UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

ATTACCO DI TIPO DENIAL OF SERVICE ALLE RETI CELLULARI

Relatore: Prof. Mauro Migliardi

Laureando: Stefano Leggio

ANNO ACCADEMICO: 2020-2021

Data di laurea: 20/09/2021

Indice

Elenco delle figure

Elenco delle abbreviazioni

MS Mobile system. 16

MSC Mobile switching center. 6

1 Introduzione

Le reti cellulari rappresentano un punto nevralgico per le nostre comunicazioni. Per questo, la loro sicurezza è fondamentale per garantire un normale funzionamento di tutti i servizi a cui ormai ci siamo abituati.
La nuova tecnologia di quinta generazione è ormai vicina ad essere implementata su larga scala per permettere lo sviuluppo del mondo IOT *Internet Of Things*. Questa nuova tecnologia stravolge numerosi paradigmi strutturali che sono stati utilizzati fin'ora nelle generazioni precedenti, introducendo nuove sfide nell'ambito della loro sicurezza.

1.1 Struttura del documento

Il documento è strutturato in modo da fornire al lettore le competenze e terminologie adeguate per comprendere tutti i dettagli della vulnerabilità scoperta.
L'elaborato inizia con una breve panoramica sulla rete cellulare, descrivendo genericamente la sua struttura e architettura.
Dato che le specifiche dell'architettura di una rete cellulare sono molto diverse a seconda della generazione, è stato necessario illustrare l'evoluzione delle varie tecnologie: da 1G a 5G. Per ogni generazione verranno illustratate prevalentemente le sue propietà architetturali oltre che le principali novità introdotte. Successivamente, verrà introdotta la tipologia dell'attacco trattato, ossia il *Denial of Service*, spiegano in cosa consiste e come si applica alle reti cellulari. Inoltre, verranno illustrate le misurazioni necessarie per valutare l'efficienza di un attacco.
Nel seguente capitolo, verranno analizzati nel dettaglio i sistemi di identificazione per le varie generazioni cellulari. Questo perchè è nel loro funzionamento che sono preseti le vulnerabilità sfruttate per l'attacco. Successivamente, verrà trattato l'attacco di tipo *Denial of Service* alle reti UMTS, spiegando il suo funzionamento e i risultati che sono stati ottenuti in [4]. Infine, verrà discusso una potenziale replicazione in una architettura 5g. Inoltre, verranno evidenziate altre possibili vulnerabilità presenti in questa ultima generazione.

1.2 Scopo della tesi

Questo elaborato si vuole occupare di analizzare l'attacco di tipo *Denial of Service* alle reti UMTS illustrato in [4] e scoprire se questo potrebbe risultare efficacie nelle ultime tecnologie cellulari 5g.

2 La rete cellulare

2.1 Definizione

La rete cellulare è la struttura *hardware* e *software* che consente il corretto funzionamento delle comunicazioni cellulari. Grazie alla loro capillarità, i vari gestori telefonici riescono a garantire il servizio per la gran parte del territorio mondiale.

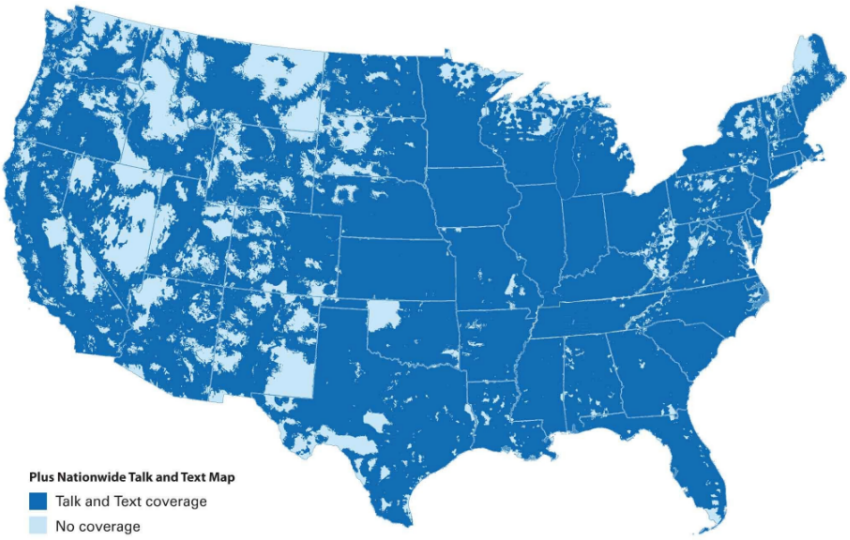

Figura 1: Mappa compertura AT&T negli USA

La loro struttura e architectura hanno subito numerosi cambiamenti nel corso delle generazioni, in particolare con la rete 5g. Si possono comunque identificare degli elementi chiave che sono presenti in tutte le generazioni:

- UE *User Equipment* ovvero il dispositivo cellulare
- RAN *Radio Access Network* ovvero l'infrastruttura fisica di antenne per la ricezione e trasmissione di informazioni per il dispositivo
- *Mobile Core* ovvero i componenti della sua architettura

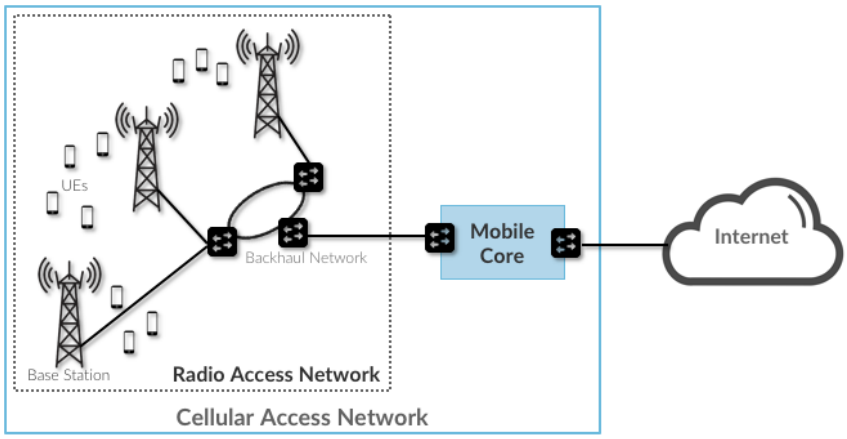

Figura 2: Schema di una rete cellulare

2.2 Infrastruttura

Per rendere possibile il collegamento di dispositivi in zone molto vaste vengono usati i ripetitori di segnale chiamati *base station*. Questi vengono disposti in modo capillare sul territorio, suddividendolo in diverse aree di competenza chiamate celle. Ognuna di queste può gestire un numero limitato di dispositivi in contemporanea, che chiameremo *mobile station*, per questo, in caso di aree densamente popolate vengono ridotte le aree di competenza di ciascuna antenna. Le celle quindi, possono avere una dimensione variabile che dipende dal contesto in cui devono essere inserite.

Figura 3: Base station

Ogni cella ha un determinato raggio di azione che dipende dalle caratteristiche fisiche dell'antenna stessa. Inoltre, ha a disposizione un determinato range di frequenze su cui instaurare la comunicazione con i vari dispositivi, che solitamente sono differenti rispetto a quelle usate dalle celle vicine per evitare interferenze. Celle sufficientemente distanti possono utilizzare le stesse frequenze poiché non corrono il rischio di interferenza, questo rappresenta un grande vantaggio per questa tecnologia.

Figura 4: SIM *Subscriber Identity Module*

2.3 Architettura

L'architettura di una rete cellulare può essere risassunta con alcuni fondamentali componenti. La *mobile sation* si connette all'antenna della zona di competenza ossia la *base transceiver station*, quest'ultima quando riceve l'informazione la inoltra alla rispettiva *base station controller*, ossia un componente che si occupa di raggruppare diverse *base station*. Diversi *BSC* sono raggruppati nel *mobile switching centre* Mobile switching center (MSC)

3 Generazioni cellulari

Nel corso degli anni, si sono susseguite diverse generazioni di tecnologie cellulari, che hanno apportato notevoli cambiamenti alla loro architettura. Di seguito verranno presentati le principali caratteristiche delle diverse generazioni cellulari, in modo tale da rendere di facile comprensione l'analisi dei meccanismi di identificazione che verranno approfonditi nelle prossime sezioni.
Oltre ad elencare le principali caratteristiche di ogni generazione verranno analizzate nel dettaglio le specifiche dell'architettura di rete.

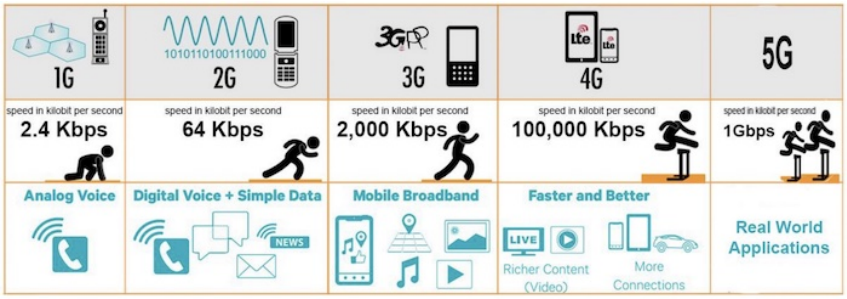

Figura 5: Schema delle generazioni cellulari

3.1 1G

La generazione 1G è uno dei primi standard di comunicazione cellulare. Il suo funzionamento era completamente analogico e ormai è stata rimpiazzata totalmente dalle generazioni digitali successive.
L'architettura di questa generazione è molto semplice, è composta da tre componenti principali:

