dAuth -**Decentralizing LTE** Authentication and Roaming

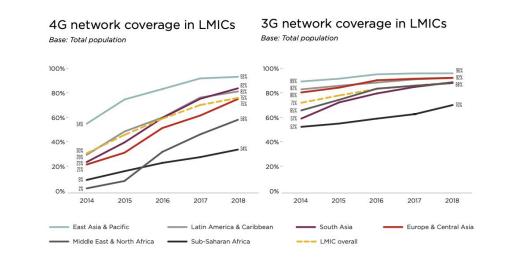
Sudheesh Singanamalla, Esther Jang, Nick Durand, Matthew Johnson, Spencer Sevilla, Kurtis Heimerl

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.



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?

W

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)

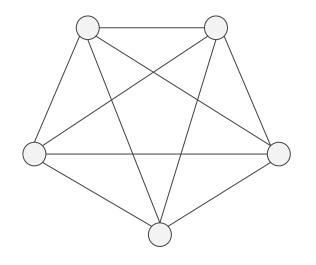
Roaming between telecom operators is a business decision, managed by physical agreements between network operators

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.



7

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)



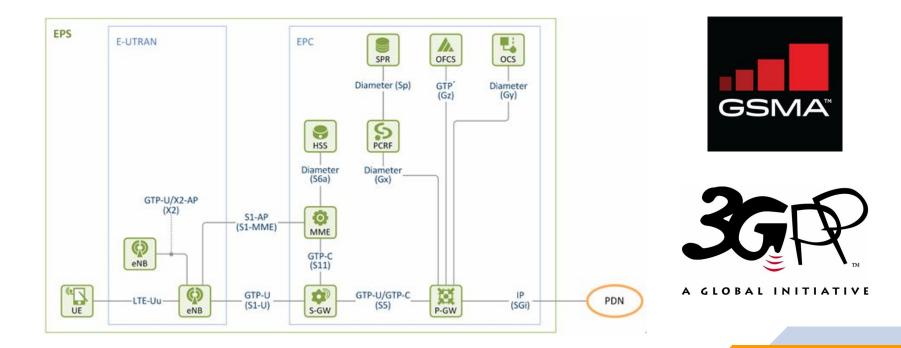
Primer into LTE Networks

- 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



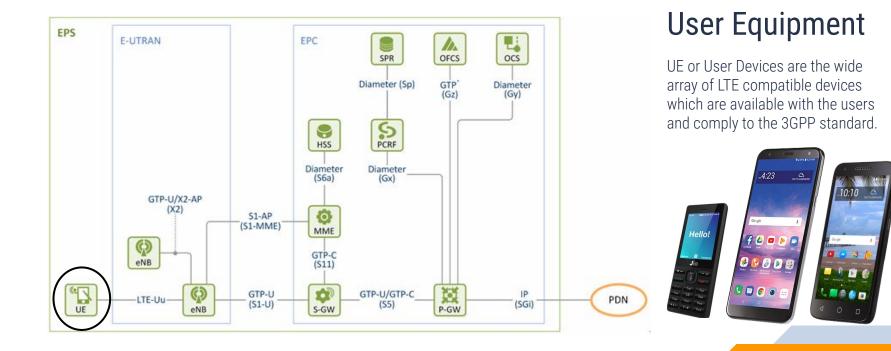
W

LTE Network Reference Architecture



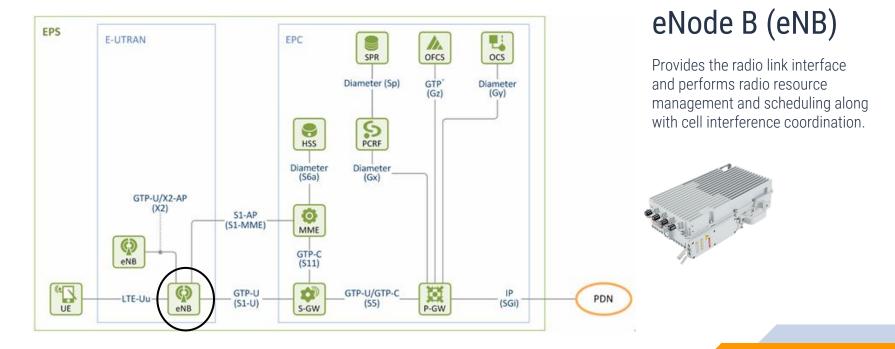


LTE Network Architecture : User Equipment



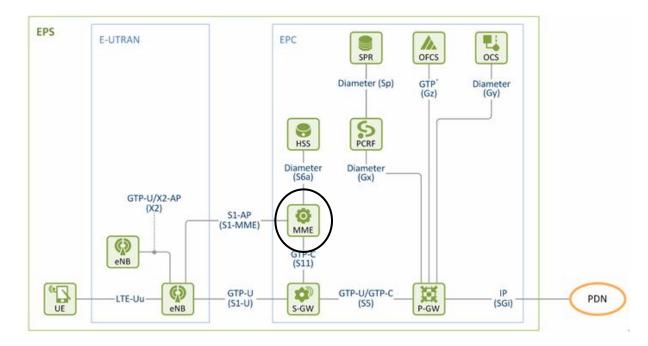


LTE Network Architecture : eNB (Base Station)





LTE Network Architecture : Mobility Management

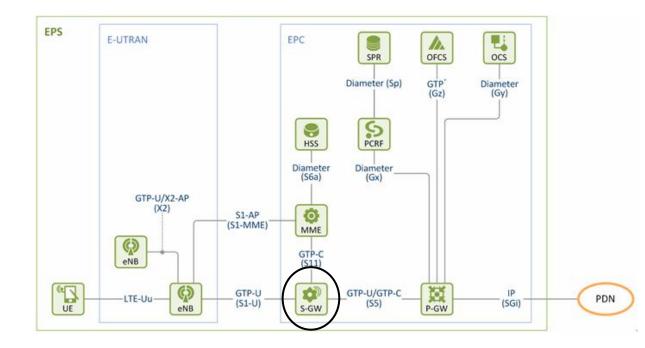


MME

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



LTE Network Architecture : Serving Gateway



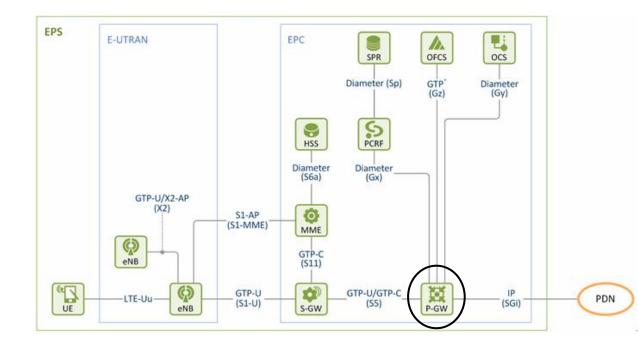
Serving Gateway (S-GW)

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

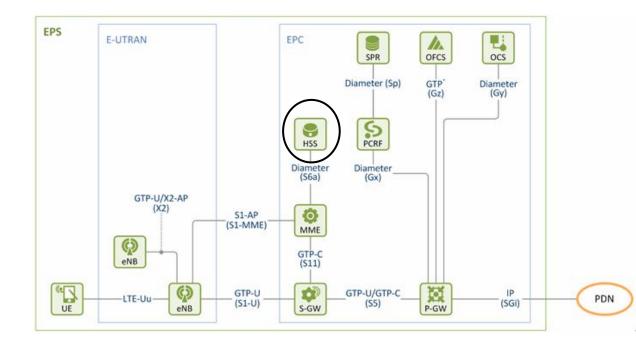


Packet Data Network Gateway (P-GW)

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



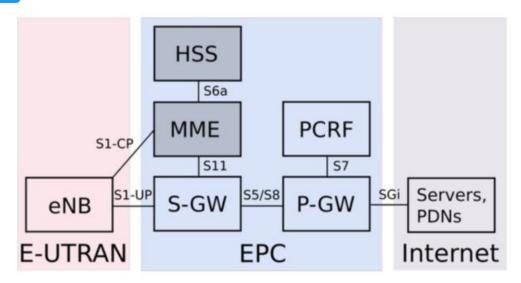
HSS

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

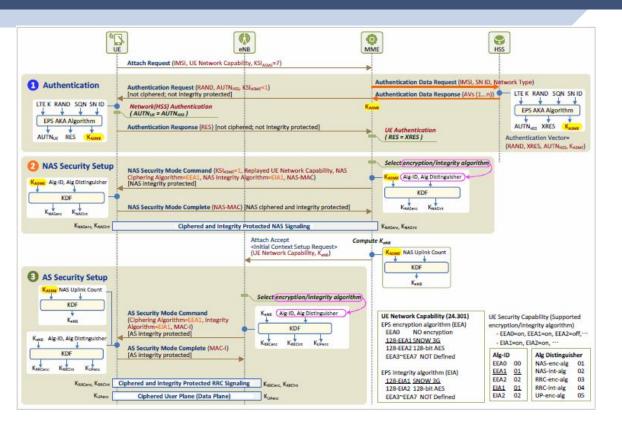




Moves the data center EPC to the edge!

