



UNIVERSITÀ
DEGLI STUDI
DI PADOVA



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:

Indice

1	Introduzione	4
1.1	Struttura del documento	4
1.2	Scopo della tesi	4
2	La rete cellulare	5
2.1	Definizione	5
2.2	Infrastruttura	5
2.3	Architettura	6
3	Generazioni cellulari	7
3.1	1G	7
3.2	2G	7
3.2.1	GSM	8
3.2.2	GPRS	8
3.2.3	EDGE	8
3.3	3G	8
3.3.1	UMTS	8
3.3.2	HSPA/HSPA+	8
3.4	4G	8
3.5	5G	8
4	Attacco Denial of Service	10
4.1	Definizione	10
4.2	Vulnerabilità nelle reti cellulari	10
4.3	Misurazione	10
5	Sistema di identificazione	11
5.1	2G	11
5.2	3G	11
5.3	4G	11
5.4	5G	11
6	Attacco alle reti UMTS	12
6.1	Funzionamento	12
6.2	Analisi dei risultati	12
7	Attacco alle reti 5G	13
7.1	Replicazione attacco	13
7.2	Altre vulnerabilità	13
8	Conclusioni	14

Elenco delle figure

1	Mappa compertura AT&T negli USA	5
2	Base station	5
3	Schema delle generazioni cellulari	7
4	Architettura 1G	7
5	Architettura GSM e GPRS	8
6	Architettura UMTS	8
7	Architettura LTE	9
8	Architettura 5G	9
9	Distributed Denial of Service	10

Elenco delle abbreviazioni

MS Mobile system. 11

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.

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 illustrate prevalentemente le sue proprietà architettureali oltre che le principali novità introdotte. Successivamente, verrà introdotta la tipologia dell'attacco trattato, ossia il *Denial of Service*, spiegando 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 pretesi 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 [2]. 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 [2] e scoprire se questo potrebbe risultare efficace 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.

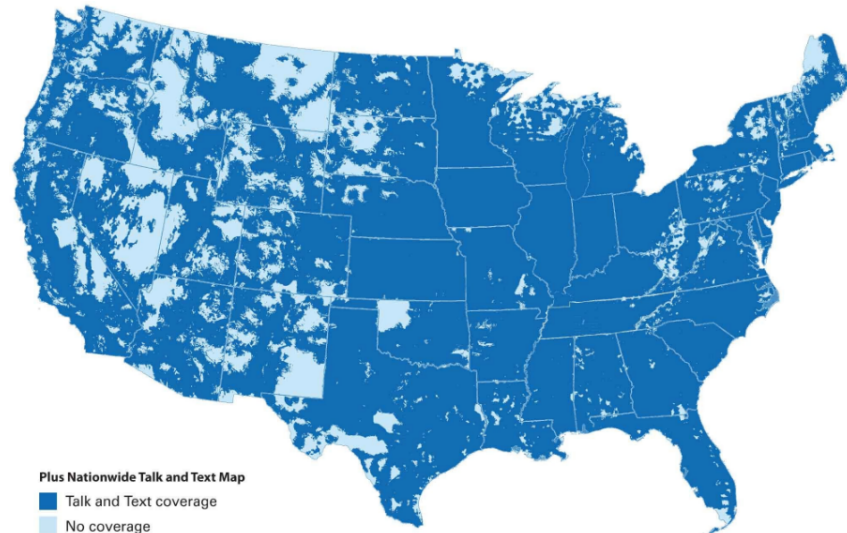


Figura 1: Mappa copertura AT&T negli USA

La loro struttura e architettura ha subito notevoli cambiamenti nel corso degli anni, nelle prossime sezioni si analizzeranno gli elementi fondamentali di una rete cellulare che qualsiasi generazione possiede.

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 2: Base station

Ogni cella ha un determinato raggio di azione determinato 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.

2.3 Architettura

L'architettura di una rete cellulare può essere risassunta con alcuni fondamentali componenti. La *mobile station* 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.