- Antenne per la trasmissione
- *Mobile Telephone Switching Office* (MTSO)
- Unità mobile (cellulare)

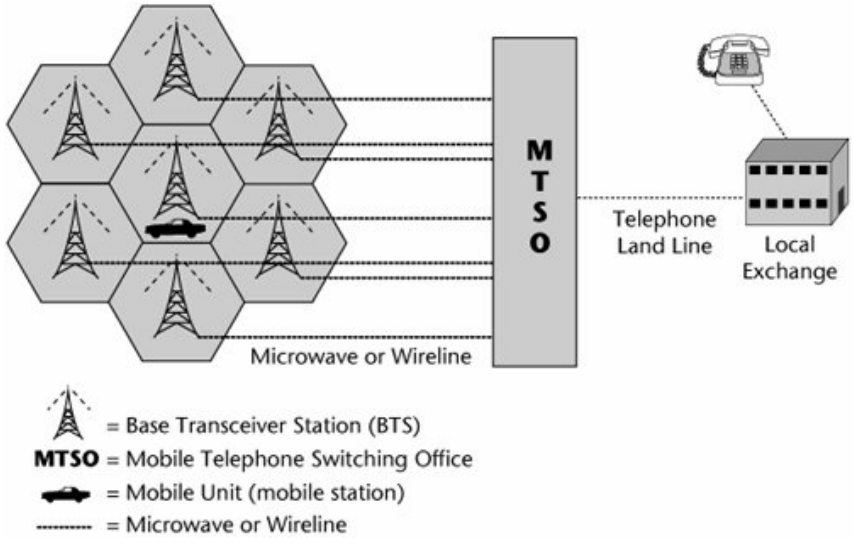

Figura 6: Architettura 1G

Si basava sulla *frequency-division multiple access* (FDMA) in cui ogni dispositivo che si connetteva alla stazione radio aveva assegnata una specifica sotto banda[5].

3.2 2G

A differenza della prima generazione, la seconda introuduce per la prima volta una rete completamente digitale. La seconda generazione cellulare è composta da diverse versioni che si sono susseguite nel corso degli anni aggiungendo nuove funzionalità. Anche la sua architettura subisce delle modifiche, per questo verranno trattate in seguito.

3.2.1 GSM

Il GSM, ovvero *Global System for Mobile Communications* è uno standard di seconda generazione che introuduce importanti novità. Le principali caratteristiche introdotte sono:

- Maggiori velocità di trasmissione
- Cifratura della comunicazione
- Introduzione di nuovi servizi come gli SMS

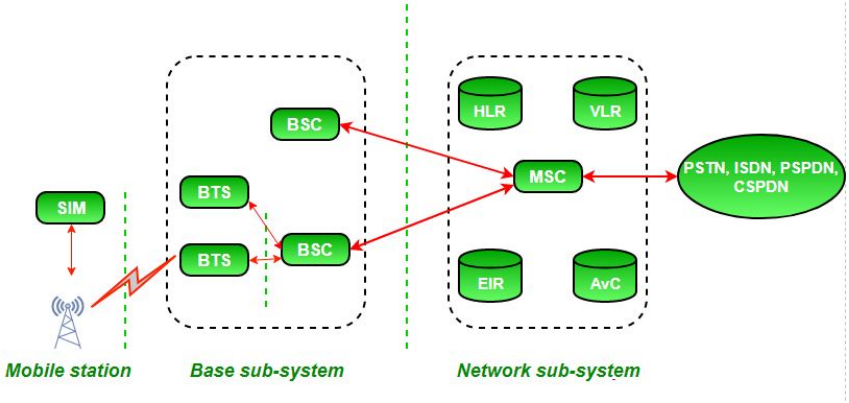

Figura 7: Architettura GSM

La sua architettura è composta da due macro aree: La BSS *Base Station SubSystem* e la NSS *Network SubSystem*. Il BSS è l'insieme delle antenne ricevitori, rappresentano il primo collegamento con il MS. Il MS si collega alla BS di riferimento, viene identificato tramite l'HLR *Home Location Register*, ovvero un *database* che contiene tutte le informazioni necessarie per la gestione dei *subscribers*. Le chiamate e messaggi vengono smistati nella rete telefonica tramite il *Mobile Switching Centre* (MSC).

3.2.2 GPRS

La rete *General Packet Radio Service* (GPRS) introduce per la prima volta un trasferimento dati a commutazione di pacchetto per rendere possibile l'utilizzo dei servizi *internet* con il proprio dispositivo cellulare[8]. La sua architettura è la stessa di quella del GSM ma con dei componenti aggiuntivi che consentono la trasmissione dei pacchetti. Per esempio, il SGSN *Serving GPRS Support Node* è un componente predisposto per la gestione dei dispositivi connessi alla rete.

