicando una suddivisione del tempo in intervalli. Ad ogni utente viene assegnata una rapida successione di time-slot, durante i quali può avvenire la

trasmissione. Una volta finito il singolo intervallo, deve aspettare il proprio turno per poter trasmettere nuovamente. La successione di slot è talmente rapida da far sembrare le diverse trasmissioni simultanee. Allocando per ogni utente una discreta quantità di banda, si permette una conversazione simultanea. [17]
È possibile anche, oltre al servizio telefonico, effettuare l'invio di dati. Il servizio SMS (Short Message Service) permette di inviare e ricevere messaggi alfanumerici di massimo 160 caratteri.
Si sviluppano poi i protocolli GPRS (General Packet Radio Service) e in seguito EDGE (Enhanced data rates for GSM evolution) che migliorano quello precedente. Entrambi sono compresi nella tecnologia 2.5G, in quanto appunto migliorativi del 2G e più distanti dalla tecnologia successiva.
Questi permettono ai dispositivi mobili la navigazione in internet e l'accesso a servizi multimediali [8], grazie all'invio e alla ricezione di pacchetti attraverso le onde radio della rete cellulare.
Viene utilizzato il sistema CDMA (Code Division Multiple Access), il quale permette la trasmissione simultanea di dati, senza la necessità di multiplexing basato sul tempo o sulla frequenza. In un sistema CDMA, molti utenti utilizzano sempre la stessa banda di frequenza e si distinguono al ricevitore attraverso un codice di diffusione univoco.[3]
I vantaggi rispetto al TDMA sono un alto valore di data rate e un'alta flessibilità e in più non c'è bisogno di sincronizzazione. [17]

1.2.1 Architettura 2G

L'architettura GSM è divisa in tre parti principali: BSS (Base Station Subsystem), NSS (Network Subsystem) e NMS (Network Management System).

- Base Station Subsystem
  La BTS (Base Transceiver Station) ha la funzione di essere uno snodo per tutta l'infrastruttura di rete. Trasmette il segnale nel formato desiderato, codifica e decodifica i segnali ed encripta i flussi di dati. È collegata ai dispositivi mobili tramite interfaccia aerea. La trasmissione e ricezione del segnale dalla stazione base avviene tramite antenne direzionali e omnidirezionali.
  Il BSC (Base Station Controller) è un controllore dell'infrastruttura, specialmente delle stazione base.

- Network Subsystem
  È costituita da uno Switch o MSC (Mobile Switching Center) che si occupa della commutazione, necessaria per le interconnessioni di utenze

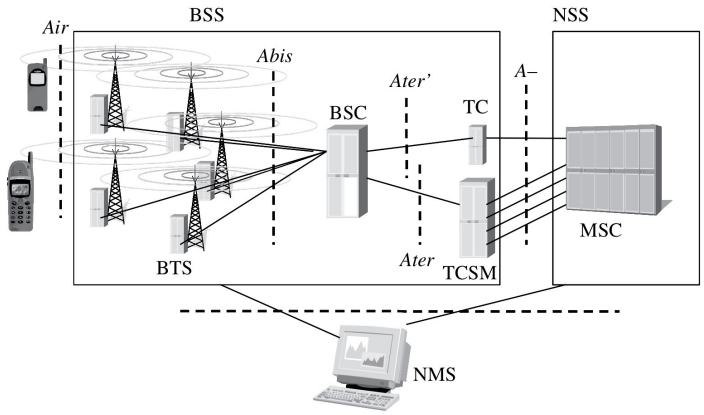

Figura 1.1: Architettura di seconda generazione [12]

mobili e fisse. Fa uso del HLR (Home Location Register), un database che contiene delle informazioni relative all'utente mobile, che rimangono invariate durante tutto il tempo in cui è registrato.
Poi il VLR (Visitor Location Register) è un database di natura dinamica. È associato a una regione e i suoi dati passano da un registro all'altro, in base alla regione in cui si trova l'utente.
L'AUC (Authentication Center) ha il compito di protezione della rete da utenti falsi e utilizza due principali modalità di protezione: l'incriptazione degli utenti e la loro autenticazione.

- Network Management System
  Assicura un buon funzionamento della rete, monitorandola, raccoglie dati e analisi sulla performance, avvisa, generando segnali di allarme, se ci sono degli errori o malfunzionamenti e, in alcune situazioni, è anche in grado di correggerli.

1.3 3G

L'avvento dello standard 3G all'inizio del nuovo millennio porta uno spostamento dell'attenzione dai sistemi voice-centric a quelli data-centric, cioè basati sulla trasmissione di dati multimediali. Viene introdotta così la possibilità di trasmettere video, di effettuare videochiamate e di utilizzare la connessione internet ad alta capacità di banda.
L'IMT-2000 è il primo standard internazionale, in contrasto con i precedenti, i quali variano da un continente all'altro.

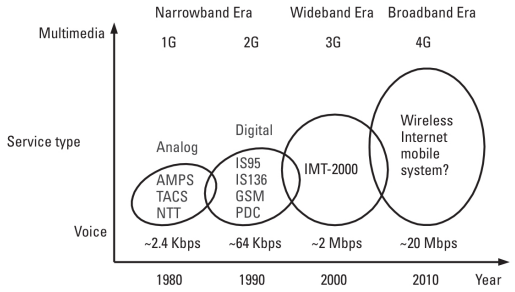

Figura 1.2: Evoluzione dei servizi [3]

Nel grafico della figura 1.2 sono evidenziati i nomi dei diversi standard precedenti e come cambia nel corso degli anni la tipologia di servizio richiesto.
Il sistema 3G è basato sulla tecnologia W-CDMA (Wideband Code Division Multiple Access), una versione su larga banda della CDMA. È in grado di operare in trasmissione duplex, cioè consentendo la propagazione di due segnali in contemporanea in senso opposto su una stessa via di trasmissione, in due modalità: TDD (Time Division Duplex) e FDD (Frequency Division Duplex). La modalità TDD è caratterizzata dalla trasmissione su time-slot alternati su uno stesso canale di frequenza; la modalità FDD utilizza, invece, due canali di frequenza separati.[3]
La W-CDMA permette di incrementare il throughput e la capacità, migliorare la copertura e ridurre il ritardo grazie all'accesso ai pacchetti ad alta velocità, HSPA (High Speed Packet Access), e all'accesso ai pacchetti in uplink e downlink ad alta velocità, rispettivamente HSUPA e HSDPA.
Questa accelerazione di trasmissione porta gli smartphone a supportare molti servizi e applicazioni, come ad esempio i VOD (Video On Demand), i LBS (Location-Based Services), la MTV (Mobile TV) e la VC (Video Conference).
Tutta questa disponibilità e miglioramento di servizi causa un ingente aumento di consumo di internet mondiale. [4]

1.3.1 Architettura 3G

L'architettura 3G consiste in due parti principali: la RAN (Radio Access Network), che si compone di elementi radio ed elementi di trasmissione, e la CN (Core Network).

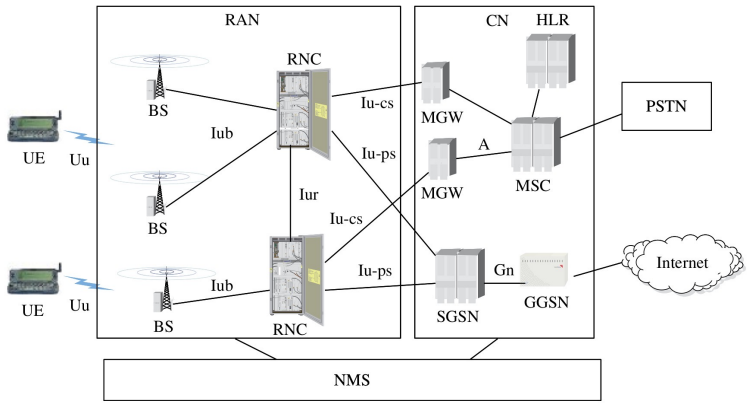

Figura 1.3: Architettura di terza generazione [12]

- Radio Access Network
  Ha il compito di gestione delle risorse radio e delle telecomunicazioni e i suoi elementi principali sono le BS (base stations), anche dette NodeB, e il RNC (Radio Network Controller).
  Le BS fungono da interfaccia tra la rete e l'interfaccia aerea. Sono simili alle stazioni base dell'architettura 2G. Alcuni compiti di cui si occupano riguardano la trasmissione e la ricezione del segnale, la codifica di canale e la propagazione del segnale.
  Il RNC invece fa da tramite tra la BS e la CN(Core Network) e si occupa del controllo delle risorse radio, senza l'aiuto della CN, cosa che succedeva invece nell'architettura precedente.

