УДК 004.056.5

Д.І. Прокопович-Ткаченко

Академія митної служби України, Дніпропетровськ

ДОСЛІДЖЕННЯ ПРОТОКОЛІВ АВТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ ДОСТУПУ В БЕЗПРОВОДОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Проведені дослідження протоколів автентифікації та авторизації в сучасних бездротових телекомунікаційних системах та мережах дозволили встановити, що основними застосовуваними механізмами є протоколи RSA та/або EAP із певними функціями розподілу ключів. Їх використання дозволяє провести односторонню (АС) або двосторонню (АС і БС) автентифікацію та створити відповідну ієрархію ключів авторизації безпроводового доступу.

Ключові слова: *безпека, інформаційна система, безпроводова телекомунікаційна мережа.*

Вступ

Для вирішення задач автентифікації та авторизації в безпроводових телекоммунікаційних системах і мережах, які побудовано відповідно до специфікації міжнародних стандартів серії IEEE 802.16, використовуються засоби протоколу EAP (Extensible Authentication Protocol), криптографічного протоколу RSA (Rivest, Shamir і Adleman), а також засоби протоколу управління ключами PKM (Privacy and Key Management protocol) для безпечного розподілу ключової інформації [1 – 6].

Протоколи автентифікації і авторизації призначено для забезпечення вимог сервіс-провайдерів (NSP, Network Service Provider) та користувачів. З одного боку, автентифікація дозволяє встановити достовірність користувача та пристрою, який використовує користувач.

За допомогою процедури авторизації сервіс-провайдер NSP встановлює відповідність між автентифікованим користувачем та переліком доступних йому сервісів.

Таким чином, сервіс-провайдери можуть бути упевнені в тому, що доступ до мережі буде надано тільки їх клієнтам, і що вони використовуватимуть тільки ті сервіси, за які сплатили.

З іншого боку, підрівень безпеки стандартів IEEE 802.16 задовольняє основним вимогам користувачів, а саме, вимоги в конфіденційності і цілісності даних, що передаються в мережі, а також в тому, що клієнт завжди зможе дістати доступ до сплачених ним сервісів [7].

Метою статті є аналіз схеми автентифікації та авторизації доступу в типовій безпроводовій телекомунікаційній системі, побудованої відповідно до специфікації міжнародних стандартів серії IEEE 802.16 [1 – 7], дослідження основних компонентів та застосовуваних перетворень, які визначають послідовність дій, яку потрібно виконати для вирішення задач автентифікації та авторизації доступу.

1. Дослідження протоколу автентифікації та авторизації доступу відповідно до специфікації PKMv1

Схема автентифікації та авторизації доступу відповідно до специфікації PKMv1 в телекомунікаційній системі, побудованої за IEEE 802.16, наведена на рис. 1. Відповідно до цієї схеми використовується така послідовність передачі службових повідомлень [1 – 7].

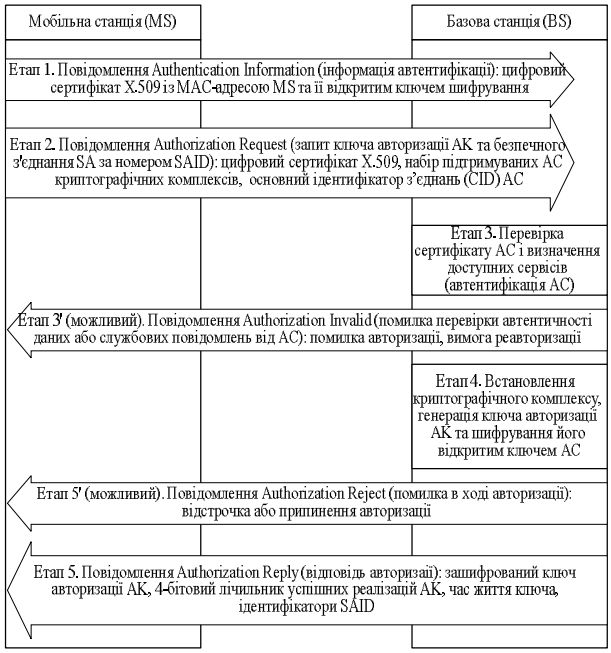

Рис. 1. Схема автентифікації та авторизації доступу в телекомунікаційній системі, побудованої за IEEE 802.16 (відповідно до PKMv1)

На першому етапі абонентська станція (АС) посилає базовій станції (БС) повідомлення Authentication Information. Воно містить цифровий сертифікат X.509, закладений в АС виробником або сторонньою організацією. Сертифікат містить також

MAC-адресу АС і її відкритий ключ шифрування. Сама АС, відповідно має секретний ключ, який відповідає цьому переданому відкритому ключу.

