https://www.5gsting.com

5Gsting

Solution Against Fake Base Stations

Issue of Fake Base Station

- The issue of FBS aka “Fake Base Station” has been around since start of mobile networks

- PAST
  - Expensive to exploit; Voice tapping was main motive

- TODAY
  - Very easy to exploit; Multiple motives involving eavesdropping, tapping and manipulating of Data streams

Recent FBS related Attacks Coverage In Media

https://i.blackhat.com › USA-19 › Wednesday › u... PDF

New Vulnerabilities in 5G Networks - Black Hat

https://www.ericsson.com › blog

3GPP Release 15 and the battle against false base stations ...

The New York Times

Evidence of stingrays found in Washington, DC, Homeland ...

http://14.139.122.13 › jspui › bitstream › IJARCE... PDF

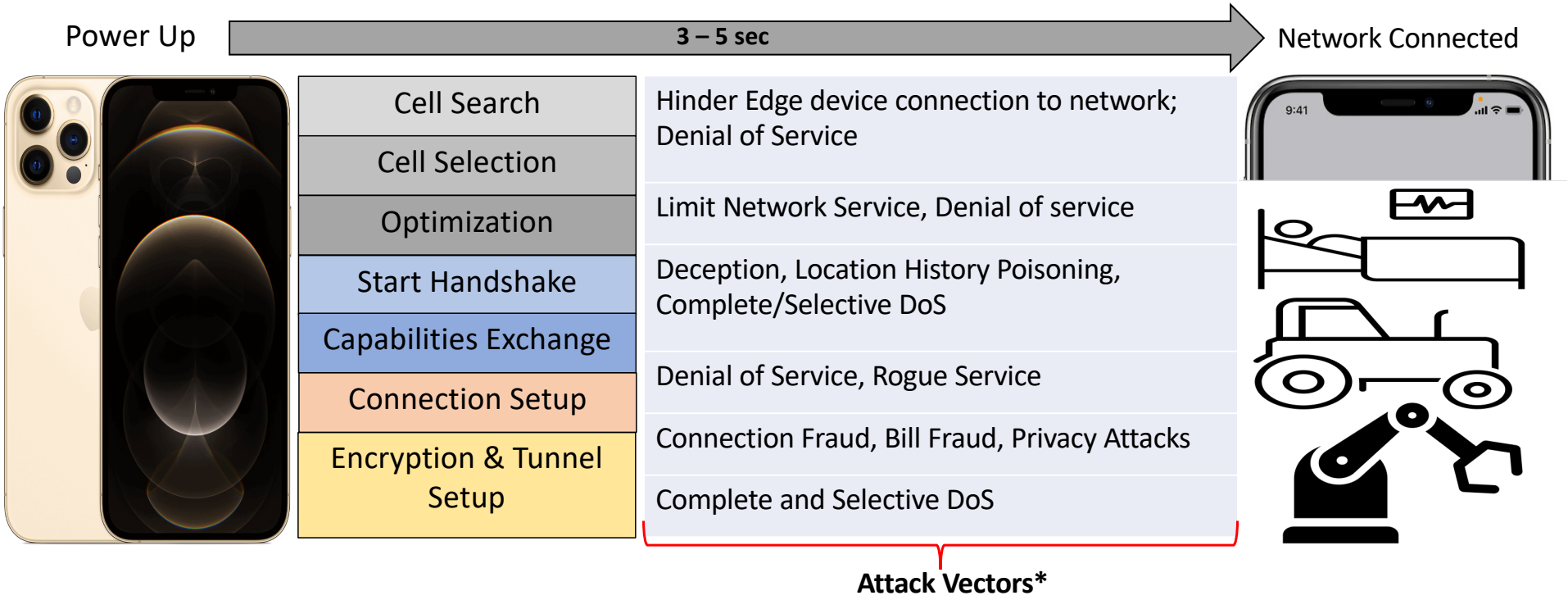
False base station attack in GSM Network Environment

DDoS attacks and 5G: everything you need to know

Michael Schachter | March 22, 2021

Only Few Days Ago

Attacks due to FBS across 4G, 5G [Before Encryption]



* True for **all Devices** using any Wireless Standards: 4G, 5G, LTE-M, NbIOT, V2X, WiFi using Fake Base Station/SDR

Why care NOW ??

			
TECHNOLOGY	2G, 3G	4G, 4G(Adv), 4G(Pro)	5G NR, 5G SA, mmWave, NbIOT, V2X
COMMON USAGE	Human to Human	Machine to Machine	Internet of Things
DEVICE TYPE	Mobile Phones mainly	Mobile Phones mainly, Emergence of Connected Devices	**By 2023*, 29.3 Billion Devices out of which 14.7 Billion devices will be M2M/IOT** (i.e. nearly 50% split)**
DIFFICULTY LEVEL TO DO FBS ATTACKS	Very Difficult & Very Expensive	Difficult and Very Expensive	**Easiest and Cheapest (SDR and Open Source)**