- Core Network
  È la corrispondete della NSS nella tecnologia 2G, con il 3G viene integrata e modificata. Si costituisce di due parti fondamentali: il dominio di commutazione di circuito, CS, e il dominio di commutazione di pacchetto, PS.
  La parte CS è quello "ereditato" dall'architettura 2G del controllo e della gestione delle chiamate. Alcuni elementi compresi in questa parte sono il HLR, il VLR, di cui abbiamo spiegato la funzione nella sezione dedicata all'architettura 2G, e il GMSC (Gateway Mobile Switching

Center), il quale agisce da interfaccia tra la rete mobile e le reti CS esterne, gestendo le connessioni per le chiamate entranti e uscenti.
La sezione PS è dedicata invece alla comunicazione dei dati. Gli elementi costitutivi di questa parte sono il SGSN (Serving GPRS Support Node), che agisce da interfaccia tra la RAN e il dominio di commutazione di pacchetto, e il GGSN (Gateway GPRS Support Node), il quale fa da collegamento tra la rete 3G e le reti PS esterne.

- Network Management System
  Il NMS ha la stessa funzione di controllo del buon funzionamento che aveva nella precedente architettura 2G, con l'aggiunta di gestione dei dati a commutazione di pacchetto. Nell'architettura 3G questo sistema diventa più efficiente e incrementa la sua funzione di risoluzione autonoma di alcuni problemi rispetto al precedente.

1.4 4G

La tecnologia 4G viene sviluppata nell'ultimo decennio ed è quella maggiormente usata ancora oggi, in quanto è il sistema più avanzato e aggiornato disponibile. Si è passati da una connessione internet a bassa velocità di dati a un alto valore di data rate.[13]
Le maggiori differenze tra le due tecnologie riguardano la metodologia di accesso ai dati, il data transfer rate (tasso di trasferimento dati), la terminologia di trasmissione e la sicurezza.[4] Esistono due sistemi per il 4G: il WiMAX (Worldwide Interoperability for Microwave Access) e il sistema LTE (Long Term Evolution), che viene sviluppato in seguito. In realtà i due sistemi sono similari e quello maggiormente utilizzato è il LTE. È un sistema interamente a commutazione di pacchetto che ha una bassa complessità (anche nell'architettura) e che fornisce un'alta qualità del servizio (QoS) e degli alti data rate.[12]
Si tratta di una tecnologia completamente IP-based per la quale tutti gli utenti possono comunicare, trasferire dati dovunque sono e in qualunque momento ed è quindi in grado di offrire servizi e trasportare dati in tempo reale.
Nella figura 1.4 è possibile notare come si è gradualmente passati dall'esclusiva commutazione di circuito a una commutazione di pacchetto.

1.4.1 Architettura 4G

L'architettura 4G risulta composta da una rete di accesso, chiamata E-UTRAN (Evolved UMTS Terrestrial Radio Access Network) e da una rete

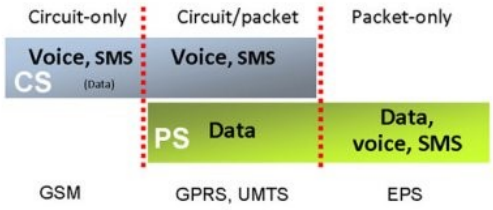

Figura 1.4: Cambiamento dei circuiti[9]

principale, EPC (Evolved Packet Core).

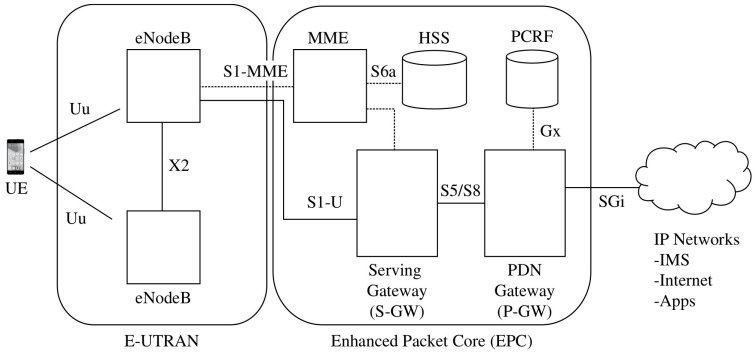

Figura 1.5: Architettura di quarta generazione [12]

- Evolved UMTS (Universal Mobile Telecommunication System) Terrestrial Radio Access Network
  Ha funzioni di controllo delle risorse radio e di gestione delle risorse dinamiche.
  Al suo interno sono comprese le eNodeB, delle stazioni base migliorate rispetto a quelle del 3G, che si occupano di eseguire operazioni di basso livello per i dispositivi connessi e mandar loro trasmissioni radio.

- Evolved Packet Core Network
  È suddivisa in varie parti con funzioni differenti. La MME (Mobility Management Entity) si interfaccia con la rete di accesso e connette i device dell'utente al gateway di servizio, si occupa sia di segnalamento che di funzioni di control plane.[12] Inoltre è responsabile anche dell'interazione tra LTE e le reti delle tecnologie precedenti.
  Il S-GW(Serving Gateway) crea una connessione per i dati tra le stazioni base e il P-GW (Packet Data Network Gateway), che invece congiunge lo User Equipment alle reti IP esterne: ha una funzione simile

ai GGSN (Gateway GPRS Support Node) dell'architettura precedente. Infine il HSS (Home Subscriber Server) è il database centrale, che contiene tutte le informazioni relative all'utente e all'abbonamento associato ad esso.

Capitolo 2

La tecnologia 5G

2.1 Perchè necessitiamo del 5G

Negli ultimi anni abbiamo assistito e assisteremo a una crescita esponenziale del traffico mobile.
È cresciuto il numero di dispositivi mobili e anche la scelta di utilizzare apparecchi sempre più "affamati di dati", cioè che richiedono un consumo sempre maggiore di dati.

Device	Relative data usage
Feature phone	1x
Smart phone	24x
Handheld gaming console	60x
Tablet	122x
Laptop	515x

Figura 2.1: Consumi di diverse tipologie di dispositivo [13]

È esploso il mondo dell'IoT (Internet of Things), cioè una rete di oggetti tecnologici connessi a internet e in grado di comunicare tra loro, creando un sistema in cui ogni dispositivo è rintracciabile attraverso il nome e la posizione associata. Questo ha molte applicazioni in vari ambiti, dalla creazione di case intelligenti, alle automobili moderne, alla smart agricolture. Si arriverà all'IoE (Internet of Everything), mondo in cui ogni persona sarà servita da decine a centinaia di dispositivi. Un altro fattore che sta provocando un così ingente aumento del traffico dati è l'espansione di applicazioni multimediali come l'UHD (Ultra - High Definition), i video 3D, come pure la realtà aumentata, in cui si aggiungono elementi multimediali allo spazio fisico esistente, incrementando l'esperienza umana, e quella virtuale, in cui si crea una realtà

tridimensionale che l'utente può vivere in modo immersivo.
Il report annuale dell'azienda Cisco sull'Internet prevede che entro il 2023 ci saranno 5.3 miliardi di utenti internet globali, 3.6 dispositivi e connessioni pro capite e la velocità media globale della banda larga fissa sarà di 110 Mbps.[2]

2.2 Obiettivi del 5G

Il 5G non si propone solamente di essere un'evoluzione della tecnologia precedente, con maggiori prestazioni e minori costi, ma sarà una vera e propria piattaforma di rete innovativa, che offrirà nuovi servizi e amplierà le vedute a un vero ecosistema digitale.
Il principale lavoro di standardizzazione e di esposizione dei requisiti fondamentali a livello internazionale è svolto da 3GPP (Third Generation Partnership Project) che, sin dalla tecnologia GSM, definisce le generazioni radiomobili. Inoltre il lavoro è completato da ITU-R, il quale ha formalizzato i requisiti per quanto riguarda le prestazioni della nuova tecnologia radio 5G con l'IMT-2020.
La figura 2.2 mostra un triangolo, all'interno del quale sono rappresentate le maggiori applicazioni che usufriuranno del 5G, mentre ai vertici sono presenti i tre macro requisiti principali.

