Захист інформації

УДК 004.056.5

Д.І. Прокопович-Ткаченко

Академія митної служби України, Дніпропетровськ

МАТЕМАТИЧНА МОДЕЛЬ АВТОРИЗАЦІЇ ТА АВТЕНТИФІКАЦІЇ БЕЗПРОВОДОВОГО ДОСТУПУ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Пропонується математична модель авторизації та автентифікації безпроводового доступу, яка дозволяє врахувати колізійні властивості формованих ключів авторизації для оцінки безпеки телекомунікаційних систем та мереж. Обгрунтовуються вимоги до схеми авторизації та автентифікації, виконання яких дозволяє забезпечити потрібні ймовірнісно-часові показники формованих ключів авторизації доступу для підвищення безпеки безпроводових телекомунікаційних систем і технологій.

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

Вступ

Протоколи автентифікації і авторизації, які використовуються в сучасних телекомунікаційних системах і мережах, призначено для забезпечення сучасних вимог безпеки та надання відповідних послуг сервіс-провайдерам (NSP, Network Service Provider) та користувачам [1 – 7]. Автентифікація дозволяє встановити достовірність користувача та пристрою, за допомогою авторизації сервіс-провайдер NSP встановлює відповідність між автентифікованим користувачем та переліком доступних йому сервісів. Таким чином, доступ до мережі надається тільки вповноваженим на це клієнтам, із забезпеченням вимог конфіденційності і цілісності даних, а також доступності інформаційних сервісів.

Проведені дослідження [8] протоколів автентифікації та авторизації дозволили встановити, що основними застосовуваними механізмами є RSA та/або EAP-авторизація із відповідними функціями розподілу ключів. Їх використання дозволяє провести односторонню або двосторонню 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.

В роботі пропонується математична модель авторизації та автентифікації безпроводового доступу, яка дозволяє врахувати колізійні властивості формованих ключів авторизації для оцінки безпеки телекомунікаційних систем та мереж. Обгрунтовуються вимоги до схеми авторизації та автентифікації, виконання яких дозволяє забезпечити потрібні ймовірнісно-часові показники формованих ключів авторизації доступу для підвищення безпеки безпроводових телекомунікаційних систем і технологій.

1. Автентифікація та авторизація доступу в безпроводових телекомунікаційних системах та мережах відповідно до специфікації IEEE 802.16

Для вирішення задач автентифікації та авторизації в безпроводових телекомунікаційних 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 – 8].

Схема автентифікації та авторизації доступу відповідно до специфікації PKMv1 наведена у [8, стор. 119, рис. 1] . Відповідно до цієї схеми використовується така послідовність передачі службових повідомлень. Відповідно до специфікації PKMv2 можливі три схеми автентифікації та авторизації [1 – 8]: 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 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 відповідно до PKMv2 наведена у [8, стор. 121, рис. 2].

Дослідження протоколів автентифікації та авторизації підключень в сучасних безпроводових телекомунікаційних системах та мережах показують, що властивості формованих ключів авторизації визначають рівень безпеки телекомунікаційних систем і мереж при наданні безпроводового доступу.

Для врахування певних властивостей формованих ключів авторизації при оцінці безпеки телекомунікаційних систем та мереж пропонується математична модель авторизації та автентифікації безпроводового доступу.

2. Математична модель авторизації та автентифікації безпроводового доступу

Для формалізованого опису всіх етапів автентифікації та авторизації безпроводового доступу в сучасних телекомунікаційних системах та мережах, які побудовано відповідно до специфікації міжнародних стандартів серії IEEE 802.16, будемо використовувати наступні позначення:

– pre-PAK – головний ключ авторизації (pre-Primary Authorization Key), який отримано в результаті виконання протоколу автентифікації та авторизації із застосуванням алгоритму RSA;

– EIK – ключ цілісності (EAP Integrity Key for authenticating Authenticated EAP message), який формується із застосуванням спеціальної функції Dot16KDF, та який призначено для забезпечення цілісності та автентичності переданих даних протоколу EAP;

– PAK – первинний ключ авторизації (Primary Authorization Key), який формується із застосуванням спеціальної функції Dot16KDF, та який призначено для формування ключа авторизації AK (Authorization Key);

– MSK – майстер-ключ сеансу (Master Session Key), який формується в процесі автентифікації EAP та призначений для формування парного майстер ключа PMK (Pairwise Master Key);