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

W

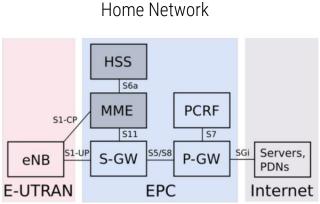
Technical Complexities of Roaming

Telecom operators perform roaming in multiple ways posing different challenges:

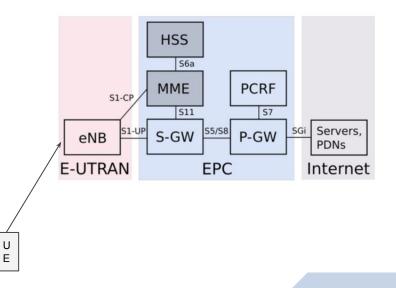
- 1. The roaming core network requests subscribers' home network for necessary authentication values needing reliable connectivity between operators.
 - a. Users experience higher latencies since all requests are tunnelled home.
- 2. The symmetric key and state corresponding to the user could be exchanged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



Current Roaming Practices - Fully connected networks



Roaming Network

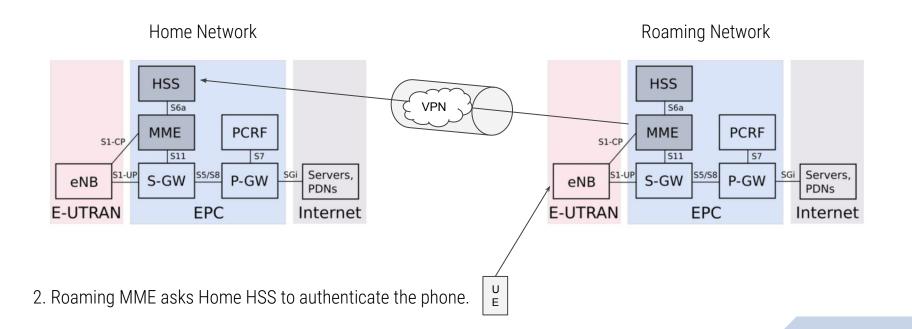


1. UE Connects to the Roaming eNB

21



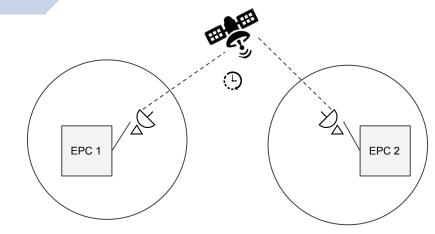
Current Roaming Practices - Fully connected networks



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

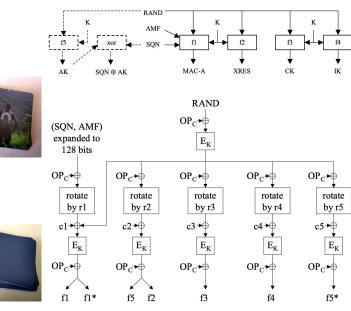


SIM Cards & Milenage

- 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 (27 bits) + IND (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]:

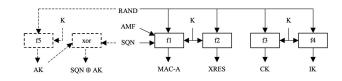
- 0000 : EIA0 Null Integrity Protection Algorithm
- 0001 : 128-EIA1 SNOW 3G
- 0010 : 128-EIA2 AES

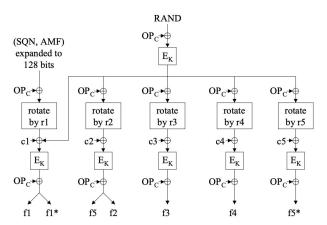
Cipher Algorithms [CK]:

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



A GLOBAL INITIATIVE





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

Steps in Authentication: Attach, Identity Requests

0.	Time	Source	Destination	Protocol	Length	Info
	74 4.265354	127.0.0.1	127.0.0.4	DIAME	1.000	cmd=Device-Watchdog Reguest(280) flags=R appl=Diameter Common Messages(0) h2h=31a76920 e2e=38
	75 4.265548	127.0.0.4	127.0.0.1	DIAME		cmd=Device-Watchdog Answer(280) flags= appl=Diameter Common Messages(0) h2h=31a76920 e2e=383
3	124 7.707434	127.0.0.1	127.0.0.5	DIAME		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	DIAME		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	S1AP/		InitialUEMessage, Attach request, PDN connectivity request
2	135 9.965614	128.208.49.48	128.208.49.18	S1AP/		DownlinkNASTransport, Identity request
13	136 9.996435	128.208.49.18	128.208.49.48	S1AP/	144	UplinkNASTransport, Identity response
1	137 9.996771	127.0.0.1	127.0.0.4	DIAME	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	DIAME	376	cmd=3GPP-Authentication-Information Answer(318) flags=-P appl=3GPP S6a/S6d(16777251) h2h=31a76
8	150 9.999177	128.208.49.48	128.208.49.18	S1AP/	140	DownlinkNASTransport, Authentication request
1	152 10.176918	128.208.49.18	128.208.49.48	S1AP/	144	UplinkNASTransport, Authentication response
	153 10.177248	128.208.49.48	128.208.49.18	S1AP/	120	DownlinkNASTransport, Security mode command
1.0	159 10.216759	128.208.49.18	128.208.49.48	S1AP/	136	UplinkNASTransport, Security mode complete
	133 10.210/33					
	160 10.217244 procedureC criticalit value value value	ode: id-initialUEMe y: ignore (1) UEMessage	127.0.0.4	DIAME	328	<pre>cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38</pre>
	<pre>160 10.217244 v Initiatingme procedured criticalit value v Initial v prote</pre>	ssage code: id-initialUEMe y: ignore (1) UEMessage coclIEs: 5 items em 0: id-eNB-UE-SIA em 1: id-NAS-PDU em 2: id-TAI em 3: id-EUTRAN-CGI	ssage (12) >-ID	DIAME	328	cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38
	<pre>160 10.217244 v Initiatingme procedured criticalit value v Initial v prote b It b It</pre>	ssage code: id-initialUEMe y: ignore (1) UEMessage occlIEs: 5 items em 0: id-eNB-UE-SIA em 1: id-NAS-PDU em 2: id-TAI em 3: id-EUTRAN-CGI em 4: id-RRC-Establ	ssage (12) ?-ID ishment-Cause			<pre>cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38</pre>
000	160 10.217244 Thread the second seco	ssage ode: id-initialUEMe y: ignore (1) UEMessage collEs: 5 items em 0: id-NAS-PDU em 1: id-NAS-PDU em 1: id-NAS-PDU em 2: id-TAI em 4: id-RC-Establ 0 66 a0 b3 cc 46 c	ssage (12) >-ID ishment-Cause 6 06 01 06 08 00 ···	····· · · F··	* * * *	<pre>cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38</pre>
2000	160 10.217244 Thread the second seco	ssage ode: id-initialUEMe y: ignore (1) UEMessage collEs: 5 items m 0: id-eNB-UE-SIAI em 1: id-HAS-PDU em 2: id-TAI em 3: id-EUTRAN-CGI em 4: id-RCC-Establ 0 06 a0 b3 cc 46 c 0 64 0 0 00 40 84 d	ssage (12) >-ID ishment-Cause 6 06 01 06 08 00 ··· 5 d8 80 d0 31 12 E·		*****	<pre>cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38</pre>
000 010 020 030	<pre>160 10.217244</pre>	sage ode: id-initialUEMe y: ignore (1) UEMessage me 0: id-eNB-UE-SIAI em 1: id-ANS-PDU em 2: id-TAI em 3: id-EUTRAN-CGI em 4: id-RRC-EstabL 0 66 a0 b3 cc 46 c 0 64 0 40 40 44 d c b4 8e 3c a9 T3 7 23 51 3b 00 01 0	<pre>ssage (12) >-ID ishment-Cause 6 06 01 06 08 00 5 d8 80 d0 31 12 E: a 40 9a 6b 5d bd 0 00 00 00 00 12 </pre>		· · 1 ·	cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38
2000 210 220 230 230	<pre>160 10.217244</pre>	ssage ode: id-initialUEMe vignore (1) UEMessage collEs: 5 items collEs: 5 items em em 0: id-eNB-UE-STAB em 1: id-NAS-FDU em 1: id-MAS-FDU id id-ME-Establ id id id-ME-Establ id id id id-ME-Bas id id id <mas< td=""> id id id id id id id <t< td=""><td>ssage (12) >-ID ishment-Cause 6 06 01 06 08 00 ··· 5 d8 80 d0 31 12 E· 4 09 36 50 db ··· 0 00 00 00 01 2 ··· 2 00 02 00 1a 00 ···</td><td></td><td>1. k]</td><td>cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38</td></t<></mas<>	ssage (12) >-ID ishment-Cause 6 06 01 06 08 00 ··· 5 d8 80 d0 31 12 E· 4 09 36 50 db ··· 0 00 00 00 01 2 ··· 2 00 02 00 1a 00 ···		1. k]	cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38
000 010 020 030 040 050	<pre>160 10.217244</pre>	sage ode: id-initialUEMe y: ignore (1) UEMessage colIEs: 5 items id-eNB-UE-SIAI em 0: id-eNB-UE-SIAI em 1: id-NAS-PDU em 2: id-TAI em 4: id-RRC-Establ 0 66 a0 b3 cc 46 c 0 64 04 00 40 84 d c b4 86 3c a9 T3 0 66 a0 61 00 61 0 0 60 40 50 00 10 0 0 00 87 40 0 71 0	<pre>ssage (12) >-ID ishment-Cause 6 06 01 06 08 00 5 d8 80 d0 11 22 E- 4 40 9a 6b 5d bd 0 00 00 00 00 12 2 00 02 00 1a 00 2 00 62 00 1a 00 2 0b f6 1 Pf 04 55 OF</pre>		···1· ···E	cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38
2000 210 220 230 240 250 250	<pre>160 10.217244</pre>	sage ode: id-initialUEMe ode: id-initialUEMe UEMessage collEs: 5 items collEs: 5 items em em 0: id-eNB-UE-STAB em 1: id-NAS-FDU em 1: id-NAS-FDU em 1: id-MAS-FDU 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0:	Ssage (12) ID ishment-Cause 6 06 01 06 08 00 5 08 80 d0 31 12 E- 4 09 a6 55 db 0 00 00 00 00 12 2 00 62 00 1a 00 2 00 62 00 1a 00 2 00 65 62 2 00 65 62		· . 1. · k] · E	cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38
2000 210 220 230 240 250 250 260 250 260 270	160 10.217244 v Intractinger procedured criticality v alue v Initial v prote b It b It b It b It b It c Value 0 00 00 10 00 10 80 00 31 30 80 01 01 70 63 30 00 11 10 15	sage ode: id-initialUEMe y: ignore (1) UEMessage colIEs: 5 items id-eNB-UE-SIAI em 0: id-eNB-UE-SIAI em 1: id-NAS-PDU em 2: id-TAI em 4: id-RRC-Establ 0 66 a0 b3 cc 46 c 0 64 04 00 40 84 d c b4 86 3c a9 T3 0 66 a0 61 00 61 0 0 60 40 50 00 10 0 0 00 87 40 0 71 0	<pre>ssage (12) >-ID ishment-Cause 6 06 01 06 08 00 5 d8 80 00 11 2 E- 4 40 99 6b 5d bd 0 00 00 00 00 12 2 00 02 00 1a 00 2 00 62 00 1a 00 2 0b f6 19 f0 45 09 0 c0 00 00 05 02 c 08 02 31 03 f5 1 </pre>		· 1. • k] · · · E • 1 · ·	cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38
000 010 020 040 050 050 050 060 070 080 090	<pre>160 10.217244 v Intractinger procedured criticalit v alue v Initial v value v Initial v prott b It b It b It b It b It c b It c b It c b It c c c c c c c c c c c c c c c c c c c</pre>	sage ode: id-initialUEMe y: ignore (1) UEMessage me 0: id-eNB-UE-SIAI me 0: id-eNB-UE-SIAI me 1: id-ANS-PDU me 1: id-ANS-PDU me 1: id-ANS-PDU me 1: id-ANS-PDU me 1: id-ANS-PDU 0 66 a0 b3 cc 46 c 0 64 04 00 40 84 d c b4 86 3c a9 173 0 66 a0 81 cc 46 c b 46 82 c a9 173 7 23 51 3b 00 81 0 0 80 80 90 88 00 0 1 36 b8 0 a7 41 0 0 57 2b 85 f0 70 c 1 97 64 50 00 81 5	<pre>ssage (12) >-ID ishment-Cause 6 06 01 06 08 00 5 d8 80 d0 31 12 E a 40 9a 6b 5d bd 0 00 00 00 00 12 2 00 02 00 1a 00 2 00 62 00 1a 00 2 0b f6 1p f0 45 0P 0 c0 d0 00 05 02 c 08 02 31 03 f5 1 0 14 34 e2 91 81 4 02 60 04 5d 01 </pre>		· 1. · k] · · · · E · · · · · · · · · · · · · · ·	cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38

Frame (192 bytes) Bitstring tvb (4 bytes)

