

УДК 621.396.4

Є. О. ЛОСЄВ, аспірант;

А. О. ПИШКО, магістрант,

Державний університет телекомунікацій, Київ

Модифікована архітектура Wi-Fi OFFLOAD

Завдяки урізноманітненню персональних пристроїв з'являється попит на дедалі швидкісніший зв'язок. Щоб упоратися зі зростанням обсягів трафіку, операторам мобільних мереж необхідно впроваджувати більш швидкісні та економічно вигідні радіотехнології, підвищувати просторову ефективність мереж шляхом розгортання малих стільників, забезпечуючи при цьому збалансований розвиток гетерогенних мереж.

Оператори мобільного зв'язку планують розвантажити свої мережі від трафіку даних у найбільш вигідний спосіб, поліпшивши свій економічний стан. Такий підхід виник через те, що подальші технологічні розробки та удосконалення стільникової архітектури стикаються з фізичними обмеженнями. Окрім того, забезпечення високої пропускної здатності та високої швидкості передавання даних потребує значних економічно невиправданих капітальних вкладень.

Оскільки вже чимало років поспіль трафік передавання даних у мережах стільникового зв'язку неухильно зростає, операторам у цій ситуації залишається лише одна можливість для задоволення потреб своїх клієнтів — підвищувати щільність покриття, забезпечуючи цим самим більшу смугу пропускання в розрахунку на одного абонента. У підвищенні щільності покриття немає нічого поганого, якщо не брати до уваги економічних показників обладнання однієї встановленої станції.

Іншим варіантом вирішення проблеми є технологія Wi-Fi Offload, покликана розвантажити мережі мобільних операторів від трафіку передавання даних за рахунок застосування технології Wi-Fi. У цьому разі трафік передавання даних абонентів виводиться з мережі мобільного оператора в окрему радіомережу, що працює з використанням власних магістральних каналів. Також з'являється можливість надання абонентам послуг через партнерські мережі аналогічно до того, як це робиться, коли абонент перебуває в роумінгу.

Актуальність модифікації архітектури Wi-Fi Offload зумовлена тим, що завдяки такій модифікації користувач матиме змогу отримувати високоякісний доступ до інтернет-ресурсів або ж до сервісу мобільного оператора. Оператор, у свою чергу, зможе обслуговувати додаткову кількість абонентів, а також зменшити завантаженість своїх макро-стільників.

Ключові слова: мобільна мережа; Wi-Fi Offload; розвантаження; архітектура; LTE.

Вступ

Консорціум 3GPP запропонував використання *Access Network Discovery and Selection Function (ANDSF)* для активації передавання даних між обладнанням різних технологій доступу [1], а також упровадив альтернативні механізми вивантаження, такі як *IP Flow Mobility* [2], *Selected IP Traffic Offload (SIPTO)*, *Local IP Access (LIPA)* [3], *Seamless Internetworking Flow Mobility (SIFM)* [4] та *Multipath TCP (MPTCP)* [5]. Зазначені механізми мають, утім, недоліки, що призводять до затримки в автентифікації устаткування користувача обладнання (UE) під час процедури розвантаження [6].

Основна частина

У цій статті описано безшовну архітектуру між мережами LTE та Wi-Fi, яка усуває недоліки існуючих архітектур щодо розвантаження стільникової мережі. Ідеться про використання пакетного шлюзу PGW в ядрі LTE, та доповнення основної мережі Wi-Fi двома компонентами (модулями): *Access Network Query Protocol-Data Server (ANQP-DS)* та *Access Zone Control (AZC)*.

Запропонована авторами модифікована архітектура Wi-Fi включає в себе додатковий блок, призначений для зберігання автентифікаційних даних користувача, що зменшує час затримки автентифікації. Наведено порівняння зазначеного методу з чинним стандартом EAP-AKA, здійснюване за такими показниками, як пропускна здатність та затримка автентифікації UE при розвантаженні.

Упровадження додаткових модулів AZC та ANQP-DS дасть змогу обслуговувати обладнання користувача при переході з мережі LTE в мережу Wi-Fi. У запропонованій архітектурі шлюз PGW працюватиме як IP-якір для фіксування єдиної (сталой) IP-адреси при переміщенні між різними мережами. У свою чергу, у мережі Wi-Fi ANQP-DS та AZC керуватимуть мобільністю обладнання користувача. Зокрема, AZC керуватиме балансуванням завантаження точок доступу; ANQP-DS зберігатиме інформацію про зазначене обладнання та профіль мережі Wi-Fi. Описане далі вирішення сприятиме підвищенню пропускної здатності мережі Wi-Fi завдяки розподілу устаткування користувача в точках доступу за допомогою нововведеного модуля AZC.