– PMK – парний майстер-ключ, який формується із застосуванням спеціальної функції Dot16KDF, та який призначено для формування ключа авторизації AK;

– Dot16KDF - спеціальна функція, яка призначена для для формування псевдовипадкових послідовностей, які використовуються у якості ключів різного призначення, в тому числі, і для формування ключа авторизації AK;

– SSID – ідентифікатор мобільної станції, для якої виконана автентифікація EAP;

– BSID – ідентифікатор базової станції;

– AK – ключ авторизації, який надає права авторизованого доступу та із застосуванням якого формується решта ключів, в тому числі ключів шифрування трафіку TEK (Traffic Encryption Key).

Основною функцією, яка застосовується під час формування ключів авторизації, є спеціальна функція

Dot16KDF(key, astring, keylength),

аргументами якої є такі значення:

– key – секретний ключ, який ініціює функцію Dot16KDF, тобто задає конкретне правило її обчислення;

– astring – значення, яке подається на вхід функції Dot16KDF у якості відкритого параметру, тобто параметру, на який не накладається вимага секретності;

– keylength – несекретний параметр, який визначає бітову довжину виходу перетворення, тобто бітову довжину значення функції Dot16KDF за введеними key та astring.

Конкретна реалізація обчислення функції Dot16KDF залежить від певних налаштувань і може бути побудована одним із сучасних криптографічних алгоритмів. Зокрема, за специфікацією протоколів безпеки стандартів серії IEEE 802.16 у якості базового криптографічного алгоритму пропонується використовувати блокове симетричне шифрування AES (наприклад, в режимі CMAC), алгоритм якого стандартизовано в федеральному стандарті США FIPS-197. Допускається також застосування алгоритму ключового ґешування HMAC із використанням стандартизованої функції SHA.

При авторизації із використанням алгоритму RSA правило формування ключів цілісності EIK та первинних ключів авторизації PAK із застосуванням спеціальної функції Dot16KDF за визначеними (наперед заданими) ідентифікаторами мобільної та базової станції та головним ключем авторизації pre-PAK задається наступним математичним виразом:

$$EIK \mid PAK = Dot16KDF(pre\text{-}PAK, SSID \mid BSID \mid \mid \text{“EIK+PAK”}, 320), \quad (1)$$

де x | y – є конкатенацією бітових послідовностей x та y, тобто, якщо бітову довжину keylength значення функції Dot16KDF задано у 320 бітів, тоді бітові довжини ключа цілісності EIK та первинного ключа авторизації PAK дорівнюють 160 бітів кожна.

При застосуванні для авторизації алгоритму RSA правило формування ключів авторизації безпроводового доступу визначається за наступним виразом:

$$AK = Dot16KDF(PAK, SSID \mid BSID \mid \text{“AK”}, 160). \quad (2)$$

Таким чином, при використанні алгоритму RSA відбувається встановлення первинного, загального для БС і АС ключового матеріалу - головного ключа AK (pre-Primary AK, pre-PAK). За допомогою Dot16KDF з pre-PAK формується 160-бітовий PAK, з якого, у свою чергу, за допомогою Dot16KDF генерується AK. Ієрархія ключів у разі RSA-авторизації представлена на рис. 1.

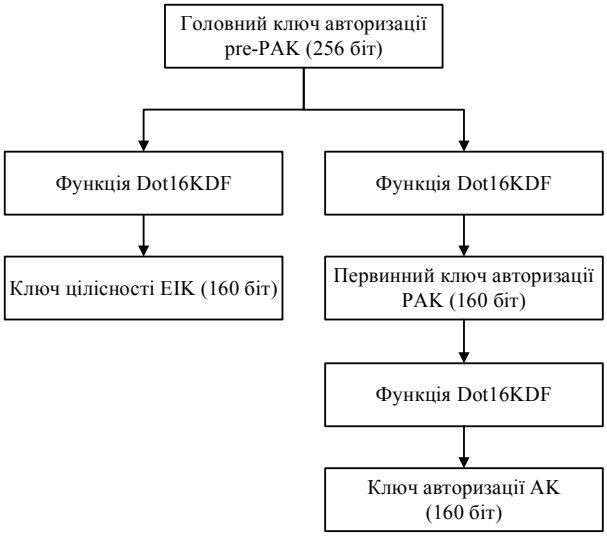

Рис. 1. Ієрархія ключів
при застосуванні RSA-авторизації

Таким чином, алгоритм формування ключа авторизації AK подамо такою послідовністю кроків:

Крок 1. Введення головного ключа авторизації pre-PAK;

Крок 2 Формування ключа цілісності EIK та парного ключа авторизації PAK за виразом (1);

Крок 3. Формування ключа авторизації AK за виразом (2);

Крок 4. Вивід сформованого ключа авторизації AK.

