



Free5GCのUE/RAN疑似プログラムについて

NTT ネットワークサービスシステム研究所

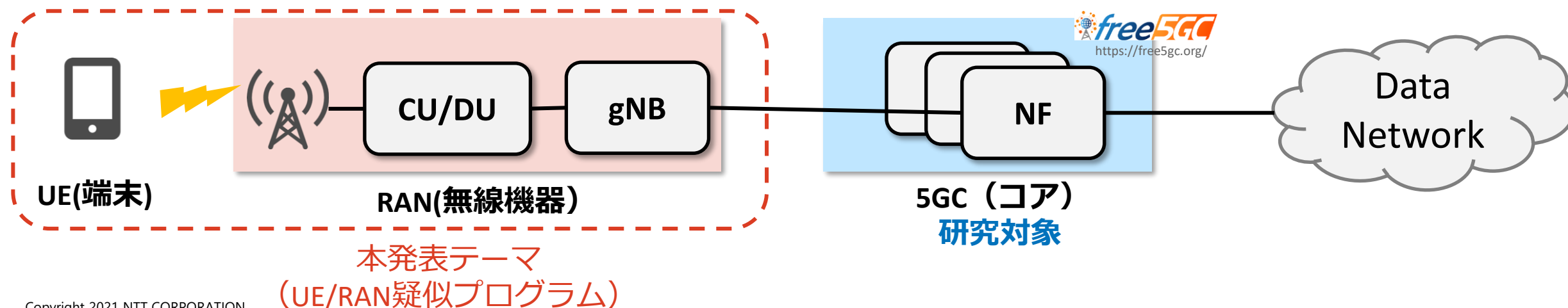
上酔尾 一真

2021年2月4日 Open Mobile Network Infra Meetup #1

□ 5GCの試験に必要なUE/RAN疑似プログラムの開発についてご紹介

□ 取り組み背景

- 手軽に5GCを試したい
 - › UE/RANがないと5GCを試せない。
 - › 職場の検証環境は試験機を利用。（リソースが限られているので自由には使えない...）
- 5GCの中身を理解したい
 - › 5G-SAは開発過渡期で不具合多いためトラブル時に解析が必要。
 - › プロトコルと実装の理解を深めたい



UE/RAN疑似ソフトウェアについて



□ OSS

- LTEと比較して5Gのソフトウェアはまだまだ開発過渡期
- 以下のOSSの開発が活発（個人開発？）
 - › *hhorai/gnbsim* (<https://github.com/hhorai/gnbsim>)
 - › *aligungr/ueransim* (<https://github.com/aligungr/UERANSIM>)

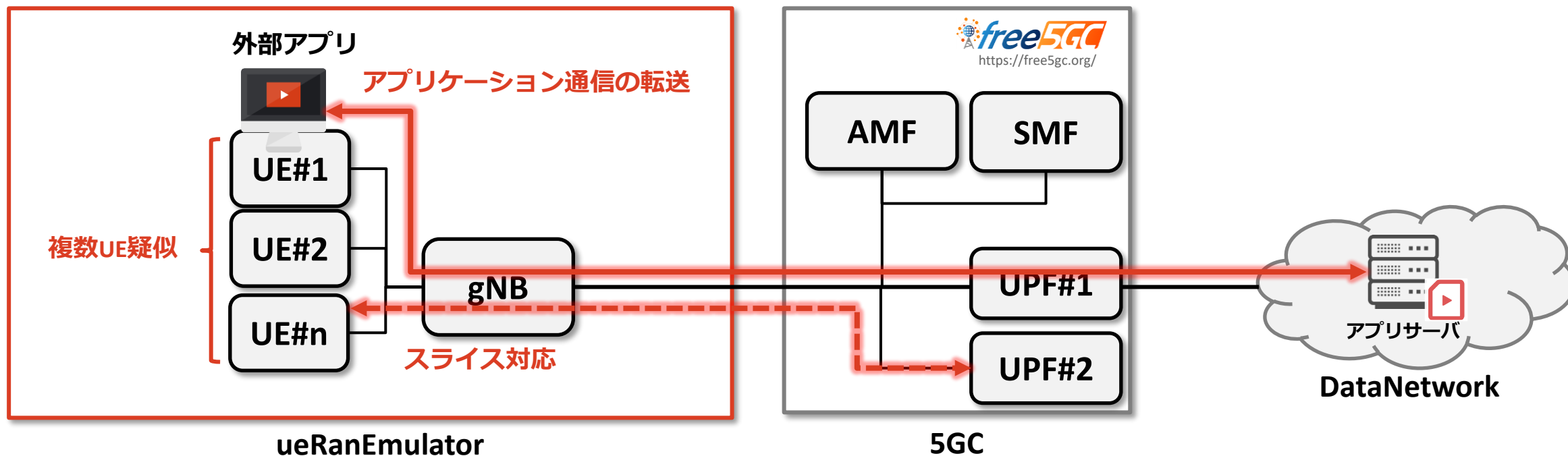
□ Free5GCに同梱([free5gc/test/ueRanEmulator](#))