* Cisco Annual Report (2018-2023) White Paper

** A growing number of M2M applications, such as smart meters, video surveillance, healthcare monitoring, transportation, and package or asset tracking, are contributing in a major way to the growth of devices and connections. (Cisco Annual Report)

DEMO

A military video application leveraging Edge architecture has been developed:

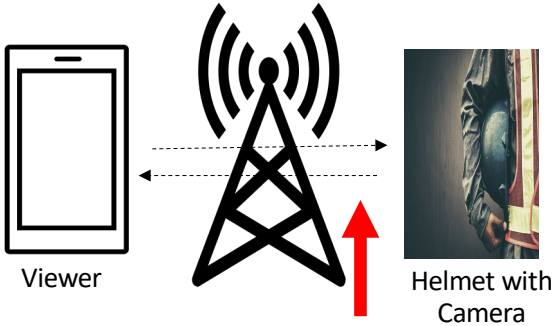
Edge Computing is used for

a. Frontline Soldier view (Instant processing of video feed from solider camera)
b. Platoon Leader view (Offering multiple feeds from different soldiers on front lines)

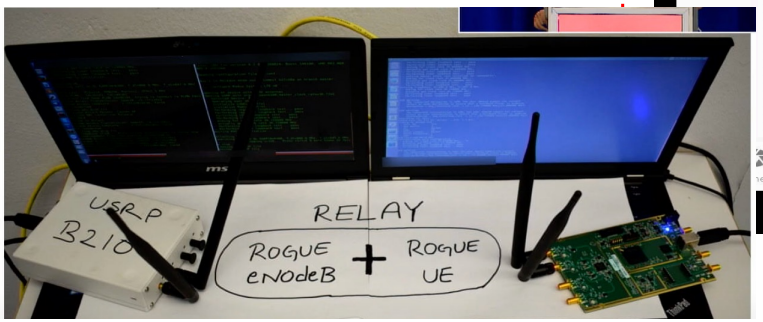
Traditional Datacenter

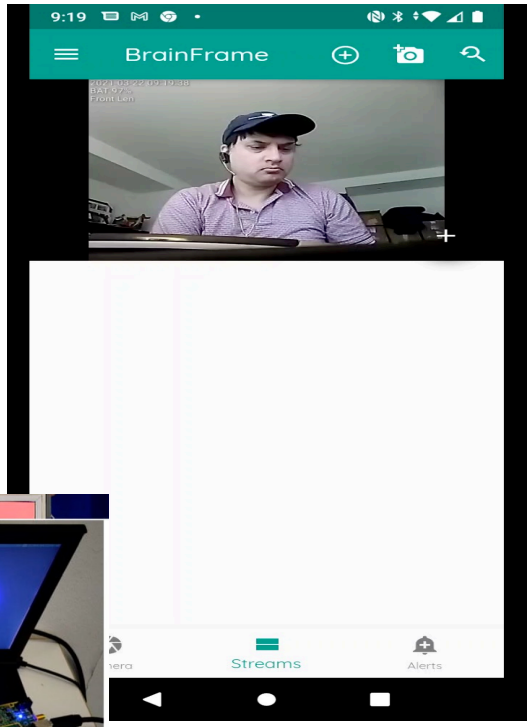
It is assumed that commander operations (offering feeds from multiple platoons) is done at Headquarters i.e., Outside of Edge Computing

OTA Edge Attack – Frontline Soldier View



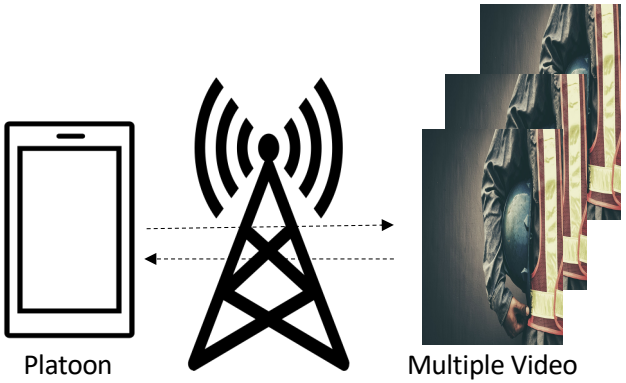
*** FBS Attacks / Jamming Attacks can happen to any IOT or military device(s)**



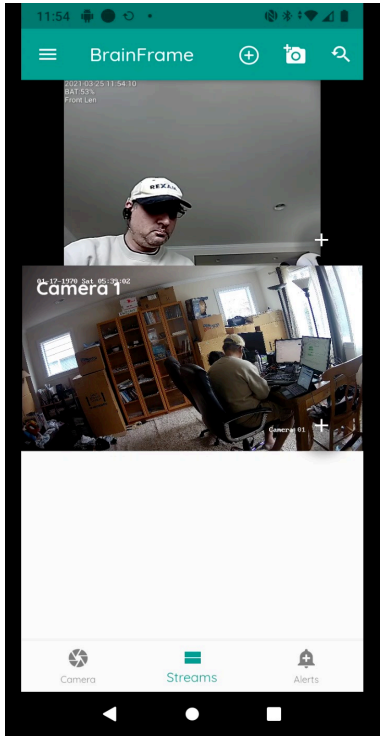


1. We have created an app called “Brainframe”; being used to view a LIVE feed from the edge IP camera device embedded in a military helmet
2. A telecom connection is being used for broadcast
3. An attacker tries to alter the video connection OTA
4. Our agent is embedded within the camera and upon detection displays the message on the stream

