УДК 621.391

МОДИФІКОВАНИЙ СПОСІБ АВТЕНТИФІКАЦІЇ ДЛЯ ТЕХНОЛОГІЇ WI-FI DATA OFFLOADING

Лашко А.Ю., Курдеча В.В.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: artemuio@gmail.com

Modified method of authenticating for wi-fi data offloading technology

To address the high (re-)authentication delays and UE identity discloser, we propose a fast local re-authentication method. Our method offers mutual authentication mechanism and guaranties data confidentiality by using hybrid cipher cryptosystem.

Мережі третього покоління (3G) можуть забезпечити безпечне рішення з підключення з низькою швидкістю передачі даних. Хоча бездротова мережа забезпечує високу швидкість передачі даних в невеликій географічної області, тому об'єднання 3G і WLAN можуть надати додаткове рішення для мережі [1]. Ця взаємодія потребує забезпечення безпечної та швидкої автентифікації без впливу на безпеку служби в обох мережах. EAP-AKA і EAP-SIM - це механізми автентифікації, прийняті проектом партнерства 3-го покоління (3GPP) для вертикальної передачі обслуговування між мережами 3G і WLAN. Метод EAP-AKA має кілька недоліків, таких як відображення ідентифікатора користувача, висока затримка автентифікації і додаткове споживання смуги пропускання [2].

Модифікований метод повторної автентифікації буде заснований на стандарті EAP-AKA і використовувати гібридний ключовий протокол (Elliptic Curve with symmetric key). Для цього методу достатньо одного повного циклу автентифікації [3] між локальним сервером WAAA (WLAN Authentication Authorization and Accounting server) і 3G-HAAA (Home Authentication Authorization and Accounting server) при повній автентифікації користувача. Він перевіряє справжність UE (User Equipment) локально, на WAAA в процесі повторної автентифікації. Це також спрощує схему автентифікації, зменшує затримку автентифікації і кількість ключів автентифікації, забезпечує взаємну автентифікацію і захищає ідентифікаційні дані користувача.

Для того, що б усунути високі (повторні) затримки автентифікації і позбутися проблеми розкриття особистості UE можна використовувати цей модифікований метод. Даний метод не потребує будь-яких модифікацій існуючих 3G-WLAN-інфраструктур або використання операцій відкритого ключа. Пропонується механізм взаємної автентифікації, який гарантує конфіденційність даних з використанням гібридної криптосистеми шифрування. У цьому процесі автентифікації необхідно п'ять вузлів:

- UE,
- точка доступу (AP),
- бездротової аутентифікаційний сервер (WAAA),
- сервер аутентифікації 3G (HAAA)
- база даних користувачів 3G (HLR / HSS).

Припустимо, що:
- Безпечний канал між AP, WAAA, HAAA і HSS.
- WAAA відповідає за кілька точок доступу.
- UE може ідентифікувати ідентифікатор сервера AAA і AP (Access Point).
-Кожен сервер автентифікації HAAA має відомий відкритий ключ шифрування.
- Кожне UE має пару попередньо розділених секретних ключів з сервером HLR.
Цей метод повної автентифікації повинен змінити існуючу повну автентифікацію EAP-AKA, щоб прибрати проблему розкриття особистості UE і запустити нову ключову інфраструктуру.

Пропонується змінити існуючу схему EAP-AKA повної автентифікації, для того щоб обійти проблему розкриття ідентифікаційних даних користувача. Рисунок 1 показує запропонований спосіб.