- Free5GCの動作確認を行うためのテストプログラム (v3.0.4で追加)
- 様々なパラメータが固定値で装置登録/疑似トラフィック送信のみ可能
- Free5GCの実装なので5GCの理解にも役立ちそう

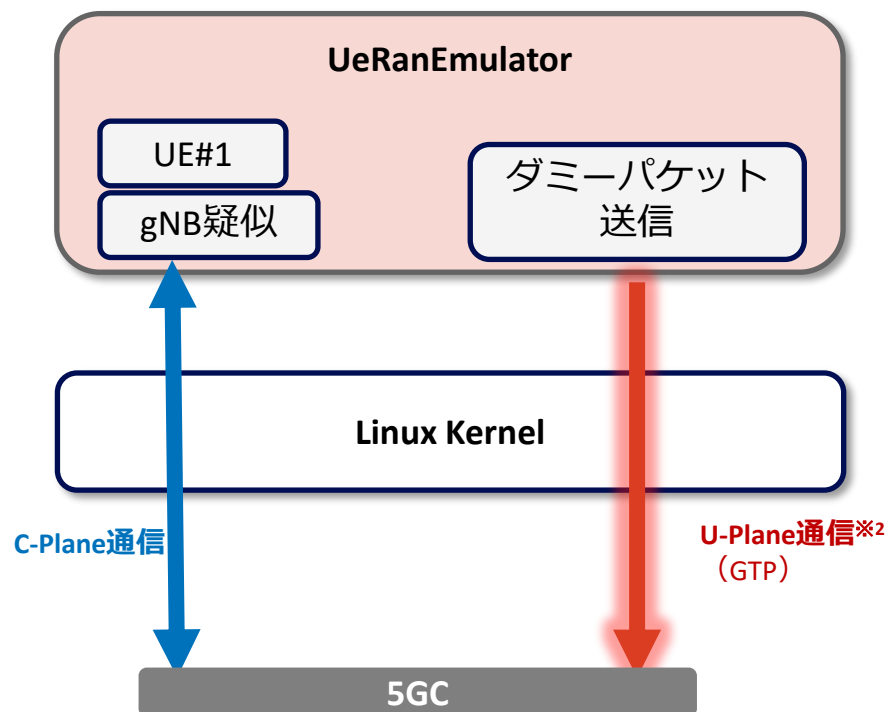
本発表ではueRanEmulatorを改良

□ 5GCの負荷試験/スライス試験ができるような機能を実現

- › アタッチ/デタッチ、PDUセッション確立
- › アプリケーション通信の転送
- › 複数UE疑似（10～100台）
- › スライス対応、SST/SD/DNNに応じた振り分け