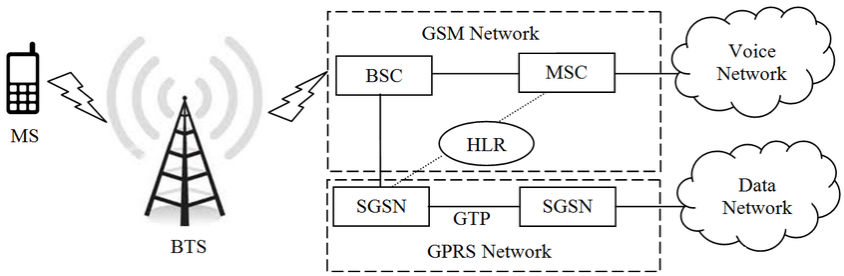

Figura 8: Architettura GPRS

3.2.3 EDGE

Evoluzione del GPRS che consente maggiori velocità, l'architettura resta invariata.

3.3 3G

L'architectura della terza generazione riprende quella già vista nella seconda. Infatti, questa generazione ha avuto come principale obbiettivo quello di consolidare l'integrazione della rete internet nei sistemi cellulari ed aumentare le velocità di trasmissione per consentire l'utilizzo di nuovi servizi. Le reti di terza generazione possono essere divise in tre componenti fondamentali:

- UE *User equipment*
- RNS *Radio Network Subsystem*
- *Core Network*

3.3.1 UMTS

L'UMTS ovvero *Universal Mobile Telecommunications System* è il primo standard di terza generazione.

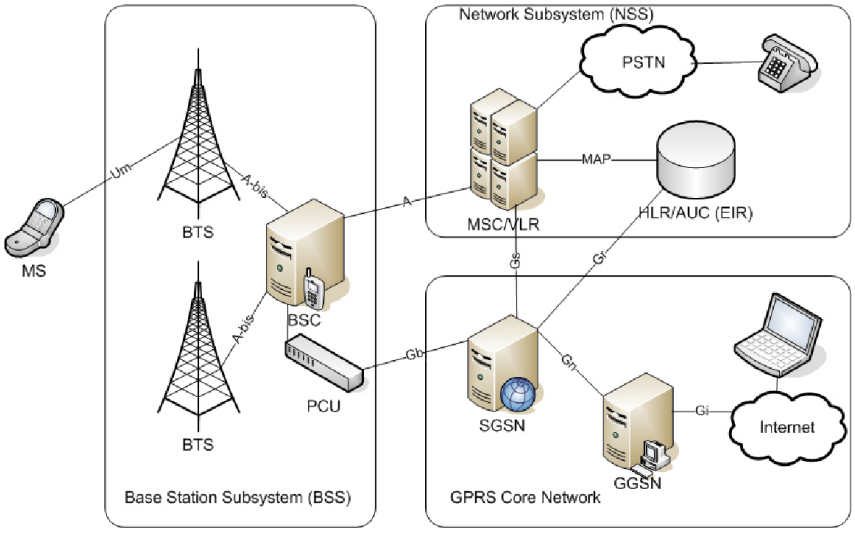

Figura 9: Architettura UMTS

3.3.2 HSPA/HSPA+

Evoluzione del UMTS per consentire velocità maggiori apportando modifiche nella trasmissione del segnale. Con questo nuovo standard si riescono a raggiungere velocità di 42 Mb/s.