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

 $UE \rightarrow eNB \rightarrow MME$

27

Steps in Authentication: Authentication Info. Request

O Time Source Destination Protocol Length Info 74 4.263534 127.6.0.1 127.8.0.4 DIAME_ 144 cmd=Device=Watchdog Request(280) flags= appl=Diameter Common Messages(0) hzh=31 124 7.70734 127.8.0.1 127.8.0.5 DIAME_ 144 cmd=Device=Watchdog Request(280) flags= appl=Diameter Common Messages(0) hzh=11 125 7.70734 127.8.0.5 127.8.0.5 DIAME_ 144 cmd=Device=Watchdog Request(280) flags= appl=Diameter Common Messages(0) hzh=11 125 7.70734 127.8.0.5 127.8.0.1 DIAME_ 136 and Device=Watchdog Request(280) flags= appl=Diameter Common Messages(0) hzh=11 125 9.906435 128.208.49.18 128.208.49.18 128.208.49.18 128.208.49.18 127.40.0.4 DIAME_ 244 cmd=3GPD-Authentication=Information Answer(130) flags=RP appl=3GPP S6a/S6d(16777 128 9.908744 127.40.0.1 127.40.0.4 DIAME_ 236 cmd=3GPD-Authentication-Information Answer(130) flags=RP appl=3GPP S6a/S6d(16777 128 9.908744 128.208.49.18 128.208.49.48 SIAP/- 140	appl=Diameter Common Messages(0) h2h=31a76920 e2e=38_ ppl=Diameter Common Messages(0) h2h=31a76920 e2e=38_ appl=Diameter Common Messages(0) h2h=1a677df2 e2e=38_ pl=Diameter Common Messages(0) h2h=1a677df2 e2e=38_ tivity request 310) flags=RP appl=3GPP 56a/56d(16777251) h2h=31a7_ 10) flags=-P appl=3GPP 56a/56d(16777251) h2h=31a7_	Time 74 4.265				Expression
74 4.265354 127.0.0.1 127.0.0.4 DIAME_ 144 cmd=Device-Watchdg Request(280) flags= appl=Diameter Common Messages(0) h2h=31 75 4.265364 127.0.0.1 127.0.0.5 DIAME_ 144 cmd=Device-Watchdg Request(280) flags= appl=Diameter Common Messages(0) h2h=31 124 7.767434 127.0.0.5 DIAME_ 144 cmd=Device-Watchdg Request(280) flags= appl=Diameter Common Messages(0) h2h=31 125 7.767532 127.0.0.5 DIAME_ 144 cmd=Device-Watchdg Request(280) flags= appl=Diameter Common Messages(0) h2h=1a 134 9.05514 128.286.49.18 SIAP/_ 192 DownlinMMSTransport, Identity request 135 9.965614 128.286.49.18 SIAP/_ 192 DownlinMMSTransport, Identity request 137 9.096771 127.0.0.4 DIAME_ 324 ced326PP-Authentication-Information Assec(1310) flags=-P appl=36PP S6a/S6d(16777 138 9.999177 128.286.49.48 128.288.49.48 SIAP/_ 140 DownlinMMSTransport, Authentication reguest 1310.172748 128.288.49.48 SIAP/_ 120 DownlinMMSTransport, Authentication reguest 135 10.715918 128.288.49.48 SIAP	ppl=Diameter Common Messages(0) h2h=31a76920 e2c=383_ appl=Diameter Common Messages(0) h2h=1a677df2 e2c=38_ ppl=Diameter Common Messages(0) h2h=1a677df2 e2c=387_ tivity request 318) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a7_ 18) flags=-P appl=3GPP S6a/S6d(16777251) h2h=31a7_	74 4.265	Source	-		
75 4.265548 127.0.0.4 127.0.0.1 DIAME_ 156 cmd=Device-Watchdog Answer(280) flags= appleDiameter Common Messages(0) h2h=11 124 7.797632 127.0.0.5 127.0.0.5 DIAME_ 144 cmd=Device-Watchdog Request(280) flags= appleDiameter Common Messages(0) h2h=1a 134 9.965372 128.208.49.18 128.208.49.18 SIAP/_ 192 InitalUEMessage, Attach request, PDM connectivity request 135 9.96634 128.208.49.18 128.208.49.18 SIAP/_ 192 InitalUEMessage, Attach request, PDM connectivity request 136 9.996435 128.208.49.18 128.208.49.18 SIAP/_ 140 DomlinMMASTransport, Identity request 137 9.99643 127.0.0.1 DIAME_ 37 Cmd=2GPP-Authentication-Information Request(318) flags=P appl=3GPP S6a/S6d(16777 138 9.99674 127.0.0.1 DIAME_ 37 Cmd=2GPP-Authentication-Information Request(318) flags=P appl=3GPP S6a/S6d(16777 139 9.99977 128.208.49.18 128.208.49.18 SIAP/_ 140 DomlinMASTransport, Authentication request 139 108.10779 128.208.49.18 128.208.49.18 SIAP/_ 128 DomlinMASTransport, Sec	ppl=Diameter Common Messages(0) h2h=31a76920 e2c=383_ appl=Diameter Common Messages(0) h2h=1a677df2 e2c=38_ ppl=Diameter Common Messages(0) h2h=1a677df2 e2c=387_ tivity request 318) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a7_ 18) flags=-P appl=3GPP S6a/S6d(16777251) h2h=31a7_					
124 7.707434 127.0.0.5 DIAME_ 144 cmd=Device-Watchdog Request(280) flags=R appleDiameter Common Messages(0) h2h=1a 134 9.965512 128.288.49.18 128.288.49.18 128.288.49.18 128.288.49.18 51AP/_ 192 InitialUEMessage, Attach request, PDM connectivity request 135 9.965614 128.288.49.18 128.288.49.18 51AP/_ 140 DownLinMMSTransport, Identity request 136 9.996571 127.0.0.4 DIAME_ 324 cmd=3CPP-Authentication-Information Request(318) flags=R appl=3CPP S6a/S6d(16777) 137 9.996771 127.0.0.4 DIAME_ 324 cmd=3CPP-Authentication-Information Request(318) flags=R appl=3CPP S6a/S6d(16777) 138 9.999177 128.288.49.48 128.288.49.48 S1AP/_ 144 DownLinMMSTransport, Authentication request 139 19.21671 128.288.49.48 128.288.49.48 S1AP/_ 140 DownLinMMSTransport, Authentication request 139 10.217248 128.288.49.48 128.288.49.48 S1AP/_ 120 DownLinMMSTransport, Security mode command AVP: 128.288.49.18 128.288.49.48 S1AP/_ 120 DownLinMMSTransport, Security mode command	appl=Diameter Common Messages(0) h2h=1a677df2 e2e=38_ ppl=Diameter Common Messages(0) h2h=1a677df2 e2e=387_ tivity request 318) flags=RP appl=3GPP 56a/56d(16777251) h2h=31a7_ 18) flags=-P appl=3GPP 56a/56d(16777251) h2h=31a7_	75 4.265				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 DIAME 156 cmd=Doutcowstration Antome (280) flags= appl=Diameter Common Messages(0) h2h=lad 134 9.65514 128.208.49.18 128.208.49.18 128.208.49.18 51AP/- 196 DownlinkMSTransport, Identity request 135 9.996455 128.208.49.18 128.208.49.18 51AP/- 104 DplinkMSTransport, Identity request 136 9.996454 127.0.0.4 127.0.0.4 01AME 376 cmd=30P-Authentication request 1018) flags=NP	ppl=Diameter Common Messages(8) h2h=1a677df2 e2e=387_ tivity request 318) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a7_ 18) flags=-P appl=3GPP S6a/S6d(16777251) h2h=31a76_					
134 9.965372 128.288.49.18 128.288.49.48 51AP/_ 192 InitialUHessage, Attach request, PDN connectivity request 135 9.96545 128.288.49.18 128.288.49.18 128.288.49.18 51AP/_ 144 UplimMASTransport, Identity request 137 9.996474 127.0.0.4 01AWL 324 cmd=3GPP-Authentication-Information Answer(310) flags=RP appl=3GPP S6a/S6d(16777 158 9.999174 128.288.49.18 128.288.49.18 51AP/_ 140 DownlinkMASTransport, Authentication request 153 10.177248 128.288.49.18 128.288.49.18 51AP/_ 140 DownlinkMASTransport, Authentication request 153 10.177248 128.288.49.18 128.288.49.48 51AP/_ 120 DownlinkMASTransport, Authentication request 159 10.217244 127.0.0.1 127.0.0.4 DIAME_ 328 cmd=3GPP-Uplate-Location Request(316) flags=RP	tivity request 318) flags=RP appl=3GPP 56a/S6d(16777251) h2h=31a7. 18) flags=-P appl=3GPP 56a/S6d(16777251) h2h=31a76.					144 cmd=Device-Watchdog Request(280) flags=R appl=Diameter Common Messages(0) h2h=1a677df2 e2e=38