Архітектуру мережі LTE унаочнює рис. 1, з якого випливає, зокрема, що в цій мережі існують чотири компоненти EPS: MME, SGW, PGW та HSS.

© Є. О. Лосєв, А. О. Пишко, 2018

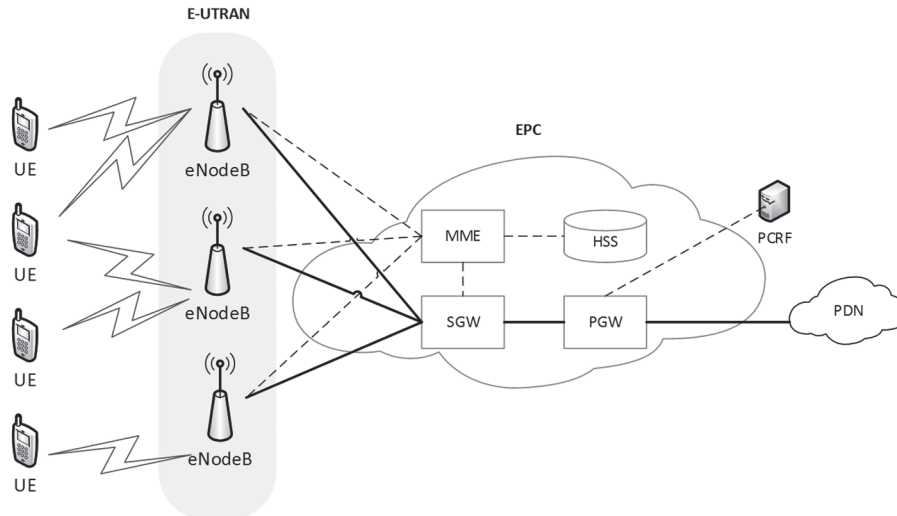


Рис. 1. Архітектура мережі LTE

Компонент MME контролює більшість операцій, виконуваних у EPC. Основною функцією MME є керування відстеженням місцезнаходження обладнання користувача, коли воно переміщується в зоні впливу eNodeB. MME взаємодіє з трьома іншими компонентами EPC — HSS, SGW і PGW [7]. MME для автентифікації та авторизації цього обладнання має функціонал автентифікації, який взаємодіє з компонентом HSS для реалізації цих операцій, оскільки база даних HSS зберігає всю інформацію, пов'язану з функціональними можливостями MME. MME є контрольним вузлом, через який проходить увесь сигнальний трафік між UE і Core Network (CN). Протоколи, використовувані для передавання контрольного трафіку між UE і CN, відомі як NAS (*Non-Access Stratum*). Функції, виконувані MME, поділяються на такі два типи: *управління потоками* та *управління підімкненнями*.

Управління потоками. До цієї області належить рівень управління (керування) сесіями (layer management session) протоколів NAS, у рамках якого відбуваються процеси створення, підтримання та вилучення потоків.

Управління підімкненнями. У межах цієї функціональності здійснюється підімкнення абонентів до мережі, а також формуються правила шифрування та кодування між UE і мережею.

Компонент SGW (*Serving Gateway*) — це шлюз, який з'єднує інтерфейс між EPC та E-UTRAN. Для кожного мобільного пристрою, пов'язаного з EPC, є тільки один SGW у даний момент часу. SGW міститься лише на площині користувача, беручи на себе відповідальність за пересилання пакетів даних від PGW до eNodeB і підтримуючи сеанс пересилання даних. Тому він може бути названий місцевим, або мобільним, якорем. Окрім того, коли мобільний пристрій переміщується з поточного eNodeB в інший, SGW підтримує сеанс для UE при перемиканні між різними eNodeB. SGW обробляє і передає дані, що надходять від UE в підсистему базових станцій оператора, а також дані, що йдуть у зворотному напрямі. Цей вузол також відповідає за деякі операції, пов'язані із забезпеченням мобільності користувача. Усі IP-пакети, які стосуються UE, передаються через SGW, який є анкерним для потоків даних, коли UE переміщується між різними базовими станціями (eNodeB). При цьому SGW зберігає всю інформацію про потоки UE, коли UE перебуває в режимі холостого ходу (у режимі очікування). Також SGW тимчасово накопичує дані, відправлені до UE, доти, доки MME запускає процедуру пейджингу (paging) UE, щоб створити потоки для передавання даних на UE.

