

dAuth - Decentralizing LTE Authentication and Roaming

Sudheesh Singanamalla, Esther Jang, Nick Durand, Matthew Johnson, Spencer Sevilla, Kurtis Heimerl

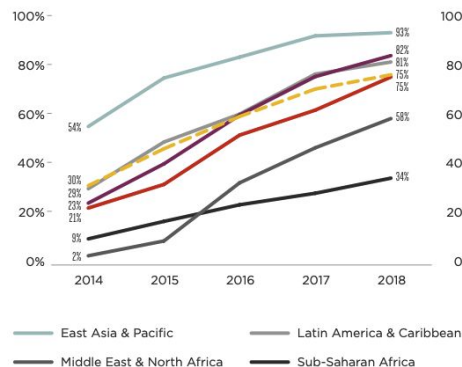
University of Washington, Seattle

The Case for Rural Community Networks and Rural Connectivity

- ~1 Billion people live outside mobile broadband coverage
- 400 Million people live outside any mobile coverage
- Telecom operators have rolled out 2G/3G networks as far as economically and commercially viable.

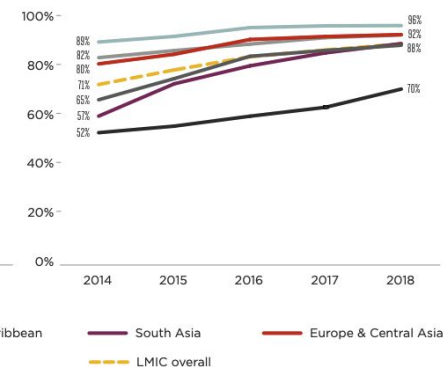
4G network coverage in LMICs

Base: Total population



3G network coverage in LMICs

Base: Total population



Rural Community Networks

Advantages:

- Built by and for their users
- Run cooperatively
- Optimized for local needs
- Sustainable in rural areas
- Leverages local resources
- Provides local services



Rural Community Networks

Constraints:

- Backhaul satellite connectivity
- Localized Radius of connectivity
- Intermittent power supply



“ *Why can't Telcos set up infrastructure and improve connectivity in rural areas? What happens when users in community cellular networks move outside network range?* ”

Challenges with Traditional LTE Networks

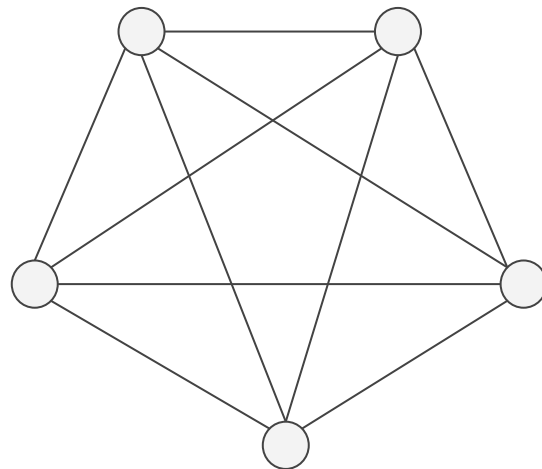
- Not economically viable to extend and deploy infrastructure to remote rural areas.
- Primarily profit driven and cannot cater to local desires (eg. free calls within communities)
- Roaming between telecom operators is a business decision, managed by physical agreements between network operators

Exponential Complexity of Roaming Agreements

Every single large telecom operator needs to have a roaming agreement with *at least* with one mobile network in each country to allow their users to roam.

(Many countries still do not allow national roaming)

This might only be possible for large telcos like Verizon/AT&T/T-Mobile.



“ *Can we provide Cellular data access in rural remote areas?*

Can we enable these users to roam between different communities?

Primer into LTE Networks

- A. LTE Network is called an Evolved Packet System (EPS) and is an end-to-end all IP network comprising of 2 parts
 - a. E-UTRAN (Radio Access Network)

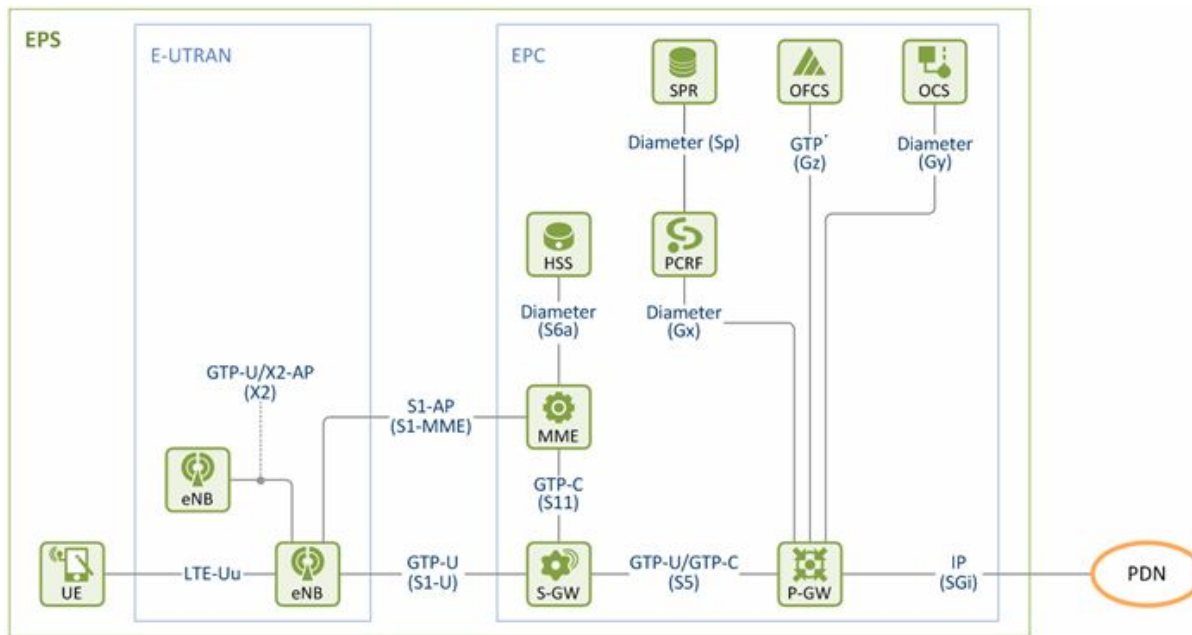


Primer into LTE Networks

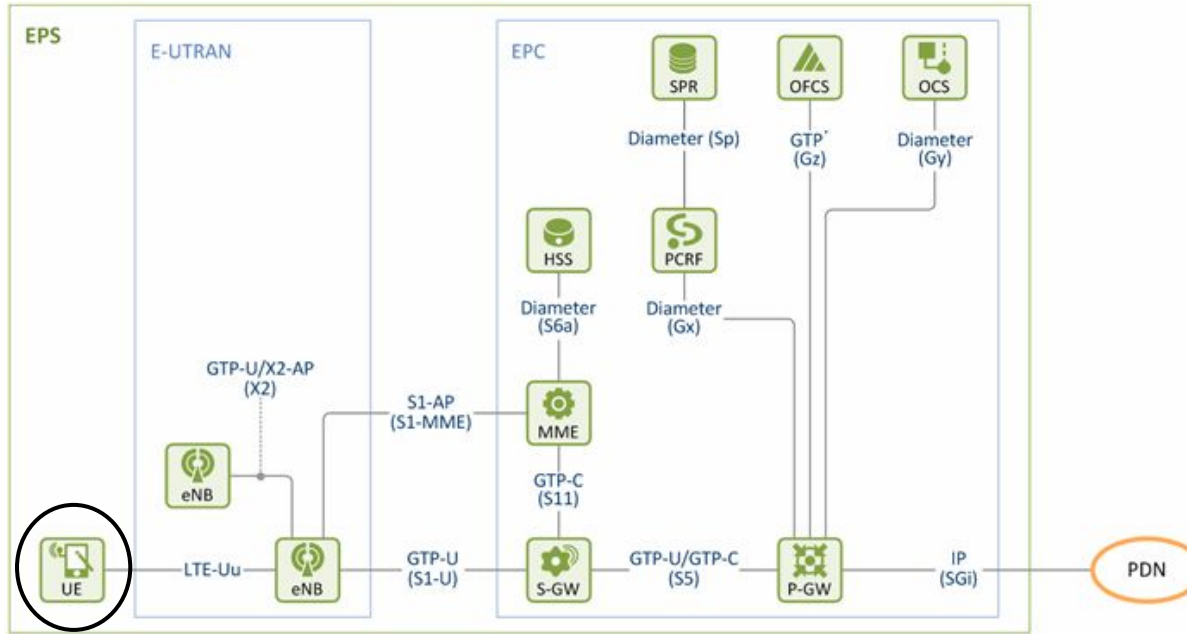
- A. LTE Network is called an Evolved Packet System (EPS) and is an end-to-end all IP network comprising of 2 parts
 - a. E-UTRAN (Radio Access Network)
 - b. Enhanced Packet Core Network