OTA Broadcast Attack – Platoon Leader View



Solution can detect infected feed(s) from multiple feeds



Double Click to PLAY video

5Gsting Solution and Architecture Details

Features	Delivery Model	STATUS
FCC Database; War Driving; Other Social Networks	SaaS Service w. thin client (AWS, GCP and Azure)	Fully Operational and Available at • Amazon Web Services Marketplace • Azure Web Services • Google Cloud Platform (Beta)
Inter-Agent; Inter-Networks Data Exchange		
Ability to Detect Fake Base Stations by L2 RIL (Radio Information Layer) Inspection*	Agent Installation	Current Support • Python • FreeRTOS + • AWS GreenGrass
Ability to Protect against Fake Base Stations Attacks*		

Lookup Service

Full Protection

* RIL inspection requires Radio Chipset Assessment

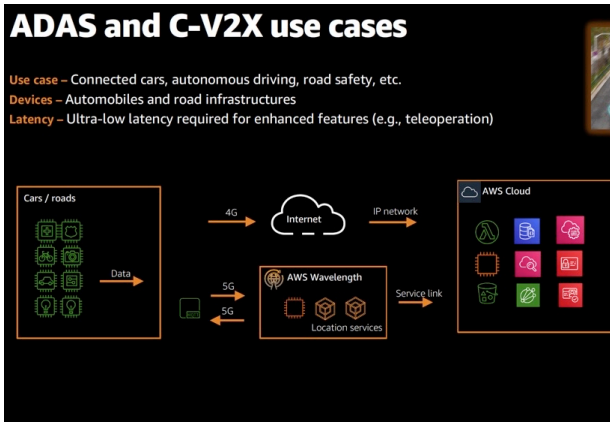
Features

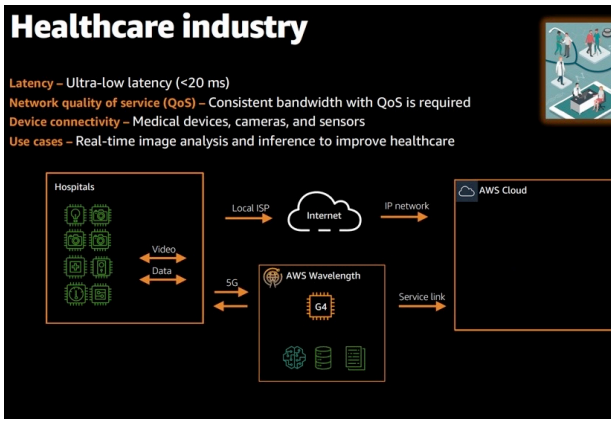
- ✓ Plug-n-play SaaS service (AWS, GCP, Azure)
- ✓ Small Footprint (few Kb)
- ✓ AI / ML based
- ✓ Detection and Protection against FBS
- ✓ Protection against SON poisoning
- ✓ Network detection (private LTE) of FBS
- ✓ Optimized Handover mechanism

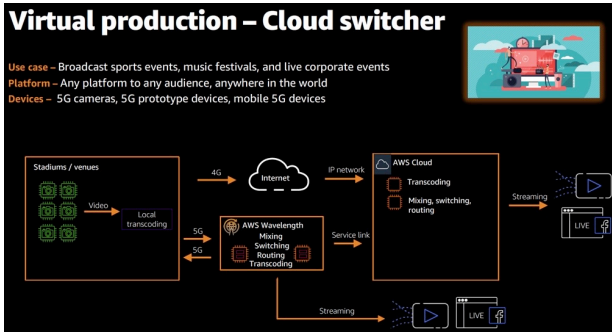
Reference Architecture

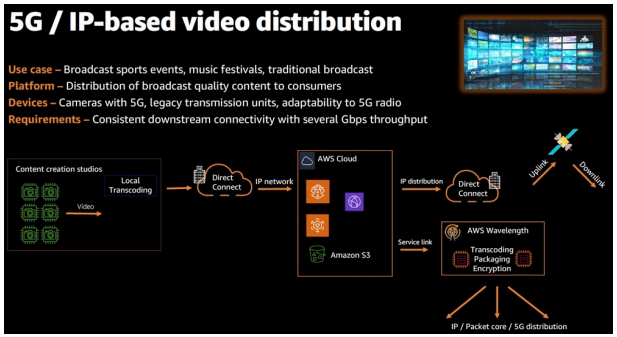
5G network will carry 35% of mobile traffic globally by 2024; 75% of enterprise-generated data will be created and processed outside a traditional data center by 2025