Окрім перелічених функцій SGW виконує ще й деякі адміністративні завдання у візитній мережі. Наприклад, збір інформації для виконання операцій списання за рахунком.

Компонент PGW (*Packets Data Network Gateway*) — це шлюз, підімкнений до EPC із зовнішньої IP-мережі.

Компоненти PGW, призначивши IP-адресу (IPv4, IPv6) устаткування користувача, забезпечує підімкнення цього устаткування до певної мережі [8]. PGW працює як IP-прив'язка для підтримання однієї IP-адреси під час мобільності між службами 3GPP і не-3GPP, а також діє як домашній агент (HA). Окрім того, PGW несе відповідальність за якість обслуговування (QoS), здійснюваного відповідно до політики та умов PCRF компонента QoS у IMS. У разі, коли мобільний пристрій запитує носій або носій має встановити для виклику IMS, PGW та PCRF взаємодіють один з одним, аби переконатися, що політика стосовно цього носія була правильна.

Компонент HSS (*Home Subscriber system*) — це сервер для зберігання авторизаційної інформації та профілів абонентів; цей компонент є своєрідною базою даних для зберігання всієї інформації стосовно

користувача. HSS поєднує дві функції — реєстру даних про SIM-карти відповідного оператора мобільного зв'язку, коли кожній SIM-карті відповідає унікальний ідентифікатор — так званий IMSI, який є ключовим полем для кожного запису в HLR, та центру автентифікації (AuC). HSS несе відповідальність за зберігання та оновлення пов'язаних із підпискою користувачів даних, що включають у себе:

- адресу та ідентифікаційний номер користувача;
- профіль користувача;
- інформацію про автентифікацію та авторизацію мережі (шифрування шляху та захист цілісності).

У разі переходу UE з мережі LTE до мереж Wi-Fi, усі підписки на дані необхідно запитувати в LTE для підтримання безперервності під'єднання до мережі навіть для того UE, яке уже було ідентифіковано в мережі LTE.

Розглянемо запропоновану автором модифіковану архітектуру мережі Wi-Fi, в яку додано два компоненти для керування цією мережею (рис. 2). Перший компонент забезпечує керування доступом (AZC) і відповідає за обробку даних про AP та UE. У такому разі після переходу UE до мережі Wi-Fi відповідне устаткування може переміщуватися між різними AP без потреби повторного запиту до LTE. Другий компонент *Access Network Query Protocol-Data Server (ANQP-DS)* відповідає за збирання та зберігання даних, необхідних абонентові з мережі LTE, щоб залишатися під'єднаним до мережі Wi-Fi без перерви в отриманні послуг.

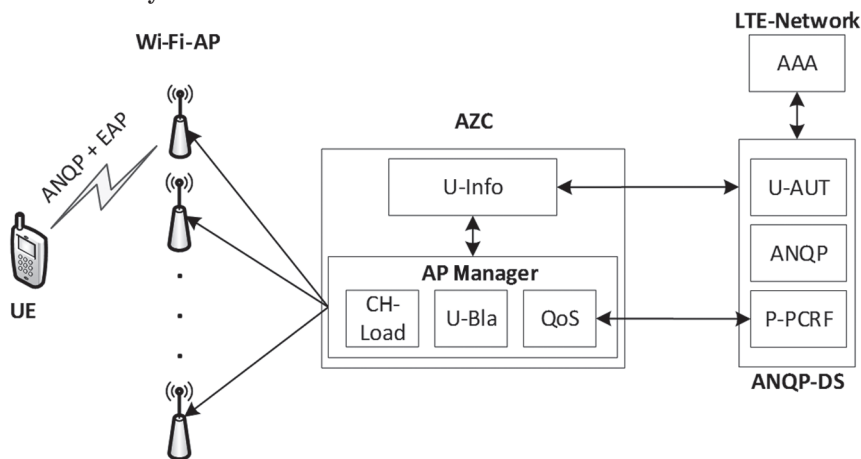


Рис. 2. Компоненти керування Wi-Fi мережею

Компонент AZC (Access Zone Control) відповідає за керування всім устаткуванням користувача та всіма точками доступу в зоні дії покриття Wi-Fi. Він складається з двох функціональних компонентів, що взаємодіють один з одним, маючи на меті керування безперебійною мобільністю, балансуванням навантаження UE в зоні покриття AP, а також і підтримкою QoS для окремого користувача в зоні мережі Wi-Fi.