Основні властивості формованих ключів авторизації AK визначаються таким чином певними властивостями головного ключа авторизації pre-PAK та спеціальної функції Dot16KDF.

При авторизації із використанням алгоритму EAP правило формування ключів цілісності EIK та парних майстер ключів із застосуванням функції Dot16KDF за визначеними (наперед заданими) ідентифікаторами мобільної та базової станції та майстер-ключем сеансу MSK задається наступним математичним виразом:

$$EIK \mid PMK = truncate\ (MSK, 320)\ . \qquad (3)$$

Наступний вираз задає правило формування ключів авторизації безпроводового доступу із використанням алгоритму EAP:

$$AK = Dot16KDF(PMK, SSID \mid BSID \mid\ \text{“AK”}, 160)\ . \qquad (4)$$

Таким чином, при використанні EAP-авторизації, первинним, загальним для БС і АС ключовим матеріалом є 512-бітовий майстер-ключ сеансу MSK (див. рис. 2). Шляхом скорочення MSK до 160 битів АС і автентифікатор отримують парний майстер-ключ PMK.

Після цього з PMK за допомогою функції Dot16KDF генерується AK, а для PMK встановлюється час життя, до закінчення якого повинна бути проведена реавтентіфікація. Інакше, автентифікація проводиться спочатку. Ієрархія ключів у разі EAP-авторизации представлена на рис. 2.

Рис. 2. Ієрархія ключів
при застосуванні EAP-авторизации

Алгоритм формування ключа авторизації AK при застосуванні протоколу EAP подамо такою послідовністю кроків:

Крок 1. Введення майстер-ключа сеансу MSK;

Крок 2. Формування парного ключа майстер-ключа PMK за виразом (3);

Крок 3. Формування ключа авторизації AK за виразом (4);

Крок 4. Вивід сформованого ключа авторизації AK.

Таким чином, основні властивості формованих ключів авторизації AK визначаються певними властивостями майстер-ключа сеансу MSK та спеціальної функції Dot16KDF.

При сумісному використанні RSA і EAP проводяться обидві процедури авторизації, які описані вище. За допомогою pre-PAK також створюється 160-бітовий ключ EIK для автентифікації повідомлень EAP. В результаті AC володіє як PAK, так і PMK, з яких за допомогою функції Dot16KDF генерується AK.

$$AK = Dot16KDF\ (PAK \oplus PMK, SSID \mid BSID \mid \mid\ \text{“AK”}, 160). \qquad (5)$$

Ієрархія ключів у разі RSA-EAP-авторизації представлена на рис. 3. Алгоритм формування ключа авторизації AK при сумісному застосуванні протоколу EAP та алгоритму RSA подамо такою послідовністю кроків:

Крок 1. Введення головного ключа авторизації pre-PAK та майстер-ключа сеансу MSK;

Крок 2. Формування ключа цілісності EIK та парного ключа авторизації PAK за виразом (1);

Крок 3. Формування парного ключа майстер-ключа PMK за виразом (3);

Крок 4. Формування ключа авторизації AK за виразом (5);

Крок 5. Вивід сформованого ключа авторизації AK.

Властивості формованих ключів авторизації AK визначаються у цьому випадку певними властивостями головного ключа авторизації pre-PAK майстер-ключа сеансу MSK та спеціальної функції Dot16KDF.