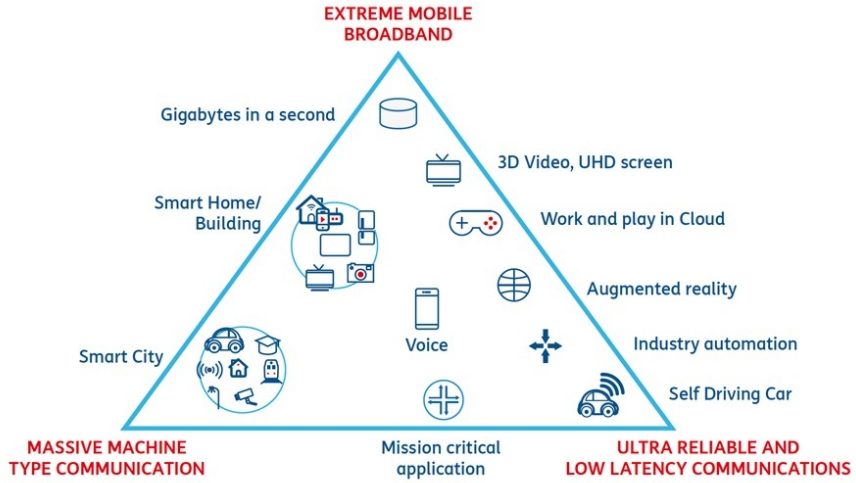

Figura 2.2: Requisiti e applicazioni del 5G [16]

Il primo requisito riguarda l'estensione della banda, eMBB(enhanced Mobile BroadBand), con prestazioni che arriveranno fino a 20Gbps in downlink[14].

Inoltre è richiesta una mMTC (massive Machine Type Communication), cioè una connettività rivolta ad applicazioni per dispositivi a basso costo e a limitato consumo energetico. Le app scambiano piccole quantità di dati da milioni di oggetti e li dirigono verso piattaforme Cloud.
L'ultimo vertice del triangolo si riferisce invece alla URLLC (Ultra Reliable and Low-Latency Communication), cioè alla latenza molto bassa, utile in tutti quegli ambiti in cui è richiesto uno scambio di dati affidabile, ininterrotto e con bassissimi ritardi.
Infine questa nuova tecnologia porta con sè un cambio di paradigma nel mondo dei servizi. Le precedenti generazioni prevedono un *design orizzontale*, secondo il quale uno stesso sistema di servizi viene proposto a differenti clienti.
Col 5G, invece, ci sarà un *design verticale*, in cui si prevede una suddivisione dei servizi e il loro sviluppo in base alle esigenze delle differenti classi d'utenza, chiamate verticals. [1]

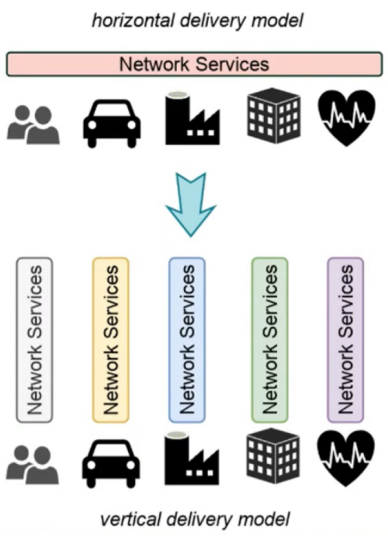

Figura 2.3: Cambio di modello di erogazione dei servizi [1]

Le novità presentate, che saranno tangibili da tutta la popolazione, si possono riassumere in tre categorie [4].

- Una categoria incentrata sugli utenti finali, ai quali sarà assicurata una connettività continua, 24 ore su 24 tutti i giorni, un incremento delle performance, che saranno sempre migliori e veloci.
  Inoltre le connessioni saranno più affidabili e sicure su tutti i device e gli oggetti connessi in rete.

- Un'altra categoria, a cui sono indirizzate le novità della nuova tecnologia, sono i content provider, ovvero i fornitori di servizi. Sarà disponibile un servizio di trasporto intelligente, un'ottimizzazione logistica e dei processi, dei servizi di monitoraggio. In aggiunta ci saranno sensori più moderni e avanzati, insieme a una moltitudine di servizi, ad esempio quelli veicolari.

- Infine per gli operatori di rete sarà garantita una maggiore scalabilità, cioè si potrà apportare minime modifiche al sistema hardware o software nel caso in cui vari in modo ingente la mole o la tipologia di dati che si sta trattando, garantendo una buona funzionalità del sistema. Sarà incrementata anche l'efficienza energetica e la sicurezza in ambito di comunicazioni infrastrutturali.

2.3 Architettura 5G e innovazioni

Con l'architettura della nuova tecnologia si passa da sistemi chiusi, con software proprietario e hardware specializzato, a un modello che prevede il disaccoppiamento tra il livello software e quello hardware. Il primo diventa per la maggior parte open source, mentre il secondo si fa sempre più di tipo standard, cosa che permetterà una riduzione dei costi.
L'obiettivo è quello di gestire sempre più processi e funzionalità software, allocandoli dinamicamente su hardware distribuito.
Questo cambio di paradigma ha portato all'introduzione di tecnologie come SDN (Software Defined Network) e NFV (Network Function Virtualization), di cui verrà spiegato il significato in seguito.

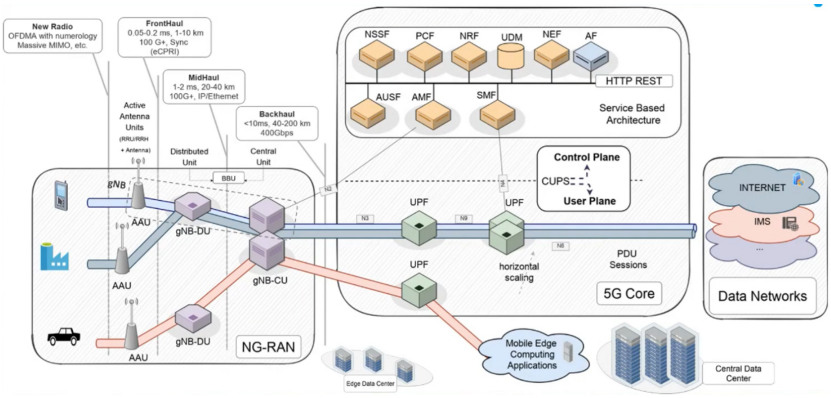

Figura 2.4: Architettura 5G [1]

L'utente, come nelle reti precedenti, deve essere in grado di comunicare con gli altri utenti e reti attraverso una connessione, chiamata PDU (Protocol Data Unit) Session. La rete ha il compito di mantenere attiva questa connessione, tramite opportune configurazioni, al fine di supportare l'attività dell'utente.
Come nelle precedenti tecnologie, l'architettura è suddivisa in due parti: la Radio Access Network, qui chiamata NG-RAN, e la Core Network, nominata 5G Core.