Розглянемо докладніше складові AZC.

U-Info. Ця складова є своєрідним блоком пам'яті для збереження ідентифікаційної інформації UE. Коли UE вперше переходить із мережі LTE в мережу Wi-Fi, усі відповідні дані включаються в U-Info. Як правило, коли UE переходить від однієї точки доступу до іншої, це устаткування має бути щоразу автентифіковане, може викликати затримку при передаванні даних. Тому дані про зазначене устаткування включаються в U-Info відразу після успішного завершення процесу автентифікації; при переході UE до іншої точки доступу в радіусі зони покриття Wi-Fi процес автентифікації не потрібен, оскільки UE рухається в межах однієї зони покриття AZC.

Менеджер служби доступу (AP Manager). Функціональність цієї складової полягає в тому, щоб аналізувати точки доступу в зоні мережі Wi-Fi на предмет завантаженості каналу, балансувати завантаження точки доступу в межах певної зони покриття та підтримувати QoS для окремого користувача.

ANQP-DS (Access Network Query Protocol-Data Server). Ця складова являє собою сервер даних, що зберігає дані, пов'язані з користувачем, котрий раніше перебував у мережі LTE (профіль користувача, абонентський ідентифікатор, інформація про автентифікацію тощо), для керування безшовністю при переході користувача до мережі Wi-Fi. Як впливає з рис. 2, ANQP-DS складається з трьох компонентів: U-AUT, ANQP, P-PCRF.

U-AUT — компонент, який має зберігати інформацію про автентифікацію користувача з HSS у мережі LTE. Коли UE робить запит на приєднання до мережі Wi-Fi вперше, U-AUT збирає автентифікаційну інформацію з HSS. Ця інформація ідентична використовуваній інформації мережі LTE (механізми захисту EAP для автентифікації користувачів), аби дозволити користувачеві приєднатися до цієї мережі.

ANQP — компонент, що відповідає за зберігання інформації, пов'язаної з операторською мережею, та можливостями цієї мережі, такими як поточна пропускна здатність, кількість користувачів в окремій точці доступу та інформація постачальника. При цьому автори запропонували такий підхід: UE робить запит щодо мережної інформації, яка зберігається в даному блоці, перед вибором точки доступу для приєднання до мережі.

P-PCRF забезпечує копіювання правил QoS із мережі LTE та їх збереження для реалізації в зоні мережі Wi-Fi. Коли UE переходить до мережі Wi-Fi, йому потрібно призначити IP-адресу поточної служби (можливо, ту саму, яка раніше використовувалася, або деяку іншу). Тому, коли PGW призначає IP-адресу для UE в мережі Wi-Fi, вона також необхідна для ідентифікації політики правил QoS для послуги. Копії згаданих правил формує PCRF в LTE до P-PCRF у разі, якщо будь-які зміни статусу в мережі негативно впливають на ефективність мережі для служб UE, AZC буде обробляти вимоги QoS для поточної служби UE, запитуючи P-PCRF замість того, аби знову переходити в мережу LTE.

ANQP (Access Network Query Protocol) протокол типу запит-відповідь, що використовується мобільними пристроями для отримання інформації, котра включає в себе глобальне унікальне ім'я оператора хот-спота, список партнерських мереж, доступні типи IP-адрес (IPv4, IPv6) та інші дані, які мобільний пристрій може використовувати для вибору мережі. ANQP передає метадані, корисні для процесу вибору мережі мобільного пристрою, включаючи доменне ім'я оператора AP, IP-адреси (адреси інтернет-протоколів) доступні в AP, а також інформацію про потенційних роумінг-партнерів, доступних через AP.

Для забезпечення під'єднання до відповідної мережі в середовищі неоднорідного доступу протокол повинен зробити запит на зазначену далі інформацію.