3.4 4G

3.4.1 LTE

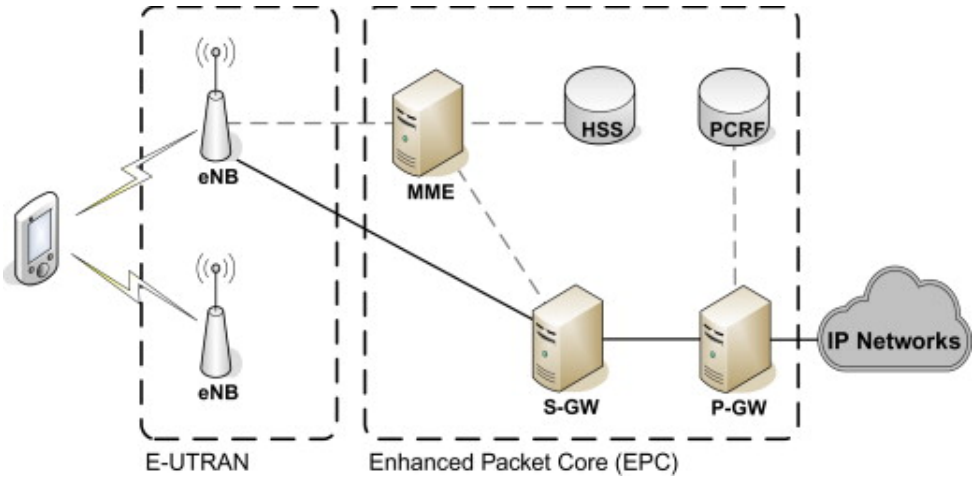

Figura 10: Architettura LTE

3.5 5G

Il 5G, ovvero lo standard di quinta generazione rappresenta l'ultima frontiera della tecnologia cellulare. Il suo principale scopo è consentire l'*Internet of Things* massivo, ossia un *network* che sia in grado di gestire la connessione di molti dispositivi con latenze molto piccole. Per consentire velocità fino a 10 Gb/s si sono dovute apportare importanti modifiche strutturali che rendono la sua architettura molto diversa da quelle viste fin'ora.
L'architettura implementata prende il nome di *Service-Base Architecture* (BSA). La BSA consiste nel dividere tutte le funzioni in una serie di *microservices*[6]. Questa nuova struttura è stata introdotta per garantire la scalabilità del sistema, migliorare le prestazioni (velocità) e per permettere di realizzare il *massive IOT*, che richiede la gestione simultanea di molti dispositivi.
I principali blocchi che la compongono sono:

- AMF *Core Access and Mobility Management Function* responsabile dell'autenticazione e autenticazione del dispositivo.
- SMF *Sesson Management Function* per la gestione della sessione di ogni UE.
- PCF*Policy Control Function* per la gestione delle *policy*
- UDM *Unified Data Management* per la gestione dell'identità dell'utente, questo compito era precedentemente svolto da HSS o HLR.
- AUSF *Authentication Server Function* per effettuare l'autenticazione dell'utente.
- SDSF *Structured Data Storage Network Function* è un helper per la memorizzazione di dati strutturati.
- UDSF *Unstructured Data Storage Network Function* è un helper per la memorizzazione di dati non strutturati.
- NEF *Network Exposure Function* per esporre determinate funzionalità a servizi di terze parti.
- NRF *NF Repository Function* per scoprire tutti i servizi disponibili.
- NSSF *Network Slicing Selector Function* per selezionare una determinata partizione di *network*.
- UPF *User Plane Function* trasporta il traffico dal RAN all'internet.

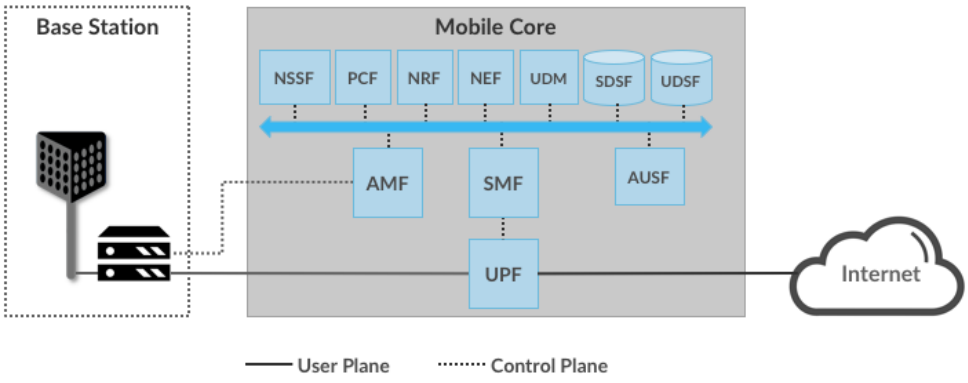

Figura 11: Architettura 5G[6]

3.5.1 Network Slicing

Il *Network Slicing* rappresenta una delle caratteristiche più importanti del 5G. Con questo termine si intende il partizionamento della rete in diversi "piani" ciascuno con caratteristiche e requisiti particolari, indipendente e autonomo. Questo risulta fondamentale nella realizzazione dell' IOT massivo, infatti in questo modo la gestione del traffico terrà conto dell'applicazione che viene utilizzata nel dispositivo per decidere quali prestazioni sono richieste da quel dispositivo.

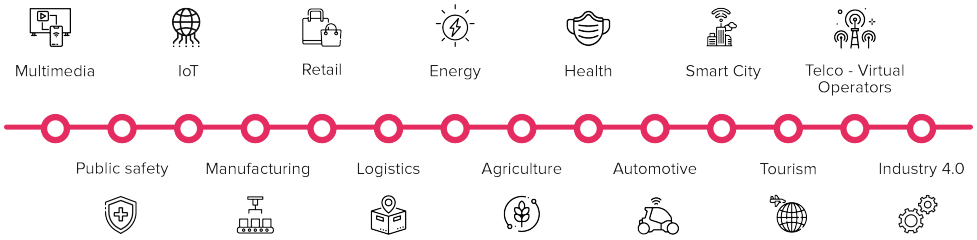

Figura 12: Esempi di applicazioni per il 5G

La realizzazione del *Network Slicing* avviene tramite i *Software Degined Network* che nella prossima sezione verranno approfonditi.