135 9.965614 128.288.49.48 128.288.49.18 S1AP/_ 180 DownLinkWASTransport, Identity request 136 9.996571 127.6.0.4 DIAME_ 372 cmto250P_Authentication_Information Request(318) flags=RP appl=3GPP 56a/56d(16777 148 9.990744 127.6.0.4 127.0.0.4 DIAME_ 372 cmto250P_Authentication_Information Request(318) flags=RP appl=3GPP 56a/56d(16777 148 9.990744 127.0.0.4 DIAME_ 376 cmto250P_Authentication_Information Request(318) flags=RP appl=3GPP 56a/56d(16777 158 9.990744 128.286.49.48 128.286.49.18 SIAP/_ 144 DPulinkWASTransport, Scurity mode command 159 10.170714 128.286.49.18 128.288.49.18 SIAP/_ 120 DownLinkWASTransport, Scurity mode compand 159 10.216759 128.286.49.18 128.288.49.18 SIAP/_ 120 DownLinkWASTransport, Scurity mode compand 159 10.216759 128.286.49.18 127.0.0.4 DIAME_ 328 cmd=30P-Update_Location Request(316) flags=RP- appl=36PP 56a/56d(16777251) h2h=3 AVP: Origin-Realm(236) L=19 f=-M- val=Localdomain N/Y N/Y N/Y N/Y N/Y Side(316) flags=RP- ap	318) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a7_ 18) flags=-P appl=3GPP S6a/S6d(16777251) h2h=31a76_					
136 9.99643 128.288.49.18 128.288.49.48 51AP/_ 144 Uplinklastransport, identity response 137 9.99643 127.6.0.4 127.6.0.4 0DME. 224 cod.560P-Authentication-Information Request[318] flags=RP appl=3GPP 56a/56d(16777. 136 9.99917 128.288.49.48 128.288.49.48 128.288.49.48 51AP/_ 144 DownLinkWaStransport, Authentication request 135 10.177248 128.288.49.48 128.288.49.48 51AP/_ 144 DownLinkWaStransport, Authentication request 159 10.2175748 128.288.49.18 51AP/_ 144 DownLinkWaStransport, Security mode command 159 10.217244 127.0.0.1 127.0.0.4 DIAME 328 cmd=3GPP-Update-Location Request(316) flags=RP	18) flags=-P appl=3GPP \$6a/\$6d(16777251) h2h=31a76_					
137 127.0.0.1 127.0.0.4 D144E 324 Cmt=36PP-Authenticition-Information Assequent(318) flags=RP appl=36PP 56a/56d(16777) 148 9.999177 128.288.49.48 128.288.49.48 128.288.49.48 128.288.49.48 128.288.49.48 128.288.49.48 128.288.49.48 SIAP/- 140 DownLinMASTransport, Authentication request 153 10.177248 128.288.49.48 128.288.49.48 SIAP/- 140 DownLinMASTransport, Authentication request 159 10.216759 128.288.49.18 128.288.49.18 SIAP/- 120 DownLinMASTransport, Security mode command 159 10.216759 128.288.49.18 127.0.0.4 DIAHE 326 cmd=3GPP-Update-Location Request(316) flags=RP	18) flags=-P appl=3GPP \$6a/\$6d(16777251) h2h=31a76_					
148 9.99874 127.0.0.4 127.0.0.1 DIAME_ 376 cmd=3CPP_Authentication_Information Answer(318) flags=-P appl=3CPP 56a/56d(16777; 150 9.99874 128.288.49.48 128.288.49.48 SIAP/- 140 DownLinMWASTransport, Authentication reguest 153 10.176218 128.288.49.48 128.288.49.18 SIAP/- 120 DownLinMWASTransport, Authentication reguest 153 10.177246 128.288.49.18 128.288.49.18 SIAP/- 120 DownLinMWASTransport, Security mode command 159 10.217244 127.0.0.1 127.0.0.4 DIAME_ 328 cmd=3CPP_Update_Location Request(316) flags=RP	18) flags=-P appl=3GPP \$6a/\$6d(16777251) h2h=31a76_	136 9.996	435 128.208.49.18	128.208.49.48	S1AP/	
150 9.999177 128.288.49.48 128.288.49.18		137 9.996	5771 127.0.0.1	127.0.0.4		324 cmd=3GPP-Authentication-Information Request(318) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a7
152 10:17618 128.288.49.18 128.288.49.48 51AP/_ 124 UplinkMASTransport, Authentication response 153 10:17724 128.288.49.18 128.288.49.18 51AP/_ 120 DownlinkMASTransport, Security mode compate 159 10:21724 127.8.0.1 127.0.0.4 01AME_ 328 cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP 56a/56d(16777251) h2h=37 AVP: Origin-Realm(296) 1=19 f=-Mval=Locatiomain aver. val=1054000000000 AVP: User-Hame(1) 1-23 f=-M-val=10540000000000 aver. val=105400000000000000000000000000000000000		148 9.998	127.0.0.4	127.0.0.1	DIAME	376 cmd=3GPP-Authentication-Information Answer(318) flags=-P appl=3GPP S6a/S6d(16777251) h2h=31a76
153 19.177248 128.288.49.48 128.288.49.18 51AP/_ 120 DownLinkWaSTransport, Security mode compacts 160 10.217244 127.6.0.4 127.0.0.4 DIAME_ 320 cmd=3GPP-Update_Location Request(316) flags=RP appl=3GPP 56a/56d(16777251) h2h=3 AVP: Origin-Realm(280) l=19 fs-H- val=localdomain NAME_ Origin-Realm(281) l=19 fs-H- val=localdomain NAME_ AVP: Origin-Realm(281) l=19 fs-H- val=localdomain NAME_ NAME_ NameL NameL NameL VVP: Userination-Realm(281) l=19 fs-H- val=localdomain NAME_ NameL Name	RP appl=3GPP 56a/56d(16777251) h2h=31a76922 e2e=38_					
159 102.16759 128.208.49.18 128.208.49.48 51AP/_ 136 UplinkWASTransport, Security mode complete 160 10.21724 127.0.0.1 127.0.0.4 DIAME_ 328 cmd=3GPP-Update_Location Request(316) flags=RP appl=3GPP 56a/56d(16777251) h2h=3 AWP: Origin-Realm(236) l=19 f=-M- val=localdomain AWP: User-Hame(1) l=23 f=-M- val=3054000000000 AVP: Requested-EUTRNA-Authentication-Info Val=Scaldomain AVP: Requested-EUTRNA-Authentication-Info Nadatory: Set AVP Length: 44 - - V Requested-EUTRNA-Authentication-Info: 00000582c0000010000028af000000100000584c000010_ AVP: Requested-Vectors(1410) l=16 f=WH vn== V Requested-EUTRNA-Authentication-Info: 00000582c0000010000028af00000010	RP appl=3GPP 56a/56d(16777251) h2h=31a76922 e2e=36_	152 10.17	6918 128.208.49.18	128.208.49.48	S1AP/	144 UplinkNASTransport, Authentication response
160 127.0.0.1 127.0.0.4 DIAME_ 328 cmd=3GPP-Update-Location Request(316) flags=RP- appl=3GPP S6a/S6d(16777251) h2h=3 AVP: Origin-Real(296) l=19 f=-M- val=Locatiomain AVP: User-Name(1) L=23 f=-M- val=D054000000000 AVP: User-Name(1) L=23 f=-M- val=D0540000000000 AVP: User-Name(1) L=23 f=-M- val=D0540000000000 AVP: User-Name(1) L=23 f=-M- val=D0540000000000 AVP (Idgs: 0xc0, Vendor-Specific: Set, Mandatory: Set AVP Flags: 0xc0, Vendor-Specific: Set, Mandatory: Set AVP: Number-Of-Requested-UTRNA-Authentication-Info AVP cost 04 00 00 07 64 04 07 60 16 00 01 E-4-0 0 00000584c0000010. V Requested-UTRNA-Authentication-Info: 00000582c0000010000028af0000000000000000000000000000000	RP appl=3GPP 56a/56d(16777251) h2h=31a76922 e2e=38_	153 10.17	7248 128.208.49.48	128.208.49.18	S1AP/	120 DownlinkNASTransport, Security mode command
AVP: Origin Northerlanding > AVP: Origin Northerlanding > AVP: Origin Northerlanding > AVP: User-Name(1) L=23 f=-M- val=localdomain > AVP: User-Name(1) L=23 f=-M- val=0als4000000000 > AVP: Kequested-UIRAN-Authentication-Info > AVP: Code: 1408 Requested-UIRAN-Authentication-Info > AVP Flags: 0xc0, Vendor-Specific: Set, Mandatory: Set AVP Length: 44 > AVP: Requested-UURAN-Authentication-Info > AVP: Requested-UURAN-Authentication-Info > AVP Length: 44 > AVP: Number-Of-Requested-Vectors(1410) L=16 f=WH- vnd=TGPP val=1 > V0 00 60 v0 00 v0	PP appl=3GPP 56a/56d(16777251) h2h=31a76922 e2e=38	159 10.21	128.208.49.18	128.208.49.48	S1AP/	136 UplinkNASTransport, Security mode complete
 A MP: p: drigin-Real(296) l=19 f=-M- val=localdomain A MP: Destination-Real(296) l=19 f=-M- val=localdomain A MP: Lestration-Real(283) l=19 f=-M- val=localdomain A MP: User-Name(1) l=23 f=-M- val=01054000000000 A MP: Requested-EUTRAN-Authentication-Info(1408) l=44 f=VM- vnd=TGPP A MP Flags: 0xc0, Vendor-Specific: Set, Mandatory: Set A MP Flags: 0xc0, Vendor-Specific: Set, Mandatory: Set A MP: Setted-EUTRAN-Authentication-Info: A MP: Requested-EUTRAN-Authentication-Info A MP Flags: 0xc0, Vendor-Specific: Set, Mandatory: Set A VP: Number-Of-Requested-Vectors(1410) l=16 f=VM- vnd=TGPP val=1 A for 0 to 5 to to to 0 to 0 to 0 to 0 to 0 t		160 10.21	127.0.0.1	127.0.0.4	DIAME	328 cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38
AVP: Number-Of-Requested-Vectors(1410) l=16 f=VM- vnd=TGPP val=1 10 40 60 50 60 <			ana Aug Mandan Cassifi.	. Cat Mandatamus Cat		
▶ AVP: Number-Of-Requested-Vectors(1410) l=16 f=VM- vnd=TGPP val=1 Number-Of-Requested-Vectors(1410) l=16 f=16 f=0		► AVP Fla		:: Set, Mandatory: Set		