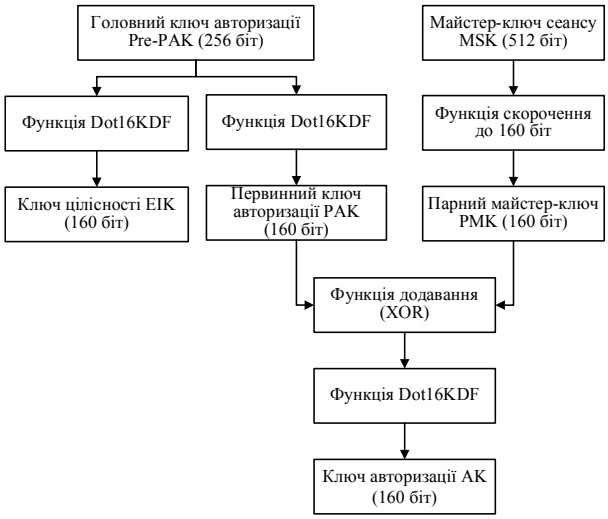

Рис. 3. Ієрархія ключів
при застосуванні RSA-EAP-авторизації

В пропонованій математичній моделі авторизації та автентифікації безпроводового доступу для оцінки безпеки телекомунікаційних систем та мереж врахуються колізійні властивості формованих ключів авторизації АК. Для вирішення цієї задачі використаємо такі припущення:

– введений головний ключ авторизації pre-PAK та/або майстер-ключ сеансу MSK було сформовано випадково, рівноймовірно та незалежно один від одного;

– спеціальна функція Dot16KDF побудована із застосуванням криптографічно стійкого алгоритму, наприклад, алгоритму AEC та/або HMAC;

– ідентифікатори мобільної SSID та базової BSID станції, які використовуються як аргумент функції Dot16KDF, сформовано відкритим способом (без збереження в таємниці цих ідентифікаторів).

Введені припущення повністю відповідають основним положенням, які викладено в специфікації стандартів серії IEEE 802.16. При цьому, перше та друге припущення задовольняє виконанню вимог щодо забезпечення ймовірнісно-часових та статистичних властивостей ключів авторизації АК доступу:

– ймовірність викриття P_B правила їх формування АК визначається криптографічними властивостями функції Dot16KDF, яка за умови застосування криптографічно стійкого алгоритму із випадковим, рівноймовірним та незалежним один від одного введеним ключем ініціації (головним ключем авторизації pre-PAK та/або майстер-ключем сеансу MSK) визначається за нижньою межею, тобто $P = 2^{-160}$;

– безпечний час $T_Б$ функціонування ключів авторизації АК, який як зворотна величина до ймовірності P_B викриття із врахуванням обчислювальних можливостей зловмисника буде дорівнювати $T_Б = 2^{160} / (\gamma \cdot \Psi)$. Якщо припустити, що зловмисник володіє надпотужними обчислювальними можливостями, тобто, наприклад, може виконувати 10^{15} переборів ключів авторизації АК за секунду (обчислювальні потужності всього світу менші за цю оцінку), тоді $T_Б > 10^{25}$ років, що значно більше ніж термін життя ключів авторизації доступу;

– статистичні властивості формованих ключів авторизації доступу визначаються статистичними властивостями вихідних послідовностей функції Dot16KDF, яка за умови застосування криптографічно стійкого алгоритму із випадковим, рівноймовірним та незалежним один від одного введеним ключем ініціації (головним ключем авторизації pre-PAK та/або майстер-ключем сеансу MSK) є статистично безпечним генератором псевдовипадкових послідовностей.

Втім, зазначені позитивні ймовірнісно-часові та статистичні властивості ключів авторизації доступу, які формуються із використанням спеціальної функції Dot16KDF, не гарантують виконання вимог щодо до ймовірності збігу $P_З$ ключів авторизації доступу АК.

Пропонована математична модель дозволяє врахувати колізійні властивості формованих ключів авторизації для оцінки безпеки безпроводових телекомунікаційних систем та мереж наступним чином.

Позначимо через

$$K_1, K_2, \ldots, K_n \qquad (6)$$

та

$$K'_1, K'_2, \ldots, K'_n \qquad (7)$$

послідовність випадково, рівноймовірно та незалежно один від одного введених ключів ініціації, тобто головних ключів авторизації pre-PAK та майстер-ключів сеансу MSK, відповідно.

Позначимо також через

$$AK_1, AK_2, \ldots, AK_n \qquad (8)$$

послідовність формованих за розглянутими вище схемами ключів авторизації доступу.

У разі застосування RSA-авторизації кожен з ключів авторизації доступу визначається такою функцією:

$$AK_i = \text{Dot16KDF}\,(PAK_i, \text{SSID} \mid \text{BSID} \mid \text{“AK”}, 160), \quad (9)$$

де $PAK_i = \text{Truncate}\,(\text{Dot16KDF}(K_i, \text{SSID} \mid \text{BSID} \mid \mid \text{“EIK+PAK”}, 320), 160)$

є і-м первинним ключем авторизації, який сформовано відповідно до (1).