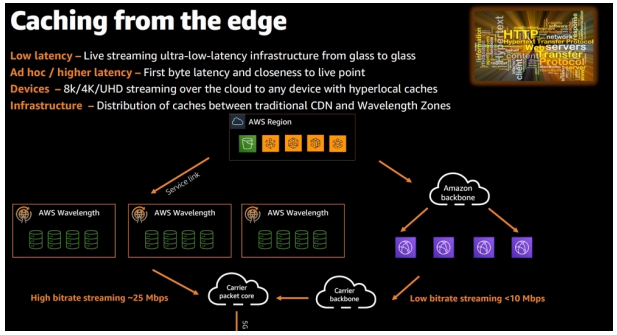
Machine Learning and Artificial intelligence are key ENABLERS



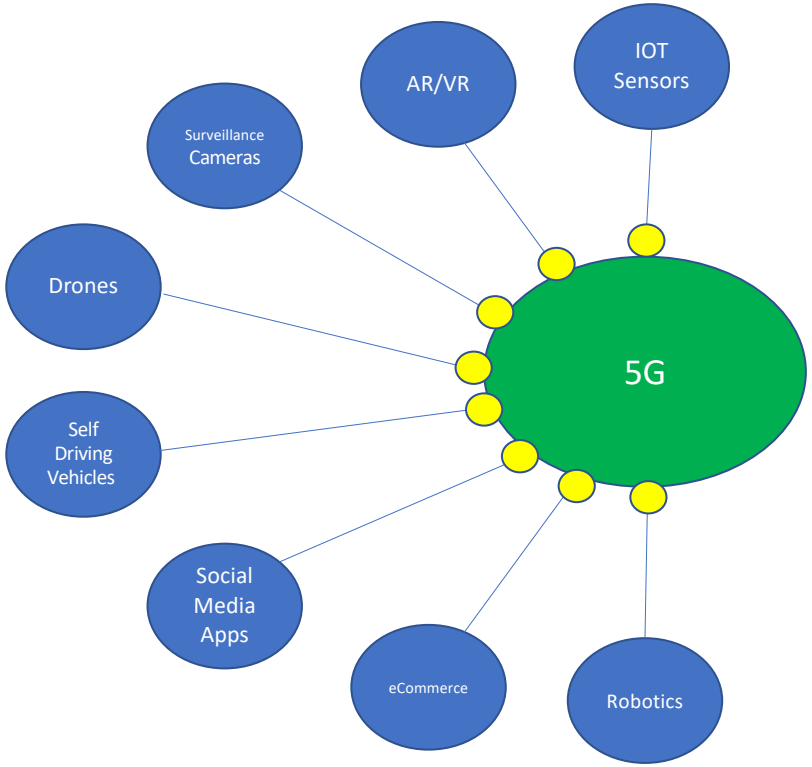








mmWave (USA Leading the way)



1. Vast Potential of 5G across multiple different sectors, geography and demographics
2. Reliance on Fast Data Transfer and service continuity
3. Zero Trust connections / VPN connections a possibility
4. However; ALL solutions need to connect & stay connected on to a trusted network.

Founders

- Founded August 2019, by x-Symantec and x-Microsoft folks
- Sudhanshu (Sid) Harshavat – Founder
  - 20+ yrs experience in Technology
  - Worked at Motorola, Symantec
  - Northwestern University, Masters in Wireless Communications
- Vikram Kapoor - Co-Founder
  - 25+ yrs experience in Technology
  - Worked at Motorola, Microsoft, T-Mobile
  - MBA, University of Chicago; MS in Wireless Communication (USF)