- Місце розташування — поле, що визначає місце в мережі, котре може знадобитися користувачеві у процесі вибору мережі.
- Тип автентифікації. У цьому полі можна визначити додаткову інформацію, необхідну для під'єднання до мережі, наприклад, ім'я користувача та пароль для точки доступу.
- Інформація про стільникову мережу 3GPP.

Пропоновану архітектуру інтегрованих мереж LTE і Wi-Fi унаочнює рис. 3, у верхній частині якого зображено компоненти LTE EPC, а в нижній — компоненти мережі Wi-Fi. Як ми бачимо, PGW працює як агент мобільності, підтримуючи потік IP для UE, коли UE переміщується з мережі LTE в мережу Wi-Fi. Оператор, маючи на меті зменшити навантаження мережі LTE, переспрямовує деякі активні додатки UE від LTE до мережі Wi-Fi без затримки (FTP-файли та веб-сторінки) [9]. У цьому разі IPS надсилає контрольний запит до UE стосовно даних про доступні точки доступу Wi-Fi, після чого вибирає найбільш прийнятний AP для об'єднання в AZC.

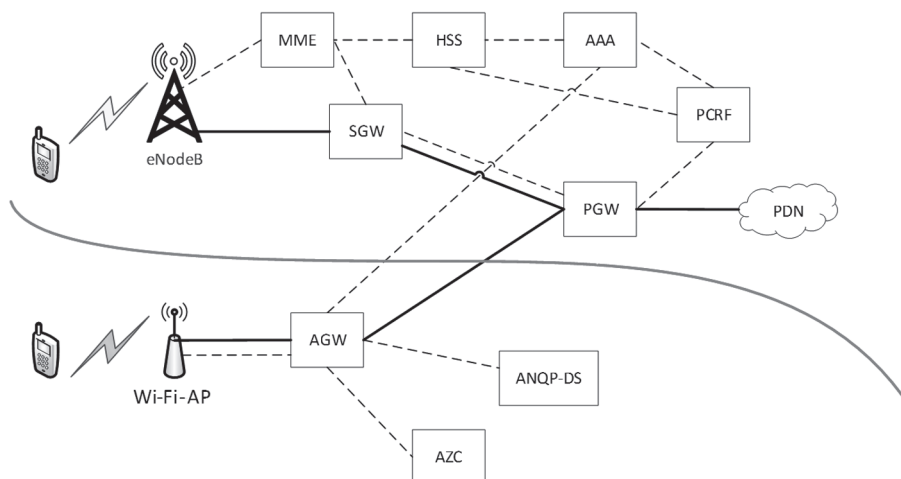


Рис. 3. Інтегровані мережі LTE і Wi-Fi

Головну увагу зосереджено на мережі Wi-Fi після того, як користувач переходить із мережі LTE в мережу Wi-Fi. При такому переході устаткування користувача сканує доступні точки доступу Wi-Fi, як це зображено на рис. 4. Для виявленої точки доступу це устаткування надсилає запити для з'єднання із зазначеною точкою, а далі воно порівнює інформацію ANQP-UE з інформацією ANQP-AP. За наявності розбіжності UE шукатиме іншу AP, а за відсутності розбіжності надсилає точці доступу повідомлення про підтвердження інформації авторизації. Точка доступу передає повідомлення щодо підтвердження серверу ANQP-DS для автентифікації UE. Один із серверів ANQP-DS автентифікує UE за допомогою однієї з моделей EAP, що її використовує UE. У нашому випадку ми застосовуємо той самий метод

автентифікації мережі, яким послуговується мережа LTE. Оскільки UE вперше приєднується до мережі Wi-Fi, то ANQP-DS робить запит до сервера AAA в мережі LTE для авторизації поточного UE. Якщо сервер AAA не розпізнає UE, то він відповідає ANQP-DS повідомленням про те, що неавторизоване устаткування користувача намагається приєднатися до мережі Wi-Fi. ANQP-DS надсилає відхилене повідомлення до AP, яке потім пересилається до UE.

В іншому разі, якщо AAA визнає UE, то AAA об'єднує додаткову інформацію про UE і надсилає її до ANQP-DS. Коли AAA надсилає прийняте повідомлення до ANQP-DS, то ANQP-DS додає UE до U-Info в AZC, аби констатувати, що UE перевірено і повторна автентифікація при переміщенні між AP Wi-Fi не знадобиться. Це зрештою зменшить час затримки для повторної автентифікації UE у процесі переходу UE між AP Wi-Fi (див. рис. 4).