10 45 00 01 34 62 04 06 <td< th=""><th></th><th>▶ AVP Fla AVP Ler</th><th>ngth: 44</th><th>-</th><th></th><th></th></td<>		▶ AVP Fla AVP Ler	ngth: 44	-		
22 77 00 00 04 08 d4 07 1c 95 08 33 7b a0 57 aa 3b		► AVP Fla AVP Ler ▼ Request	ngth: 44 ted-EUTRAN-Authentication-	-Info: 00000582c000001	0000028af000	
20 77 00 00 00 04 06 04 06 04 06 04 06 04 06 04 06 04 06 04 06 04 06		► AVP Fla AVP Ler ▼ Request	ngth: 44 ted-EUTRAN-Authentication-	-Info: 00000582c000001	0000028af000	
38 80 18 91 5e ff 20 00 01 10 <td< td=""><th></th><td>► AVP Fla AVP Ler ▼ Request</td><td>ngth: 44 ted-EUTRAN-Authentication-</td><td>-Info: 00000582c000001</td><td>0000028af000</td><td></td></td<>		► AVP Fla AVP Ler ▼ Request	ngth: 44 ted-EUTRAN-Authentication-	-Info: 00000582c000001	0000028af000	
10 eb 33 99 e5 91 00 91 00 c7 00 91 36 01 00 23		 AVP Fla AVP Ler Request AVP: AVP: 45 00 02 	ngth: 44 ted-EUTRAN-Authentication : Number-Of-Requested-Vect 5 04 05 05 05 05 05 05 05 05 05	-Info: 00000582c000001 ors(1410) l=16 f=VM- v c cc c	0000028af000 /nd=TGPP val: -4@- @	=1
30 31 à7 69 21 38 37 01 d4 00 00 01 à7 69 02 1:187		 AVP Fla AVP Ler Request AVP: AVP: 45 00 02 7f 00 00 	ngth: 44 ted-EUTRAN-Authentication : Number-Of-Requested-Vect 3 34 8c 1a 40 00 40 06 a 1 34 8c 1a 40 00 40 06 5 08 3	-Info: 00000582c000001 ors(1410) l=16 f=VM- v 0 00 00 01 00 00 f a4 7f 00 00 01 E 8 7b a0 57 aa 3b	0000028af000 /nd=TGPP val: -4@.@@	=1
60 61 62 62 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 64 65 65 65 <td< td=""><th></th><td> ► AVP Fla AVP Ler ▼ Request ► AVP: ► AVP: 0 45 00 00 20 7f 00 00 80 18 01 </td><td>ngth: 44 ted-EUTRAN-Authentication: Number-Of-Requested-Vect 3 04 06 06 06 06 06 06 06 1 34 8c 1a 40 00 40 06 a 0 04 88 04 0f 1c 95 08 3 1 5e ff 2b 00 08 01 01 0</td><td>-Info: 00000582c000001 ors(1410) l=16 f=VM- v f a4 7f 00 00 01 E 8 7b a0 57 aa 3b 8 0a a3 bb 1f 91</td><td>0000028af000 /nd=TGPP val .4@.@</td><td>=1</td></td<>		 ► AVP Fla AVP Ler ▼ Request ► AVP: ► AVP: 0 45 00 00 20 7f 00 00 80 18 01 	ngth: 44 ted-EUTRAN-Authentication: Number-Of-Requested-Vect 3 04 06 06 06 06 06 06 06 1 34 8c 1a 40 00 40 06 a 0 04 88 04 0f 1c 95 08 3 1 5e ff 2b 00 08 01 01 0	-Info: 00000582c000001 ors(1410) l=16 f=VM- v f a4 7f 00 00 01 E 8 7b a0 57 aa 3b 8 0a a3 bb 1f 91	0000028af000 /nd=TGPP val .4@.@	=1
70 31 35 37 30 30 35 39 31 33 39 3b 31 3b 61 70 70 15708591 39;1;app 80 57 73 35 61 00 00 01 15 40 00 00 c 00 00 00 00s6a		 ► AVP Fla AVP Ler ▼ Request ► AVP: 00 00 00 00 00<td>ngth: 44 ted-EUTRAM-Authentication: Number-Of-Requested-Vect 3 48 Cc 1a 40 00 40 66 a 0 44 88 d4 71 C 95 88 3 1 5e ff 2b 00 00 01 91 60 80</td><td>-Info: 00000582c000001 ors(1410) l=16 f=VM- v 6 00 00 01 00 f a4 7f 00 00 01 E- f a4 7f 00 00 01 E- 8 0a a3 bb 1f 91 3 e 01 00 00 23</td><td>0000028af000 /nd=TGPP val: -4 ·@ @ </td><td>=1. </td>	ngth: 44 ted-EUTRAM-Authentication: Number-Of-Requested-Vect 3 48 Cc 1a 40 00 40 66 a 0 44 88 d4 71 C 95 88 3 1 5e ff 2b 00 00 01 91 60 80	-Info: 00000582c000001 ors(1410) l=16 f=VM- v 6 00 00 01 00 f a4 7f 00 00 01 E- f a4 7f 00 00 01 E- 8 0a a3 bb 1f 91 3 e 01 00 00 23	0000028af000 /nd=TGPP val: -4 ·@ @ 	=1.
99 00 00 01 08 40 00 00 17 6d 6d 65 2e 6c 6f 63 61		 ► AVP Fla AVP Ler ▼ Requestine ► AVP: ■ AVP: ■ AVP: ■ 45 00 01 ■ 45 00 01	ngth: 44 ted-EUTRAN-Authentication: Number-Of-Requested-Vect 3 00 00 00 00 00 00 00 00 1 34 8cl a4 00 04 00 6c 0 04 88 d4 0f 1c 95 08 3 1 5c ff 2 b0 08 00 101 0 9 c5 01 00 01 00 c0 08 0 9 21 38 37 01 d4 00 00 00	-Info: 00000582c000001 ors(1410) L=16 f=VM-v f a4 77 00 00 01 E 8 7b a0 57 aa 3b 0 aa 3 bb 1f 91 1 3e 01 00 00 23 - 1 07 40 00 00 22 -	0000028af000 /nd=TGPP val: -4 @ @ . 	=1
a0 6c 64 6f 6d 61 69 6e 00 00 00 128 40 00 00 13 ldomain ····(@···		 ► AVP Fla AVP Ler ▼ Request ► AVP: ■ AVP: 00 00 00 00 76 00 00 00 18 01 00 18 02 00 00 18 02 01 00 00 01 10 00	ngth: 44 ted-EUTRAN-Authentication- Number-Of-Requested-Vect 3 48 cc la 40 00 40 06 a 0 44 86 d4 67 lc 95 08 3 1 5c ff 2b 00 00 01 01 c0 00 9 c5 10 00 100 c0 00 0 9 21 33 37 01 d4 00 00 6 9 21 63 61 66 66 6	-Info: 00000552c00001 ors(1410) l=16 f=VM- v or or or or or f a4 7f 00 00 01 E- 8 7b a0 57 aa 3b 8 0a a3 bb 1f 91 1 3e 01 00 00 23 1 07 40 00 00 22 1: f 6d 61 69 63 b	0000028af000 /nd=TGPP val: -4 @ @	=1 • • • • • • • • • • • • • •
		 ▷ AVP Fla AVP Ler ▼ Request ▷ AVP: ○ 00 00 00 ○ 00 00 00 ○ 00 00 00 ○ 00 00 00 ○ 00 00	ngth: 4 ted-EUTRAH-Authentication- Number-Of-Requested-Vect 5 00 00 00 00 00 00 01 1 34 8c la 40 00 40 06 0 48 8d 40 fl 12 50 03 1 5e ff 2b 00 00 01 01 0 9 c5 10 00 100 c 20 00 9 21 38 37 01 44 00 00 0 5 26 6c f6 36 16 6c 64 6 7 30 30 35 39 31 33 39 3 6 10 00 00 15 40 00 0	-Info: 00000552c000001 ors(1410) l=16 f=VM- v f a4 77 00 00 01 E. 8 0a a5 bb 1f 91 13 e 01 00 00 23 1 07 40 00 00 22 1 1 07 40 00 00 22 1 f 6d 61 69 c3 b b 31 3b 61 70 70 15 0 0c 00 00 00 1 _ 55	0000028af000 /nd=TGPP val: -4	=1
		 ▷ AVP Fla AVP Ler ▼ Request ▷ AVP: ○ 00 00 00 00 80 00 00 80 00 00 80 00 01 35 33 00 00 00 	ngth: 4 ted-EUTRAN-Authentization: Number-Of-Requested-Vect 1 34 & C 1a 40 00 40 66 0 46 88 44 71 C 59 68 1 56 ft 2b 00 68 01 10 0 9 5 51 00 01 00 40 00 40 5 26 66 67 63 61 66 64 6 5 26 66 67 63 61 66 64 6 5 26 66 73 61 80 00 8 6 84 00 00 01 75 40 00 8 1 88 40 00 01 76 64 00 7 1 88 40 00 01 76 65 66 00 7 1 88 40 00 01 76 65 66 00 7 1 88 40 00 00 7 1 86 40 00 00 00 7 1 86 40 00 00 00 00 00 00 00 00 00 00 00 00	-Info: 00000582c000001 ors(1410) l=16 f=VM- v 0 00 00 01 l=16 8 7b a0 57 aa 3b 10 a0 57 aa 3b 11 3e 01 00 00 21 l 13 e 01 00 00 22 1 1 6d 61 69 6e 3b mm 5 31 3b 61 70 70 15 3 13 c 01 70 70 1 5 2 e 6 C 6 6 36 1	0000028af000 rnd=TGPP valu -4- @ @	=1
b® 6c 6f 63 61 6c 64 6f 6d 61 69 6e 00 00 01 1b localdom ain 00 49 00 00 13 6c 6f 63 61 6c 64 6f 6d 61 69 6e 00 00localdomain.		 ▷ AVP Fla AVP Ler ▼ Request ▷ AVP: ○ 00 00 00 01 45 000 01 02 7f 00 00 03 10 47 60 04 135 33 05 f 73 34 06 06 00 00 06 06 461 	ngth: 4 Ced-EUTRAW-Authentication- Number-Of-Requested-Vect 9 00 00 00 00 00 00 1 34 8c la 40 00 40 45 0 40 86 4d 07 1c 95 00 3 1 5e ff 2b 00 80 41 01 8 9 c 51 00 01 80 c 40 00 9 21 38 37 01 44 00 00 9 21 38 37 01 44 00 00 5 26 c 6f 65 16 15 c 46 6 7 30 30 35 39 31 33 39 1 66 10 00 01 75 40 00 1 84 00 00 01 75 60 60 1 86 40 00 00 17 66 60	Info: 00008582c00001 ors(1440) l=16 f=M+ or 00 or 10 or f ad 7f 80 00 01 E 7 ba 07 as a b 80 as 3b 1f 91 13 e 01 00 02 3 1 07 40 00 02 2 1 07 40 00 00 2 f de 15 96 c b m m b 31 3b 61 70 70 5 2 e 6 c 6f 63 61 5 2 e 6 c 6f 63 61 2 8 40 00 00 13 1d	0000028af000 rnd=TGPP val 	=1
		 ▶ AVP Fla AVP Ler ▼ Request ▶ AVP: ♥ AvP	ngth: 4 ted-EUTRAN-Authentication: Number-Of-Requested-Vect 1 34 & C la 40 00 40 66 a 0 44 88 4d 91 12 95 083 1 5e ff 2b 00 00 10 10 0 9 21 38 57 01 64 00 60 0 9 21 38 57 01 64 00 00 9 21 39 57 01 64 00 00 9 21 30 57 01 64 00 9 21 30 57 01 9 21	Info: 0000852c00001 org(1410) l=16 f=VM- v 0 0 0 0 0 0 0 0 f 44 7 f 00 00 01 E 18 0 13 0 0 0 1 8 0 10 0 0 1 8 0 10 0 0 1 8 0 10 0 0 1 0 7 40 0 0 0 2 1 0 7 40 0 0 0 2 1 0 7 40 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 2 0 0 0 0 0 0 0 0 0 0 1 2 2 6 6 6 1 1 28 4 0 0 0 0 1 3 2 6 0 0 0 0 0 1 1 2 8 4 0 0 0 0 1 1 0 0 0 0 0 0 0 1 1 0 0 0 0 0	0000028af000 rnd=TGPP val: -4@	=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.