1G	2G	3G	4G	5G
				
speed in kilobit per second 2.4 Kbps	speed in kilobit per second 64 Kbps	speed in kilobit per second 2,000 Kbps	speed in kilobit per second 100,000 Kbps	speed in kilobit per second 1Gbps
Analog Voice	Digital Voice + Simple Data	Mobile Broadband	Faster and Better	Real World Applications
				

Figura 3: 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)

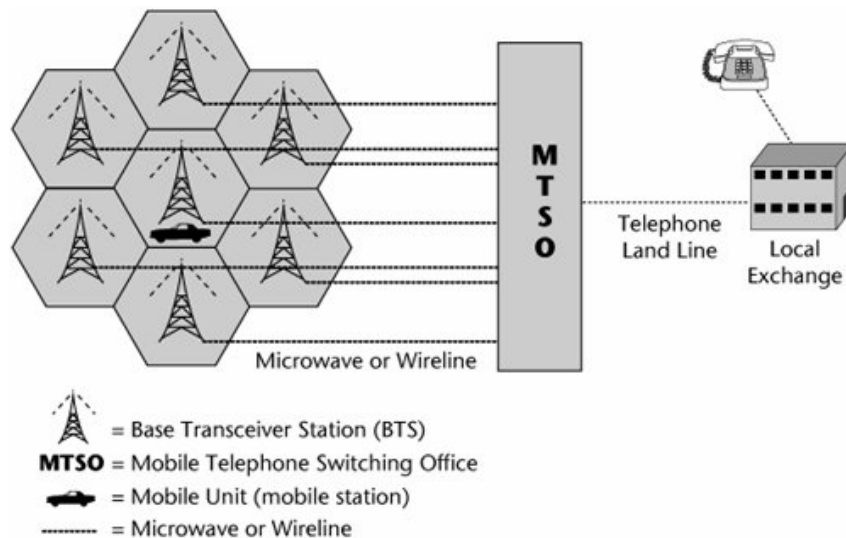


Figura 4: Architettura 1G

Si basava sulla *frequency-division multiple access* (FDMA) in cui ogni dispositivo che si connetteva alla stazione radio aveva assegnata una specifica sotto banda[3].

3.2 2G

La seconda generazione cellulare è composta da diverse versioni che si sono susseguite nel corso degli anni aggiungendo nuove funzionalità. La sua architettura verrà poi usata come base per le versioni successive. Il MS si collega alla BTS di riferimento

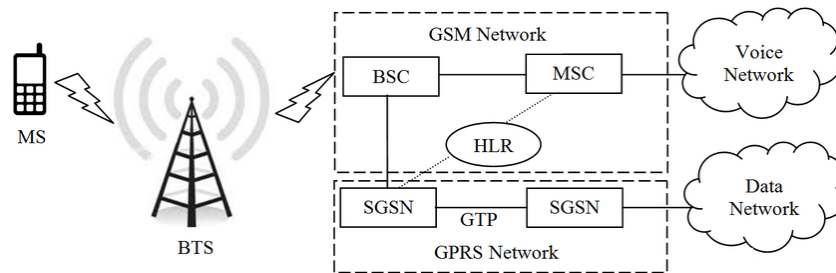


Figura 5: Architettura GSM e GPRS

3.2.1 GSM

3.2.2 GPRS

3.2.3 EDGE

Evoluzione del GPRS che consente maggiori velocità.