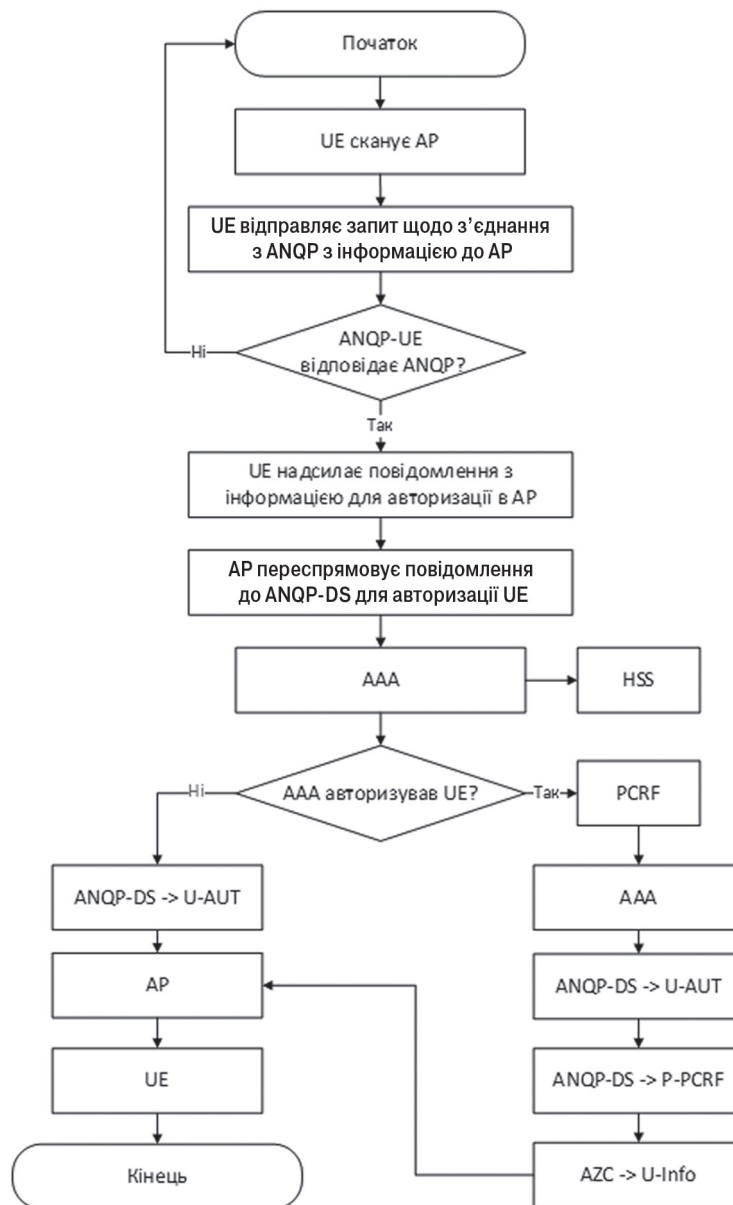


Рис. 4. Робочий процес між LTE та Wi-Fi

Остаточні результати нашого дослідження сформулюємо, скориставшись імітаційним моделюванням. Параметри моделювання, що характеризують топологію мережі симулятора, візьмомо такі. Пропускна здатність каналу LTE становить 100, а мережі Wi-Fi — 54 Мбіт/с. Усі UE під'єднано до мережі LTE або до мережі Wi-Fi. Було зроблено припущення, що дані трафіку в кожному UE максимально можуть становити 1 Мбіт/с, а максимальна кількість UE в LTE, яка не викликає затримки, дорівнює 25. Із рекомендацій щодо розвантаження відомо: IP-поток для веб та FTF не чутливі до затримки [9]. Трафік (відео та голосовий) доцільно тримати в мережі LTE, оскільки він дуже чутливий до затримки. До мережі Wi-Fi є сенс розвантажувати IP-поток, нечутливі до затримки.

Параметри імітаційної моделі

Швидкість передавання інформації	1 Гбіт/с
Пропускна здатність каналу LTE	100 Мбіт/с
Пропускна здатність Wi-Fi	54 Мбіт/с
Обсяг кешу в UE	1 Мбод для додатка

Середню пропускну здатність кожного додатка UE при різних значеннях завантаженості мережі наведено на рис. 5. Як бачимо, здатність практично однакова при кількості UE від 10 до 20 на 1 Мбіт/с кожної програми. У разі сценарію без розвантаження при збільшенні кількості UE пропускна здатність різко зменшується.