LTE Network Reference Architecture



LTE Network Architecture : User Equipment

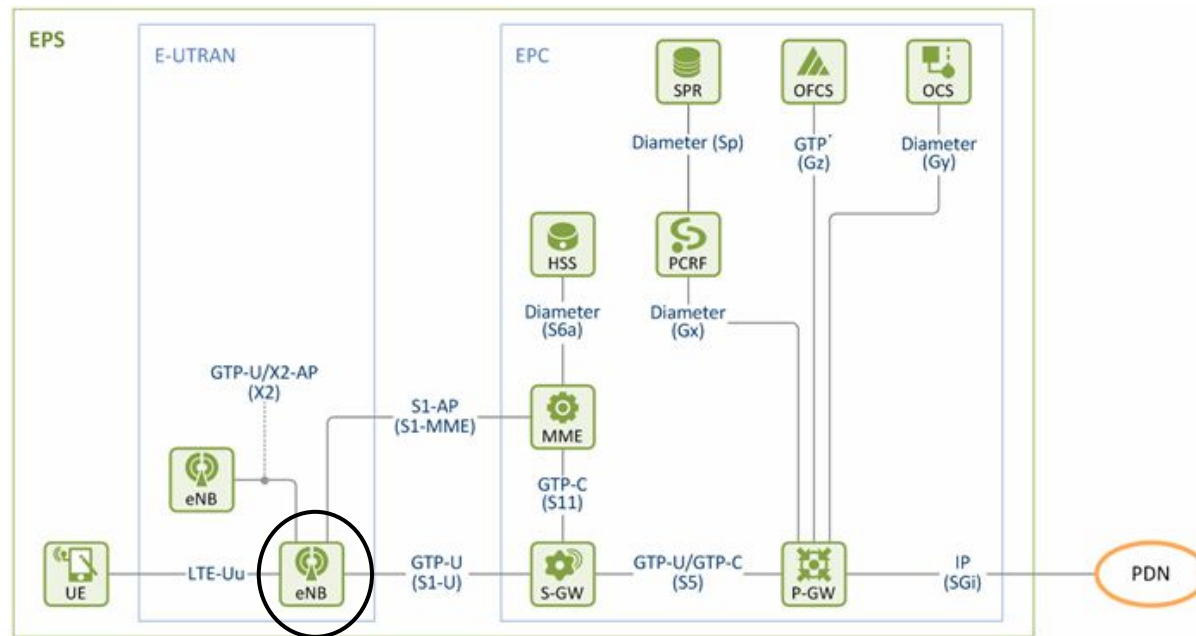


User Equipment

UE or User Devices are the wide array of LTE compatible devices which are available with the users and comply to the 3GPP standard.



LTE Network Architecture : eNB (Base Station)

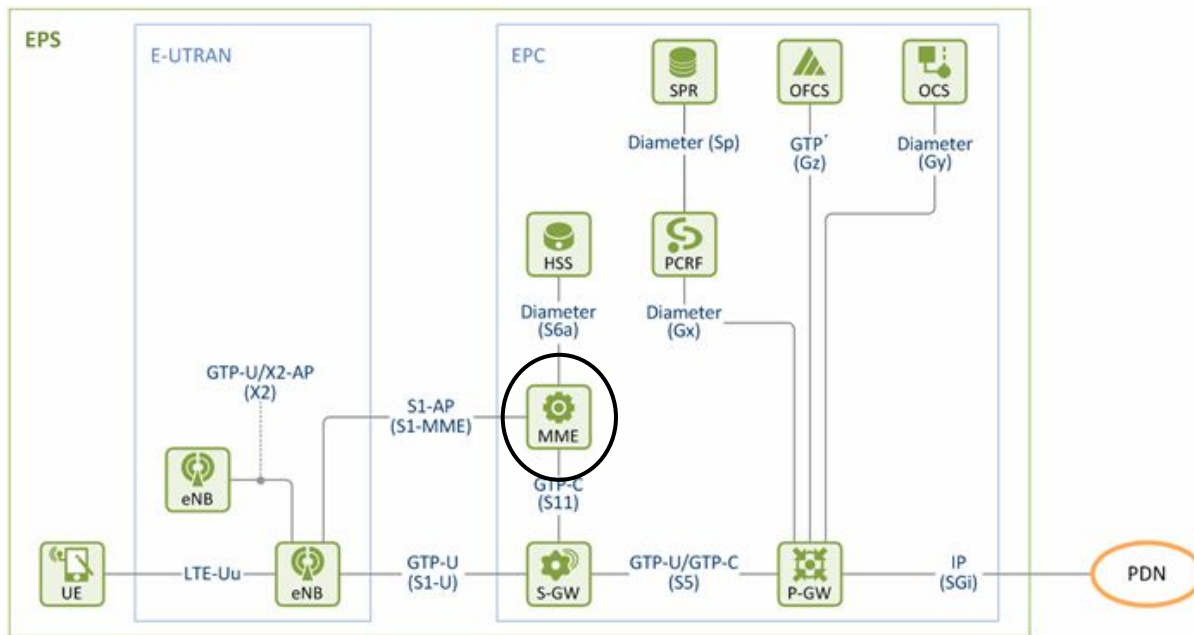


eNode B (eNB)

Provides the radio link interface and performs radio resource management and scheduling along with cell interference coordination.



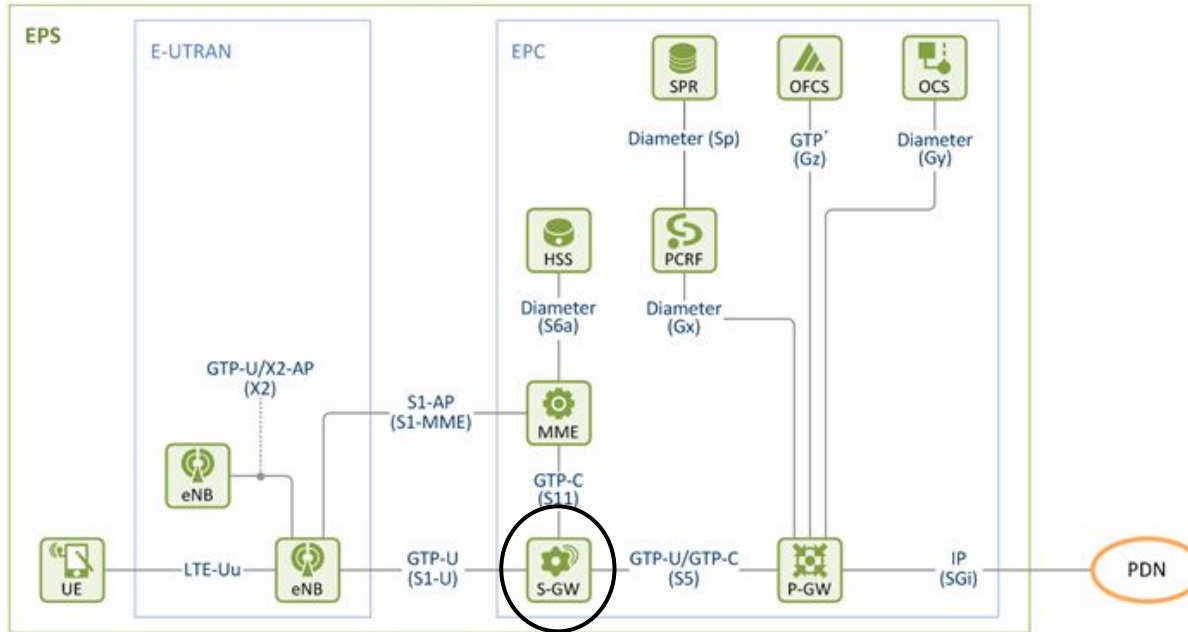
LTE Network Architecture : Mobility Management



MME

Performs necessary roles in User Authentication, signaling along with session and mobility management. (eg cell tracking, handover management etc..)