ueRanEmulatorの実装概要



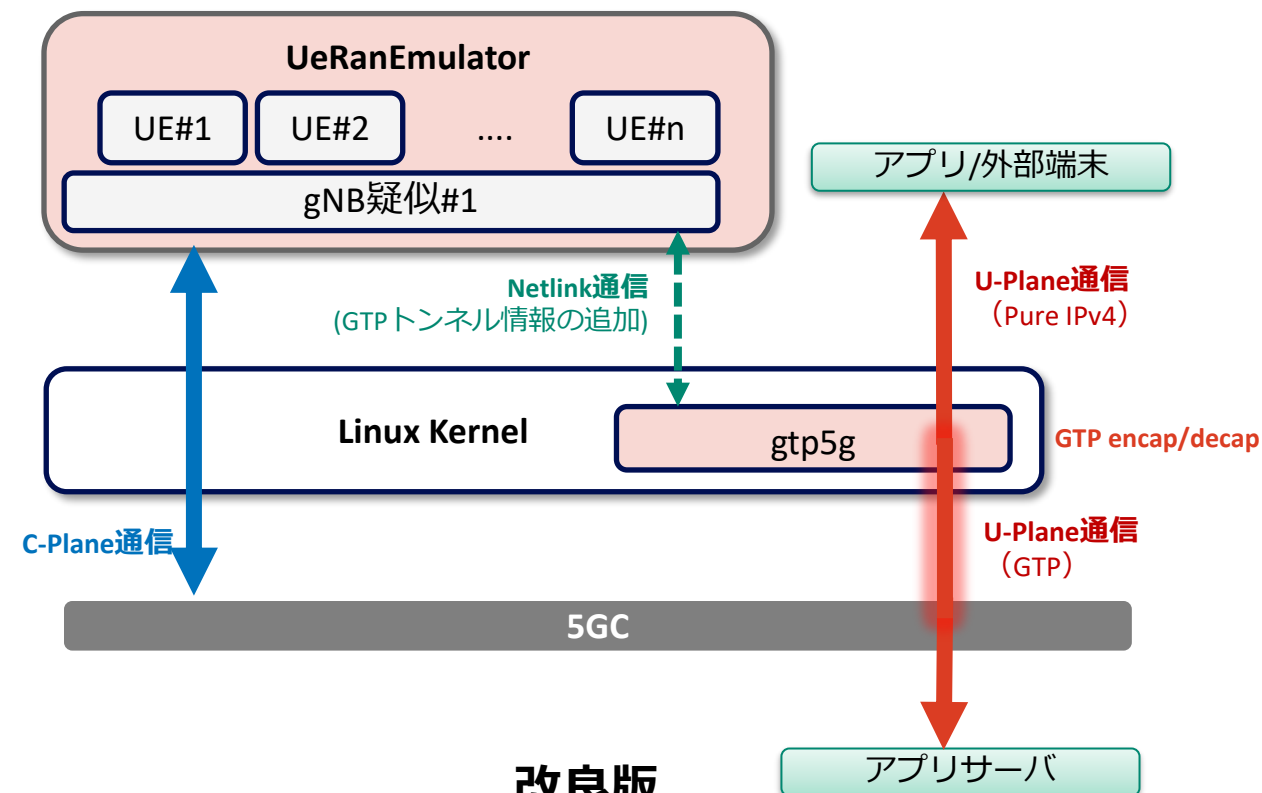
もともとの実装

できること

- 1台のUE/RAN(gNB)を疑似して5GCにアタッチ
- U-Plane疑似通信 (送信のみ)
- 一部パラメータ認証情報 (IMSI/K等) をConfigで指定可能

※1 一部固定値のため、5GCと不整合が発生して通信に失敗する場合あり。

※2 指定した宛先へのUDPパケット送信のみ可能。



改良版

できること

- 複数gNB/UE疑似して5GCへアタッチ/デタッチ
- 外部アプリのトラフィック転送 (上下通信)