3.5.2 Software Defined Network

I *Software Defined Network* (SDN) sono dei programmi per la virtualizzazione della rete. Sono necessari per interfacciarsi a livello applicativo con i dispositivi cellulari in modo da gestire il traffico della rete in modo efficace[1].

4 Attacco Denial of Service

L'attacco di tipo *Denial of Service* (DOS) consiste nel rendere non disponibili servizi offerti da computer o altri dispositivi [3]. Questo avviene esasperando di richieste la macchina o infrastruttura che viene scelta come vittima.

4.1 Vulnerabilità nelle reti cellulari

Le reti cellulari non sono esenti da questo tipo di attacchi, anzi, sono una delle tipologie più frequenti e sopratutto difficile da risolvere poichè le vulnerabilità che sfruttano sono organiche nell'architettura della rete. Sono diversi i componenti che possono essere vulnerabili a un attacco DOS in una rete cellulare, gli obiettivi identificati come ottimi sono quelli che comportano un maggior utilizzo delle risorse della rete. Nelle prossime sezioni verranno illustrate le principali metodologie per fare un attacco di tipo *Denial of Service* alle reti cellulari[7].

4.1.1 Radio Jamming

Il *Radio Jamming* è una tipologia di attacco *Denial of Service* che consiste nel disturbare il segnale cellulare emettendo delle onde radio. La realizzazione di questo tipo di attacco è molto semplice, basta procurarsi un trasmettitore che invia segnali ad alta energia nella banda cellulare di riferimento.
Un miglioramento del classico *radio jamming* è lo *smart jamming* che consiste nel saturare uno o più canali di comunicazione della rete. Questo fa sembrare il *network* non disponibile a tutti gli utenti collegati a quella determinata cella.

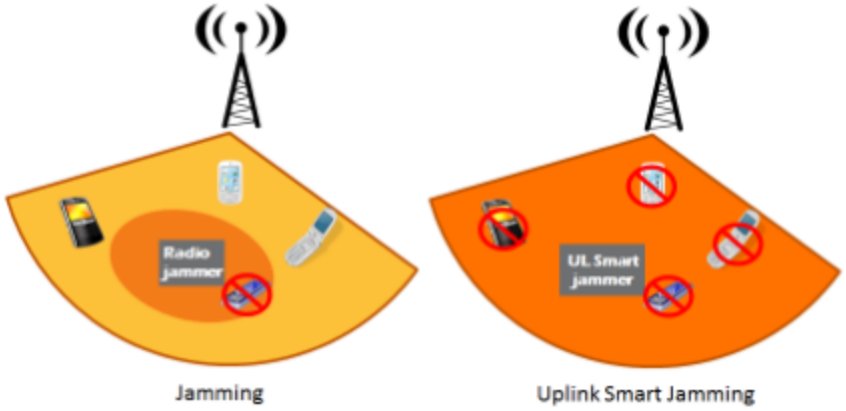

Figura 13: *radio* e *smart jamming*[7]

4.1.2 Vulnerabilità di sistema

Un altro classico modo per creare un interruzione di sistema in una rete cellulare è sfruttando le classiche vulnerabilità che si presentano spesso in qualsiasi tipo di computer. Questo ovviamente perchè tutta l'architettura di una rete cellulare non è altro che *server* con specifiche particolari.

4.1.3 Botnet

Questa è sicuramente una delle tipologie più diffuse, ed è il classico esempio di *Distributed Denial Of Service*. L'attaccante, in questo caso, dispone del controllo di un grande numero di dispositivi infettati da *malware* che possono essere attivati da lui per esasperare di richieste un determinato servizio.

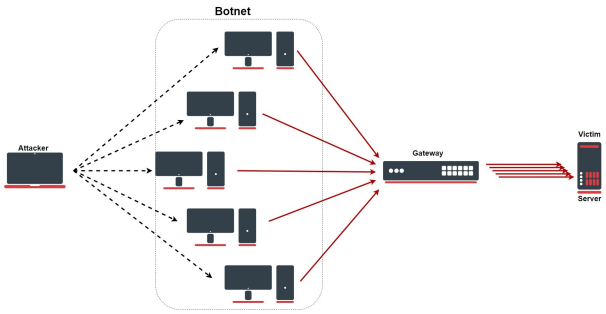

Figura 14: Distributed Denial of Service

4.1.4 Saturazione dell'autenticazione

Questo è uno dei più pericolosi poichè molto difficile da risolvere dato che è intrinseca nella architettura del sistema. E' la tipologia di vulnerabilità che è stata scelta per confrontare la sicurezza della architettura 5G con quelle precedenti. Il suo funzionamento si basa sull'esasperare di richieste di autenticazione i sistemi identificativi delle reti cellulari, che solitamente sono i componenti con più traffico della rete. Per esempio, nelle generazioni 2G e 3G, è la HLR che viene identificata come componente critico del sistema. Ad aumentare la pericolosità di questa vulnerabilità è la possibilità di creare computazioni nel *Core Network* senza essere effettivamente autenticati, e quindi senza disporre di una SIM valida. Questa tipologia di attacchi, definiti come SIM-less, verranno presi come riferimento per sfruttare questa vulnerabilità come illustrato per le reti GSM[2] e UMTS[4].