3.3 3G

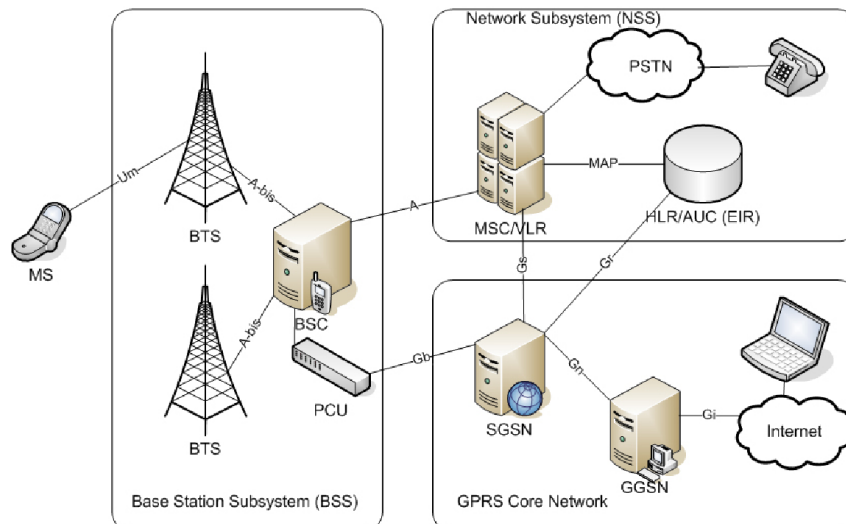


Figura 6: Architettura UMTS

3.3.1 UMTS

3.3.2 HSPA/HSPA+

3.4 4G

3.5 5G

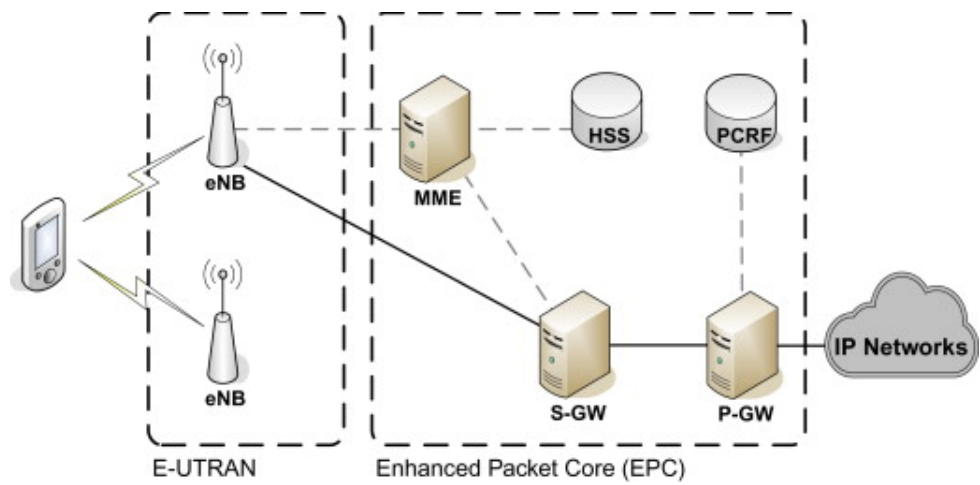


Figura 7: Architettura LTE

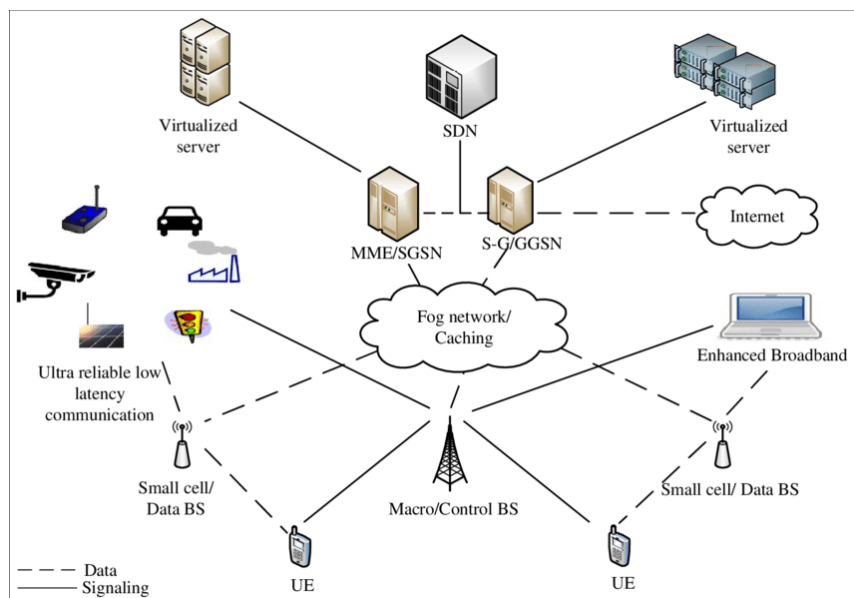


Figura 8: Architettura 5G

4 Attacco Denial of Service

4.1 Definizione

L'attacco di tipo *Denial of Service* (DOS) consiste nel rendere non disponibili servizi offerti da computer o altri dispositivi [1]. Questo avviene esasperando di richieste la macchina o infrastruttura che viene scelta come vittima. Le risorse della vittima verranno quindi interrogate in modo massivo fino al punto di indurre il sistema al collasso.

Una variante dell'attacco DOS è il *Distributed Denial of Service* (DDOS), in cui l'attaccante non è composto solamente da una sola macchina, ma bensì da una rete intera chiamata *botnet*. Questa seconda versione è più difficile da realizzare ma al tempo stesso molto più efficace. Solitamente, la *botnet* è composta dagli *zombies*, ovvero dispositivi di utenti normali ignari del fatto di essere stati infettati da un *malware* che consente all'attaccante di averne il controllo.

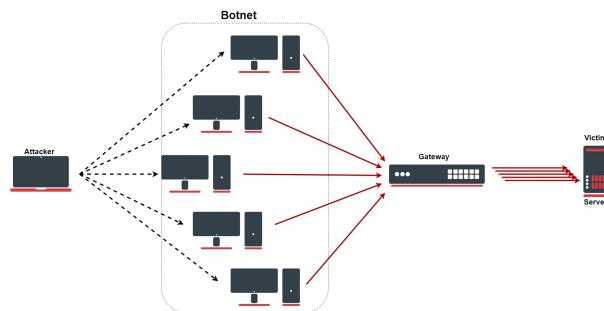


Figura 9: Distributed Denial of Service

4.2 Vulnerabilità nelle reti cellulari

Le reti cellulari non sono esenti da questo tipo di attacchi, anzi, sono una delle tipologie più frequenti e soprattutto 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. Nel caso delle reti cellulari, le maggiori criticità sono rilevate nei meccanismi di identificazione degli utenti, poichè durante queste procedure si è in grado di interrogare direttamente il *database* che contiene le informazioni degli utenti. Questo