Таким чином, маємо наступний ланцюг послідовностей головних ключів авторизації K_i, первинних ключів авторизації PAK_i, та ключів авторизації доступу AK_i (рис. 4).

У разі застосування EAP-авторизації кожен з ключів AK_i авторизації доступу визначається функцією:

$$AK_i = \text{Dot16KDF}\,(PMK_i, \text{SSID} \mid \text{BSID} \mid \text{“AK”}, 160), \quad (10)$$

де $PMK_i = \text{Truncate}\,(\text{Truncate}\,(K'_i, 320), 160)$

є і-м парний майстер-ключем, який сформовано відповідно до (3).

Відповідний ланцюг послідовностей майстер-ключів сеансу K'_i, парних майстер-ключів PMK_i, та ключів авторизації доступу AK_i зображено на рис. 5.

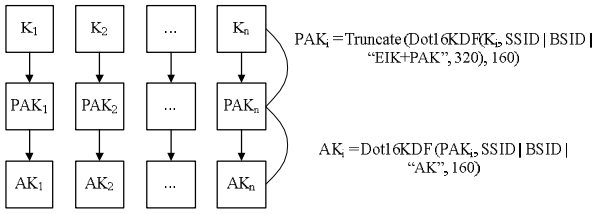

Рис. 4. Ланцюг послідовностей головних ключів авторизації K_i, первинних ключів авторизації PAK_i, та ключів авторизації доступу AK_i (при застосуванні RSA-авторизації)

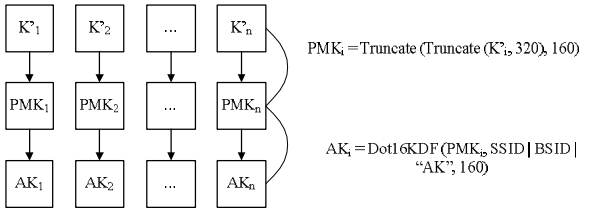

Рис. 5. Ланцюг послідовностей майстер-ключів сеансу K_i, парних майстер-ключів PMK_i, та ключів авторизації доступу AK_i (при застосуванні EAP-авторизації)

У разі сумісного застосування RSA-EAP-авторизації кожен з ключів AK_i визначається функцією:

$$AK_i = \text{Dot16KDF}\ (PAK_i \oplus PMK_i,\ \text{SSID} \mid \mid \text{BSID} \mid \text{“AK”},\ 160), \qquad (11)$$

де $PAK_i = \text{Truncate}\ (\text{Dot16KDF}(K_i,\ \text{SSID} \mid \mid \text{BSID} \mid \text{“EIK+PAK”},\ 320),\ 160)$

та $PMK_i = \text{Truncate}\ (\text{Truncate}\ (K'_i,\ 320),\ 160)$

є і-м первинним ключем авторизації та парним майстер-ключем, які сформовано відповідно до (1), (3).

Відповідний ланцюг послідовностей головних ключів авторизації K_i, первинних ключів авторизації PAK_i, майстер-ключів сеансу K'_i, парних майстер-ключів PMK_i, та ключів авторизації доступу AK_i зображено на рис. 6.

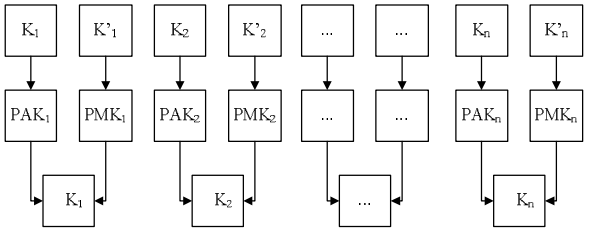

Рис. 6 Ланцюг послідовностей головних ключів авторизації K_i, первинних ключів авторизації PAK_i, майстер-ключів сеансу K'_i, парних майстер-ключів PMK_i, та ключів авторизації доступу AK_i (при застосуванні RSA-EAP-авторизації)

Колізійні властивості формованих ключів авторизації визначаються як за колізійними властивостями послідовностей головних ключів авторизації та/або майстер-ключів сеансу, так і періодичними властивостями вихідних послідовностей функції Dot16KDF. Ці залежності випливають з наступних тверджень.