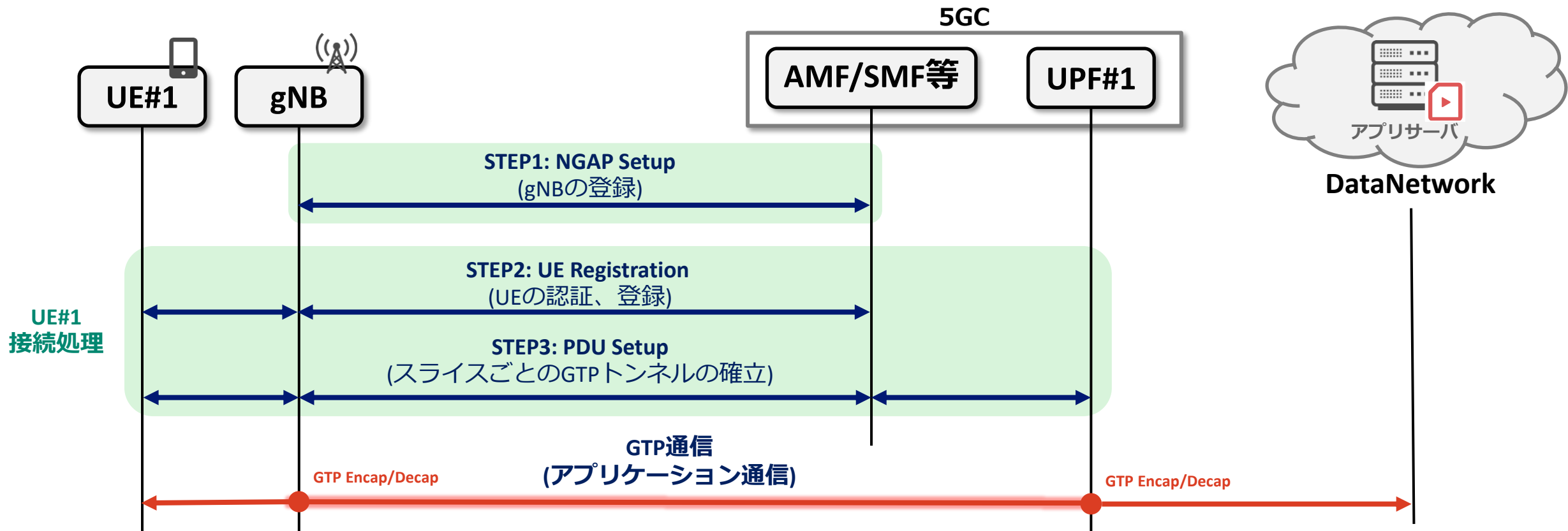
ポイント

- パラメータのハードコーディングを削除 (ネゴシエーション時に取得)
- U-Plane処理はFree5GC UPFと同じカーネルモジュールを利用 (gtp5g)

UE/RAN接続シーケンス（概略）

□ UE/gNBの接続は大まかに3つのステップで処理される。

- › Step1: NGAPセットアップ
- › Step2: UE認証、5GCへの登録
- › Step3: PDUセッション確立



UE認証処理（概略図）

- UEは事前登録情報に加えて動的生成される情報で認証する。
- 認証情報を正しく使わないと、以降の処理でMACエラーが発生する。



UE認証情報（事前登録）

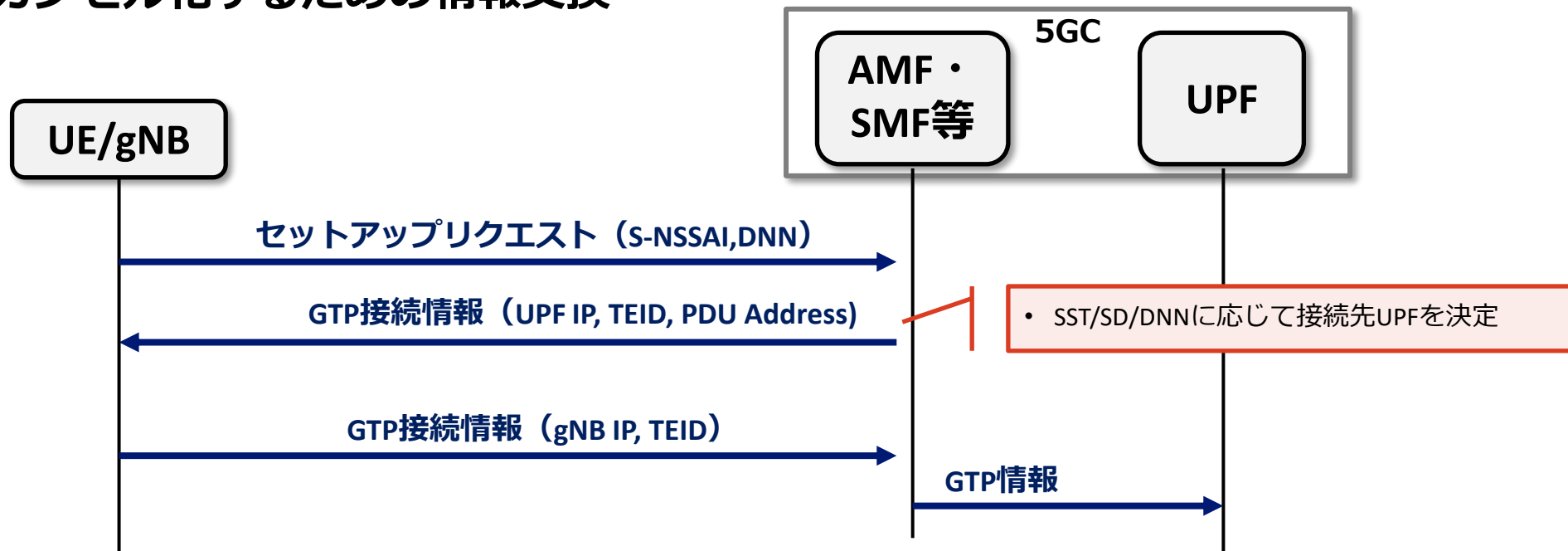
パラメータ	概要
PLMN	事業者識別子
IMSI	PLMN + ユーザ識別子
K	暗号鍵
OP/OPc	オペレーターコード