LTE Network Architecture : Serving Gateway

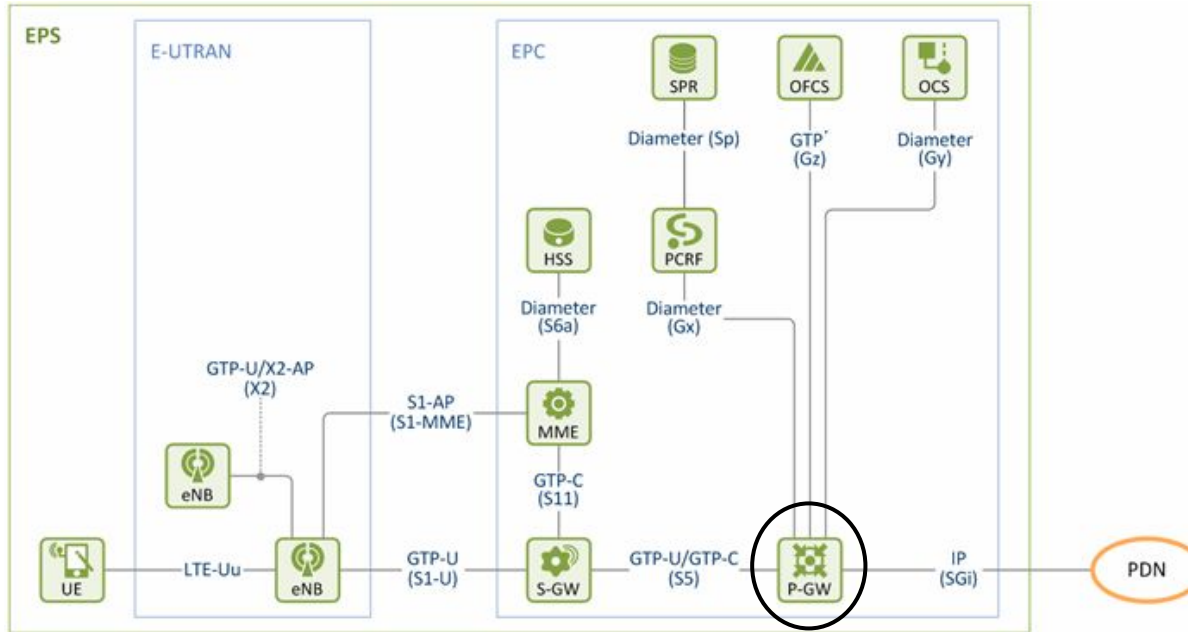


Serving Gateway (S-GW)

Routes and forwards user data packets and allows traffic management between LTE and other 2G/3G systems to P-GW.

Manages and stores state/context of different UEs

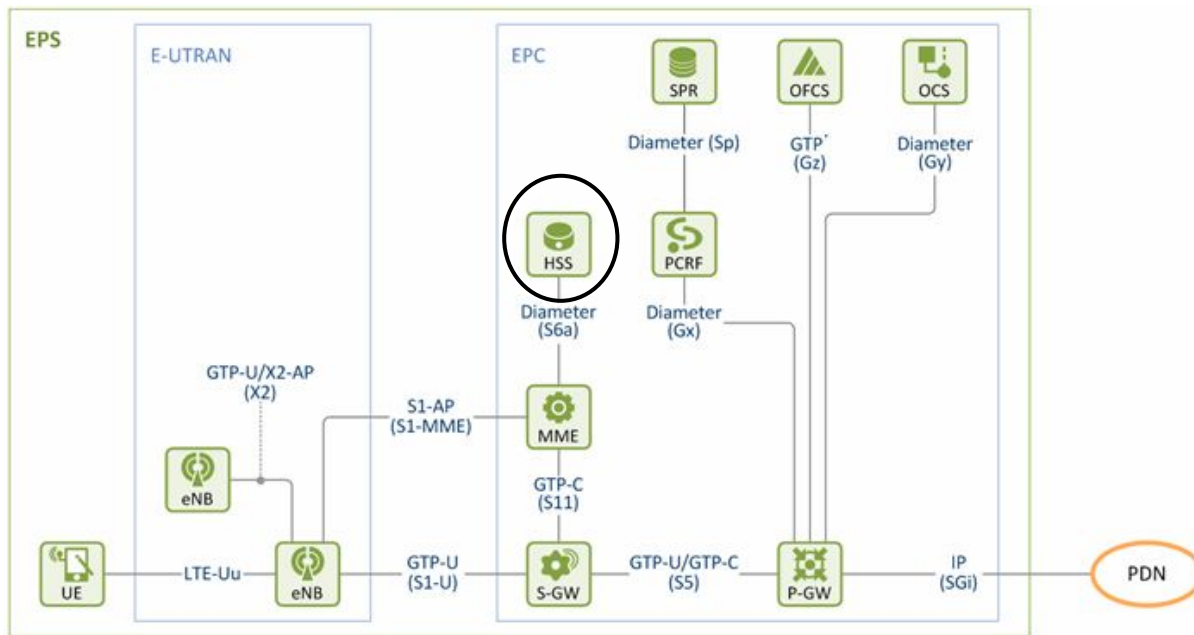
LTE Network Architecture : Packet Data n/w Gateway



Packet Data Network Gateway (P-GW)

PDN Gateway that provides connectivity from the UE to external packet data networks (Internet) and performs policy enforcement and lawful interception, packet screening.

LTE Network Architecture : Home Subscriber Server



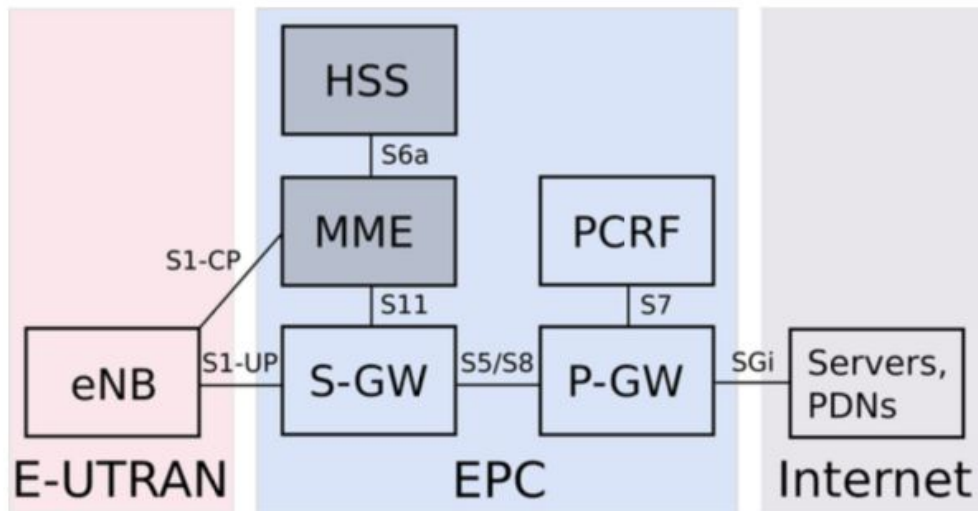
HSS

Central Database that contains user related and subscription related information such as SIM card keys, type of subscription, data limits, etc.,

Stripping down LTE Network Architecture



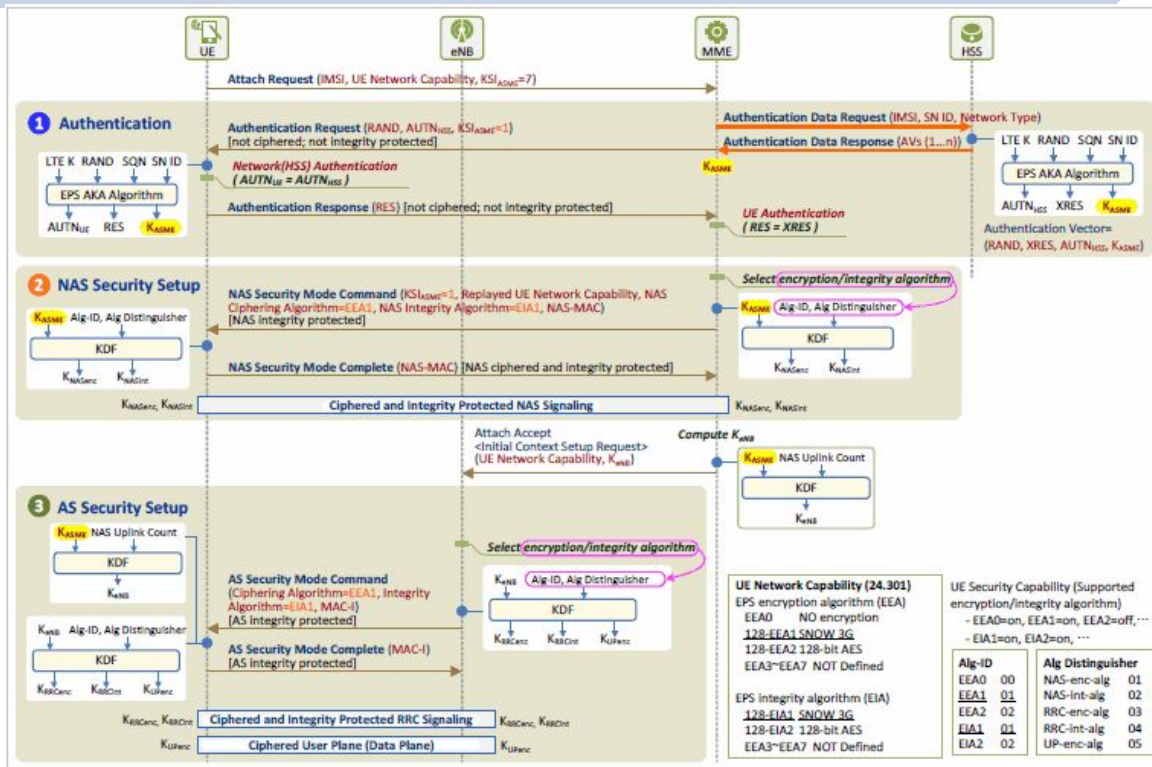
Open5Gs - An open source implementation of EPC



Moves the data center EPC to the edge!