- **Next Generation-RAN**
  È la sezione dell'architettura più vicina all'utente ed è formata da stazioni radio base, chiamate gNodeB. Ognuna di esse serve una cella di territorio ed è disgregata funzionalmente in tre parti, secondo quanto dice lo standard.
  La prima parte consiste nell'AAU (Active Antenna Unit), la quale genera e riceve segnali sull'interfaccia radio dedicata. Questa si chiama NR (New Radio) e offre larga banda e bassissima latenza, grazie a una modulazione OFDMA (Orthogonal Frequency-Division Multiplexing), migliorata rispetto a quella del 4G, e all'utilizzo ingente di antenne multiple, massive MIMO (Multiple-Input and Multiple-Output), già utilizzate nel 4G in modo più contenuto. La tecnologia MIMO permette di incrementare la velocità di trasmissione e aumentare il flusso di dati senza modificare la larghezza di banda. Sfrutta il multipath, fenomeno naturale di propagazione delle onde radio, grazie al quale i segnali raggiungono l'antenna ricevente facendo due o più percorsi.[6]
  Nel mezzo c'è la gNB-DU (gNodeB Distributed Unit), la quale trasmette i segnali all'AAU tramite l'interfaccia FrontHaul. La gNB-DU si occupa della parte più bassa della pila protocollare della NG-RAN. Necessita di sincronizzazione con la AAU e di larga banda sulla FrontHaul. Perciò la gNB-DU e la AAU devono essere poste vicine nello stesso sito cellulare.
  L'ultimo elemento della NG-RAN è la gNB-CU (gNodeB Central Unit), che si occupa della parte protocollare alta dell'interfaccia radio, trasmettendo pacchetti sulla gNB-DU. Quest'ultime non necessitano di sincronizzazione e comunicano tramite interfaccia MidHaul, che ha requisiti di banda più laschi rispetto al FrontHaul. Perciò la gNB-CU non necessita di essere posizionata sotto al sito, ma può stare in datacenter più centrali della rete.
  Nelle tecnologie precedenti la DU e la CU erano unificate in un unico elemento, la BBU (Base Band Unit). Il nuovo standard prevede invece la loro disgregazione.

- **5G Core**
  La Core Network non è più definita in termini di nodi, bensì di funzioni. Questo favorisce un'implementazione innovativa rispetto alle generazioni precedenti, grazie all'utilizzo della tecnologia SDN (Software Defined Network), secondo la quale il traffico sulla rete e la comunicazione con l'infrastruttura hardware sottostante sono gestiti da programmi software.
  Le UPF(User Plane Function) rappresentano l'evoluzione della strategia di separazione tra Control e User Plane (CUPS, Control and Data Plane Separation). Sono in sostanza nodi di commutazione implementati via software. Costituiscono la PDU Session in questa parte di struttura.
  Sul piano di controllo, invece, sono presenti funzioni che hanno il compito di supervisionare i servizi offerti all'utenza. Alcune CPF(Control Plane Function) sono la AMF (Access ad Mobility Management Function) e la SMF (Session Management Function). Si ha quindi un disaccoppiamento funzionale della 5G Core, in cui tante singole funzioni si occpuano di un singolo compito.
  Un'altra innovazione è la modalità di comunicazione tra funzioni di controllo, le quali non parlano più attraverso difficili protocolli, bensì attraverso interfacce web di tipo HTTP REST. L'architettura diventa quindi Service Based, ovvero basata sui servizi e non più su interfacce protocollari. In aggiunta è possibile decidere dove installare le funzioni softwarizzate, se nell'Edge Data Center o nella parte centrale della rete, il Central Data Center.
  Infine si ha anche la scelta sulla quantità di repliche di funzioni da installare, per adattare al meglio il sistema al carico richiesto dall'utenza. Questa è l'implementazione del nuovo paradigma di scalabilità orizzontale (Horizontal Scalability).

2.3.1 Modalità di installazione del 5G

Esistono due modalità di installazione della rete 5G: NSA (Non-Stand Alone) e SA (Stand Alone).
La prima modalità d'installazione è quella maggiormente utilizzata nella fase iniziale dello sviluppo delle architetture, in quanto si integra con struttura del 4G e prevede l'utilizzo di una connettività duale. Vi sono delle celle 4G, che lavorano tramite interfaccia LTE, e delle celle 5G, gestite tramite interfaccia NR, ed entrambe utilizzano una Core Network 4G e l'interfaccia LTE. La

nuova tecnologia funge quindi da *extra data pipe*, nel caso ci sia l'esigenza di una rete più performante e ci sia copertura 5G disponibile.
Il cellulare, che deve essere compatibile con il 5G e operare in modalità NSA, si connette contemporaneamente a due stazioni radio base, una 4G e l'altra 5G. L'obiettivo principale di questa soluzione è la soddisfazione del requisito sulla banda, eMBB (enhanced Mobile BroadBand).
In futuro, invece, si passerà alla modalità SA, che prevede l'utilizzo della 5G Core, Core Network di quinta generazione, completamente softwarizzabile, e dell'interfaccia 5G NR.
Questo permetterà a tutti di usufruire a pieno di tutti i servizi offerti dalla nuova tecnologia, incluso il network slicing.
Quando un dispositivo 5G è sotto una zona coperta da 5G, questo è ancorato alla 5G Core, che diventa responsabile di tutta la gestione della sua mobilità. Nel momento in cui non è più presente una copertura 5G, il device si attacca a una rete LTE/EPC di quarta generazione. In altre parole la modalità SA lavora alternativamente in *5G mode* o *4G mode*.[10]

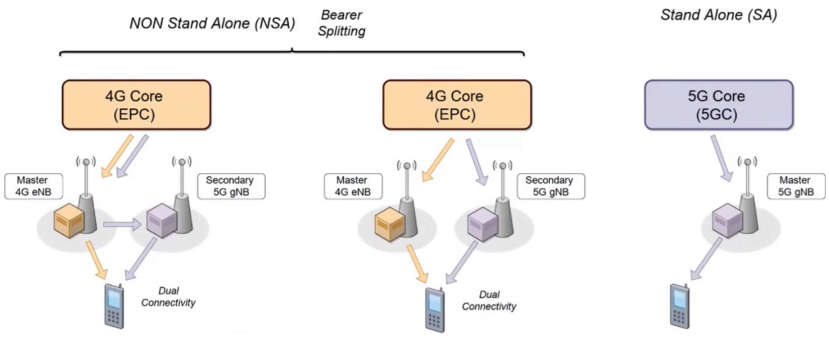

Figura 2.5: Modalità di installazione dell'architettura 5G [1]

Confronto tra le due modalità

Per quanto riguarda la durata della batteria del dispositivo in modalità NSA bisogna evidenziare il fatto che è necessario mantenere simultaneamente i collegamenti di trasmissione radio di entrambe le tecnologie. Questo richiede una condivisione della potenza di trasmissione totale del dispositivo e ciò porta a una durata della batteria più breve. Il device in modalità SA, invece, avrà un'autonomia di batteria maggiore, in quanto connesso a una sola tecnologia.
Esaminando i tre tipici stati di funzionamento di un dispositivo, *idle mode*, *connected mode* e *data transmission mode*, come dimostra la fonte [10], si

nota maggiormente la differenza di consumo di potenza nel momento di trasmissione di dati.
Considerando le prestazioni, poi, quelle di un dispositivo connesso in modalità NSA sono peggiori rispetto all'altra modalità, perchè il device può essere soggetto a mutue interferenze, dovute al simultaneo mantenimento di due collegamenti radio.
Inoltre è importante porre attenzione sull'interoperabilità della rete 4G e 5G, per garantire una continuità nell'offerta del servizio all'utente. Per la modalità NSA non c'è interscambio tra le due reti, in quanto il dispositivo è ancorato nella rete LTE e il servizio vocale è fornito da essa.
Un device SA, invece, cambia l'ancoraggio alla rete più performante disponibile e usufruibile in quel momento. Il servizio vocale è gestito in due modi. Quando la copertura lo permette, è garantito dalla 5G Core, assicurando il simultaneo utilizzo di servizio vocale e altri tipi di servizi 5G. Nel momento in cui non è disponibile la rete 5G, avviene la cosiddetta *EPS fallback*, il device ritorna ad attaccarsi alla rete LTE, interrompendo così i servizi usufriubili attraverso la rete 5G. La EPS fallback non supporta simultaneamente voce e servizi dati 5G. [10] Per quanto riguarda questo ultimo aspetto, la modalità NSA è migliore, in quanto compie un "passaggio di consegne" all'interno del sistema.
Segue una tabella riassuntiva per evidenziare in modo chiaro le caratteristiche di entrambe le modalità di installazione e utilizzo della nuova tecnologia.

