دانشکده مهندسی کامپیوتر

مباحث ویژه ۲

بهار ۱۴۰۱

تمرین سوم

احراز اصالت در شبکه‌های نسل چهارم

استاد درس . . . . . دکتر دیانت

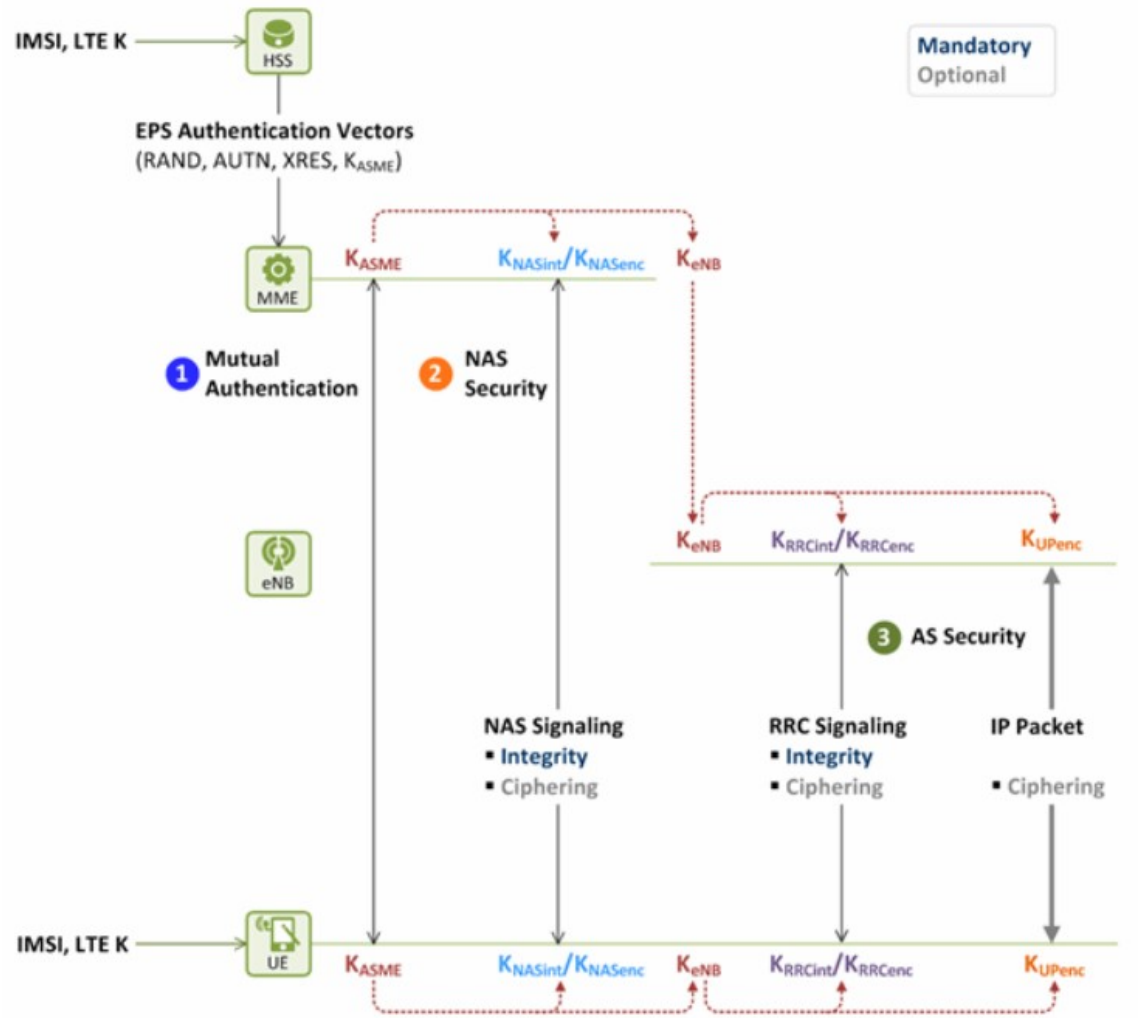
نام . . . . . علی صداقی

شماره دانشجویی ۹۷۵۲۱۳۷۸

فهرست مطالب

۱ Introduction

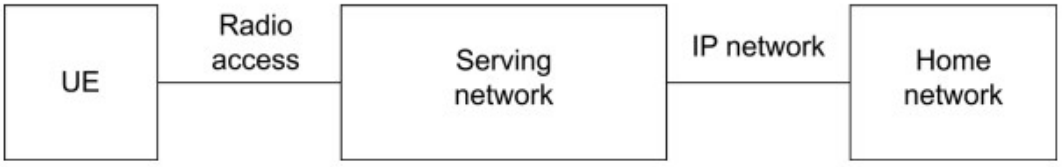
روش احراز اصالت شبکه‌های تلفن نسل چهارم به صورت 4G EPS-AKA می‌باشد. در این تمرین می‌خواهیم این روش را مورد بررسی قرار دهیم. در شکل زیر خلاصه‌ای از احراز هویت در نسل چهارم وجود دارد. سایر نسل‌ها در کلاس درس مورد بررسی قرار گرفت.



شکل ۱: احراز اصالت در نسل چهارم

۲ معماری شبکه‌های سلولی

از منظر اهراز اصالت، یک شبکه سلولی از سه مولفه اصلی تشکیل شده است. این مولفه‌ها در شکل زیر نمایش داده شده اند.