認証処理で生成される主な情報

パラメータ	概要
SQN	シーケンス番号
RAND	乱数
MAC	メッセージ認証コード
RES	ユーザ応答
AUTN	SQN/AMF/MACで生成

PDUセッション(GTPトンネル確立) (概略図)

□ GTPでカプセル化するための情報交換



ネゴシエーション時に生成される主な情報

パラメータ		概要
5GCが払い出し	GTP-TEID	GTP通信を識別するためのID
	UPF IP	GTP通信で利用するUPFのIPアドレス
	PDU Address	UEに払い出されるIPアドレス
UE/gNBが通知	gNB IP	GTP通信で利用するgNBのIPアドレス
	GTP-TEID	GTP通信を識別するためのID
	S-NSSAI	スライス識別子 (SST/SDで生成)

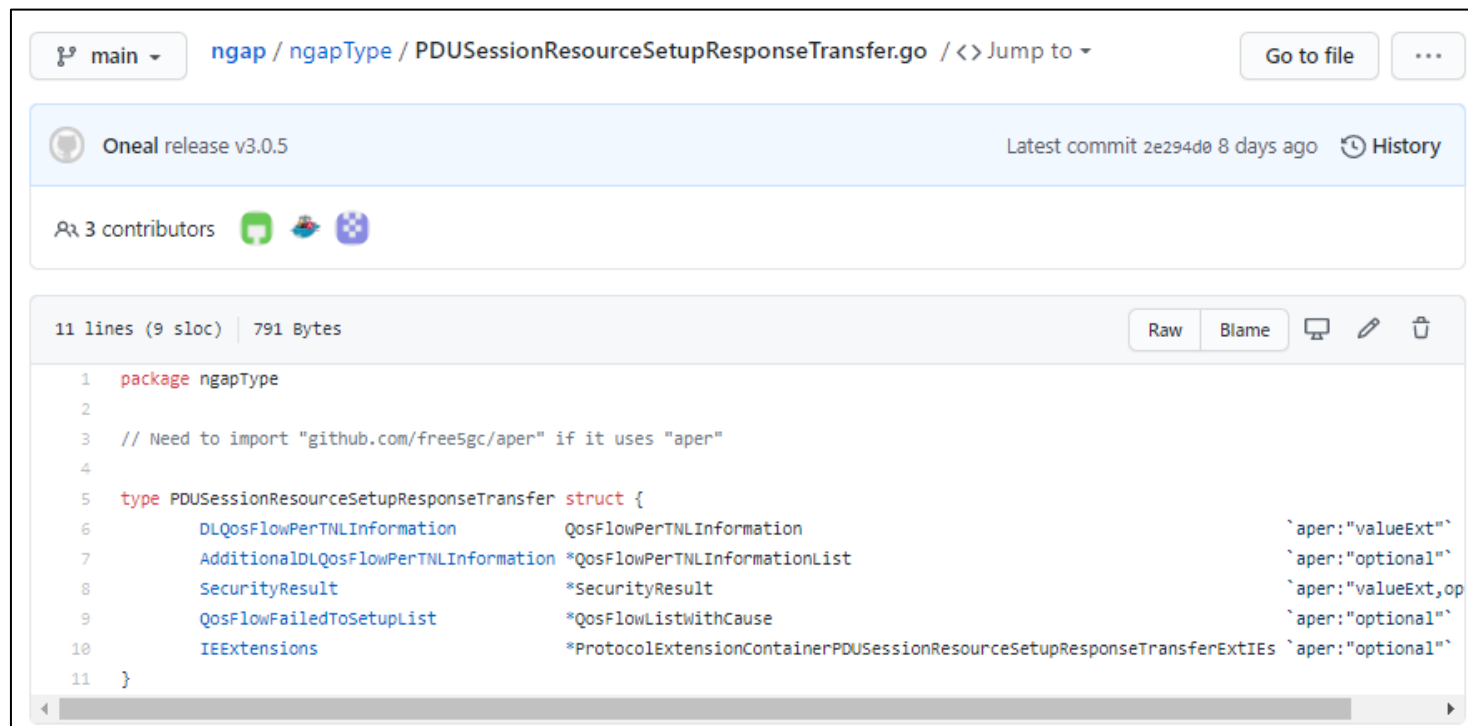
□ UE/RAN～5GC間にはNG Application Protocolで通信される

