Sujet 4TC-ARM, TP2 Wireshark & NAS
Avril 2020
Version 1.0

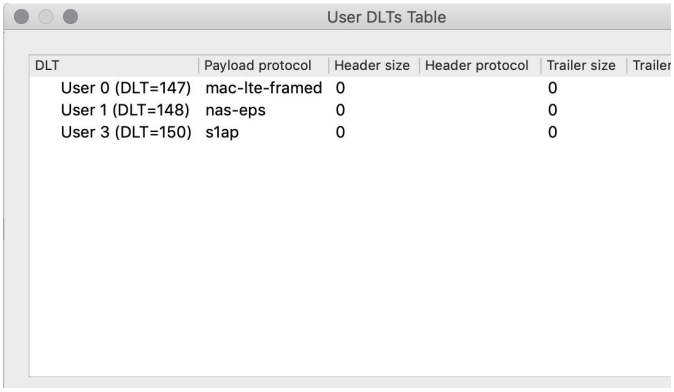
Auteur : Razvan Stanica
Rédaction : Razvan Stanica, Fabrice Valois

Nous allons analyser des traces de réseaux cellulaire 3G/4G en utilisant Wireshark[1], célèbre outil d'analyse de traces réseaux que vous avez déjà utilisé dans les TPs du domaine Réseau. Toutes les traces sont disponibles sur moodle Télécommunications / TC-4 / TC-4-R-ARM :

- Traces d'un appel téléphonique 3G
- Traces d'un appel VoIP 4G
- Traces d'un handover 4G inter-MME
- Traces d'une procédure d'attachement
- Traces d'une navigation sur le web en 4G

Les traces ont été collectées par Romain Pujol[2] sur un réseau cellulaire déployé au sein de l'équipe de recherche Inria Agora[3] et se basant sur srsLTE[4]. srsLTE fourni l'ensemble des briques logicielles pour la mise en place d'un d'un coeur de réseau, d'un réseau d'accès incluant les eNodeB et un terminal utilisateur. D'un point de vue matériel, tout fonctionne sur des PC portables[5] aux configurations raisonnables mais requiert des USRP pour l'interface radio logicielle. Nous utilisons ce réseau dans la bande de fréquences libres 5GHz. L'utilisation de srsLTE couplé à Wireshark nous permet donc d'analyser des traces côté UE, eNodeB et EPC, mais pas sur l'interface air.
Pour pouvoir analyser les traces, veuillez utiliser une version récente de Wireshark et faire les configurations suivantes :

- Preferences / Protocols / DLT_USER
- Edit Encapsulation Table
- Ajouter les entrées suivantes :



[1] https://www.wireshark.org/, dernière consultation : mardi 7 avril 2020.
[2] Romain Pujol est doctorant à l'INSA Lyon et au laboratoire CITI. Il travaille dans l'équipe Inria Agora et fait sa thèse sous la direction de Fabrice Valois et Razvan Stanica sur l'amélioration des mécanismes d'associations des utilisateurs dans les réseaux cellulaires en général, et dans les réseaux *self-deployables* en particulier.
[3] https://team.inria.fr/agora/, dernière consultation : mardi 7 avril 2020.
[4] https://github.com/srsLTE/srsLTE, dernière consultation : mardi 7 avril 2020.
[5] Voire même sur des Raspberry Pi4 : https://docs.srslte.com/en/latest/app_notes/source/pi4/source/, dernière consultation : mercredi 10 juin 2020.

Section I : Appel 3G

Ressource à télécharger : Traces d'un appel téléphonique 3G

On démarre par les traces de l'appel voix en 3G et nous allons nous concentrer sur les messages NAS[6] entre le RAN et le CN. Vous noterez que dans les traces, nous ne voyons pas les messages RRC, ni les canaux logiques, etc. Comme l'architecture d'un réseau 3G, dans le domaine circuit, est construite autour de : UE ←→ eNodeB ←→ RNC ←→ MSC, cette trace a donc été collectée entre le RNC et le MSC. Souvenez-vous qu'un réseau 3G n'est pas un réseau *full IP* : il utilise des protocoles spécifiques comme SCTP, protocole de transport (donc de bout-en-bout) dédié au dialogue entre le RNC et le MSC, avec une logique proche de TCP. On peut voir les messages SCTP et les SACK utilisés dans les traces sur lesquelles nous allons travailler.
Vous trouverez deux traces : `originating call` et `terminating call`. La première correspond à un utilisateur qui appelle quelqu'un, tandis que la seconde correspond à un utilisateur qui est appelé. Attention, il n'y a pas de lien entre les deux traces qui ont été capturées à des instants différents. Nous n'avons pas non plus retravaillé l'horodatage des messages pour faire apparaître une quelconque synchronisation.
Dans l'archive que vous avez téléchargé, vous trouverez également deux fichiers PDF. Ils détaillent, grâce à un chronogramme, ce qui se passe côté RAN, ainsi que les phases de connexion RRC, attachement CN et authentification. C'est ce que nous avons observé lors de la séance précédente.
Pour visualiser uniquement les messages RANAP, utiliser le filtre `ranap` dans Wireshark. Notez que dans votre fenêtre, la valeur 4096 correspond à l'identité du RNC, tandis que la valeur 8192 correspond à l'identité du MSC.

Débutons par la trace côté de l'appelant (**`originating call`**).

Q1.1. Quel protocole NAS transmet le message CM Service Request ? Quel service est demandé par le mobile dans ce message ?

Q1.2. Quel algorithme de chiffrement est connu par le mobile ?

Q1.3. A quoi sert, selon vous, le message `RANAP Common ID`, transmis par le MSC au RNC ?