Cheapest computer we could buy. Currently is actively running in **Bokondini, Indonesia** supporting **hundreds** of active users

Traditional LTE Authentication



Authentication: Check if the user device with the SIM card is actually owned by the network which it is trying to connect to.

Bidirectional authentication

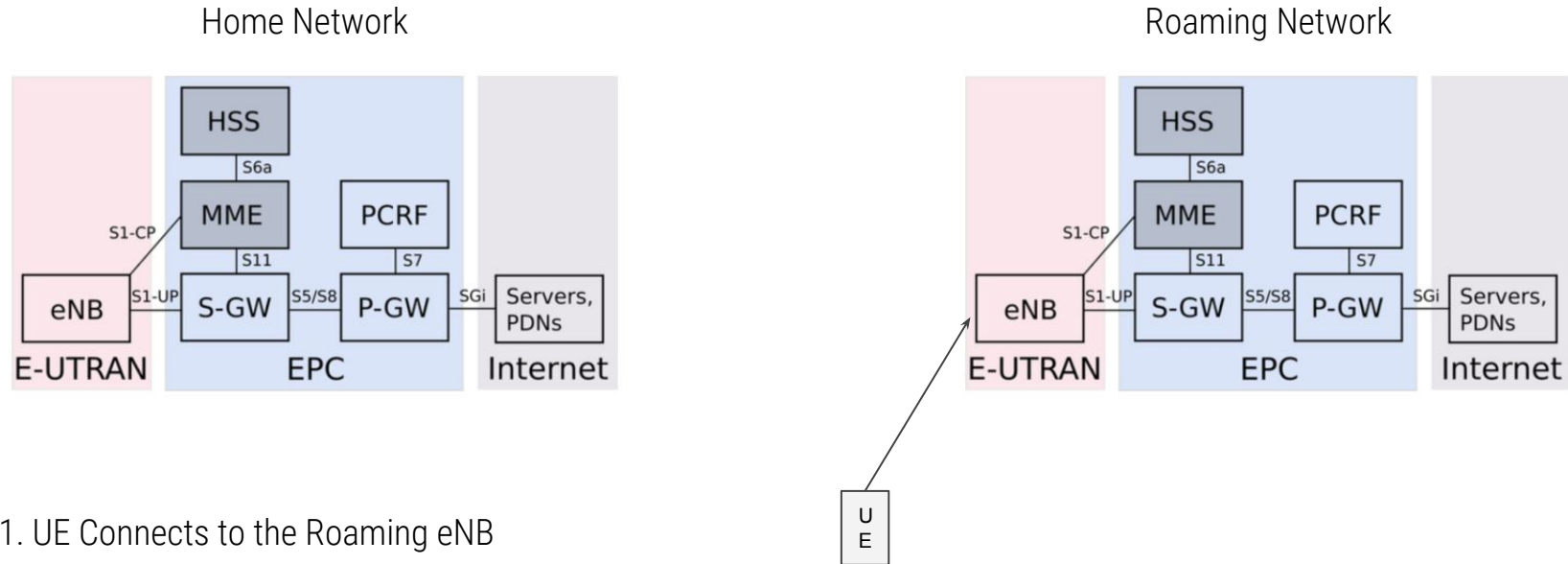
1. UE authenticates and validates the network
2. Network authenticates and validates the UE

Technical Complexities of Roaming

Telecom operators perform roaming in multiple ways posing different challenges:

1. The roaming core network requests subscribers' home network for necessary authentication values needing reliable connectivity between operators.
 - a. Users experience higher latencies since all requests are tunnelled home.
2. The symmetric key and state corresponding to the user could be exchanged between operators over an encrypted channel.
 - a. Raises security concerns

Current Roaming Practices - Fully connected networks

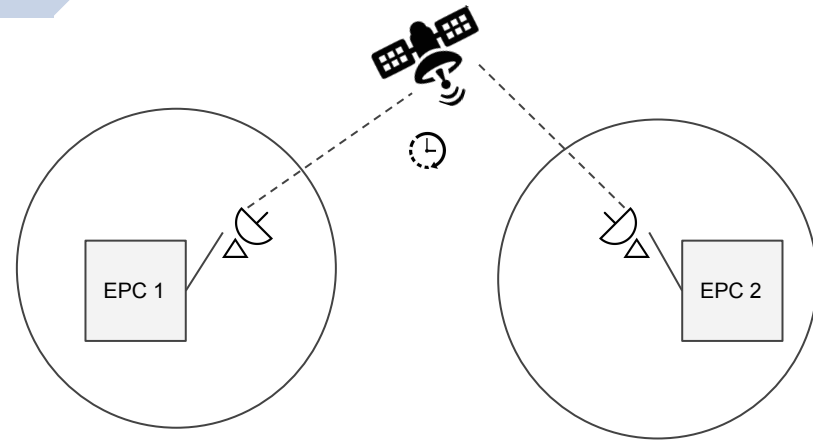




Current Roaming Practices - Fully connected networks

Challenges/Limitations:

- The EPC cores need to be fully available for allowing roaming users to connect to the network
- All the network traffic is tunneled from the roaming EPC to the Home EPC resulting in higher latencies for data usage
- The architecture would not work in disconnected settings like in community cellular networks challenged by power outages, failure of backhaul connectivity

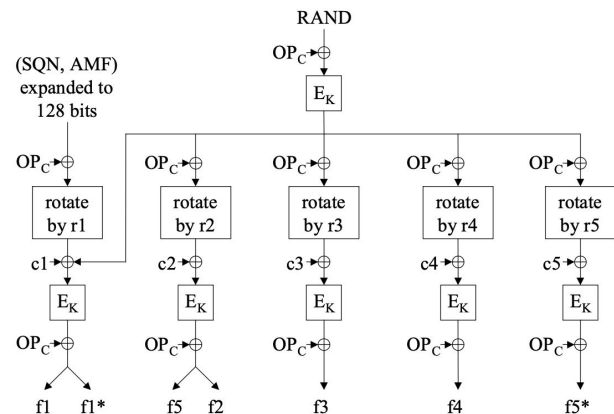
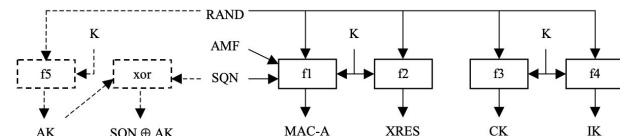


SIM Cards & Milenage

- Inexpensive to manufacture / get SIM cards printed
- Standardized authentication algorithms (**Milenage**) using symmetric key AES 128 bit encryption.

SIM Cards and HSS contain the following to make authentication happen using symmetric key cryptography:

- Symmetric key (K)
- AMF (Authentication Management Field)
- SEQ (Sequence Number)
- IMSI (International Mobile Subscriber Identity)



Definition of f1, f1*, f2, f3, f4, f5 and f5*

SIM Sequences and SQN construction from SEQ

- 4 Octet sequences which are single use and monotonically increasing
 - $SQN = SEQ \text{ (27 bits)} + IND \text{ (5 bits)}$

The SQN state is maintained in the HSS database.

SIM Cards use the SEQ numbers from a specific row as sequence numbers

Usage of a SEQ invalidates unused SEQ values before that in a given row.

0	32	64
1	33	65
2	34	66
...
31	63	95

Milenage Function outputs

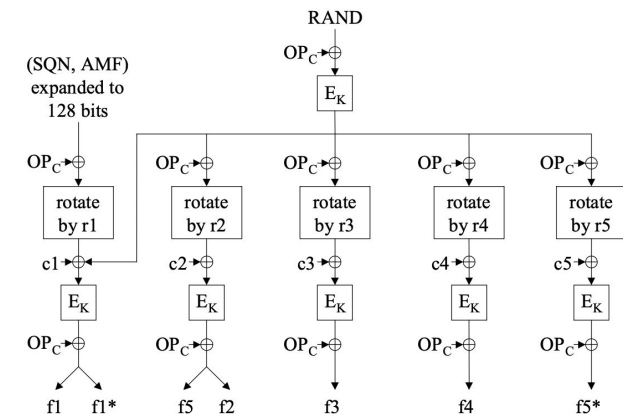
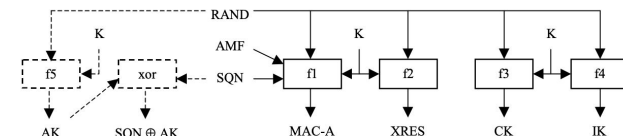
- **f1**: Computes MAC_A
- **f2345**: Computes $XRES, CK, IK, AK$
- **KDF**: Computes K_{asme} from
 - $IMSI, SQN, PLMN, CK, IK, RAND$

Integrity Algorithms [IK]:

- 0000 : EIA0 Null Integrity Protection Algorithm
- 0001 : 128-EIA1 SNOW 3G
- 0010 : 128-EIA2 AES

Cipher Algorithms [CK]:

- 0000 : EEA0 Null Ciphering Algorithm
- 0001 : 128-EEA1 SNOW 3G based algorithm
- 0010 : 128-EEA2 AES based algorithm



Definition of f1, f1*, f2, f3, f4, f5 and f5*

Steps in Authentication: Attach, Identity Requests

No.	Time	Source	Destination	Protocol	Length	Info
74	4.265354	127.0.0.1	127.0.0.4	DIAM...	144	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=31a76920 e2e=38...
75	4.265548	127.0.0.4	127.0.0.1	DIAM...	156	cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=31a76920 e2e=383...
124	7.707434	127.0.0.1	127.0.0.5	DIAM...	144	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=1a677df2 e2e=38...
125	7.707632	127.0.0.5	127.0.0.1	DIAM...	156	cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=1a677df2 e2e=387...
134	9.965372	128.208.49.18	128.208.49.48	SIAP/..	192	InitialUEMessage, Attach request, PDN connectivity request
135	9.965614	128.208.49.48	128.208.49.18	SIAP/..	108	DownlinkNASTransport, Identity request
136	9.966435	128.208.49.18	128.208.49.48	SIAP/..	144	UplinkNASTransport, Identity response
137	9.996771	127.0.0.1	127.0.0.4	DIAM...	324	cmd=3GPP-Authentication-Information Request(318) flags=RP--- appl=3GPP S6a/S6d(16777251) h2h=31a7...
148	9.998744	127.0.0.4	127.0.0.1	DIAM...	376	cmd=3GPP-Authentication-Information Answer(318) flags=P--- appl=3GPP S6a/S6d(16777251) h2h=31a76...
150	9.999177	128.208.49.48	128.208.49.18	SIAP/..	148	DownlinkNASTransport, Authentication request
152	10.176918	128.208.49.18	128.208.49.48	SIAP/..	144	UplinkNASTransport, Authentication response
153	10.177248	128.208.49.48	128.208.49.18	SIAP/..	128	DownlinkNASTransport, Security mode command
159	10.216759	128.208.49.18	128.208.49.48	SIAP/..	136	UplinkNASTransport, Security mode complete
160	10.217244	127.0.0.1	127.0.0.4	DIAM...	328	cmd=3GPP-Update-Location Request(316) flags=RP--- appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38...

InitiatingMessage	
procedureCode: id-initialUEMessage (12)	
criticality: ignore (1)	
value	
InitialUEMessage	
protocolIEs: 5 items	
Item 0: id-eNB-UE-SIAP-ID	
Item 1: id-NAS-PDU	
Item 2: id-TAI	
Item 3: id-EUTRAN-CGI	
Item 4: id-RRC-Establishment-Cause	

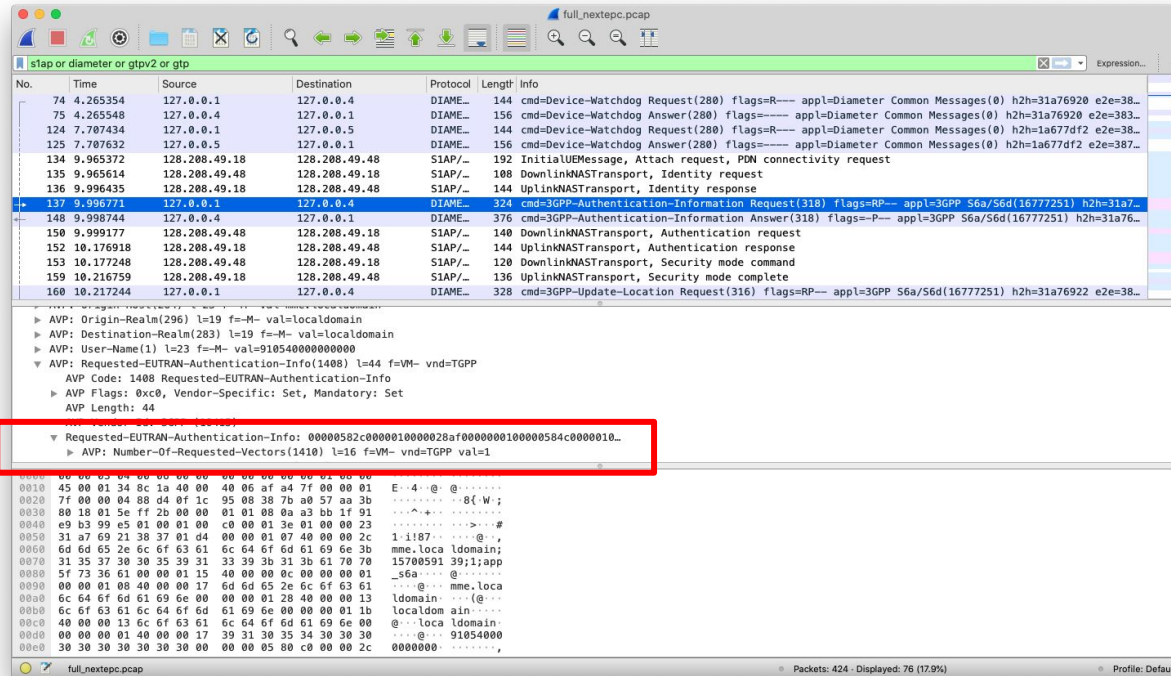
0000	00 00 00 01 00 06 a0 b3 cc 46 c6 06 01 06 08 00F.....
0010	45 02 00 b0 00 0d 40 00 40 84 d5 d8 80 00 31 12	E.....@.....1.
0020	80 d0 31 30 ac b4 8e 3c a9 17 3a 40 9a 6b 5d bd	..10...<...@.k.]
0030	00 03 00 8d a7 23 51 3b 00 01 00 00 00 00 12	...#0;.....
0040	00 0c 40 79 00 00 05 00 08 00 02 00 02 00 1a 00	...@y.....
0050	51 50 17 e6 3d af b0 0a 07 41 02 00 f6 19 f0 45	QP.....A.....E
0060	00 01 01 f0 00 5f 2b 05 f0 f0 c0 0d 00 05 02<.....
0070	31 d0 11 d1 52 19 f0 45 00 01 5c 08 02 31 03 f5	1...R...E...1...
0080	e0 3e 90 11 03 57 58 b2 20 0a 60 14 34 e2 91 81	>...WX...4...
0090	00 12 3e 80 40 08 00 02 1f 00 04 02 60 04 5d 01	...>@.....].
00a0	03 e0 00 43 00 06 00 19 f0 45 00 01 00 64 40 08	...C.....E...d0
00b0	00 19 f0 45 00 00 10 10 00 86 40 01 30 00 00 00	...E.....@...0...

Communication between the User Device and the eNB which is registered with the MME

The UE Identifies network capabilities, algorithms to use and session identifiers

UE → eNB → MME

Steps in Authentication: Authentication Info. Request



The image shows a Wireshark packet capture of network traffic. The top pane displays a list of packets, and the bottom pane shows the details of the selected packet (No. 137). A red box highlights the 'Requested-Authentication-Info' AVP in the details pane.

No.	Time	Source	Destination	Protocol	Length	Info
74	4.265354	127.0.0.1	127.0.0.4	DIAMETER	144	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=31a76920 e2e=38...
75	4.265548	127.0.0.4	127.0.0.1	DIAMETER	156	cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=31a76920 e2e=38...
124	7.787434	127.0.0.1	127.0.0.5	DIAMETER	144	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=31a76920 e2e=38...
125	7.787632	127.0.0.5	127.0.0.1	DIAMETER	156	cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=31a76920 e2e=38...
134	9.965372	128.208.49.18	128.208.49.48	SIAP/_	192	InitialUEMessage, Attach request, PDN connectivity request
135	9.965614	128.208.49.48	128.208.49.18	SIAP/_	108	DownlinkKNASTransport, Identity request
136	9.996435	128.208.49.18	128.208.49.48	SIAP/_	144	UplinkKNASTransport, Identity response
137	9.996771	127.0.0.1	127.0.0.4	DIAMETER	324	cmd=3GPP-Authentication-Information Request(318) flags=RP--- appl=3GPP S6a/S6d(16777251) h2h=31a7...
148	9.998744	127.0.0.4	127.0.0.1	DIAMETER	376	cmd=3GPP-Authentication-Information Answer(318) flags=P--- appl=3GPP S6a/S6d(16777251) h2h=31a76...
150	9.999177	128.208.49.48	128.208.49.18	SIAP/_	140	DownlinkKNASTransport, Authentication request
152	10.176918	128.208.49.18	128.208.49.48	SIAP/_	144	UplinkKNASTransport, Authentication response
153	10.177248	128.208.49.48	128.208.49.18	SIAP/_	120	DownlinkKNASTransport, Security mode command
159	10.216759	128.208.49.18	128.208.49.48	SIAP/_	136	UplinkKNASTransport, Security mode complete
160	10.217244	127.0.0.1	127.0.0.4	DIAMETER	328	cmd=3GPP-Update-Location Request(316) flags=RP--- appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38...