Відразу після надсилання повідомлення Authentication Information АС посилає повідомлення Authorization Request, в якому запрошує у БС загальний ключ авторизації (Authorization Key, AK), а також запрошує встановлення безпечного з'єднання (Security Association, SA). За визначенням, яке використовується у специфікації стандартів серії IEEE 802.16, під безпечним з'єднанням розуміється сукупність інформації, яка дозволяє здійснювати безпечний обмін даними між АС і БС. Зокрема, до інформації SA відноситься використовуваний криптографічний комплекс, вектори ініціалізації, ключі TEK і час їх життя. Як вже було відмічено, час життя TEK обмежений, і для постійного підтримування SA АС доводиться отримувати нові ключі через певні проміжки часу.

Безпечне з'єднання SA визначається своїм номером SAID (Security Association Identifier). Цей номер, разом з AK, АС запрошує у БС в повідомленні Authorization Request. Повідомлення містить наступну інформацію [1-7]:

– цифровий сертифікат X.509;

– набір підтримуваних АС криптографічних комплексів;

– основний ідентифікатор з'єднань (Connection Identifier, CID) АС, який, у разі позитивної відповіді від БС, буде привласнений SAID.

На стороні NAP (Network Access Provider) і NSP (Network Service Provider) здійснюється перевірка сертифікату АС і визначення доступних цій АС сервісів, тобто відбувається авторизація.

Далі БС встановлює загальний з АС підтримуваний криптографічний комплекс, генерує AK, шифрує його відкритим ключем АС і посилає їй повідомлення Authorization Reply, що містить [1-7]:

– зашифрований ключ авторизації AK;

– 4-бітовий лічильник успішних реалізацій AK;

– час життя ключа;

– ідентифікатори SAID, які БС надає АС для встановлення одного або декілька безпечних з'єднань SA.

У разі виникнення помилок в ході авторизації БС надсилає АС повідомлення Authorization Reject, в якому БС може вимагати від АС або відстрочити спроби авторизації, або припинити ці спроби зовсім (якщо неможливо визначити виробника АС, або не вдається перевірити її цифровий сертифікат, або не представляється можливим погоджувати криптографічний комплекс і т. д.).

Ключ авторизації AK має обмежений термін життя, тому АС (як і БС) повинна періодично оновлювати AK, посилаючи запити Authorization Request. Для того, щоб безпечне з'єднання SA не уривалася на час зміни ключів, АС повинна зберігати одночасно два ключа авторизації AK - поточний і новий, причому такі, що перекривають один одний наполовину за часом дії. Як тільки закінчується термін дії поточного ключа авторизації AK, АС переходить на новий AK (який стає поточним) і посилає Authorization Request для отримання нового AK.

Якщо на стороні БС відбудеться помилка перевірки автентичності даних або службових повідомлень від АС (тобто при підозрі на дію зловмисника), БС може надіслати АС повідомлення Authorization Invalid з вимогою реавторизації.

2. Дослідження протоколу автентифікації та авторизації доступу відповідно до специфікації PKMv2

Відповідно до специфікації PKMv2 можливі три схеми автентифікації та авторизації [1-7]:

– із застосуванням алгоритму RSA (одностороння автентіфікция АС);

– із застосуванням протоколу EAP (двостороння автентифікація: АС і БС);

– комбінація алгоритмів RSA і протоколу EAP (двостороння автентифікація: АС і БС).

Перша схема автентифікації та авторизації (із застосуванням схеми RSA) ідентична розглянутій вище схемі в протоколі PKMv1.