Q1.4. Pourquoi, alors que les messages sont chiffrés, on les voit en clair dans Wireshark ?

Q1.5. Que pouvez-dire de l'IMSI ?

Q1.6. Pourquoi utilise-t'on l'IMSI dans ces messages du CN et non pas le TMSI ?

Q1.7. Quel protocole NAS génère le `DirectTransfer (DTAP) (CC) Setup` ?

Q1.8. Quel est le numéro appelé par le mobile ? (attention, dans notre cas il ne s'agit pas d'un vrai numéro de mobile car c'est un scénario de test sur une plateforme d'expérimentation)

Q1.9. Quels sont les codecs supportés par l'UE ?

Q1.10. Quel est le rôle du message `RAB-AssignmentRequest` transmis par le MSC ?

[6] Un glossaire est disponible à la fin du sujet.

Q1.11. Le MSC répond au message `DirectTransfer DTAP (CC) Setup` par un message `DirectTransfer DTAP (CC) Call Proceeding`. Quel est le rôle de ce message ?

Q1.12. Le message suivant est `DirectTransfer DTAP (CC) Alerting`. Quel est le rôle de ce message envoyé à l'UE ?

Q1.13. Quel message indique que l'appelé a décroché ?

Q1.14. Comment est encapsulé l'appel téléphonique, par quel ensemble de protocoles ?

Q.1.15. A la fin de l'appel, après avoir arrêté la connexion CC (`DirectTransfer DTAP (CC) Release Complete`), on voit aussi un message `Iu Release Command`. A quoi sert ce message ?

Basculons maintenant sur la trace de l'appelé (**`terminating call`**). Conservons le filtre `ranap` dans Wireshark.

Q1.16. Après le paging, l'appelé reçoit un message `DirectTransfer (DTAP) (CC) Setup` ? Est-ce le même message `DirectTransfer (DTAP) (CC) Setup` transmis par l'appelant ?

Q.1.17. On observe également un message `DirectTransfer (DTAP) (CC) Alerting` du côté de l'appelé. Quel est le rôle de ce message dans ce cas ? Est-ce qu'il précède ou il succède au message `DirectTransfer (DTAP) (CC) Alerting` que nous avons vu côté appelant ?

Q.1.18. Lorsque nous avons étudié la trace `originating call` précédemment, nous avons vu que les codecs supportés par le terminal appelant étaient listés. Dans quel message l'UE appelé annonce-t'il la liste de ses codecs disponibles ?

Q.1.19. Quelle est la signification du message `DirectTransfer (DTAP) (CC) Release` par rapport au message `DirectTransfer (DTAP) (CC) Release Complete` ?

Section 2 : Appel 4G VoIP
Ressource à télécharger : Traces d'un appel VoIP 4G

La trace étudiée ici se déroule bien après les phases d'attachement, d'authentification, de mise en place du bearer, etc. que nous avons étudié lors du premier TP. N'hésitez pas à retourner voir pour appréhender le comportement de l'utilisateur dans son ensemble.
Rappelons que nous sommes ici entre le eNodeB et le MME.

Q.2.1. On observe les mêmes messages d'attachement que lors du premier TP. La seule exception sont les messages `DownlinkNASTransport, ESM information request` et `UplinkNASTransport, ESM information response` qui apparaissent en plus. Pourquoi le MME envoie-t'il cette demande ?

Q.2.2. On utilise deux protocoles différents au niveau de l'appel : un pour la signalisation, l'autre pour transporter la voix. Quels sont ces protocoles ?

Section 3 : Handover 4G inter-MME
Ressource à télécharger : Traces d'un handover 4G inter-MME

Dans le cas d'un handover intra-MME (*i.e.*, on reste dans le même MME), alors il n'y a pas de traces entre le RAN et le CN car tous les messages sont internes au MME. Dans le cadre de la trace que vous venez d'ouvrir sur Wireshark, prenez soin d'observer les adresses IPs utilisées : on voit deux MMEs et deux eNodeBs.

Q.3.1. Quelle est la raison d'exécution de ce handover ?

Q.3.1. Combien de temps dure l'exécution du handover ?

Q.3.2. Quelles sont les adresses IP des eNodeBs et des MMEs impliqués ?

Q.3.3. Sur quelle interface circule cette demande de handover ?

Q.3.4. Quelles sont les Id. de la cellule source et de la cellule destination du handover ?

Q.3.5. Quelles sont les ressources transférées entre les MMEs ?

Q.3.6. L'interface radio étant chiffrée, que se passe-t'il lors du handover : une nouvelle clef de chiffrement/déchiffrement est-elle calculée ou la clef actuelle est-elle transférée ?

Glossaire du TP2, Wireshark & NAS

AMR-WB	Adaptive Multi-Rate Wideband
AS	Access Stratum
BCD	Binary Coded Decimal
CC	Call Control
CM	Call Management
CN	Core Network
DTAP	Direct Transfer Application Part
EFR	Enhanced Full Rate
ESM	EPS Session Management
IP	Internet Protocol
MCC	Mobile Country Code
MNC	Mobile Network Code
MM	Mobility Management
MME	Mobility Management Entity
MSC	Mobile Switch Center
NAS	Non Access Stratum
pDCP	Packet Data Convergence Protocol
pDCP-SN	Packet Data Convergence Protocol Sequence Number
RAB	Radio Access Bearer
RAN	Radio Access Network
RANAP	Radio Access Network Application Part
RNC	Radio Network Controller
RRC	Radio Resource Controller
SACK	Selective ACK
SCTP	Stream Control Transmission Protocol
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UE	User Equipment
USRP	Universal Software Radio Peripheral