Твердження 1. У разі виникнення колізії (збігу) головних ключів авторизації та/або майстер-ключів сеансу формовані ключі авторизації доступу будуть також повторюватися, тобто буде виникати їхня колізія (збіг).

Доказ. Припустимо, що деякі елементи з послідовності (6) та/або послідовності (7) повторюються, тобто для деяких і та j при $i \neq j$ виконується рівність:

$$K_i = K_j \quad \text{та/або} \quad K'_i = K'_j,$$

тобто відбувається колізія (збіг) окремих головних ключів авторизації та/або майстер-ключів сеансу.

Використовуючи формули (10) – (11) запишемо відповідні рівняння для різних випадків застосування схеми авторизації:

– у разі SA-авторизації

$AK_i = \text{Dot16KDF}\ (\text{Truncate}\ (\text{Dot16KDF}(K_i,\ \text{SSID} \mid \text{BSID} \mid \text{“EIK+PAK”},\ 320),\ 160),\ \text{SSID} \mid \text{BSID} \mid \text{“AK”},\ 160),$

$AK_j = \text{Dot16KDF}\ (\text{Truncate}\ (\text{Dot16KDF}(K_j,\ \text{SSID} \mid \text{BSID} \mid \text{“EIK+PAK”},\ 320),\ 160),\ \text{SSID} \mid \text{BSID} \mid \mid \text{“AK”},\ 160);$

– у разі EAP-авторизації

$AK_i = \text{Dot16KDF}\ (\text{Truncate}\ (\text{Truncate}\ (K'_i,\ 320),\ 160),\ \text{SSID} \mid \text{BSID} \mid \text{“AK”},\ 160),$

$AK_j = \text{Dot16KDF}\ (\text{Truncate}\ (\text{Truncate}\ (K'_j\ 320),\ 160),\ \text{SSID} \mid \text{BSID} \mid \text{“AK”},\ 160);$

– у разі RSA-EAP-авторизації

$AK_i = \text{Dot16KDF}\ (\text{Truncate}\ (\text{Dot16KDF}(K_i,\ \text{SSID} \mid \text{BSID} \mid \text{“EIK+PAK”},\ 320),\ 160) \oplus \text{Truncate}\ (\text{Truncate}\ (K'_i,\ 320),\ 160),\ \text{SSID} \mid \text{BSID} \mid \text{“AK”},\ 160),$

$AK_j = \text{Dot16KDF}\ (\text{Truncate}\ (\text{Dot16KDF}(K_j,\ \text{SSID} \mid \text{BSID} \mid \text{“EIK+PAK”},\ 320),\ 160) \oplus \text{Truncate}\ (\text{Truncate}\ (K'_j,\ 320),\ 160),\ \text{SSID} \mid \text{BSID} \mid \text{“AK”},\ 160).$

Аргументи функції Dot16KDF в правій частині кожного з математичних виразів при будь якій схемі авторизації є тотожними, тобто при $i \neq j$, якщо виконується рівність $K_i = K_j$ та/або $K'_i = K'_j$ завжди виконуються наступні рівності:

– у разі SA-авторизації

$AK_i = \text{Dot16KDF}\ (PAK_i,\ \text{SSID} \mid \text{BSID} \mid \text{“AK”},\ 160) = = \text{Dot16KDF}\ (PAK_j,\ \text{SSID} \mid \text{BSID} \mid \mid \text{“AK”},\ 160) = AK_j;$

– у разі EAP-авторизації

$AK_i = \text{Dot16KDF}\ (PMK_i,\ \text{SSID} \mid \text{BSID} \mid \text{“AK”},\ 160) = = \text{Dot16KDF}\ (PMK_j,\ \text{SSID} \mid \text{BSID} \mid \text{“AK”},\ 160) = AK_j;$

– у разі RSA-EAP-авторизації

$AK_i = \text{Dot16KDF}\ (PAK_i \oplus PMK_i,\ \text{SSID} \mid \text{BSID} \mid \text{“AK”},\ 160) = = \text{Dot16KDF}\ (PAK_j \oplus PMK_j,\ \text{SSID} \mid \text{BSID} \mid \text{“AK”},\ 160) = AK_j.$

Практично це означає, що у разі виникнення колізії (збігу) головних ключів авторизації та/або майстер-ключів сеансу формовані ключі авторизації доступу будуть також повторюватися, тобто буде виникати їх колізія (збіг).