- › protocolIEsというリストでメッセージが格納される。
- › NGAPで使われるメッセージはfree5gc/ngapのライブラリで定義されている。
- › IEをパースしてNGAPライブラリでメッセージ内容を参照、作成する。
- › バイトオーダの違いに注意が必要

NGAPパケットキャプチャ

```
▼ NG Application Protocol
  ▼ NGAP-PDU: successfulOutcome (1)
    ▼ successfulOutcome
      procedureCode: id-PDUSessionResourceSetup (29)
      criticality: reject (0)
    ▼ value
      ▼ PDUSessionResourceSetupResponse
        ▼ protocolIEs: 3 items
          > Item 0: id-AMF-UE-NGAP-ID
          > Item 1: id-RAN-UE-NGAP-ID
          > Item 2: id-PDUSessionResourceSetupListSRES
```

NGAPライブラリ (<https://github.com/free5gc/ngap/>)



```
main ▾  ngap / ngapType / PDUSessionResourceSetupResponseTransfer.go / <> Jump to ▾  Go to file  ...

Oneal release v3.0.5  Latest commit 2e294d0 8 days ago  History

3 contributors

11 lines (9 sloc)  791 Bytes  Raw  Blame  📄  ✎  🗑

1  package ngapType
2
3  // Need to import "github.com/free5gc/aper" if it uses "aper"
4
5  type PDUSessionResourceSetupResponseTransfer struct {
6      DLQosFlowPerTNLInformation      QosFlowPerTNLInformation      `aper:"valueExt"`
7      AdditionalDLQosFlowPerTNLInformation *QosFlowPerTNLInformationList `aper:"optional"`
8      SecurityResult                  *SecurityResult                `aper:"valueExt,op"`
9      QosFlowFailedToSetupList        *QosFlowListWithCause          `aper:"optional"`
10     IEEExtensions                    *ProtocolExtensionContainerPDUSessionResourceSetupResponseTransferExtIEs `aper:"optional"`
11 }
```

メッセージ処理 - 2

□ メッセージは暗号化/ASN.1エンコードの処理が必要

- › free5gc/nas, free5gc/aperを利用して処理する。
- › キャプチャ時はNEA0を設定する。(非暗号化)

NGAPパケットキャプチャ (暗号化状態)

✓	pDUSessionNAS-PDU: 7e0258e069fe023731c7df4b0b8d289b16057632db8eca21...
✓	Non-Access-Stratum 5GS (NAS)PDU
✓	Security protected NAS 5GS message
	Extended protocol discriminator: 5G mobility management messages (126)
	0000 = Spare Half Octet: 0
 0010 = Security header type: Integrity protected and ciphered (2)
	Message authentication code: 0x58e069fe
	Sequence number: 2
✓	Plain NAS 5GS Message
	Extended protocol discriminator: Unknown (55)
✓	Not a NAS 5GS PD 55 (Unknown)
	> [Expert Info (Error/Protocol): Not a NAS 5GS PD 55 (Unknown)]
✓	Data (73 bytes)
	Data: 7e0258e069fe023731c7df4b0b8d289b16057632db8eca21...

NGAPパケットキャプチャ (NEA0)

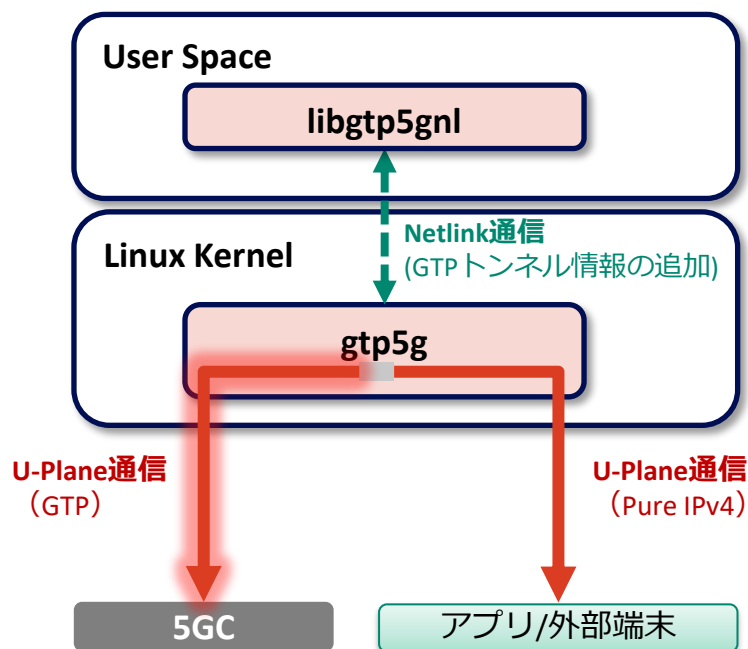
✓	Plain NAS 5GS Message
	Extended protocol discriminator: 5G session management messages (46)
	PDU session identity: PDU session identity value 10 (10)
	Procedure transaction identity: 0
	Message type: PDU session establishment accept (0xc2)
	0001 = Selected SSC mode: SSC mode 1 (1)
	> PDU session type - Selected PDU session type
	> QoS rules - Authorized QoS rules
	> Session-AMBR
	> 5GSM cause
	> PDU address
	> S-NSSAI
	> QoS flow descriptions - Authorized
	> Extended protocol configuration options
	> DNN