Details of Packet 137:

- AVP: Origin-Realm(296) l=19 f=M- val=localdomain
- AVP: Destination-Realm(283) l=19 f=M- val=localdomain
- AVP: User-Name(1) l=23 f=M- val=9105400000000000
- AVP: Requested-EUTRAN-Authentication-Info(1408) l=44 f=VM- vnd=TGPP
- AVP Code: 1408 Requested-EUTRAN-Authentication-Info
- AVP Flags: 0xc0, Vendor-Specific: Set, Mandatory: Set
- AVP Length: 44
- Requested-Authentication-Info: 00000502c000010000020af0000000100000584c0000010...
- AVP: Number-Of-Requested-Vectors(1418) l=16 f=VM- vnd=TGPP val=1

AIR happens between the MME and the HSS where the MME requests the HSS for Authentication Vectors and validation for a specific user trying to connect.

MME → HSS/AuC

Steps in Authentication: Authentication Info. Answer

No.	Time	Source	Destination	Protocol	Length	Info
74	4.265354	127.0.0.1	127.0.0.4	DIAHE_	144	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=31a76920 e2e=3B...
75	4.265548	127.0.0.1	127.0.0.1	DIAHE_	156	cmd=Device-Watchdog Answer(280) flags=----- appl=Diameter Common Messages(0) h2h=31a76920 e2e=3B...
124	7.707434	127.0.0.1	127.0.0.1	DIAHE_	144	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=1a677df2 e2e=3B...
125	7.707632	127.0.0.1	127.0.0.1	DIAHE_	156	cmd=Device-Watchdog Answer(280) flags=----- appl=Diameter Common Messages(0) h2h=1a677df2 e2e=3B...
134	9.965372	128.208.49.18	128.208.49.48	SIAP/_	192	InitialUEMessage, Attach request, PM connectivity request
135	9.965614	128.208.49.48	128.208.49.18	SIAP/_	188	DownlinkNASTransport, Identity request
136	9.996435	128.208.49.18	128.208.49.48	SIAP/_	144	UplinkNASTransport, Identity response
137	9.996771	127.0.0.1	127.0.0.4	DIAHE_	324	cmd=3GPP-Authentication-Information Request(318) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=31a7...
148	9.998744	127.0.0.4	127.0.0.1	DIAHE_	376	cmd=3GPP-Authentication-Information Answer(318) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=31a76...
149	9.999177	128.208.49.48	128.208.49.18	SIAP/_	140	DownlinkNASTransport, Authentication request
152	10.176918	128.208.49.48	128.208.49.18	SIAP/_	144	UplinkNASTransport, Authentication response
153	10.177248	128.208.49.18	128.208.49.48	SIAP/_	120	DownlinkNASTransport, Security mode command
159	10.216759	128.208.49.18	128.208.49.48	SIAP/_	136	UplinkNASTransport, Security mode complete
160	10.217244	127.0.0.1	127.0.0.4	DIAHE_	328	cmd=3GPP-Update-Location Request(316) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=3B...

AVP Length: 132

AVP Vendor Id: 3GPP (10415)

- E-UTRAN-Vector: 000005a7c00001c00002af3d35d8afd2f4a53ff0cf171414d5882
 - AVP: RAND(1447) l=28 f=M- vnd=TGPP val=3d35d8afd2f4a53ff0cf171414d5882
 - AVP: XRES(1448) l=20 f=M- vnd=TGPP val=78110ea32820580
 - AVP: AUTN(1449) l=28 f=M- vnd=TGPP val=42de69bd1b798000c562ffe1d8efc353
 - AVP: KASME(1450) l=44 f=M- vnd=TGPP val=9f3b71b305e918f39333b338c9856daadb8a117966fbfd...
- AVP: Origin-Host(264) l=23 f=M- val=hss.localdomain
- AVP: Origin-Realm(296) l=19 f=M- val=localdomain
- AVP: Result-Code(268) l=12 f=M- val=DIAMETER_SUCCESS (2001)
- AVP: Auth-Session-State(277) l=12 f=M- val=NO_STATE_MAINTAINED (1)

```

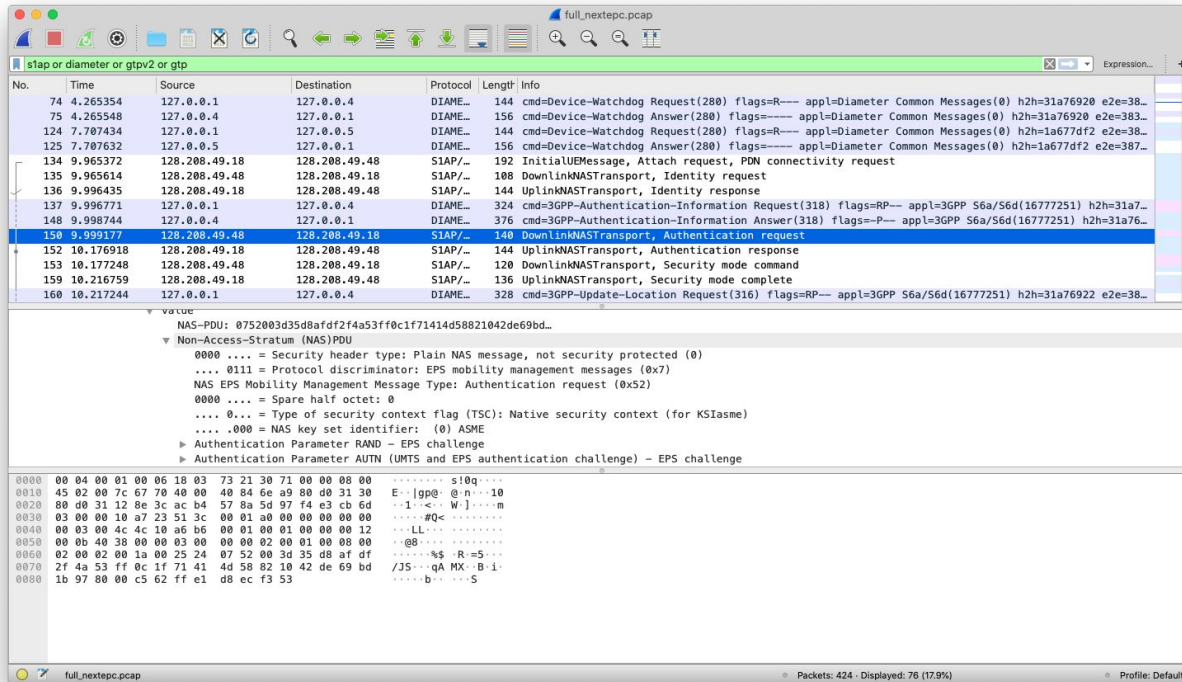
0000 00 00 03 04 00 06 00 00 00 00 00 00 00 00 00  E..h.Og.@.<.....
0010 45 00 01 68 12 4f 40 00 04 06 29 3c 7f 00 00 04      .....W.p.:#
0020 7f 00 00 01 0f 1c 08 04 a0 57 aa 3b 55 08 39 7b  .....g...b.b.Aa
0030 09 10 01 67 ff 5f 00 00 01 01 00 00 e9 b3 b0 4a  .....J
0040 aa bb 1f 91 01 00 01 34 a0 00 01 3e 01 00 00 23  .....4@>.....J
0050 31 a7 69 21 38 37 01 04 00 00 01 07 40 00 00 2c  1:187.....@.;
0060 6d 6d 65 2e 6c 6f 63 61 6c 64 6f 6d 61 69 6e 3b  mme.lcda localma;
0070 31 35 37 30 30 35 39 31 33 39 3b 31 3b 61 70 70  17500591 39;1;app
0080 5f 73 36 61 00 00 05 85 c0 00 00 90 00 00 28 af  _sba.....
0090 00 00 05 ca 00 00 84 c0 00 00 28 af 00 00 05 a7  ....ca.....
00a0 c0 00 00 1c 00 28 af 3d 35 d8 af 2f 4a 53       ....{ =5....J$
00b0 ff 0c ef 71 41 4d 58 82 00 00 05 a8 c0 00 00 14  ....qAMX.....
00c0 00 00 28 af 78 11 0e a3 22 82 05 80 00 00 05 a9  ....x.....
00d0 c0 00 00 1c 00 28 af 42 de 69 bd 1b 97 80 00   .... B.....
00e0 c5 62 ff ef 08 ec f3 53 00 00 05 aa c0 00 00 2c  ....b.....S.....

```

The HSS responds to the request for authentication from the MME with a RAND challenge, expected response XRES, AUTN value and K_{asme} .