Твердження доведено.

Таким чином, як випливає з сформульованого та доведеного твердження, послідовність ключів авторизації доступу, які формуються розглянутим вище способом, буде мати кількість колізій (збігів ключів) не менше ніж кількість збігів в послідовностях введе-

них головних ключів авторизації та/або майстер-ключів сеансу. З цього слідує наступний, важливий з погляду рівня забезпечуваної безпеки безпроводових телекомунікаційних систем і мереж висновок: процедура введення головних ключів авторизації та/або майстер-ключів сеансу в існуючій схемі формування ключів авторизації доступу повинна передбачати контроль їхньої неповторності, що забезпечить відсутність певних колізій (збігів), викликаних наявністю колізій послідовностей ключів (6) та/або (7).

Припустимо, що сформульована умова виконується, тобто введені головні ключі авторизації та/або майстер-ключі сеансу сформовано так, що вони не збігаються протягом визначеного терміну часу, тобто виконується вимога щодо відсутності колізій в послідовностях (6) та/або (7). Тоді колізійні властивості формованих ключів авторизації визначаються періодичними властивостями вихідних послідовностей функції Dot16KDF за наступним твердженням.

Твердження 2. При відсутності колізій (збігів) головних ключів авторизації та/або майстер-ключів сеансу формовані ключі авторизації доступу будуть збігатися не частіше, ніж довжина періоду вихідної послідовності застосовуваної функції Dot16KDF.

Доказ. Збіг формованих ключів авторизації доступу буде виникати тоді, коли вихідні значення функції Dot16KDF, яку ініційовано різними головними ключами авторизації та/або майстер-ключами сеансу, співпадуть, тобто, коли виникне така подія:

$$AK_i = AK_j,$$

де – у разі SA-авторизації $K_i \neq K_j$ і

AK_i = Dot16KDF (Truncate (Dot16KDF(K_i, SSID | BSID | “EIK+PAK”, 320), 160), SSID | BSID |“AK”, 160),

AK_j = Dot16KDF (Truncate (Dot16KDF(K_j, SSID | BSID | “EIK+PAK”, 320), 160), SSID | BSID | | “AK”, 160);

– у разі EAP-авторизації $K'_i \neq K'_j$ і

AK_i = Dot16KDF (Truncate (Truncate (K'_i, 320), 160), SSID | BSID | “AK”, 160),

AK_j = Dot16KDF (Truncate (Truncate (K'_j 320), 160), SSID | BSID | “AK”, 160);

– у разі RSA-EAP-авторизації $K \neq K_j$, $K'_i \neq K'_j$ і

AK_i = Dot16KDF (Truncate (Dot16KDF(K_i, SSID | BSID | “EIK+PAK”, 320), 160) ⊕ Truncate (Truncate (K'_i, 320), 160), SSID | BSID | “AK”, 160),

AK_j = Dot16KDF (Truncate (Dot16KDF(K_j, SSID | BSID | “EIK+PAK”, 320), 160) ⊕ Truncate (Truncate (K'_j, 320), 160), SSID | BSID | “AK”, 160).

Позначимо вихід функції Dot16KDF, яку ініційовано вектором x, символом y:

$$y = \text{Dot16KDF}(x, \text{astring}, \text{keylength}),$$

а довжину періоду вихідних послідовностей y_i функції Dot16KDF як L(x), де кожне значення y_i формується із застосуванням рекурентного співвідношення

$$y_i = \text{Dot16KDF}(y_{i-1}, \text{astring}, \text{keylength}),$$
$$y_0 = x,\ i = 1, \ldots, n. \qquad (12)$$

Схематично процес формування вихідних послідовностей y_i функції Dot16KDF наведено на рис. 7.