archivio, nel caso delle reti 2G/3G è l'*Home Location Register* (HLR), e rappresenta un punto critico all'interno del *core network* poichè viene costantemente interrogato per numerose motivazioni come il cambio di posizione del dispositivo connesso ossia *update location*. Inoltre, ad aggravare il suo carico di lavoro, è il numero di utenti che deve servire spesso molto alto poichè deve servire aree geografiche molto vaste.

4.3 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 sovraccarico di richieste.

In [4] vi è una dettagliata spiegazione di come procedere con queste misurazioni e soprattutto come quantificare il numero di dispositivi che servono all'attaccante per completare l'attacco con successo.

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.

5.1 2G

5.2 3G

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 UMTS

6.1 Funzionamento

L'attacco in questione si concentra nel sistema di identificazione trattato nella sezione precedente, ovvero l'HLR. Infatti, questo componente viene spesso interrogato durante molte fasi della connessione del dispositivo, in particolare durante l'aggiornamento della posizione ovvero il cosiddetto *update location*.

6.2 Analisi dei risultati

7 Attacco alle reti 5G

7.1 Replicazione attacco

7.2 Altre vulnerabilità

8 Conclusioni

Riferimenti bibliografici

- [1] Kevin Hattingh et al. «DoS! Denial of Service». In: ().
- [2] 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.
- [3] Fredrick Njoroge e Lincoln Kamau. «A Survey of Cryptographic Methods in Mobile Network Technologies from 1G to 4G». In: (nov. 2018).
- [4] Patrick Traynor. «On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core». In: (2009).