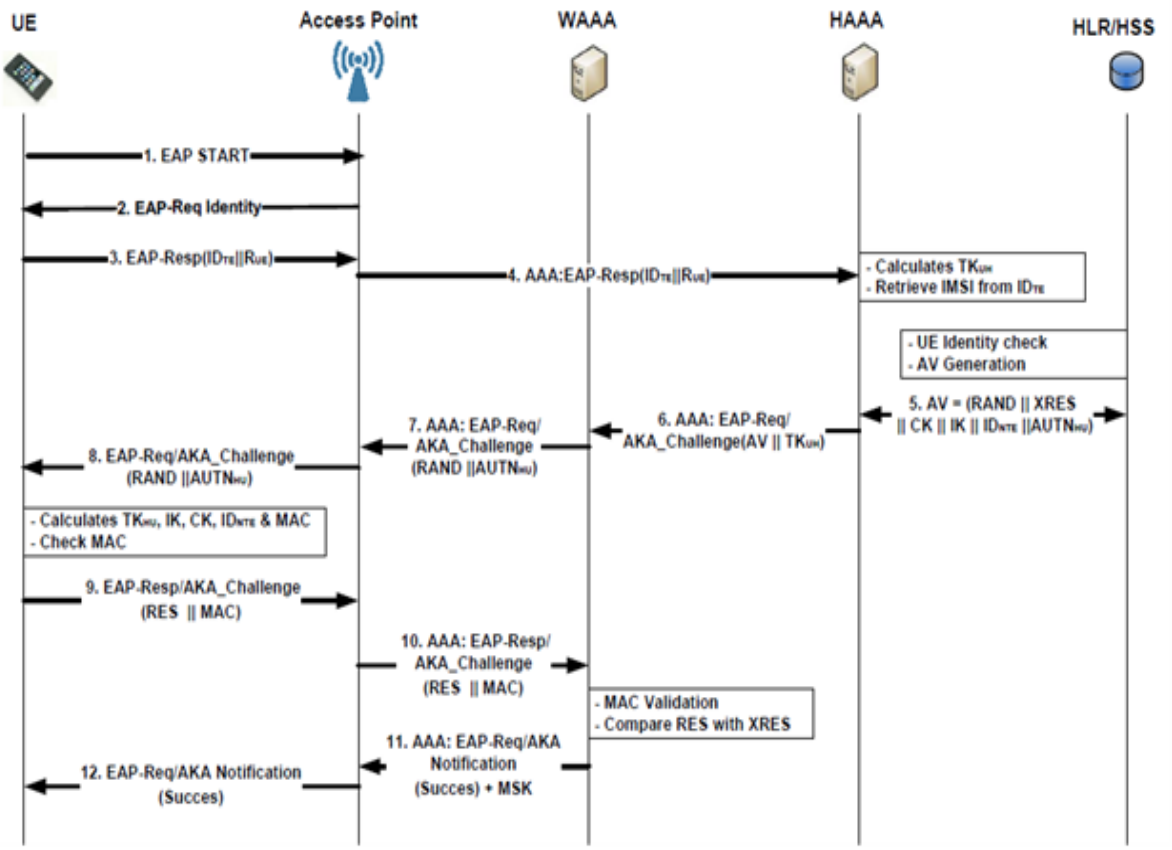

Рис.1. Повний цикл проходження автентифікації.

Цей метод може бути використаний і в разі повторної автентифікації з однією і тією ж точкою доступу або автентифікації з новою точкою доступу в одній і тій же бездротової локальної мережі.

У цьому випадку, модифікований метод за допомогою WAAA локально повторно перевіряє справжність UE від імені HAAA з використанням попереднього прийнятого ключа під час повної автентифікації. На рисунку 2 описано пропонований метод повторної автентифікації.