Схеми автентифікації та авторизації із застосуванням протоколу EAP та комбіновані схеми із алгоритмом RSA і протоколом EAP мають спільну загальну конструкцію із двома фазами: фаза EAP і фаза так званого потрійного рукостискання (3-way handshake). Загальна схема автентифікації та авторизації доступу в телекомунікаційній системі, побудованої за IEEE 802.16e (відповідно до PKMv2) зображена на рис. 2 [1 – 7].

Позначення, використані на рис. 2, відповідають схемі авторизації в типовій системі зв'язку IEEE 802.16e:

– MS - мобільна станція;

– BS - базова станція;

– AAA - сервер автентифікації, авторизації та обліку.

Перша автентифікація EAP є автентифікацією пристроїв, друга автентифікація EAP є автентифікацією користувачів, що виконується після успішного виконання першої автентифікації EAP.

На першому етапі при необхідності автентифікації пристроїв базова станція передає запит імені EAP («EAP-REQUEST/IDENTITY») на мобільну станцію, запрошуючи автентифікацію EAP.

На другому етапі, після обміну повідомленнями EAP між мобільною станцією і базовою станцією за допомогою протоколу розподілу ключів секрет-

ності (PKM)_EAP_TRANSFER в системі IEEE 802.16e, базова станція передає запит імені EAP («PKM_EAP/EAP-REQUEST/IDENTITY») на мобільну станцію . Мобільна станція відповідає передачею відповіді з ім'ям EAP («PKM_EAP/EAP-RESPONSE/IDENTITY»).