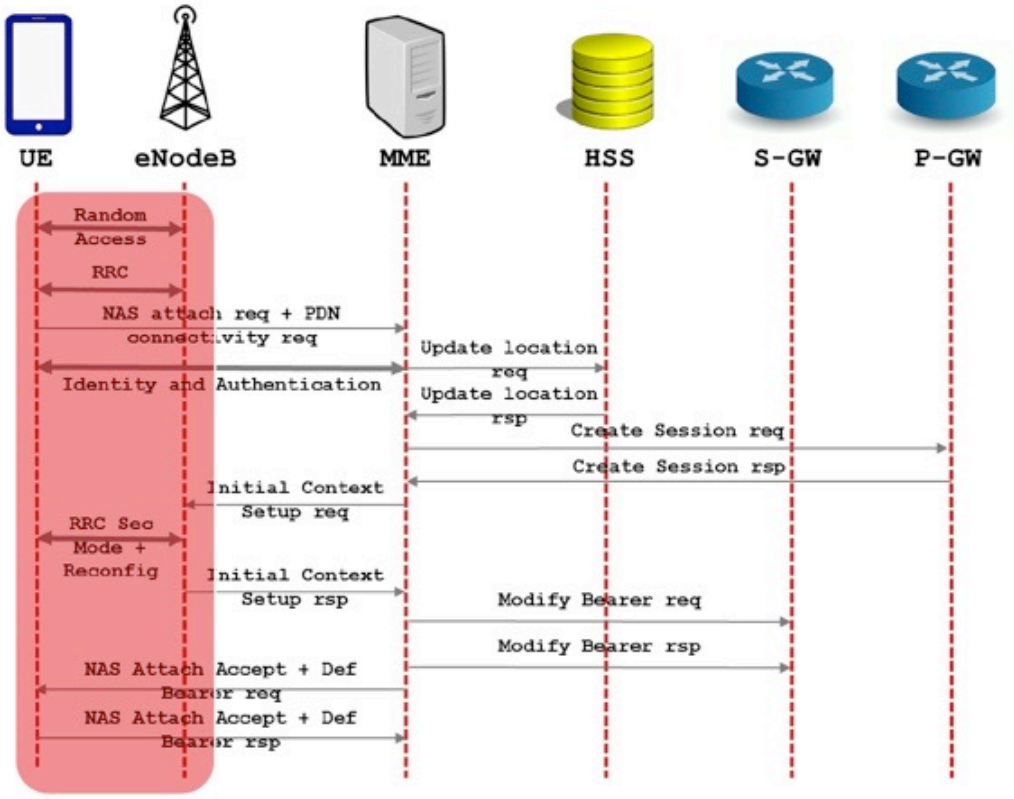
Appendix

Prone to Attacks

	GSMA	4G LTE	5G
Equipment Reqd.	$50K	$10K	$500
Level of Expertise	PH.D	MS / BS	High School
3GPP Security Focused Sub-groups	1	5-10	More than 60*
Attack Surface	Mobile to Mobile	Targeted Attacks	Enterprises*

Sources:
*3GPP TR 33.969: "Study on security aspects of Public Warning System (PWS)".
*3GPP TS 33.501: "Security architecture and procedures for 5G system"
*3GPP TS 36.331: "E-UTRA; Radio Resource Control (RRC); Protocol specification"
*Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2018. "On the Impact of Rogue Base Stations in 4G/LTE Self Organizing Networks"
*Study on 5G security enhancements against False Base Stations (FBS): Certificate based solution for Protecting System Information Messages with Digital Signature in an NPN. Roger Piqueras Jover (Under SoftHandover Consulting affiliation).

LTE ATTACH PROCEDURE



Issues in 4G

LTE ATTACH PROCEDURE

Name	Start time	DI/UI	Cell	Cell ID	Frame	Subf	RCE	Power	Length	Errs	Retrans	Decr	Valid	Sf RSSI	SINR
RACH	01:32:03.954999	U			440	1	-16.64	-57.98	0						16.64
MAC Random Access Response	01:32:03.958999	D			440	5	-16.41	-45.73	7	OK				-39.20	16.41
RRCConnectionRequest	01:32:03.964999	U			441	1	-23.85	-51.14	6	OK					23.85
RRCConnectionSetup	01:32:03.979999	D			442	6	-15.11	-42.21	26	OK				-38.72	15.11
RRCConnectionSetupComplete	01:32:04.013999	U			446	0			56	OK					
Attach Request	01:32:04.013999	U			446	0	-25.25	-49.36	53	OK					25.25
PDN Connectivity Request	01:32:04.013999	U			446	0	-25.25	-49.36	36	OK					25.25
DLInformationTransfer	01:32:04.088999	D			453	5			39	OK					
Authentication Request	01:32:04.088999	D			453	5	-15.00	-41.33	36	OK				-38.44	15.00
ULInformationTransfer	01:32:04.225999	U			467	2			22	OK					
Authentication Response	01:32:04.225999	U			467	2	-20.80	-53.66	19	OK					20.80
DLInformationTransfer	01:32:04.267999	D			471	4			17	OK					
Security Protected NAS Message	01:32:04.267999	D			471	4	-15.52	-44.04	14	OK		Not...	No...	-39.22	15.52
Security Mode Command	01:32:04.267999	D			471	4	-15.52	-44.04	8	OK				-39.22	15.52
ULInformationTransfer	01:32:04.285999	U			473	2			22	OK					
Security Protected NAS Message	01:32:04.285999	U			473	2	-22.49	-52.16	19	OK		No...	No...		22.49
Unknown NAS	01:32:04.285999	U			473	2	-22.49	-52.16	13	OK					22.49
DLInformationTransfer	01:32:04.327999	D			477	4			12	OK					
Security Protected NAS Message	01:32:04.327999	D			477	4	-14.73	-45.68	9	OK		No...	No...	-39.27	14.73
Unknown NAS	01:32:04.327999	D			477	4	-14.73	-45.68	3	OK				-39.27	14.73
ULInformationTransfer	01:32:04.345999	U			479	2			24	OK					
Security Protected NAS Message	01:32:04.345999	U			479	2	-21.36	-53.39	21	OK		No...	No...		21.36
Unknown NAS	01:32:04.345999	U			479	2	-21.36	-53.39	15	OK					21.36
SecurityModeCommand	01:32:04.472999	D			491	9			3	OK					
Ciphered RRC	01:32:04.495999	U			494	2			2	OK		No...	No...		
Ciphered RRC	01:32:04.501999	D			494	8			3	OK		No...	No...		
Ciphered RRC	01:32:04.515999	U			496	2			18	OK		No...	No...		
Ciphered RRC	01:32:04.536999	D			498	3			165	OK		No...	No...		
Ciphered RRC	01:32:04.575999	U			502	2			2	OK		No...	No...		
Ciphered RRC	01:32:04.575999	U			502	2			16	OK		No...	No...		
Ciphered RRC	01:32:04.604999	D			505	1			30	OK		No...	No...		
Ciphered data	01:32:14.426997	U			463	3			96	OK		No...			
Ciphered data	01:32:14.475997	U			468	2			40	OK		No...			
Ciphered data	01:32:14.513997	U			472	0			96	OK		No...			