$\mathsf{MME} \to \mathsf{HSS}/\mathsf{AuC}$

Steps in Authentication: Authentication Info. Answer

- 1 -					Expression
-	p or diameter or gtp			1	
D .	Time	Source	Destination		Length Info
	74 4.265354	127.0.0.1	127.0.0.4	DIAME	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	DIAME	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	DIAME	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	DIAME	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	S1AP/	192 InitialUEMessage, Attach request, PDN connectivity request
	135 9.965614	128.208.49.48	128.208.49.18	S1AP/	108 DownlinkWASTransport, Identity request
	136 9.996435	128.208.49.18	128.208.49.48	S1AP/	144 UplinkNASTransport, Identity response
	137 9.996771	127.0.0.1	127.0.0.4	DIAME	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	DIAME	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	S1AP/	140 DownlinkNASTransport, Authentication request
	152 10.176918	128.208.49.18	128.208.49.48	S1AP/	144 UplinkNASTransport, Authentication response
	153 10.177248	128.208.49.48	128.208.49.18	S1AP/	120 DownlinkNASTransport, Security mode command
	159 10.216759 160 10.217244	128.208.49.18 127.0.0.1	128.208.49.48	S1AP/ DIAME	136 UplinkNASTransport, Security mode complete 328 cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38
	100 10.21/244	127.0.0.1	127.0.0.4	DIAME	326 Cmd=3Grr=Update=Location Request(310) Trags=Rr=- appl=3Grr 56a/56u(16/7/251) hzh=31a/6922 eze=30
_		ath: 132			
	AVP Ver	dor Id: 3GPP (10415))		
			00001c000028af3d35d8a		
			M- vnd=TGPP val=3d35d		ff0c1f71414d5882
			M- vnd=TGPP val=78110		
			M- vnd=TGPP val=42de6		
				71b305e918f39	39333b338c985e6daadb8a117966fbfd3
		st(264) l=23 f=-M- v			
		alm(296) l=19 f=-M- '			
			al=DIAMETER_SUCCESS (
		0 06 00 00 00 00 0 2 4f 40 00 40 06 2		· · h · 0@ · @ ·) < ·	
		of 1c 88 d4 a0 57 a		· · · · · · · · · · · · · · · · · · ·	
		f 5f 00 00 01 01 0		··g·_··	
		1 00 01 34 40 00 0		· · · · · 4 @· · >·	
		8 37 01 d4 00 00 0 c 6f 63 61 6c 64 6		i!87@ ne.loca ldoma	
		0 35 39 31 33 39 3		5700591 39:1:	
		0 00 05 85 c0 00 0	0 90 00 00 28 af _:	s6a · · · · · · · · · ·	
	00 00 05 86 0	0 00 00 84 00 00 2			
				· · · · · (· =5 · · ·	./15
0a0	c0 00 00 1c 0				
00a0 00b0	ff 0c 1f 71 4	00 00 28 af 3d 35 d 11 4d 58 82 00 00 0 78 11 0e a3 22 82 0	5 a8 c0 00 00 14 ·	···qAMA · · · · · · · · · · · · · · · · · ·	