HSS/AuC \rightarrow MME

Steps in Authentication: Authentication Request



No.	Time	Source	Destination	Protocol	Length	Info
74	4.265354	127.0.0.1	127.0.0.4	DIAM...	144	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=31a76920 e2e=38...
75	4.265548	127.0.0.4	127.0.0.1	DIAM...	156	cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=31a76920 e2e=383...
124	7.787434	127.0.0.1	127.0.0.5	DIAM...	144	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=1a677df2 e2e=38...
125	7.787632	127.0.0.5	127.0.0.1	DIAM...	156	cmd=Device-Watchdog Answer(280) flags=---- appl=Diameter Common Messages(0) h2h=1a677df2 e2e=387...
134	9.965372	128.208.49.18	128.208.49.18	SIAP/_	192	InitialUEMessage, Attach request, PDN connectivity request
135	9.965614	128.208.49.48	128.208.49.18	SIAP/_	108	DownLinkNASTransport, Identity request
136	9.996435	128.208.49.18	128.208.49.48	SIAP/_	144	UplinkNASTransport, Identity response
137	9.996771	127.0.0.1	127.0.0.4	DIAM...	324	cmd=3GPP-Authentication-Information Request(318) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=31a7...
148	9.998744	127.0.0.4	127.0.0.1	DIAM...	376	cmd=3GPP-Authentication-Information Answer(318) flags=-P-- appl=3GPP S6a/S6d(16777251) h2h=31a76...
150	9.999177	128.208.49.48	128.208.49.18	SIAP/_	140	DownLinkNASTransport, Authentication request
152	10.176918	128.208.49.18	128.208.49.48	SIAP/_	144	UplinkNASTransport, Authentication response
153	10.177248	128.208.49.48	128.208.49.18	SIAP/_	120	DownLinkNASTransport, Security mode command
159	10.216759	128.208.49.18	128.208.49.48	SIAP/_	136	UplinkNASTransport, Security mode complete
160	10.217244	127.0.0.1	127.0.0.4	DIAM...	328	cmd=3GPP-Update-Location Request(316) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38...

NAS-PDU: 0752003d35d8afdf2f4a53ff0c1f7141d58821042de69bd...

Non-Access-Stratum (NAS) PDU

- 0000 = Security header type: Plain NAS message, not security protected (0)
- 0111 = Protocol discriminator: EPS mobility management messages (0x7)
- NAS EPS Mobility Management Message Type: Authentication request (0x52)
- 0000 = Spare half octet: 0
- 0000 = Type of security context flag (TSC): Native security context (for KSIASME)
- 0000 = NAS key set identifier: (0) ASME
- ▶ Authentication Parameter RAND - EPS challenge
- ▶ Authentication Parameter AUTN (UMTS and EPS authentication challenge) - EPS challenge

0000 00 04 00 01 00 06 18 03 73 21 30 71 00 00 00 00s10q...

0010 45 02 00 7c 67 70 40 00 00 84 6e a9 00 d0 31 30E-[gpe] @ n...10

0020 80 d0 31 12 8e 3c ac b4 57 8a 5d 97 f4 e3 cb 6d1<...W]...m

0030 03 00 00 10 a7 23 51 3c 00 01 a0 00 00 00 00 00#Q<.....

0040 00 03 00 4c 4c 10 a6 b6 00 01 00 01 00 00 12LL.....

0050 00 0b 40 38 00 00 03 00 00 02 00 01 00 00 00@.....

0060 02 00 02 00 1a 00 25 24 07 52 00 3d 35 d8 a7 df%\$...R=5...

0070 2f 4a 53 ff 0c 1f 71 41 4d 58 82 10 42 de 69 bd .../35...qA MX-B-1-

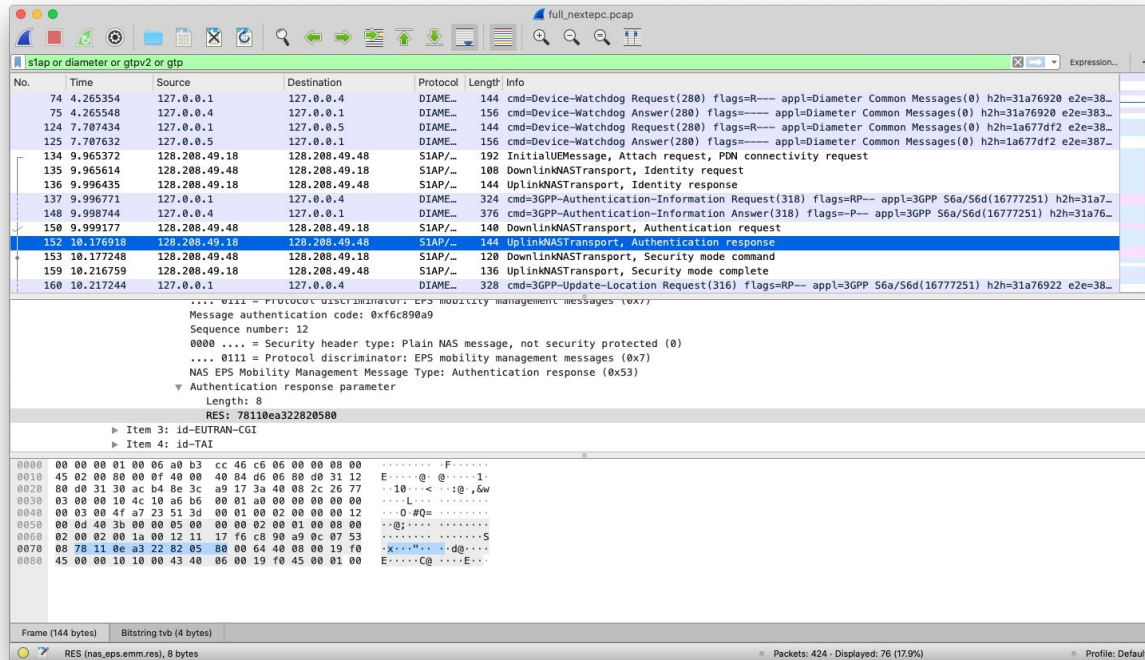
0080 1b 97 80 00 c5 62 ff e1 d8 ec f3 53b...S

The MME signals the UE with an *Authentication Request* and provides the RAND and AUTN as a challenge to compute the RES.

Downlink Transport

MME → UE

Steps in Authentication: Authentication Response



The image shows a Wireshark packet capture of an Authentication Response message. The top pane displays a list of packets, with packet 152 selected. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
74	4.265354	127.0.0.1	127.0.0.4	DIAMETER	144	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=31a76920 e2e=38...
75	4.265548	127.0.0.4	127.0.0.1	DIAMETER	156	cmd=Device-Watchdog Answer(280) flags=--- appl=Diameter Common Messages(0) h2h=31a76920 e2e=383...
124	7.707434	127.0.0.1	127.0.0.5	DIAMETER	144	cmd=Device-Watchdog Request(280) flags=R--- appl=Diameter Common Messages(0) h2h=1a677df2 e2e=38...
125	7.707632	127.0.0.5	127.0.0.1	DIAMETER	156	cmd=Device-Watchdog Answer(280) flags=--- appl=Diameter Common Messages(0) h2h=1a677df2 e2e=387...
134	9.965372	128.208.49.18	128.208.49.48	SIAP	192	InitialUEMessage, Attach request, PDN connectivity request
135	9.965614	128.208.49.48	128.208.49.18	SIAP	108	DownlinkNASTransport, Identity request
136	9.996435	128.208.49.18	128.208.49.48	SIAP	144	UplinkNASTransport, Identity response
137	9.996771	127.0.0.1	127.0.0.4	DIAMETER	324	cmd=3GPP-Authentication-Information Request(318) flags=RP--- appl=3GPP S6a/S6d(16777251) h2h=31a7...
148	9.998744	127.0.0.4	127.0.0.1	DIAMETER	376	cmd=3GPP-Authentication-Information Answer(318) flags=P--- appl=3GPP S6a/S6d(16777251) h2h=31a76...
150	9.999177	128.208.49.48	128.208.49.18	SIAP	140	DownlinkNASTransport, Authentication request
152	10.176918	128.208.49.18	128.208.49.48	SIAP	144	UplinkNASTransport, Authentication response
153	10.177248	128.208.49.48	128.208.49.18	SIAP	120	DownlinkNASTransport, Security mode command
159	10.216759	128.208.49.18	128.208.49.48	SIAP	136	UplinkNASTransport, Security mode complete
160	10.217244	127.0.0.1	127.0.0.4	DIAMETER	328	cmd=3GPP-Update-Location Request(316) flags=RP--- appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38...