RACH handshake between UE and eNB

RRC handshake between UE and eNB

Connection setup (authentication, set-up of encryption, tunnel set-up, etc)

Encrypted traffic

LTE (IN)SECURITY REDUX

IntelliJudge

Count	Name	Start time	DI/UI	Cell ID	Frame	RNTI	RCE	Power	Errs
1	RACH	00:04:42.942818	U		651		-6.42	-64.65	
2	MAC Random Access Response	00:04:42.946818	D		651		-8.50	-45.23	OK
3	RRCConnectionRequest	00:04:42.952818	U		652		-19.19	-56.46	OK
4	RRCConnectionSetup	00:04:42.967818	D		653		-9.07	-43.18	OK
5	RRCConnectionSetupComplete	00:04:43.001818	U		657				OK
6	Attach Request	00:04:43.001818	U		657				OK
7	PDN Connectivity Request	00:04:43.001818	U		657		-17.59	-60.11	OK
8	DLInformationTransfer	00:04:43.080818	D		664				OK
9	Authentication Request	00:04:43.080818	D		664		-8.86	-42.27	OK
10	ULInformationTransfer	00:04:43.213818	U		678				OK
11	Authentication Response	00:04:43.213818	U		678		-12.51	-65.43	OK
12	DLInformationTransfer	00:04:43.258818	D		682				OK
13	Security Protected NAS Message	00:04:43.258818	D		682		-8.90	-44.51	OK
14	Security Mode Command	00:04:43.258818	D		682		-8.90	-44.51	OK
15	ULInformationTransfer	00:04:43.273818	U		684				OK
16	Security Protected NAS Message	00:04:43.273818	U		684		-11.14	-64.93	OK
17	Unknown NAS	00:04:43.273818	U		684		-11.14	-64.93	OK
18	DLInformationTransfer	00:04:43.318818	D		688				OK
19	Security Protected NAS Message	00:04:43.318818	D		688		-8.88	-45.69	OK
20	Unknown NAS	00:04:43.318818	D		688		-8.88	-45.69	OK
21	ULInformationTransfer	00:04:43.333818	U		690				OK
22	Security Protected NAS Message	00:04:43.333818	U		690		-11.82	-63.66	OK
23	Unknown NAS	00:04:43.333818	U		690		-11.82	-63.66	OK
24	SecurityModeCommand	00:04:43.451818	D		702				OK
25	Ciphered RRC	00:04:43.479818	D		704				OK
26	Ciphered RRC	00:04:43.503818	U		707				OK
27	Ciphered RRC	00:04:43.524818	D		709				OK
28	Ciphered RRC	00:04:43.563818	U		713				OK
29	Ciphered RRC	00:04:43.563818	U		713				OK
30	Ciphered RRC	00:04:43.594818	D		716				OK
31	Ciphered data	00:04:52.021817	D		535				OK
32	Ciphered data	00:04:52.021817	D		535				OK
33	Ciphered data	00:04:52.113817	U		544				OK
34	Ciphered data	00:04:52.153817	U		548				OK