	NSA	SA
Durata batteria	La connettività duale consuma più velocemente batteria	La batteria dura più tempo
Performance dispositivo	Peggiori, c'è il rischio di mutue interferenze	Migliori, non c'è rischio di interferenza tra i segnali delle due reti
Interoperabilità 4G/5G	Non c'è interoperabilità, il device è ancorato sempre alla rete LTE	Switch tra le reti 4G e 5G in caso di copertura 5G non disponibile

Capitolo 3

Sicurezza e vulnerabilità delle tecnologie di reti mobili

Per un'adeguata gestione della sicurezza biogna tenere conto dei tre aspetti principali che la costituiscono: riservatezza, disponibilità dei dati e integrità di essi. Garantire la riservatezza vuol dire impedire l'accesso e la fruizione di dati a un utente non autorizzato. Inoltre le informazioni devono essere sempre disponibili e fruibili all'utenza che ha diritto ad averne accesso. Infine mantenere l'integrità dei dati significa assicurare che questi non subiscano gravi modifiche o cancellazioni a causa di danni al sistema, errori, malfunzionamenti o di azioni volontarie.
Di seguito vengono presentate le modalità che sono utlizzate dalle varie generazioni di reti mobili per garantire la sicurezza e anche le vulnerabilità che le tecnologie portano stesse con sè.

3.1 Sicurezza delle tecnologie precedenti

3.1.1 1G

La prima generazione di telefonia mobile mostra un gran numero di carenze: dalla capacità di trasmissione, a un utilizzo non adeguato dello spettro, a una bassa qualità delle chiamate vocali.
Inoltre non è previsto alcun livello di sicurezza per quanto riguarda ad esempio le intercettazioni di chiamate. A causa della natura analogica della tecnologia, non è permessa la cifratura delle informazioni e questo rende l'utente molto vulnerabile, in quanto un attaccante è in grado di intercettare una telefonata, di reperire informazioni come il numero di identificazione mobile o il numero elettronico seriale. Con questi valori poi, è possibile

clonare un dispositivo e, fingendosi l'utente, mette in atto un attacco di impersonificazione.[15]

3.1.2 2G

Con l'avvento del 2G e con il cambio dal mondo analogico a quello digitale, viene introdotta la crittografia, che permette, attraverso delle chiavi segrete, di crittare il traffico e di proteggere le informazioni.
Nasce poi il concetto di autenticazione: l'identità dell'utente viene verificata tramite SIM (Subscriber Identity Module), un scheda inserita nel dispositivo, dotata di IMSI, un codice identificativo univoco, che permette all'operatore di identificare il cliente e il numero a esso associato.[8]
Nonostante ciò, c'è comunque il rischio di multipli attacchi, come ad esempio lo spamming, cioè l'invio agli utenti di materiale non voluto. Il sistema di criptaggio è limitato solo all'interfaccia radio e si considerano come sicuri i canali di comunicazione, i quali non vengono quindi protetti da eventuali intercettazioni.

3.1.3 3G

La rete 3G vanta di un'architettura di sicurezza composta da 5 parti, che si occupano della sicurezza sicurezza di diverse sezioni: accesso alla rete, dominio della rete, dominio dell'utente, applicazioni, visibilità e configurabilità. È previsto così un sistema ad alta flessibilità, per concedere delle estensioni atte a mitigare eventuali nuove problematiche.
Malgrado ciò, la superficie di attacco si amplia sensibilmente, a causa del forte aumento di dispositivi in rete. Si manifestano infatti molti attacchi legati all'accesso di informazioni riguardanti gli utenti, all'intercettazione e all'impersonificazione, sia dell'utenza che della rete. Si aggiungono inoltre attacchi di tipo DoS(Denial of Service), man-in-the-middle, spoofing sull'aggiornamento della posizione e falsificazione della stazione base a cui ancorarsi. [15]

3.1.4 4G

Il 4G porta con sè dalla generazione precendente il paradigma del cosiddetto *Security by Design*, in cui le funzioni di sicurezza sono definite in appositi domini di sicurezza, cioè le 5 parti che abbiamo precedentemente esposto (accesso alla rete, dominio della rete, dominio dell'utente, applicazioni, visibilità e configurabilità).
Vengono introdotti nuovi algoritmi crittografici con chiavi maggiormente

strutturate, per far fronte agli attacchi legati alle generazioni di tecnologia precedente. I due maggiori algoritmi sono EEA (EPS Encryption Algorithms) e EIA (EPS Integrity Algorithms) e lavorano su chiavi lunghe il doppio rispetto a quelle usate nel 3G.[15]
Rispetto al 3G è presente poi una gestione separata della sicurezza del piano di controllo e quello di inoltro, rispettivamente *control plane e data plane*.
La rete 4G, tuttavia, è soggetta a molti attacchi derivanti dalla rete internet e dalla sua natura IP-based. Attraverso questi attacchi è assolutamente possibile colpire la rete cellulare, causando gravi danni agli utenti e al sistema. Oltre a questo, la sempre maggiore potenza computazionale dei dispositivi mobili permette ad essi di essere utilizzati per attaccare la rete cellulare.

3.2 Problematiche attuali

3.2.1 Uno sguardo alla realtà

La diffusione dell'IoT e il sempre più crescente numero di device influenzano tutti gli ambiti della nostra vita, dalla sfera privata, all'ambiente lavorativo e sociale. Di conseguenza sta aumentando la superficie a rischio di attacchi legati al mondo dell'informatica.
Secondo l'ultimo rapporto nell'edizione di Ottobre 2021 di Clusit, associazione italiana per la sicurezza informatica, negli ultimi anni si è assistito a un incredibile incremento degli attacchi nel mondo dell'informatica. Questo aumento è notevole sia dal punto di vista qualitativo che quantitativo: si regitrano perciò sempre più attacchi di una gravità molto maggiore.
Nel 2021 in Europa le vittime sono aumentate, dal 15 al 25%, mentre in America e in Asia rimangono quasi invariate, ripettivamente sono il 46% e il 29%.[5]
Il rapporto ha classificato e analizzato gli attacchi avvenuti a livello globale negli ultimi 10 anni, per un totale di oltre 13 mila attacchi, di cui 6148 si sono verificati nell'ultimo triennio.
Di seguito la figura 3.1 mostra i maggiori attacchi, suddivisi per tipologia. Si nota immediatamente come il *Cybercrime* ha dei numeri esorbitanti rispetto a tutti gli altri e il trend ne evidenzia un aumento.
Si aggiunge inoltre una tabella, la figura 3.2, che evidenzia le vittime di attacchi, suddivise per 20 macro categorie. Si nota che gli attacchi non sono mirati a uno specifico ambito, bensì comprendono molti aspetti della vita e della società.