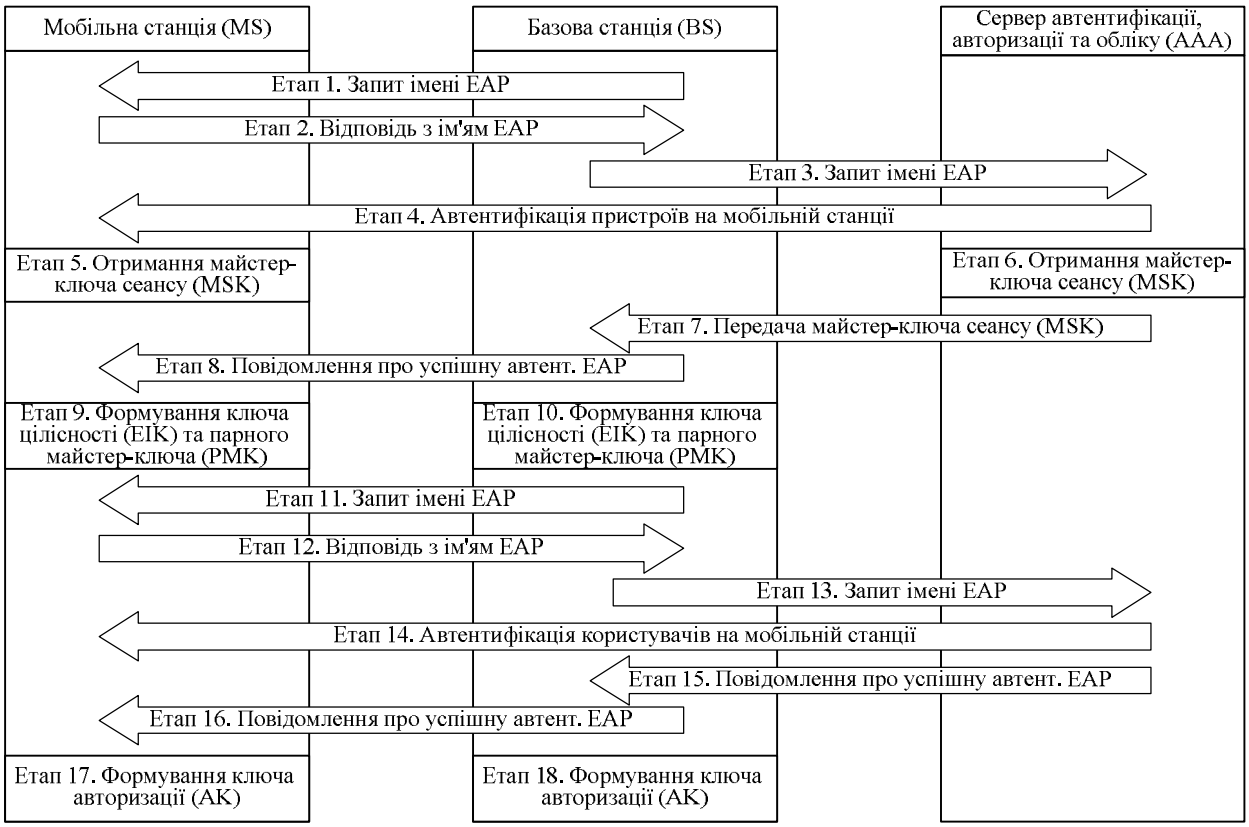

Рис. 2. Схема автентифікації та авторизації доступу в телекомунікаційній системі, побудованої за IEEE 802.16e (відповідно до PKMv2)

На третьому етапі базова станція передає запит імені EAP («PKM_EAP-EAP-RESPONSE/IDENTITY») на сервер автентифікацій, авторизації і обліку (AAA). Базова станція і сервер аутентифікацій, авторизації і обліку обмінюються повідомленнями EAP за допомогою повідомлень протоколу служби дистанційної автентифікації користувачів. Відповідно до цього базова станція передає відповідне повідомлення («RADIUS ACCESS REQEST/IDENTITY») на сервер автентифікацій, авторизації і обліку.

На четвертому етапі сервер автентифікацій, авторизації і обліку виконує автентифікацію пристроїв на мобільній станції за допомогою автентифікації повідомлень PKM_EAP з використанням протоколу захисту транспортного рівня (EAP-TLS), протоколу захисту транспортного рівня з використанням передвстановленого загального ключа (EAP-TLSPSK), протоколу для автентифікації і узгодження ключів (EAP-AKA) або протоколу EAP-PSK. В результаті автентифікації пристроїв, на п'ятому та шостому етапах, сервер автентифікацій, авторизації і обліку і мобільна станція спільно отримують майстер-ключ сеансу.

На сьомому етапі сервер автентифікацій, авторизації і обліку передає повідомлення «RADIUS ACCEPT» як повідомлення «EAP-SUCCESS» на базову станцію. Це повідомлення «RADIUS ACCEPT» включає майстер-ключ сеансу.

На восьмому етапі базова станція передає повідомлення «PKM_EAP/EAP-SUCCESS» на мобільну станцію, повідомляючи про успішну автентифікацію EAP.

На дев'ятому та десятому етапах мобільна станція і базова станція формують ключ цілісності EAP і парний майстер-ключ з мастер-ключа сеансу в процесі автентифікації пристроїв. Ключ цілісності EAP, сформований в процесі автентифікації пристроїв, використовується для захисту повідомлень EAP, що передаються в процесі другої автентифікації EAP, тобто автентифікації користувачів.

На одинадцятому етапі, при необхідності автентифікації користувачів, в процесі автентифікації користувачів базова станція передає повідомлення «PKM_EAP/EAP-REQUEST/IDENTITY» на мобільну станцію. На дванадцятому етапі мобільна станція відповідає передачею повідомлення «PKM_EAP/EAP-RESPONSE/IDENTITY».

На тринадцятому етапі базова станція перетворює повідомлення «PKM_EAP/EAP-RESPONSE/IDENTITY» у форму повідомлення «RADIUS ACCESS REQUEST/IDENTITY» і передає його на сервер автентифікацій, авторизації і обліку.

На чотирнадцятому етапі сервер автентифікацій, авторизації і обліку виконує автентифікацію користувачів на мобільній станції за допомогою аутентифікації повідомлень PKM_EAP з використанням протоколу аутентифікації EAP-MD5 або EAP-MSCHAPV2. На відміну від автентифікації пристроїв, ніякий додатковий майстер-ключ сеансу не формується, навіть в тому випадку, якщо автентифікація користувачів завершена.

Тим часом, на п'ятнадцятому етапі, базова станція приймає повідомлення «RADIUS ACCEPT» та на шістнадцятому етапі передає повідомлення «PKM_EAP/EAP-SUCCESS» на мобільну станцію.

На шістнадцятому та сімнадцятому етапах мобільна станція і базова станція формують ключ авторизації з використанням парного мастер-ключа.