メッセージ処理例

```
// NAS PDUを複合、デコードして、PDU Addressを取得
pkg := []byte(suReq.PDUSessionNASPDU.Value)
m, err := test.NASDecode(&ueinfo.ue, nas.GetSecurityHeaderType(pkg), pkg)
if m.GmmHeader.GetMessageType() == nas.MsgTypeDLNASTransport {
    dlpayload := nasMessage.NewPDUSessionEstablishmentAccept(0)
    buff := uintToByte(m.DLNASTransport.PayloadContainer.GetPayloadContainerContents())
    dlpayload.DecodePDUSessionEstablishmentAccept(&buff)
    tmpIP := dlpayload.PDUAddress.GetPDUAddressInformation()
    ueinfo.gtpinfo.ueIP = net.IPv4(byte(tmpIP[0]), byte(tmpIP[1]), byte(tmpIP[2]), byte(tmpIP[3]))
}
```

□ GTPカーネルモジュール (<https://github.com/PrinzOwO/gtp5g>)

- **gtp5g** : Free5GCで使われているGTP処理のカーネルモジュール。
UPFモード、RANモードの二つの動作モードで動く。
- **libgtp5gnl** : アプリケーションからgtp5gへエントリ追加等を行うためのライブラリ。
CLIツール (libgtp5gnl-tool) も同梱されているので、gtp5g単体を試すことも可能。



主な機能

- **GTPカプセル化/デカプセル化**
 - UPFモード : 宛先IPをもとにカプセル化
 - RANモード : 送信元IPをもとにカプセル化
- **フィルタ機能**
 - GTP転送対象をフィルタを設定可能 (動作未確認)

```
struct ip_filter_rule {
    uint8_t action;           // permit only
    uint8_t direction;        // in/out
    uint8_t proto;            // number or "ip" which is not used for matching
    struct in_addr src, smask; // ip addr or "any" -> 0.0.0.0
    struct in_addr dest, dmask; // ip addr or "any" -> 0.0.0.0
    int sport_num;            // Counter for sport
    struct range *sport;      // one value, range or not existed -> [0, 0]
    int dport_num;            // Counter for dport
    struct range *dport;      // one value, range or not existed -> [0, 0]
};
```

<https://github.com/PrinzOwO/gtp5g/blob/master/gtp5g.c>

解析・不具合切り分け - 1



- キャプチャとデバッグログをひたすら確認
- ソースコードにデバッグ用の出力を追加して深追いする
- 3GPP仕様書を理解するのは大変だけど、キャプチャとソースを追うと少し理解しやすい

Free5GCのデバッグログ（例）

```
2021-01-27T08:57:18Z [INFO][LIB][3GPP] suciPart [suci 0 208 93 0 0 0 00000000001]
2021-01-27T08:57:18Z [TRAC][UDM][UEAU] supi conversion => imsi-2089300000000001
2021-01-27T08:57:18Z [TRAC][UDM][UEAU] K [0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
2021-01-27T08:57:18Z [ERRO][UDM][UEAU] opStr length is 0
2021-01-27T08:57:18Z [TRAC][UDM][UEAU] sqnStr 16f3b3f70fcc
2021-01-27T08:57:18Z [TRAC][UDM][UEAU] sqn [22 243 179 247 15 204]
AUTN = f471f8d89f608000eada1eb1cb7c8b72
```

認証値の検証ツール

認証エラー時は外部ツールで何が間違っているか、計算処理が正しいかを検証

landslide troubleshooting tool: Spirent

(https://support.spirent.com/SpirentCSC/SC_KnowledgeView?Id=SOL14108)

カーネルモジュールの切り分け (簡易な方法)