شکل ۲: معماری شبکه‌های سلولی

UE همان سیمکارت می‌باشد که المان UICC را شامل می‌شود. این المان کلیدهای رمزنگاری را درون خود ذخیره دارد. این کلیدها با کلیدهای سمت شبکه یکی است.

Serving Network در واقع همان RAN می‌باشد که شامل تجهیزات دسترسی هوایی است. eNodeB و MME اسامی آشنایی هستند که در کلاس درس مورد بررسی قرار گرفتند.

Home Network در واقع مانند هسته شبکه هست که شامل سرورهای اهراز اصالت است. برای مثال Home Subscriber Server (HSS) گواهینامه کاربرهای اهراز اصالت شده را نگه می‌دارد.

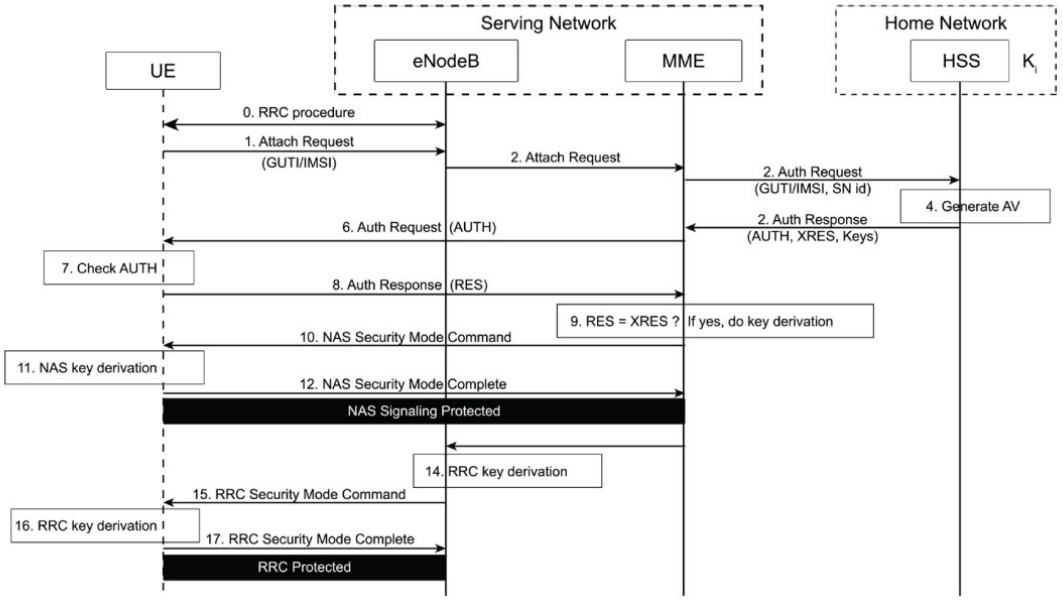
ارتباط میان Serving Network و Home Network از طریق IP برقرار است.

ماهیت‌های اصلی که تحت IP به هم متصل هستتند معمولا تحت عنوان Evolved Packet System (EPS) شناخته می‌شوند.

۳ 4G EPS-AKA

در این روش پس از کامل شدن درخواست RRC بین UE و eNodeB باعث فعال شدن EPS-AKA می‌شود. سپس یک پیام درخواست پیوست به MME ارسال می‌شود. MME نیز در پاسخ یک درخواست احراز اصالت شامل شناسه IMSI یا همان هویت UE و شناسه شبکه سرویس دهنده را به HSS واقع در Home Network ارسال می‌کند.

المان HSS عمل رمزنگاری را بر مبنای کلید مخفی مشترک Ki که میان خودش و UE مشترک است انجام می‌دهد. در نتیجه این کار یک یا چند بردار اهراز اصالت استخراج می‌شود. در یک پیام پاسخ احراز اصالت به MME ارسال می‌شود. بردار احراز اصالت یا به اختصار AV شامل یک توکن احراز اصالت به نام AUTH و یک توکن پاسخ احراز اصالت هویت مورد نظر به نام XAUTH است. داده‌های دیگری نیز در این بردار وجود دارد.



شکل ۳: رویه احراز اصالت در نسل چهارم

پس از دریافت پاسخ احراز اصالت از MME یک درخواست احراز اصالت از سوی HSS شامل توکن AUTH به UE ارسال می‌شود.

UE این توکن را با با توکن تولید شده خودش با کلید Ki مقایسه می‌کند و پس از تایید آن شبکه

را قانونی حساب می‌کند و یک پاسخ احراز اصالت به MME می‌فرستد. در این پاسخ یک توکن به نام RES وجود دارد که بر اساس Ki تولید شده است. MME این توکن را با توکن مورد انتظار خود یعنی XRES مقایسه می‌کند. در صورت برابری MME به کلید دست می‌یابد و یک دستور Se-curity Mode به UE ارسال می‌کند. سپس کلیدهایی که برای محافظت از پیام‌های سیگنالینگ NAS هستند را استخراج می‌کند. همچنین MME یک کلید برای eNodeB می‌فرستد که از آن کلیدهای محافظت از کانال RRC به دست آمده است. پس از اینکه UE نیز کلیدهای مربوطه را به دست آورد، ارتباط بین UE و eNodeB امن می‌شود.

۴ منابع

لینک پروژه لاتک درون فایل LaTeX_Link.txt موجود است.

LTE Auth

A Comparative Introduction to 4G and 5G Authentication