4.2 Misurazione

Per capire quale componente della rete sia il più vulnerabile a un attacco DOS si devono fare delle misurazioni sui vari componenti del *network*. In questo modo è possibile capire in quale punto si possono creare dei rallentamenti o *bottleneck* dovuti a un sovraffollamento di richieste.
In [9] vi è una dettagliata spiegazione di come procedere con queste misurazioni e sopratutto come quantificare il numero di dispositivi che servono all'attaccante per completare l'attacco con successo.

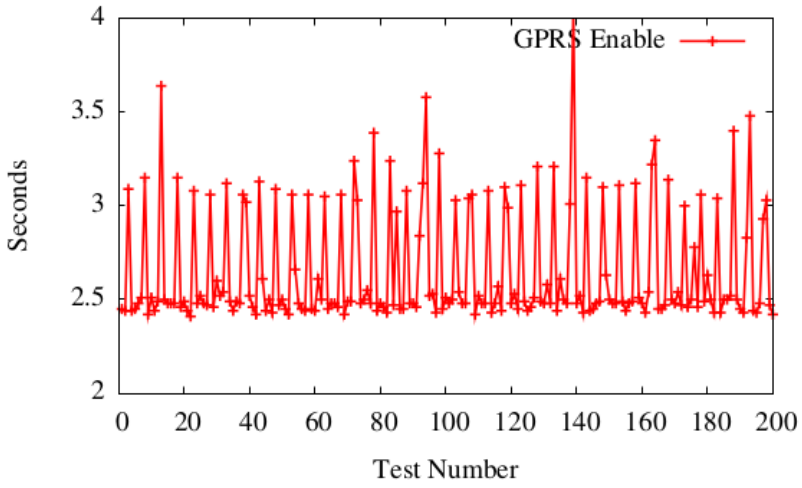

Figura 15: Misurazione tempi di risposta HLR con *location updates*[9]

5 Sistema di identificazione

Il meccanismo di identificazione è la procedura per verificare che un determinato dispositivo è abilitato a connettersi alla rete. Questo procedimento avviene tramite l'*Authentication and key agreement* (AKA), procedimento in cui il *core network* abilita un dispositivo a connettersi.
Di seguito verranno illustrate le procedure di inteficazione per le principali generazioni cellulari: dal 2G al 5G. Il 1G è stato escluso poiché ha un funzionamento completamente analogico.

5.1 2G

Nei sisteni di seconda generazione nella fase di autenticazione di un dispositivo vengono interpellati principalmente tre componenti:

1. Il dispositivo cellulare con l'apposita SIM
2. Il MSC di riferimento
3. La HLR con l'AUC per effettuare la validazione

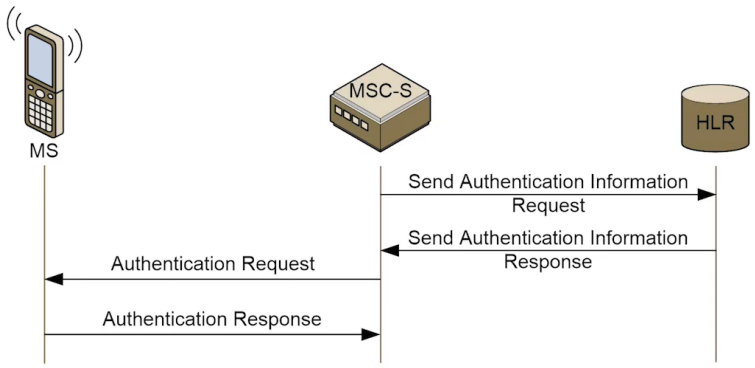

Figura 16: Identificazione nelle reti 2G

Per autenticare un dispositivo vengono generati i vettori di autenticazione nell'AUC, univochi rispetto a un determinato dispositivo identificato da un IMSI. Questi vettori poi vengono inviati all'HLR che si occuperà do verificarne la correttezza e inviare una risposta al MSC che la inoltra al MS.

