Sujet 4TC-ARM, TP1 Wireshark & Attachement
Juin 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 :

- Scénario 1 : Attachement au réseau lorsqu'un smartphone quitte le mode avion,
- Scénario 2 : Session web.

Au cours de ce premier TP, nous allons nous focaliser sur la procédure d'attachement de l'utilisateur mobile au réseau, tandis que le prochain TP sera plus focalisé sur le réseau d'accès. De nombreuses questions vont vous guider pour le premier scénario. En fin de séance, si le temps le permet, ou en dehors de cette séance encadrée, vous pouvez analyser le second scénario 2 en cherchant bien les protocoles utilisés, les services demandés, les données échangées, etc.

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 cœur 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.

Un glossaire vous est proposé à la fin du sujet.

[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.

Scénario I : Attachement au réseau
Ressource à télécharger :
Attachement au réseau lorsqu'un smartphone quitte le mode avion

Trois fichiers pcap[6] sont présents dans l'archive zip. Vous devez suivre les instructions du fichier README pour configurer Wireshark afin d'afficher les traces correctement (Wireshark : Préférences -> Protocoles -> DLT_USER, puis ajouter les lignes indiquées dans le README).

L'objectif du TP est de parcourir les trois fichiers de captures (enb.pcap, epc.cap, ue.pcap) pour comprendre le déroulement du mécanisme d'attachement. Vous allez pouvoir observer l'ensemble des protocoles sur lesquels nous avons travaillé en cours/TD : RLC, MAC, RRC, et les protocoles NAS. Attention : les trois captures correspondent au même scénario, mais enregistré à trois endroits différents (UE, eNodeB, EPC). Vous noterez que le temps n'est pas synchronisé.

Q.1.1 Quel est l'objectif de la procédure d'attachement ?

Q1.2. Le premier échange à observer, très rare dans la vraie vie, a lieu entre le eNodeB et l'EPC. Il s'agit de la mise en place de l'interface S1. C'est quoi l'interface S1 ? Quand est-ce que ces messages sont échangés dans la vraie vie ?

Q1.3. On passe maintenant du côté de l'UE. Les trois premiers messages qui apparaissent sont de type MIB et SIB. Quelles sont les différences entre ces trois messages? Sur quels canaux logiques sont-ils transmis ?

Q1.4. Le premier message MAC visible dans la trace est le message RAR. Ce message fait partie d'une série d'échanges entre l'UE et l'eNodeB. Comment appelle-t-on ces échanges ? Quels sont les autres messages ? Si certains ne sont pas visibles, pourquoi ?

Q1.5. Dans quelle zone de localisation se trouve l'utilisateur mobile ? Quel est le code de son opérateur ? Quel est son code pays ?

Q1.6. Combien de préambules sont-ils disponibles dans la cellule pour la procédure de `Random Access` ?

Q1.7. Dans le message RAR, il y a deux identifiants RNTI. Quelles sont leurs valeurs ? Quelle est la différence entre les deux ?

Q1.8. A quoi sert le champ `Timing Advance` dans le message RAR ?

Q1.9. Dans le message `RRC Connection Request`, deux identifiants sont utilisés pour l'utilisateur. Lesquels ? Pourquoi les deux sont-ils nécessaires ?

Q1.10. Quel est le premier message transmis vers le cœur du réseau? Comment est-il transmis au niveau RAN ? Question culture générale: comment appelle-t-on ce mécanisme dans un réseau ?

Q1.11. Quelle est la cause indiquée pour la demande d'attachement ?

[6] "packet capture" est une interface de programmation qui permet de capturer un trafic réseau : https://en.wikipedia.org/wiki/Pcap, dernière consultation le mercredi 10 juin 2020.

Q1.12. Quelle est la procédure démarrée par le coeur de réseau à la réception d'une demande d'attachement ?

Q1.13. Quelle identité de l'utilisateur mobile ?

Q1.14. Dans le message `NAS Identity Response`, l'UE indique son IMSI, alors qu'on avait vu dans les messages précédents qu'il possède bien un TMSI. Pourquoi ce comportement?

Q.1.15. Au niveau du réseau cœur savons-nous où est l'utilisateur dans le réseau ?

Q1.16. En parlant des messages `Identity Request` et `Identity Response`, ces messages NAS sont encapsulés par plusieurs autres protocoles sur le réseau d'accès (visibles dans la trace ue.pcap). Quels sont ces protocoles ?

Q1.17. Au niveau de l'UE, après la réception du message `Identity request`, un message de niveau MAC est envoyé (ligne 9). Des messages similaires sont ensuite envoyés tout le long de la trace. Quel est le rôle de ce message ?

Scénario 2 : Session Web
Ressource à télécharger : Session web

Trace supplémentaire à analyser librement et pour le plaisir :-)

Glossaire du TP1, Wireshark & Attachement

C-RNTI	Cell Radio Network Temporary Identifier
DNS	Domain Name System
EPC	Evolved Packet Core
GUTI	Globally Unique Temporary Identity
HSS	Home Subscriber Server
IMSI	International Mobile Subscriber Identity
MAC	Medium Access Control
MCC	Mobile Country Code
MNC	Mobile Network Code
MME	Mobility Management Entity
MIB	Master Information Block
NAS	Non-Access Stratum
QoS	Quality of Service
RA-RNTI	Random Access RNTI
RAR	Random Access Response
RLC	Radio Link Control
RNTI	Radio Network Temporary Identifier
RRC	Radio Resource Control
SAE	System Architecture Evolution
SIB	System Information Block
TMSI	Temporary Mobile Subscriber Identity
m-TMSI	MME Temporary Mobile Subscriber Identity
s-TMSI	SAE Temporary Mobile Subscriber Identity
UE	User equipment
USRP	Universal Software Radio Peripheral