ATTACCANTI PER TIPOLOGIA	2018	2019	2020	2H 2020	1H 2021	1H 2021 su 2H 2020	Trend 2021
Cybercrime	1.229	1.381	1.518	764	925	21.1%	↑
Espionage-Sabotage	203	203	264	150	95	-36.7%	↗
Hacktivism	64	48	48	21	7	-66.7%	↓
Information Warfare	58	35	44	22	26	18.2%	↑
Espionage-Sabotage + Inf. Warfare	261	238	308	172	121	-29.65%	↗

Figura 3.1: Tipologie di attaccanti [5]

VITTIME PER CATEGORIA	2018	2019	2020	2H 2020	1H 2021	1H 21 su 2H 20	TREND
Government, Military, Law Enforcement	220	233	224	120	167	39.2%	↑
Healthcare	161	186	210	117	139	18.8%	↑
Multiple Targets	326	406	401	158	121	-23.4%	↓
Information Communication Technology	191	233	269	149	113	-24.2%	↓
Education	106	140	174	103	100	-2.9%	↗
Financial, Insurance	162	107	122	66	60	-9.1%	↗
Professional, Scientific, Technical	18	19	59	27	50	85.2%	↑
Wholesale, Retail	33	45	54	31	50	61.3%	↑
Transportation, Storage	35	20	44	23	48	108.7%	↑
Manufacturing	32	32	61	32	47	46.9%	↑
News, Multimedia	70	69	43	23	38	65.2%	↑
Organizations	40	35	46	29	30	3.4%	↗
Arts, Entertainment	68	55	40	19	26	36.8%	↑
Energy, Utilities	24	25	39	13	19	46.2%	↑
Hospitability	44	27	22	12	17	41.7%	↑
Other Services	9	14	21	13	13	0.0%	-
Telecommunications	13	19	32	16	9	-43.8%	↓
Construction	1	2	7	4	3	-25.0%	↗
Agriculture, Forestry, Fishing	0	0	5	2	3	50.0%	↑
hMining, Quarrying	1	0	1	0	0	0.0%	-
TOTALE	**1.554**	**1.667**	**1.874**	**957**	**1.053**		

Figura 3.2: Tipologie di vittime [5]

3.2.2 5G

La tecnologia 5G porta con sè un grande sviluppo delle reti mobili, molte novità e tecniche d'avanguardia, ma anche una serie di vulnerabilità e problemi di sicurezza. Questi sono dovuti a differenti fattori che includono:

- la natura aperta e basata su IP dell'architettura del sistema;
- la diversità delle tecnologie di rete precedenti, che sottostanno e coesistono al 5G;
- la grande quantità di dispositivi interconnessi e la loro eterogeneità per quanto riguarda la potenza della batteria, la potenza di calcolo e le capacità di memoria;
- la natura aperta dei sistemi operativi di questi dispositivi;
- l'utilizzo dei dispositivi da parte di utenti non esperti in ambito informatico o di sicurezza.

Di seguito si esporranno alcuni dei possibili attacchi, divisi per categorie a cui sono rivolti, talvolta insieme a delle possibili contromisure e tecniche di mitigazione che potrebbero dimunuire il rischio.

User Equipment

I dispositivi mobili stanno diventando sempre più potenti e complessi, supportano una grande quantità di opzioni di connettività differenti e questo è un punto di debolezza.
Oltre che dai classici attacchi DoS (Denial of Service) via SMS o MMS, i dispositivi saranno colpiti anche da malware, ovvero software che danneggia il funzionamento del device ed è pericoloso anche per la rete.

- Mobile Malware
  I cosiddetti *mobile malware* possono sembrare proprio delle innocenti applicazioni, che i sistemi operativi aperti permettono agli utenti di scaricare. Tuttavia questi, una volta installati, hanno accesso ai dati personali e alle informazioni sensibili dell'utente, come ad esempio credenziali bancarie, chat, file audio e video, email e contatti, i quali possono essere raccolti e utilizzati dagli attaccanti.
  È possibile inoltre generare attacchi che interrompono il normale flusso dei servizi, sfruttando i cicli della CPU per fare dei calcoli fittizi, che servono solo per consumare velocamente energia e causare un esaurimento della fonte di alimentazione del device.

- 5G Mobile Botnet
  I dispositivi oggi tendono ad essere sempre accesi e connessi a internet e questo fatto può essere sfruttato dai malinenzionati per attuare attacchi controllando il dispositivo da remoto.
  I dispositivi colpiti, manovrati a distanza, rilanciano attacchi contro altre entità, che possono essere device, reti di accesso, reti centrali o altre reti esterne connesse, creando così delle *botnet*, reti di bot.

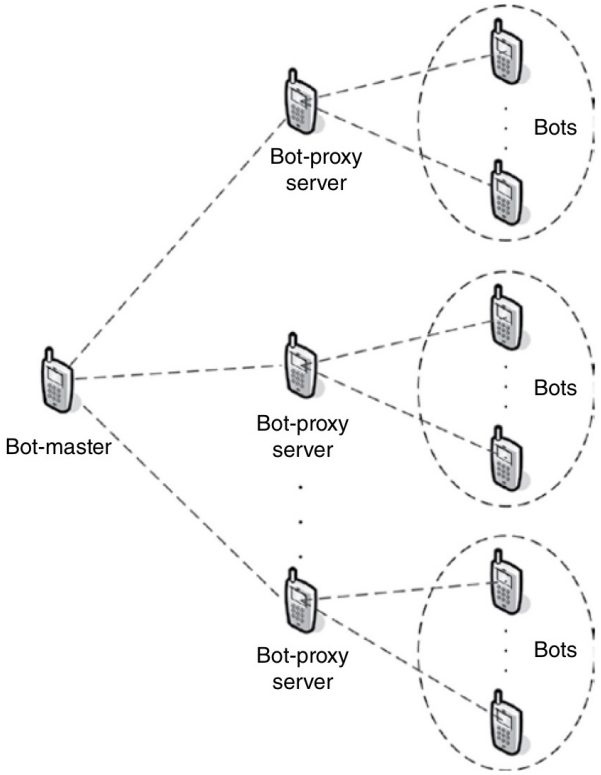

Figura 3.3: Esempio di botnet [13]

Sono tre i ruoli principali che costituiscono una rete di bot.
I *Bot-Master* sono i protagonisti maliziosi che hanno accesso e gestione della rete in via remota. Sono repsonsabili della scelta dei dispositivi che saranno vittime dell'attacco. Utilizzano tecniche http, simili a quelle usate nelle botnet di computer, oppure metodi più specifici dei dispositivi mobili, quali i messaggi SMS, per distribuire i comandi.[13]

I *Bot-Proxy Server*, invece, fungono da intermediari: possono essere dei server di controllo e comando, Control & Command Servers, che i Bot-Master utilizzano per raggiunge le loro vittime.

Infine i *Bot*, ovvero i dispositivi vittima, che sono programmati e addestrati dai Bot-Master per eseguire una serie di azioni malvagie, come ad esempio attacchi DDoS (Distributed Denial of Service) contro elementi della rete, invio di massa di messaggi spam, furto o addirittura distribuzione di dati sensibili e installazione di software malevolo su altri dispositivi.

Reti di Accesso

Le moderne reti di accesso sono molto complicate e diversificate, in quanto includono quelle delle tecnologie precedenti. Il fatto che il sistema 5G debba supportare diverse reti di accesso è positivo da una parte, in quanto gli utenti devono vivere un'esperienza fluida, senza interruzioni e malfunzionamenti, ma negativo dall'altra, perchè eredita molti problemi di sicurezza delle reti di accesso sottostanti. Di seguito si espongono degli attacchi alla rete di accesso 4G che si espandono alla nuova rete 5G.

- Tracciamento della posizione dello User Equipment
  La presenza di un determinato device in una specifica cella può avvenire attraverso due tecniche, che sono le stesse per la rete 4G e 5G.