Таким чином, в процесі автентифікації EAP системи зв'язку IEEE 802.16e, майстер-ключ сеансу формується в процесі першої автентифікації EAP.

Далі базова станція (див. рис. 2) приймає майстер-ключ сеансу, сформований в процесі першої автентифікації EAP, тобто автентифікації пристроїв, з сервера автентифікації, авторизації і обліку, а потім формує ключ цілісності EAP і парний майстер-ключ з використанням мастер-ключа сеансу. Зокрема, базова станція формує ключ цілісності EAP (EIK) і парний майстер-ключ із заздалегідь певною кількістю бітів, наприклад 160-бітовий ключ цілісності EAP і 160-бітовий парний майстер-ключ, за допомогою усікання мастер-ключа сеансу.

Висновки

Проведені дослідження протоколів автентифікації та авторизації в сучасних бездротових телекомунікаційних системах та мережах дозволили встановити, що основними застосовуваними механізмами є протоколи RSA та/або EAP із певними функціями розподілу ключів. Їх використання дозволяє провести одностороннюю (АС) або двосторонню (АС і БС) автентифікацію та створити відповідну ієрархію ключів авторизації безпроводового доступу. Саме властивості формованих ключів авторизації і визначають рівень безпеки телекомунікаційних систем і мереж при наданні безпроводового доступу.

Перспективним напрямком подальших досліджень є розробка математичної моделі авторизації та автентифікації безпроводового доступу, обґрунтування пропозицій щодо вдосконалення процедур формування псевдовипадкових ключів авторизації для підвищення безпеки телекомунікацій.

Список літератури

1. IEEE Std IEEE 802.16a 2001 IEEE Standard for Local and metroo politan area networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems. – IEEE, 8 April 2002.

2. IEEE Std IEEE 802.16c 2002. IEEE Standard for Local and mett ropolitan area networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Amendment 1: Detailed System Profiles for 10–66 GHz. – IEEE, 15 January 2003.

3. IEEE Std IEEE 802.16a 2003. IEEE Standard for Local and mett ropolitan area networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Amendment 2: "Medium Access Control Modifications and Additional Physical Layer Specifications for 2–11 GHz". – IEEE, 1 April 2003.

4. IEEE Std IEEE 802.16™™2004 (Revision of IEEE Std IEEE 802.166 2001). IEEE Standard for Local and metropolitan area networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems. – IEEE, 1 October 2004.

5. Стандарт беспроводных сетей городского масштаба. — IEEE Std 802.16™–2009.

6. Standard for local and metropolitan area networks. – IEEE Std 802.16m-2011. – 2011.

7. Рашич А. В. Сети беспроводного доступа WiMAX: учеб. пособие / Рашич А.В. – СПб.: Изд-во Политехн. ун-та, 2011. – 179 с.

Надійшла до редколегії 30.01.2013

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський національний університет радіоелектроніки, Харків.

ИССЛЕДОВАНИЕ ПРОТОКОЛОВ АВТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ ДОСТУПА В БЕСПРОВОДНЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ

Д.И. Прокопович-Ткаченко

Проведены исследование протоколов автентификации и авторизации в современных беспроволочных телекоммуникационных системах и сетях позволили установить, что основными применяемыми механизмами являются протоколы RSA та/або EAP с определенными функциями распределения ключей. Их использование позволяет провести одностороннюю (АС) или двустороннюю (АС и БС) автентификацию и создать соответствующую иерархию ключей авторизации беспроводного доступа.

Ключевые слова: *безопасность, информационная система, беспроводная телекоммуникационная сеть.*

RESEARCH OF PROTOCOLS OF AVTENTIFIKATION AND AUTHORIZING OF ACCESS IN OFF-WIRE TELECOMMUNICATION SYSTEMS AND NETWORKS

D.I. Prokopovich-Tkachenko

Conducted research of protocols of avtentifikation and authorizing in the modern wireless telecommunication systems and networks allowed to set that the basic applied mechanisms are protocols of RSA ma/або EAP with the certain functions of distributing of the keys. Their use allows to conduct one-sided (ACE) or bilateral (ACE and BS) avtentifikation and to create the proper hierarchy of the keys of authorizing of off-wire access.

Keywords: *safety, informative system, off-wire telecommunication network.*