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

 $HSS/AuC \rightarrow MME$

J / full_nextepc.pcap

Packets: 424 · Displayed: 76 (17.9%)

Profile: Defau

Steps in Authentication: Authentication Request

s1ap	or diameter or gtp	v2 or gtp			Expression
lo.	Time	Source	Destination	Protocol	Length Info
	74 4.265354	127.0.0.1	127.0.0.4	DIAME	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	DIAME	156 cmd=Device-Watchdog Answer(280) flags= appl=Diameter Common Messages(0) h2h=31a76920 e2e=383
1	24 7.707434	127.0.0.1	127.0.0.5	DIAME	144 cmd=Device-Watchdog Request(280) flags=R appl=Diameter Common Messages(0) h2h=1a677df2 e2e=38
1	25 7.707632	127.0.0.5	127.0.0.1	DIAME	156 cmd=Device-Watchdog Answer(280) flags= appl=Diameter Common Messages(0) h2h=1a677df2 e2e=387
	34 9.965372	128.208.49.18	128.208.49.48	S1AP/	192 InitialUEMessage, Attach request, PDN connectivity request
	35 9.965614	128.208.49.48	128.208.49.18	S1AP/	108 DownlinkNASTransport, Identity request
	36 9.996435	128.208.49.18	128.208.49.48	S1AP/	144 UplinkNASTransport, Identity response
	37 9.996771	127.0.0.1	127.0.0.4	DIAME	324 cmd=3GPP-Authentication-Information Request(318) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a7
	48 9.998744	127.0.0.4	127.0.0.1	DIAME	376 cmd=3GPP-Authentication-Information Answer(318) flags=-P appl=3GPP S6a/S6d(16777251) h2h=31a76
	50 9.999177	128.208.49.48	128.208.49.18	S1AP/	140 DownlinkNASTransport, Authentication request
	52 10.176918	128.208.49.18	128.208.49.48	S1AP/	144 UplinkNASTransport, Authentication response
	53 10.177248	128.208.49.48	128.208.49.18	S1AP/	120 DownlinkNASTransport, Security mode command
	59 10.216759 60 10.217244	128.208.49.18 127.0.0.1	128.208.49.48	S1AP/ DIAME	136 UplinkNASTransport, Security mode complete 328 cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38
		v value			
		0000 = 0 = 000 = ⊳ Authenticat	Spare half octet: 0 Type of security con NAS key set identific on Parameter RAND - 1	text flag (T er: (0) ASM EPS challenge	
	00 04 00 01 0	0 06 18 03 73 21 3	71 00 00 08 00		
0000		7 70 40 00 40 84 6	a9 80 d0 31 30 E	gp@·@·n· 1··<·W·]· #0<	· 10

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

Downlink Transport

$MME \rightarrow UE$

Steps in Authentication: Authentication Response

stan	or diameter or gtp	v2 or ato			Expression
-			and the set		
lo.	Time	Source	Destination		Length Info
	74 4.265354	127.0.0.1	127.0.0.4	DIAME	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	DIAME	156 cmd=Device-Watchdog Answer(280) flags= appl=Diameter Common Messages(0) h2h=31a76920 e2e=383
	24 7.707434	127.0.0.1	127.0.0.5	DIAME	144 cmd=Device-Watchdog Request(280) flags=R appl=Diameter Common Messages(0) h2h=1a677df2 e2e=38
	25 7.707632	127.0.0.5	127.0.0.1	DIAME	156 cmd=Device-Watchdog Answer(280) flags= appl=Diameter Common Messages(0) h2h=1a677df2 e2e=387
	34 9.965372	128.208.49.18	128.208.49.48	S1AP/	192 InitialUEMessage, Attach request, PDN connectivity request
	35 9.965614	128.208.49.48	128.208.49.18	S1AP/	108 DownlinkNASTransport, Identity request
1	36 9.996435	128.208.49.18	128.208.49.48	S1AP/	144 UplinkNASTransport, Identity response
1	37 9.996771	127.0.0.1	127.0.0.4	DIAME	324 cmd=3GPP-Authentication-Information Request(318) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a7
1	48 9.998744	127.0.0.4	127.0.0.1	DIAME	376 cmd=3GPP-Authentication-Information Answer(318) flags=-P appl=3GPP S6a/S6d(16777251) h2h=31a76
1	50 9.999177	128.208.49.48	128.208.49.18	S1AP/	140 DownlinkNASTransport, Authentication request
1	52 10.176918	128.208.49.18	128.208.49.48	S1AP/	144 UplinkNASTransport, Authentication response
1	53 10.177248	128.208.49.48	128.208.49.18	S1AP/	120 DownlinkNASTransport, Security mode command
1	59 10.216759	128.208.49.18	128.208.49.48	S1AP/	136 UplinkNASTransport, Security mode complete
1	60 10.217244	127.0.0.1	127.0.0.4	DIAME	328 cmd=3GPP-Update-Location Request(316) flags=RP appl=3GPP S6a/S6d(16777251) h2h=31a76922 e2e=38
		Length: 8	ion response paramete 3 10ea322820580		
		RES: 781 m 3: id-EUTRAN-CGI	10ea322820580		
		em 3: id-EUTRAN-CGI			
	▶ 10	em 4: 10-1A1			
000		0 06 a0 b3 cc 46 c		· · · · · · · F · ·	
		0 0f 40 00 40 84 d		@. @	
		: b4 8e 3c a9 17 3 : 10 a6 b6 00 01 a		10···< ··:@	
		7 23 51 3d 00 01 0		· 0 · #0= · · · ·	
		00 05 00 00 00 0		@;	
060	02 00 02 00 1a	00 12 11 17 f6 c			
		3 22 82 05 80 00 6		····"·· ··d@	
080	45 00 00 10 10	00 43 40 06 00 1	9 f0 45 00 01 00 E·	·····C@ ·····I	

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

$UE \rightarrow MME$

Steps in Authentication: Security Mode

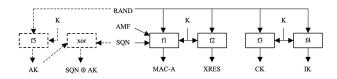
- Initialize signaling security between the UE and the MME
- UE derives corresponding CK, IK keys for encryption and Integrity algorithms

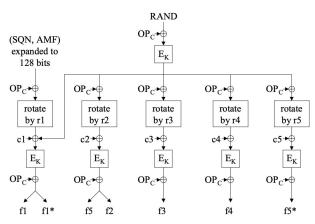
Completes Authentication and UE successfully attaches to the network.

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.

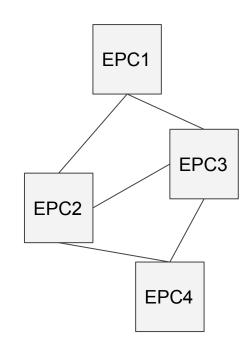




Definition of f1, f1*, f2, f3, f4, f5 and f5*

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

W

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

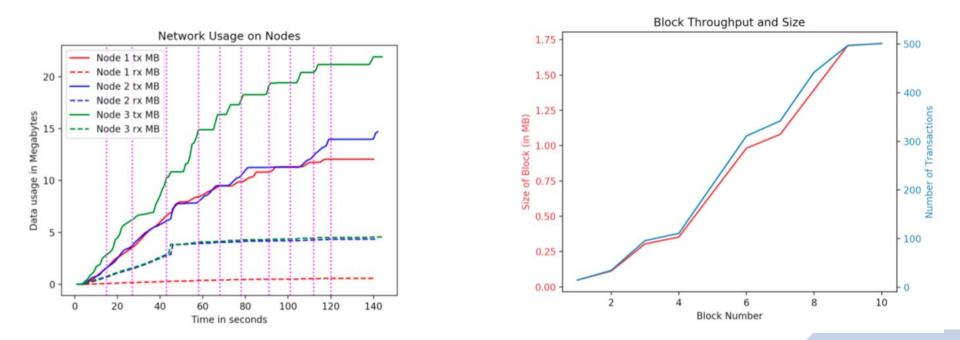
- 1x 8GB RAM Zotac Mini Computers
- 1x 4GB RAM Zotac Mini Computer
- 1x 8GB RAM Dell workstation



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)

W

W

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





Any questions? You can find me at @sudheesh001 & <u>sudheesh@cs.washington.edu</u>

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