  Il primo metodo è basato sull'identificatore temporaneo C-RNTI (Cell Radio Network Temporary Identifier), il quale fornisce un'identificazione dello User Equipment a livello di cella. Quando il dispositivo è associato alla cella, l'identificatore è assegnato dalla rete tramite un segnale di controllo ed è trasmesso in chiaro. Per questo motivo un attaccante è in grado di capire facilmente la cella a cui esso è attaccato. Il C-RNTI è assegnato a un device tramite messaggio di comando di consegna, durante il processo di trasferimento. Quindi è possibile scoprire la posizione di un determinato device tracciando la combinazione tra l'identificatore e i segnali di trasferimento, la quale permette di seguire i movimenti attraverso celle multiple.
  Due possibili soluzioni di mitigazione al problema potrebbero essere quelle di riallocare periodicamente il C-RNTI, ad esempio per uno UE che sta per molto tempo sulla stessa cella, oppure il criptaggio dei messaggi di controllo delle risorse radio, in modo tale da rendere difficile l'associazione dell'identificatore temporaneo e il mappaggio del trasferimento.[7]

La seconda tecnica è basata sul numero di sequenza dei pacchetti per il *control plane* e lo *user plane*. Un attaccante può eseguire un mapping prima e dopo un trasferimento, tra i vecchi e i nuovi identificatori C-RNTI, oppure nelle transizioni delle modalità di attività e non attività. Una soluzione a questa questione, proposta dalla fonte [7], è una discontinuità nella sequenza di numeri dei pacchetti sul piano utente e di controllo sul collegamento radio, creata attraverso degli offset casuali. Un'altra opzione è quella di utilizzare nuove chiavi per ogni eNB, in modo da poter settare la sequenza di numeri a un valore casuale.

- ATTACCHI BASATI SULLA FALSIFICAZIONE DELLO STATO DEL BUFFER
  I rapporti sullo stato del buffer vengono utilizzati per la schedulazione dei pacchetti, sono sfruttati dagli algoritmi di controllo e per il bilanciamento del carico. Se queste informazioni sul buffer vengono falsificate e trasmesse dagli attaccanti, possono cambiare i comportamenti degli algoritmi dei nodi che devono programmare l'invio dei pacchetti. L'attaccante in questo modo riesce a farsi allocare dagli algoritmi quante risorse preferisce e a comprometterlo, causando così l'allocazione di poche o nessuna risorsa per gli utenti legittimi. Avendo il controllo sull'allocazione delle risorse, l'aggressore è in grado di mettere in atto un attacco DoS.
  Inoltre anche i nuovi dispositivi che arrivano in una cella possono subire un attacco DoS. L'attaccante in questo caso afferma di avere una quantità ingente di dati da mandare, cosicchè la cella assuma che ci sia in arrivo un pesante carico di informazioni e che non accetti nuovi dispositivi in arrivo.
  Per contrastare gli attacchi basati sulla falsificazione dello stato del buffer, la fonte [7] propone l'utilizzo di un token a singolo accesso all'interno del rapporto sullo stato del buffer al livello MAC (Media Access Control). Il MAC-level, insieme con il LLC (Logical Link Control)-level, costituisce il secondo mattoncino del modello ISO/OSI. Si trova a contatto con il livello fisico e si occupa della regolamentazione dell'accesso al mezzo trasmissivo.
  Il dispositivo dovrà inviare questo token, il quale sarà diverso per ogni rapporto sullo stato del buffer durante il periodo di ricezione discontinua, per ottenere l'accesso.

- ATTACCHI TRAMITE INSERZIONI DI MESSAGGI
  I dispositivi mobili hanno la possibilità di operare in modalità DRX, cioè in ricezione discontinua, per risparmiare il consumo di batteria.

Intervallano periodi di controllo di dati provenienti dalla rete a periodi di riposo, creando così dei cicli alternati di ricezione. Durante un lungo intervallo di tempo DRX, per il dispositivo è ancora possibile la trasmissione di pacchetti, ad esempio in caso di informazioni urgenti da mandare e questo può essere fonte di problemi. Un attaccante, durante questo periodo, può iniettare nel sistema delle C-PDU, delle unità di controllo sul protocollo dati, mettendo in atto così un attacco DoS contro il dispositivo.[13] Una richiesta di capacità da parte dello UE nel rapporto dello stato del buffer in uplink potrebbe mitigare questo rischio.[7]

Reti Centrali degli Operatori di Telefonia Mobile

La rete 5G, essendo costituita da un'architettura aperta e basata su procollo IP, è molto vulnerabile e soggetta ad attacchi distribuiti di negazione di servizi, DDoS, tipologia di attacchi internet più diffusa attualmente.

- DDoS verso le core network degli operatori mobili
  Gli attacchi DoS distribuiti possono essere attuati tramite amplificazione di segnali. Una rete di bot, costituita da una moltitudine di dispositivi infetti collegati alla stessa cella, sfruttano il sovraccarico di segnalazione necessario per impostare e rilasciare il portatori radio dedicati, i quali vengono creati quando il servizio richiesto non può essere soddisfatto tramite portatori di default. Viene forzata la procedura di attivazione di molti portatori dedicati per segnali gravosi. Dopo aver ottenuto questi portatori dedicati, i bot non li useranno e, dopo la scadenza del tempo massimo dell'inattività del portatore, ha inizio la procedura di disattivazione del portatore stesso e anch'essa causa un livello alto di segnalazione. Ripetendo questi passaggi per molte volte si ha un'ingente amplificazione dei segnali e questo peggiora notevolemente le prestazioni della rete.[13]
  Una possibile tecnica per il rilevamento di questi attacchi si basa sull'analisi del numero di attivazioni e disattivazioni al minuto: un valore troppo alto di movimenti di questa tipologia al minuto indica un'attività maligna e può essere bloccata dagli operatori di rete mobile.

  In aggiunta un altro attacco di tipo DDoS nella rete 5G è molto simile a quello che, nella rete 4G, viene identificato come saturazione dell'*Home Subscriber Server*. Quest'ultimo è il database centrale della Core Network che contiene tutte le informazioni relative all'utente e all'abbonamento associato ad esso e fornisce delle funzioni ausiliarie per

l'autenticazione degli utenti e le autorizzazioni d'accesso. Anche questa tipologia d'attacco si verifica grazie a una rete di bot costituita da dispositivi mobili. È molto difficoltoso, anche se non impossibile, che i legittimi proprietari si accorgano dell'utilizzo illecito dei propri device in quanto la violazione avviene tramite silenziose richieste di servizi di rete. Secondo il lavoro della fonte [18], le botnet possono agire in modo tale da sovraccaricare una componente specifica del HSS, cioè l'*Home Location Register*, citato nei capitoli precedenti. Per fare ciò, è necessaria una grande quantità di dispositivi muniti di SIM valide, in modo che la rete inizializzi la procedura di collegamento.
Tuttavia la fonte [11] dimostra come è possibile aumentare la gravità di un attacco di questo tipo riducendo il numero di risorse e di dispositivi indispensabili per attuarlo.
Inoltre espone un'alternativa che prevede di iniettare nella rete traffico di segnali senza il bisogno di una SIM valida, ma tramite l'utilizzo di un device dedicato. Questo ha due vantaggi: ottenere le risorse necessarie senza l'interferenza di utenti ed eventuali rischi di essere scoperti e avere un maggior controllo del posizionamento del suddetto device, il quale è sotto l'esclusivo controllo dell'attaccante.
Una mitigazione proposta è il filtraggio nella Core Network, anche se potrebbe essere attuato troppo tardi per prevenire che l'utente si accorga della congestione del traffico.

La rete centrale purtroppo può essere colpita da attacchi che sono mirati a reti esterne, ad esempio le reti aziendali. La Core Network funge da gateway, cioè da via d'accesso per le reti esterne, quindi il passaggio di un ingente traffico dati inevitabimente può comprometterne le sue prestazioni.

Reti IP Esterne

Gli attacchi DoS distribuiti colpiscono anche le reti IP esterne e sono generati dalle botnet, con la procedura spiegata nel paragrafo precedente.
Inoltre le reti esterne, ad esempio quelle aziendali, possono essere compromesse da dispositivi infetti che si connettono ad esse. Al giorno d'oggi vengono utilizzati i dispositivi personali dei dipendenti all'interno dell'ambito aziendale per scopi lavorativi: hanno quindi accesso a informazioni riservate e tenute sotto stretto controllo nella rete aziendale. Questo diventa un problema nel momento in cui il device in questione è infetto da un malware ad esempio.
Per di più un'altra caratteristica dei dispositivi mobili, come già citato nei precedenti paragrafi, è la diversità delle loro capacità di connettività. Si con-

siderino non solo le tecnologie di comunicazione mobile, ma anche altri tipi di connettività, come Bluetooth, WiFi, NFC (Near Field Communication) e USB (Universal Serial Bus). I device, grazie allo sfruttamento di queste tecnologie, fungono da collegamento tra la rete e il mondo esterno, permettendo agli attaccanti di iniettare dei dati malevoli all'interno della rete.
Per limitare questo rischio, una buona pratica sta nel controllo periodico dei dispositivi pericolosi con dei software anti-malware.