Details of packet 152 (UplinkNASTransport, Authentication response):

- Sequence number: 12
- 0000 ... = Security header type: Plain NAS message, not security protected (0)
- ... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
- NAS EPS Mobility Management Message Type: Authentication response (0x53)
- Authentication response parameter
 - Length: 8
 - RES: 78110ea322820580
- Item 3: id-EUTRAN-CGI
- Item 4: id-TAI

Raw packet data (hex):

```
0000 00 00 00 01 00 06 a0 b3 cc 46 c6 06 00 00 08 00 .....F.....
0010 45 02 00 00 0f 40 00 40 84 d6 06 08 d0 31 12 E.....@: @.....1..
0020 80 d0 31 30 ac b4 8e 3c a9 17 3a 40 08 2c 26 77 ...10...< : :@, $w
0030 83 00 00 10 4c 10 a6 b6 00 01 a0 00 00 00 00 ...L.....
0040 00 03 00 4f a7 23 51 3d 00 01 00 02 00 00 12 ...0 #0= .....
0050 00 d4 40 3b 00 00 05 00 00 02 00 01 00 08 00 ..@:.....
0060 02 00 00 1a 00 12 11 17 f6 c8 90 a9 0c 07 53 .....X.....dg...
0070 00 78 11 0e a3 22 82 05 80 00 64 40 08 00 19 10 .....C@ .....E....
0080 45 00 00 10 10 00 43 40 06 00 19 f0 45 00 01 00 E.....C@ .....E....
```

The MME signals the UE with an *Authentication Request* and provides the RAND and AUTN as a challenge to compute the RES.

Uplink Transport:
Compares $XRES == RES$

UE → MME

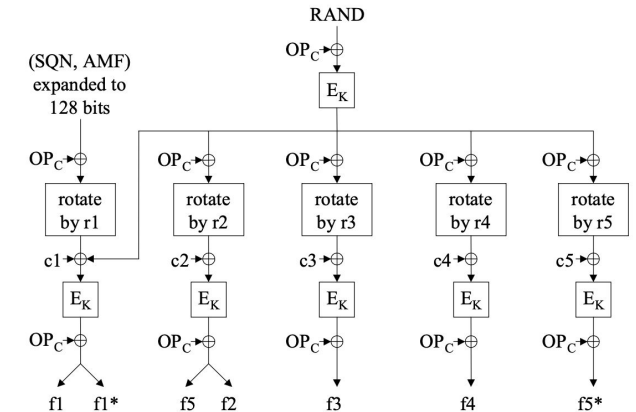
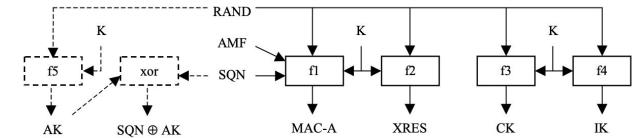
Steps in Authentication: Security Mode

- Initialize signaling security between the UE and the MME
- UE derives corresponding CK, IK keys for encryption and Integrity algorithms
- **Completes Authentication and UE successfully attaches to the network.**

Precomputing LTE Authentication Vectors (AV)

- **AUTN** = (SQN \oplus AK) + AMF + MAC_A
- **AV** = {RAND, XRES, AUTN, K_{asme}}

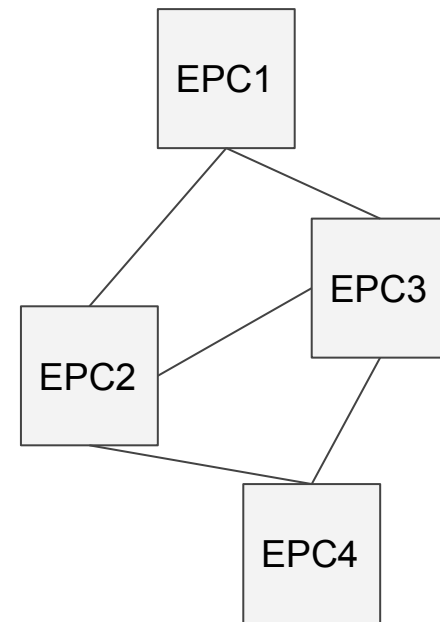
- The Home HSS creates the required authentication vectors (AVs) and publishes the vectors to other EPC nodes over a blockchain network
- The SQN construction matrix allows us to dedicate specific row(s) for roaming.
- One time usage of SEQ to create an AV prevents replay attacks and the AVs remain valid until they are used by the UE
- Any EPC participating in the blockchain network can allow users to roam.



Definition of f1, f1*, f2, f3, f4, f5 and f5*

The need for decentralization

- Multiple community cellular networks EPC cores become participants in a blockchain network
- Home network pre-computes authentication vectors and shares it with the rest of the network as a transaction
- Communities choose who they can connect to and pre-pay for total data associated with an authentication vector.



Trust & Network Model

- Never share symmetric keys needed for authentication
 - Subscriber trusts Home network provider
- Design for high network outages and high latency communication between communities
- Common policy for operation agreed upon by network operators



Implementation

- Built currently with Hyperledger Sawtooth as the blockchain layer running PoET consensus
- Generate authentication vectors (AV) with a sliding window of X usable AVs in the network
- Roaming nodes consuming the vector for user authentication report the consumption and corresponding billing/payment workflows take over
- Integrated into Open5Gs fork (uw-ictd/nextepc) in dAuth branch

Lab Experiments

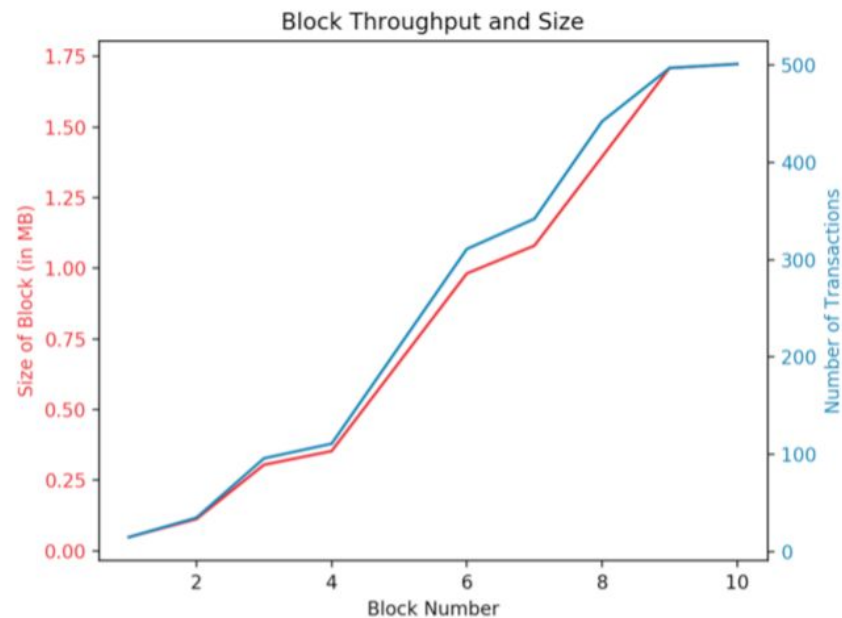
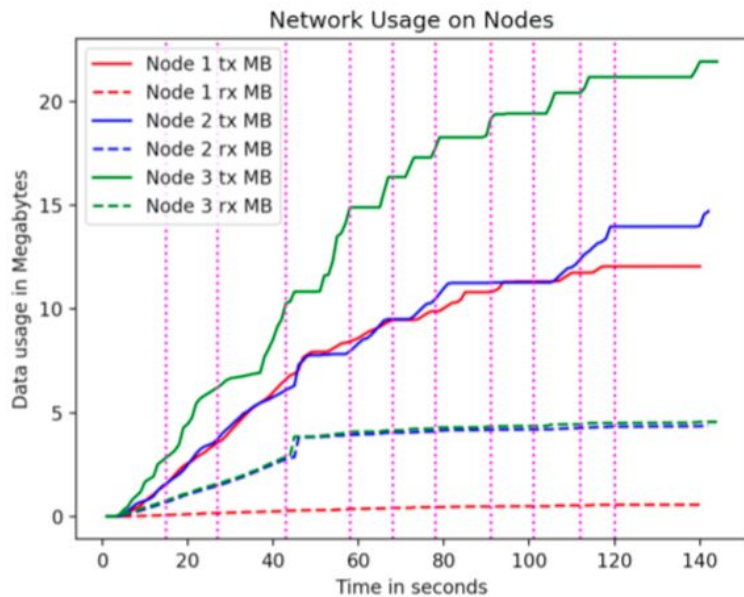
- 1x 8GB RAM Zotac Mini Computers
- 1x 4GB RAM Zotac Mini Computer
- 1x 8GB RAM Dell workstation



Running Open5Gs and Hyperledger Sawtooth with corresponding transaction processors.

2 USRP B200 mini SDRs behaving as 2 cellular networks allowing users.

Initial Results



~4 tx/s with heavy network usage (~13x more than block sizes)

Challenges & Future Work

- Blockchain consensus protocols (PoET/PBFT) are chatty and consume lots of bandwidth
- Need for tuning networking parameters to minimize the chattiness and operate better in high latency and bandwidth constrained networks
- Improving current experiments with batching
- Real world deployment experiments with the Othello Network in Seattle



THANKS!

Any questions?

You can find me at

@sudheesh001 & sudheesh@cs.washington.edu

<https://ictd.cs.washington.edu/>