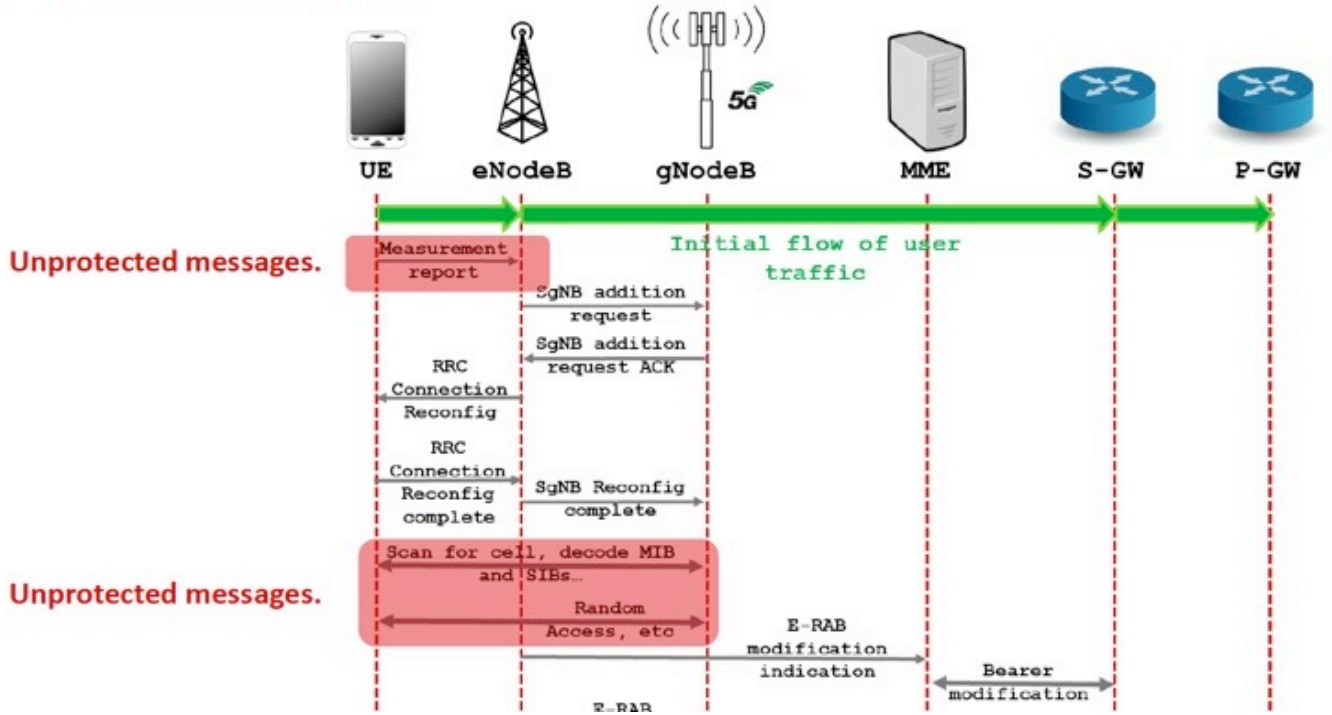
Unencrypted and unprotected. These messages can be intercepted and spoofed with open-source tools and low-cost radios

Other things sent in the clear:

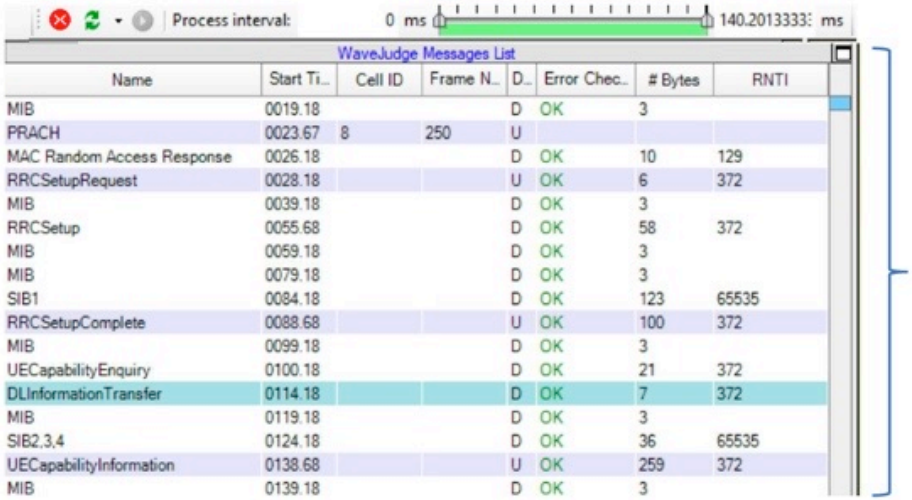
- Base station config (broadcast messages)
- Measurement reports
- Measurement report requests
- (Sometimes) GPS coordinates
- HO related messages
- Paging messages
- Etc