Capitolo 4

Conclusione

Nel corso di questo elaborato, si è fatto una panoramica storica delle tecnologie di rete mobili, dalla prima generazione nata negli anni '80, fino alla tecnologia 4G.
Di ognuna si sono analizzati gli elementi peculiari che li contraddistinguono e le novità apportate da ciascuna di esse. In aggiunta, si è esaminata anche l'architettura delle singole reti, descrivendo le componenti caratterizzanti delle due parti principali, presenti in ogni generazione: la rete di accesso e la rete centrale.
Si è proceduto poi ad esporre in maggior dettaglio la più recente tecnologia 5G. Partendo dalle motivazioni per cui la nostra società necessita di questa innovazione, si sono poi analizzati i principali obiettivi che questa tecnologia si pone e le tre macro categorie che ne benificiano: utenti finali, fornitori di servizi e operatori di rete.
In seguito si è descritta l'architettura del 5G, prestando maggiore attenzione alle novità apportate e al cambio di visione. Si è passati da un sistema chiuso con software proprietario e hardware specializzato, a un modello più aperto che prevede il disaccoppiamento tra software e hardware. Il primo diventa sempre più fondamentale e complesso, mentre il secondo diviene sempre più standard e meno costoso.
Si sono poi descritte le due modalità d'installazione della tecnologia 5G: la modalità NSA si integra con la struttura del 4G, mentre la SA è completamente autonoma. La prima, nonostante non offra tutte le funzionalità previste dal 5G, è più immediata e quindi maggiormente utlizzata nella fase di sviluppo iniziale. La seconda, invece, garantisce a pieno tutti i servizi della nuova tecnologia, ma richiede maggior tempo e risorse per l'installazione.
Nell'ultimo capitolo, seguendo lo stesso pattern di confronto delle varie tecnologie, si è approfondito il tema della sicurezza, facendo un excursus sulle vulnerabilità e sui rischi che le diverse generazioni riscontrano.

Successivamente sono presentate delle percentuali, estratte da un rapporto dell'associazione italiana per la sicurezza informatica, riferite alle tipologie di aggressori e di vittime degli attacchi informatici.
Infine sono esposti alcuni dei più comuni attacchi informatici alla rete 5G, che sono ereditati dalla precedente tecnologia di rete mobile 4G. La presentazione di essi è suddivisa per categorie a cui sono rivolti. Per alcune tipologie di attacco vengono proposte delle possibili soluzioni o mitigazioni al problema.
A conclusione di questo lavoro, si sottolinea che il 5G, nonostante porti cambiamenti in molti ambiti della nostra vita, non è esente da vulnerabilità e rischi in campo di sicurezza.
Si ritiene quindi importante considerare, oltre che l'utilità delle innovazioni, anche lo sviluppo di una cultura della sicurezza per proteggere i nostri dati e potersi affidare consapevolmente al mondo informatico.

Ringraziamenti

Alla mia famiglia, grazie di avermi supportato economicamente, ma soprattutto moralmente, dandomi sempre coraggio e spronandomi a non mollare mai.
Grazie a Massimiliano, una persona speciale per me, che ha ascoltato pazientemente i miei lamenti nei momenti di sconforto e ha gioito con me al raggiungimento dei miei traguardi, vivendoli come se fossero i suoi.
Ringrazio anche le mie amiche, che speravano diventassi un avvocato...ormai dovete arrendervi ad avere un'ingegnere informatico nel gruppo!
Infine vorrei ringraziare i miei compagni di corso per aver condiviso insieme a me quest'avventura e in particolare Jacopo, grazie di avermi aiutato a risolvere i miei mille pasticci e per aver alleggerito le giornate di studio!

Bibliografia

[1] *5G Italy 2020, CNIT TALK - Architettura e Servizi della rete 5G*. URL: https://www.youtube.com/watch?v=sH-aip7-jg0.

[2] *Cisco Annual Internet Report - Internet adoption and network performance*. URL: https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html.

[3] R. Esmailzadeh e M. Nakagawa. *TDD-CDMA for Wireless Communications*. Artech House universal personal communications series. Artech House, 2003. ISBN: 9781580537636. URL: https://books.google.it/books?id=bOeH1vMXqAUC.

[4] E. Ezhilarasan e M. Dinakaran. «A Review on Mobile Technologies: 3G, 4G and 5G». In: *2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM)*. 2017, pp. 369–373. DOI: 10.1109/ICRTCCM.2017.90.

[5] Gabriele Faggioli. *Rapporto Clusit 2021 sulla sicurezza ICT in Italia*. 2021.

[6] *FastWeb Plus-Cos'è la tecnologia MiMo*. URL: https://www.fastweb.it/fastweb-plus/digital-magazine/cos-e-la-tecnologia-mimo/.

[7] Dan Forsberg et al. «Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface». In: *2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*. 2007, pp. 1–5. DOI: 10.1109/PIMRC.2007.4394792.

[8] *Glossario di Supporto Vodafone-GPSR*. URL: https://www.vodafone.it/portal/Privati/Supporto/Glossario/gprs (visitato il 11/09/2022).

[9] *Immagine da modificare*. URL: https://www.3gpp.org/technologies/keywords-acronyms/100-the-evolved-packet-core.

[10] Guangyi Liu et al. «5G Deployment: Standalone vs. Non-Standalone from the Operator Perspective». In: *IEEE Communications Magazine* 58.11 (2020), pp. 83–89. DOI: 10.1109/MCOM.001.2000230.

[11] Alessio Merlo et al. «A Denial of Service Attack to UMTS Networks Using SIM-Less Devices». In: *IEEE Transactions on Dependable and Secure Computing* 11.3 (2014), pp. 280–291. DOI: 10.1109/TDSC.2014.2315198.

[12] Ajay R. Mishra. *Fundamentals of network planning and optimisation 2G/3G/4G : evolution to 5G*. eng. Second edition. Hoboken, NJ, USA: Wiley, 2018. ISBN: 1-119-33176-5.

[13] Jonathan Rodriguez. *Fundamentals of 5G mobile networks*. John Wiley & Sons, 2015.

[14] Andrea Silvestri. *AEIT, In primo piano: Le prospettive del 5G*. Associazione Italiana di Elettrotecnica, Elettronica, Automazione, Informatica e Telcomunicazioni -AEIT, 2018.

[15] S. Sullivan et al. «5G Security Challenges and Solutions: A Review by OSI Layers». In: *IEEE Access* 9 (2021), pp. 116294–116314. DOI: 10.1109/ACCESS.2021.3105396.

[16] *Tim-Roadmap di standardizzazione del 5G*. URL: https://www.gruppotim.it/content/tiportal/it/notiziariotecnico/edizioni-2019/n-1-2019/N4-La-roadmap-standardizzazione-5G.html.

[17] *Time Division Multiple Access (TDMA)*. URL: https://www.techtarget.com/searchnetworking/definition/TDMA.

[18] Patrick Traynor et al. «On cellular botnets: Measuring the impact of malicious devices on a cellular network core». English (US). In: *CCS'09 - Proceedings of the 16th ACM Conference on Computer and Communications Security*. Proceedings of the ACM Conference on Computer and Communications Security. Copyright: Copyright 2010 Elsevier B.V., All rights reserved.; 16th ACM Conference on Computer and Communications Security, CCS'09 ; Conference date: 09-11-2009 Through 13-11-2009. 2009, pp. 223–234. ISBN: 9781605583525. DOI: 10.1145/1653662.1653690.