- ＞ 気になるところにログ出力を追加
- ＞ 単純な方法だが、着信しているが転送されない、TEID・IPがおかしいなどの切り分けをすぐできる。

◆ログ出力処理

```
netdev_dbg(pktinfo->dev, "gtp -> IP src: %pI4 dst: %pI4\n",  
            &pktinfo->iph->saddr, &pktinfo->iph->daddr);
```

◆ログ出力例

```
# echo 'file gtp5g.c +p' > /sys/kernel/debug/dynamic_debug/control  
# tail -f /var/log/kern.log  
Jan 27 11:16:38 free5gc kernel: [70369.181825] upfgtp: ip4_find_route:  
Jan 27 11:16:38 free5gc kernel: [70369.181826] upfgtp: gtp_dev name:upfgtp  
Jan 27 11:16:38 free5gc kernel: [70369.181826] upfgtp: dst dev name:eth1  
Jan 27 11:16:38 free5gc kernel: [70369.181827] upfgtp: gtp5g_xmit_skb_ipv4  
Jan 27 11:16:38 free5gc kernel: [70369.181828] upfgtp: gtp -> IP src: 192.168.52.100 dst: 60.60.0.2
```

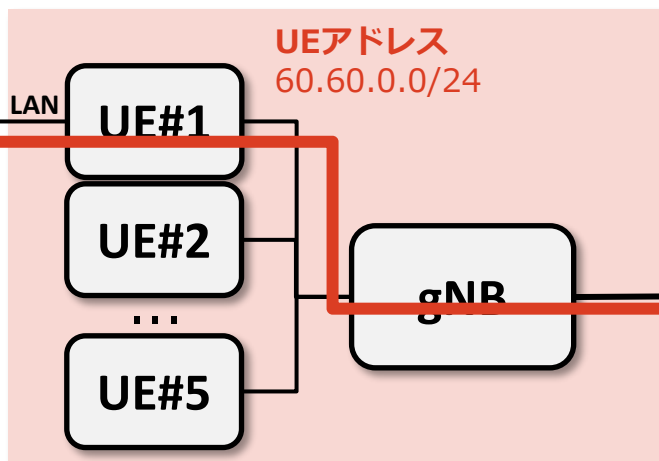
手順

1. UE5台接続
 - UE#1はLAN側の通信(iPerf)を転送
 - UE#2～5はダミー通信実施
2. GUIで接続を確認
3. iPerf実行
4. UEデタッチ

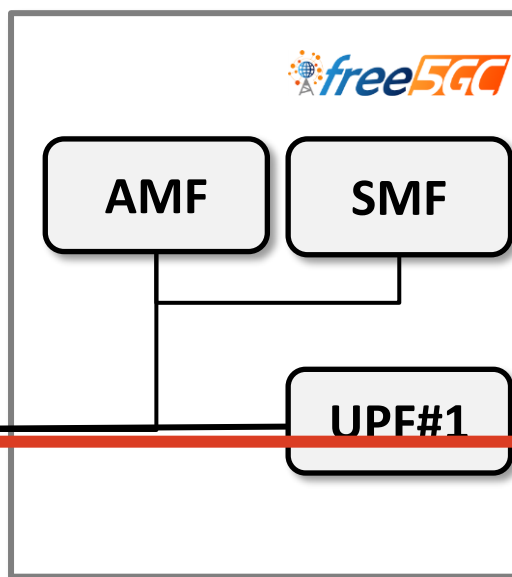
iPerfクライアント



PC



ueRanEmulator



Free5GC v3.0.5

iPerfサーバ
192.168.52.100



DataNetwork

今後の取り組み

- 手軽に構築、試験ができるようにコンテナ化、設定項目の拡張を検討中
- Free5GC v3.0.5で5GCの機能拡張がされたので、スライス試験をいろいろ実施予定
- N3IWFのクライアントも検討したい
- 他の5GCとの接続

聞きたいこと

- 試験機やOSSのエミュレータを利用していますか？自作していますか？
- どういう試験をしている（したい）か？（大量UE接続、アタッチデタッチ繰り返しなど）
- Ueransim/gnbsimについて教えてほしい

悩み事・その他

- そもそもgtp5gってなに？Linux標準搭載のgtpと何が違うのか？
- コンテナ化したいけど外部トラフィックのルーティングをどうしようか
- UE接続台数が増えるとFree5GCが落ちる

本資料では各種シーケンスを省略して記載しています。
正確な仕様は3GPPの仕様書等を参照してください。

□ 3GPP : <https://www.3gpp.org/>

□ Free5GC : <https://free5gc.org/>