5G NSA ATTACH PROCEDURE

- Then switch 5G-NR RAN…



5G NSA ATTACH PROCEDURE



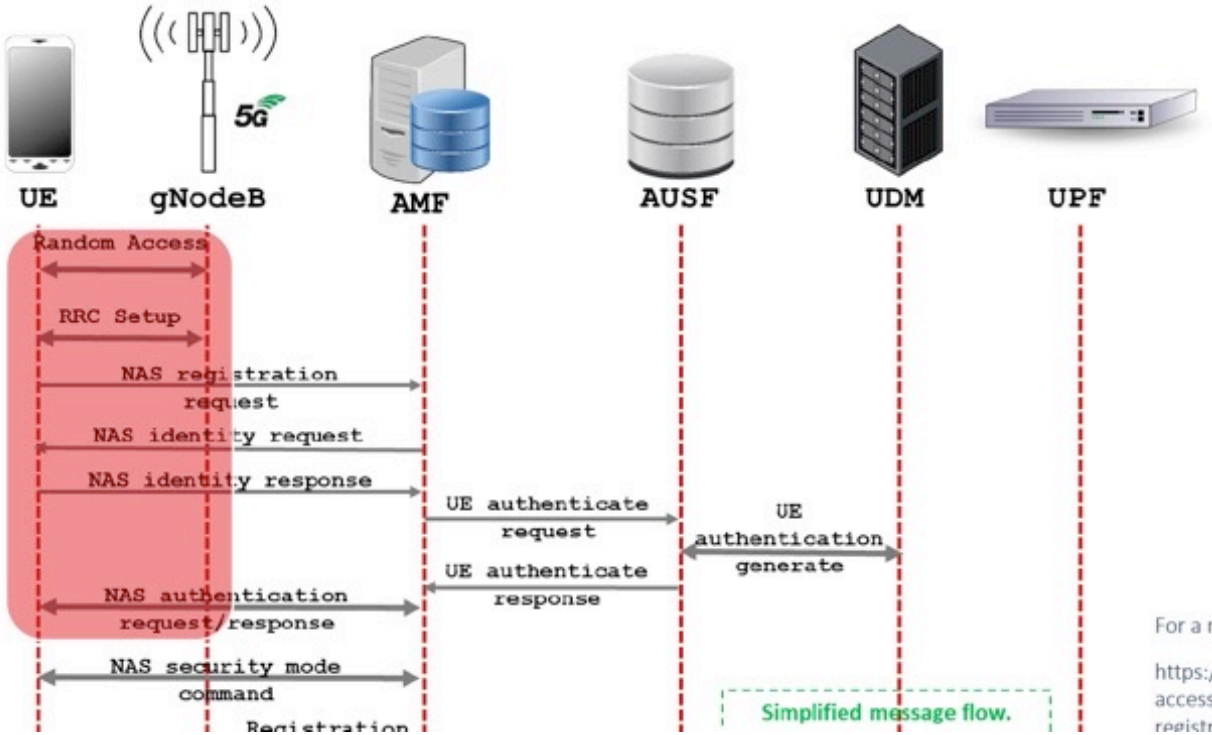
Name	Start Ti...	Cell ID	Frame N...	D...	Error Chec...	# Bytes	RNTI
MIB	0019.18			D	OK	3	
PRACH	0023.67	8	250	U			
MAC Random Access Response	0026.18			D	OK	10	129
RRCSetupRequest	0028.18			U	OK	6	372
MIB	0039.18			D	OK	3	
RRCSetup	0055.68			D	OK	58	372
MIB	0059.18			D	OK	3	
MIB	0079.18			D	OK	3	
SIB1	0084.18			D	OK	123	65535
RRCSetupComplete	0088.68			U	OK	100	372
MIB	0099.18			D	OK	3	
UECapabilityEnquiry	0100.18			D	OK	21	372
DLInformationTransfer	0114.18			D	OK	7	372
MIB	0119.18			D	OK	3	
SIB2,3,4	0124.18			D	OK	36	65535
UECapabilityInformation	0138.68			U	OK	259	372
MIB	0139.18			D	OK	3	

Unencrypted and unprotected. These messages can be intercepted and spoofed.

Other things sent in the clear:

- Base station config (broadcast messages)
- Some measurement reports
- Some measurement report requests
- Paging messages
- Etc

5G SA ATTACH PROCEDURE

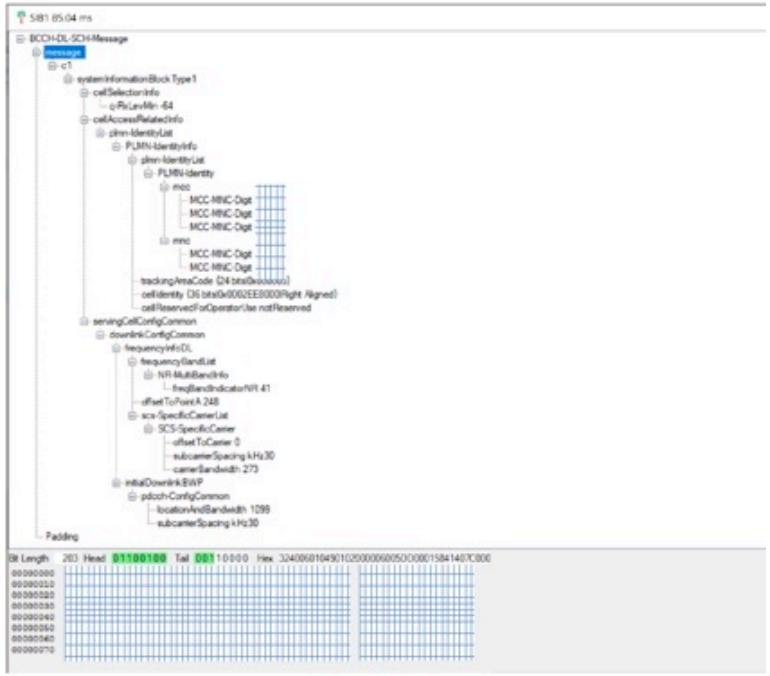


Unprotected messages.

For a mo
https://
access-r
registrat

SNIFFING 5G BASE STATION CONFIGURATION

- Capturing MIB and SIB broadcast messages
  - Identify base stations of a given operator
  - Identify ad-hoc base stations for first responders, etc
  - Optimal TX power for rogue base station
  - High priority frequencies
  - Etc
- Configure a rogue base station
- In all fairness, this is a very hard problem to solve



5G SIB1 message