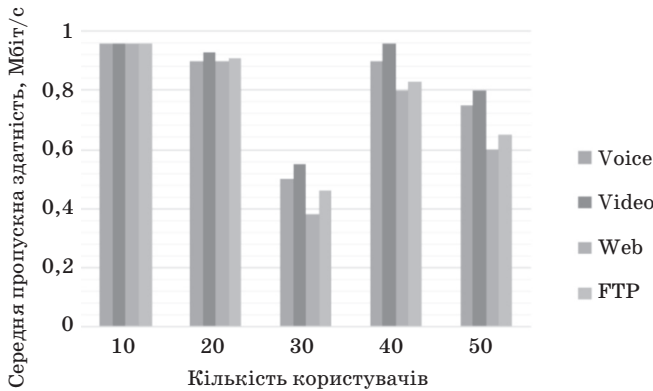


Рис. 5. Порівняльна характеристика середньої пропускну здатності для кожного додатка

Як відомо, згідно з EAP-AKA UE має на сервері AAA в LTE підлягати перевірці щоразу, коли він перемикає AP.

Натомість у нашій пропозиції просто потрібно приєднати сервер ANQP-DS для автентифікації UE. Якщо ми застосуємо EAP-AKA у швидкій передачі, час, необхідний для процедури автентифікації UE, становить 605 мс [6], тоді як у нашій пропозиції час, необхідний для автентифікації UE, становить усього 330 мс, тобто забезпечує істотний (58%) вигравш часу (див. таблицю).

Порівняння затримки автентифікації

Механізм автентифікації	Затримка автентифікації, мс
Стандарт EAP-AKA	605
Запропоноване нами рішення	330

Висновки

Запропоновано безшовну мережну архітектуру між LTE та Wi-Fi для розвантаження, із використанням PGW як прив'язки IP-потоків між LTE і Wi-Fi. Цим самим досягається підтримання безперебійного зв'язку.

Було додано два компоненти (ANQP-DS та AZC) до базової мережі Wi-Fi для керування автентифікацією UE та балансуванням навантаження UE між AP.

Додаткові блоки мережі сприяють зменшенню часу затримки автентифікації за рахунок збереження автентифікаційної інформації користувача.

Імітаційне моделювання модифікованої архітектури Wi-Fi Offload показало приріст середньої пропускну здатності мережі LTE при досягненні граничної кількості користувачів.

Список використаної літератури

1. **T. Specification.** Etsi ts 124 615. 2012. Vol. 0, no. Im. P. 0–28.
2. **T. Specification and G. Services.** 3Gpp Tr 23.829. 2011. Vol. 1, no. Release 10. P. 1–43.
3. **Sheets R.** Local area network. Pat. No.US5127067. 1985. Vol. 0. P. 0–23.
4. **Purohith D. R., Hegde A. and Sivalingam K. M.** Network architecture supporting seamless flow mobility between LTE and Wi-Fi networks // Proc. WoWMoM. 2015 A World Wirel. Mob. Multimed. Networks, 2015.
5. **Patino Gonzalez M. A., Higashino T. and Okada M.** Radio access considerations for data offloading with multipath TCP in cellular WiFi networks // Int. Conf. Inf. Netw. 2013. P. 680–685.
6. **Y. El Hajjaji El Idrissi, Zahid N. and Jedra M.** A new fast reauthentication method for the 3G-WLAN interworking based on EAPAKA // 20th Int. Conf. Telecommun. ICT 2013.

7. **Applying NFV and SDN to LTE mobile core gateways, the functions placement problem** / A. Basta, W. Kellerer, M. Hoffmann [a. all] // Proc. 4th Work. All things Cell. Oper. Appl. challenges — AllThingsCellular'14. 2014. P. 33–38.
8. **LTE mobile network virtualization Exploiting multiplexing and multi-user diversity gain** / Y. Zaki, L. Zhao, C. Goerg and A. Timm-Giel // Mob. Networks Appl. 2011. Vol. 16, no. 4. P. 424–432.
9. **Mobile Data Offload — Wi-Fi Offload** // Telecommun. Eng. Cent. 2015. Vol. 19, no. 3.
10. **USIM based Authentication Test-bed for UMTS-WLAN Handover** / H. Kwon, K. Cheon, K. Rho and A. Park // Infocom. 2006. P. 8–10.