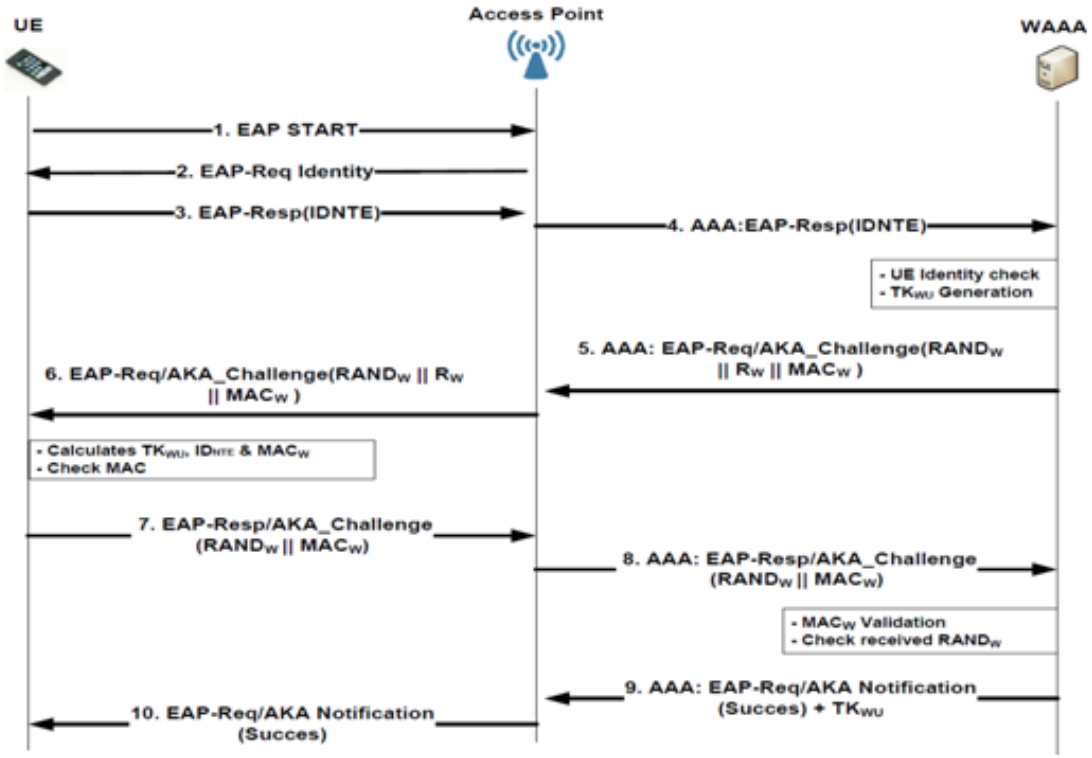

Рис.2. Повторний цикл проходження автентифікації.

Щоб уникнути розкриття ідентифікатора користувача, використовується шифрування для захисту цієї інформації. При повторній автентифікації замість постійного ідентифікатора використовується локальний ідентифікатор, який залишається після повної автентифікації. Передача локального ідентифікатора захищена одним ключем шифрування [4]. Таким чином, пропонований метод забезпечує надійний захист призначених для користувача ідентифікаторів від атак, пов'язаних з ідентифікацією.

Витрата пропускної здатності: при швидкій повторній автентифікації EAP-AKA користувач автентифікується через HAAA, а в автентифікації через модифікований метод користувач отримує доступ до мережі через WLAN-сервер автентифікації. Це може скоротити споживання смуги пропускання між HAAA і WAAA в порівнянні з повною автентифікацією EAP-AKA.

Література

1. Дундяк Р.Р., Глоба Л.С., Курдеча В.В. Перерозподіл трафіку мобільної мережі за допомогою технологій WI-FI Offloading та LTE / Молодий вчений, 6-7 травня 2016 р. – 55с.
2. C. Lim, D.-Y. Kim, O.Song, and C.-H. Choi, “SHARE: seamless handover architecture for 3G-WLAN roaming environment,” Journal of Wireless Networks, vol. 15, no. 3, pp. 353–363, 2009.
3. Prasith Sangaree P, Krishnamurthy P. A new authentication mechanism for loosely coupled 3G-WLAN integrated networks. IEEE 59th Vehicular Technology Conference, Vol. 5. Spring, pp. 2998–3003, 2004
4. A. Dutta, T. Zhang, S. Madhani, K. Taniuchi, K. Fujimoto, Y. Katsube, Y. Ohba, and H. Schulzrinne, “Secure universal mobility for wireless Internet,” in Proceedings of the 2nd ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, pp. 71-80, Oct. 2014.