5.2 3G

Nei sistemi di terza generazione i componenti utilizzati per l'identificazione di un dispositivo sono gli stessi della generazione precedente salvo qualche eccezione. Come illustrato precedentemente, come nel GPRS nelle reti 3G ci sono due *Switcing centre*: MSC per il classico circuito telefonico e il GMSC per i pacchetti di rete. L'identificazione viene completata allo stesso modo della seconda generazione, ma

Con rete 3G si intendono l'insieme delle tecnologie di terza generazione, stiamo quindi parlando di un'architettura UMTS. Un MS che si vuole collegare alla rete deve procedere con la fase di autenticazione o identificazione anche detta *Authentication and key agreement* (AKA). In questa fase, viene interrogata la rispettiva HLR/AuC dove l'IMSI del dispositivo viene validato, se tutto procede correttamente viene notificato il SGSN che inoltra al MS l'avviso di autenticazione completata.

5.3 4G

5.4 5G

6 Attacco alle reti 2G-4G

Le reti cellulari dal 2G al 4G condividono lo stesso schema architetturale generale, per questo gran parte delle vulnerabilità che vengono utilizzate negli attacchi *Denial of Service* sono comuni. Ci sono numerosi modi per fare un attacco di tipo *Denial of Service* alle reti cellulari, gran parte di questi utilizzano una *botnet* per esasperare di richieste i componenti critici del *network*, creando così i *Distributed Denial of Service*.

6.1 Attacco alle reti UMTS con dispositivi SIM-Less

In [4] è descritto un attacco di tipo *Denial of Service* alle reti UMTS, in particolare al sistema di identificazione degli utenti.
Lo studio dmostra che è possibile generare delle onerose computazioni all'interno dell'infrastruttura cellulare senza disporre di dispositivi con delle SIM valide. Inoltre, nell'attacco trattato i dispositivi che sono necessari per avere una degradazione del servizio sono un numero nettamente minore rispetto allo stato dell'arte, ciò rende la sua realizzazione molto più accessibile. Con l'inserimento di SIM valide nei dispositivi è possibile ridurre il numero di interfacce UMTS necessarie per compiere l'attacco con successo, infatti queste si riducono a qualche centinaio. Visto il numero contentuto di dispositivi che sono necessari per effettuare l'attacco, si può evitare di usare una *botnet* rendendo l'attacco molto più stabile e quindi più pericoloso.
L'attacco ha come obbiettivo la degradazione di uno dei componenti centrali dell'architettura UMTS: la HLR. Questo componente è il più semplice da attaccare poichè avvengono continue interrogazioni durante tutta la fase di autenticazione e identificazione del MS. Siccome non si tratta di una *botnet* è stata fondamentale l'analisi della capacità dei canali di comunicazione in modo tale da scoprire eventuali *bottleneck* che minerebbero l'esecuzione dell'attacco.

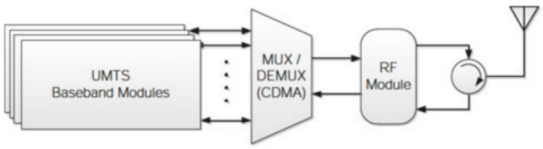

Figura 17: Dispositivo per l'attacco DOS alle reti UMTS[4]

I risultati ottenuti si basano su stime dei tempi di risposta dei componenti architetturali trattati. Questo perchè i vari MNOs non forniscono nessuna informazione ufficiale riguardo le *performance*.

7 Attacco alle reti 5G

7.1 Replicazione attacco

7.2 Altre vulnerabilità

8 Conclusioni

Riferimenti bibliografici

[1] Alcardo Alex Barakabitze et al. ≪5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges≫. In: *Computer Networks* 167 (2020), p. 106984. ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2019.106984. URL: https://www.sciencedirect.com/science/article/pii/S1389128619304773.

[2] Nicola Gobbo, Alessio Merlo e Mauro Migliardi. ≪A Denial of Service Attack to GSM Networks via Attach Procedure≫. In: (set. 2013). DOI: 10.1007/978-3-642-40588-4_25.

[3] Kevin Hattingh et al. ≪DoS! Denial of Service≫. In: ().

[4] 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.

[5] Fredrick Njoroge e Lincoln Kamau. ≪A Survey of Cryptographic Methods in Mobile Network Technologies from 1G to 4G≫. In: (nov. 2018).

[6] Larry Peterson e Oguz Sunay. *5G Mobile Networks: A Systems Approach*. URL: https://github.com/SystemsApproach/5G.

[7] Roger Piqueras Jover. ≪Security attacks against the availability of LTE mobility networks: Overview and research directions≫. In: (gen. 2013), pp. 1–9.

[8] M. Rahnema. ≪Overview of the GSM system and protocol architecture≫. In: *IEEE Communications Magazine* 31.4 (1993), pp. 92–100. DOI: 10.1109/35.210402.

[9] Patrick Traynor. ≪On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core≫. In: (2009).