Рецензент: доктор техн. наук, доцент **О. В. Шульга**, Полтавський національний технічний університет імені Юрія Кондратюка.

Е. А. Лосев, А. О. Пишко

МОДИФИЦИРОВАННАЯ АРХИТЕКТУРА WI-FI OFFLOAD

В связи с разнообразием персональных устройств появляется спрос на более скоростную связь. Чтобы справиться с ростом объемов трафика, операторам мобильной сети необходимо внедрять более скоростные и экономичные радиотехнологии, повышать пространственную эффективность путем развертывания малых сот, обеспечивая сбалансированное развитие гетерогенных сетей.

Операторы мобильной связи планируют разгрузить свои сети от трафика данных наиболее выгодным способом и улучшить свое экономическое положение. Изменение концепции также было вызвано тем фактом, что дальнейшие технологические разработки и усовершенствования сотовой архитектуры связаны физическими ограничениями. Кроме того, предоставление высокой пропускной способности и высокой скорости передачи данных требует значительных экономически неоправданных капитальных вложений.

Ввиду того, что уже несколько лет подряд трафик передачи данных в сетях сотовой связи показывает устойчивый рост, у операторов в данной ситуации остается только одна возможность для удовлетворения потребностей своих клиентов — увеличить плотность покрытия, обеспечивая таким образом большую полосу пропускания в расчете на одного абонента. В увеличении плотности покрытия нет ничего плохого, если не принимать во внимание экономические показатели оборудования одной установленной станции.

Другим вариантом решения проблемы является технология Wi-Fi Offload, призванная разгрузить сети мобильных операторов от трафика передачи данных за счет применения технологии Wi-Fi. В этом случае трафик передачи данных абонентов выводится из сети мобильного оператора в отдельную радиосеть, работающую с использованием собственных магистральных каналов. Также появляется возможность предоставления абонентам услуг через партнерские сети аналогично тому, как это делается, когда абонент находится в роуминге.

Актуальность модификации архитектуры Wi-Fi Offload обусловлена тем, что благодаря ей современному пользователю предоставляется возможность получения высококачественного доступа к интернет-ресурсам или к сервисам мобильного оператора. Оператор, в свою очередь, получает новые возможности для обслуживания дополнительного количества абонентов, а также уменьшает загруженность своих макросот.

Ключевые слова: мобильная сеть; Wi-Fi Offload; разгрузка; архитектура; LTE.

Е. О. Losev, А. О. Pyshko

MODIFIED ARCHITECTURE OF WI-FI OFFLOAD

Due to the growing variety of personal devices, there is a demand for more high-speed network connection. To cope with increasing traffic volumes, mobile network operators need to implement more high-speed and economical radio technologies, increase spatial efficiency by deploying small cells, thus ensuring balanced development of heterogeneous networks.

Mobile operators plan to unload their networks from data traffic in the most profitable way and improve their economic status. The change in concept was also due to the fact that further technological developments and improvements in cellular network architecture are impossible due physical constraints. In addition, providing high bandwidth and high data rates requires significant capital investments, which is economically not profitable.

Due to the fact that for several years now the traffic of data in cellular networks shows steady growth, operators in this situation remains only one opportunity to meet the needs of their customers — to increase the density of coverage, thus providing greater bandwidth per one subscriber. In the process of increasing in the density of the coating is right idea, but mobile operators have to take into account the economic performance of the equipment of one station.

Another solution of the problem is the Wi-Fi Offload technology, designed to unload mobile operators' networks from data traffic through the use of Wi-Fi technology. In this case, subscriber data traffic is offloaded from a mobile operator's network to a separate radio network operating using its own trunk channels. Also, it is possible to provide subscribers services through partner networks in the same way as it is done when the subscriber is in roaming.

The urgency of the modification of the Wi-Fi Offload architecture is due to the fact that it will give the modern user the opportunity to receive high-quality access to Internet resources or to the service of a mobile operator. The operator, in turn, gets the opportunity to service an additional number of subscribers, and also reduces the loading of their macros.

Keywords: mobile network; Wi-Fi Offload; offloading; architecture; LTE.