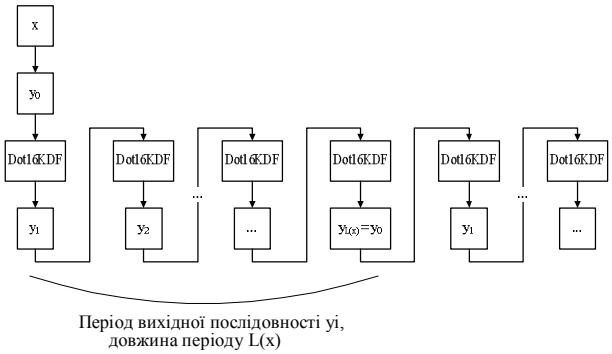

Рис. 7. Ланцюг вихідних послідовностей y_i функції Dot16KDF, який побудовано за рекурентним правилом (12)

З рис. 7 видно, що подія $y_i = y_j$ при $i \neq j$ буде виникати не частіше, ніж за довжину періоду вихідних послідовностей y_i функції Dot16KDF, тобто не менш ніж за L(x) рекурентних перетворень за виразом (12). Таким чином, при відсутності колізій (збігів) головних ключів авторизації та/або майстер-ключів сеансу формовані ключі авторизації доступу AK будуть збігатися не частіше, ніж довжина періоду L(x) вихідної послідовності y_i застосовуваної функції Dot16KDF.

Твердження доведено.

З сформульованого та доведеного ствердження випливають наступні, важливі в прикладному значенні, висновки:

– довжини періодів вихідних послідовностей застосовуваної функції Dot16KDF при кожному введеному головному ключі авторизації та/або майстер-ключі сеансу повинні бути максимізовані;

– ймовірність збігу ключів авторизації визначається через довжину періодів вихідних послідовностей застосовуваної функції Dot16KDF.

Найбільшу практичну цінність має другий висновок, бо він надає можливість для точного визначення основного показника безпеки телекомунікаційних систем та мереж пов’язаного із забезпеченням автентифікації та авторизації безпроводового доступу. Оцінки кількості збігів ключів авторизації доступу та відповідної ймовірності збігу дає наступне твердження.

Твердження 3. При відсутності колізій (збігів) головних ключів авторизації та/або майстер-ключів сеансу кількість збігів ключів авторизації доступу визначається через співвідношення максимального періоду при заданій довжині вектору ініціації та довжини періоду вихідної послідовності застосовуваної функції Dot16KDF. Ймовірність збігу визначається зворотною величиною до довжини періоду вихідної послідовності.

Доказ. Позначимо через $L_{max}(x)$ максимальний період послідовності значень y_i при заданій довжині вектору ініціації x.

Відповідно до твердження 2 формовані ключі авторизації доступу будуть збігатися не частіше, ніж дов-

жина періоду вихідної послідовності застосовуваної функції Dot16KDF, тобто подія $y_i = y_j$ при $i \neq j$ буде виникати не частіше, ніж через L(x) рекурентних перетворень за виразом (12), тобто колізія (збіг) ключів авторизації доступу буде виникати не більше $L_{max}(x)/L(x)$ разів. Якщо вектори ініціації обираються випадково, рівно ймовірно та незалежно один від одного, тоді ймовірність того, що виникне збіг ключів авторизації доступу буде визначатися через співвідношення кількості збігів до максимального періоду, тобто

$$P_З = \frac{L_{max}(x)}{L(x)} / L_{max}(x) = \frac{1}{L(x)}.$$

Твердження доведено.

Сформульоване та доведене твердження має важливий наслідок.

Наслідок твердження 3. Для виконання нижньої межі ймовірності збігу ключів авторизації необхідно забезпечити максимальний період вихідних послідовностей функції Dot16KDF.

Доказ. Використовуючи результат твердження 3, маємо

$$P_З = 1 / L(x).$$

Якщо забезпечується максимальний період формованих вихідних послідовностей маємо

$$P_З = 1 / L_{max}(x) = 2^{-len(x)}$$

де під len(x) розуміється бітова довжина вектору ініціації x.

Наслідок доведено.

Сформульовані та доведені твердження і їх наслідок разом із введеною формалізацією процесу формування ключів авторизації доступу у сукупності складають математичну модель авторизації та автентифікації безпроводового доступу, в якій враховуються колізійні властивості формованих ключів авторизації для оцінки безпеки безпроводових телекомунікаційних систем та мереж.

Висновки

Проведені дослідження із використанням запропонованої математичної моделі дозволяють обґрунтувати наступні вимоги до схеми формування ключів авторизації доступу:

– вхідні послідовності (наприклад, головні ключі авторизації та/або майстер-ключі сеансу), які використовуються у якості векторів ініціації функції генерації ключів авторизації доступу (наприклад, функції Dot16KDF) не повинні мати колізій (збігів), тобто схема їх вводу повинна передбачати певний контроль;

– реалізація функції генерації ключів авторизації доступу (наприклад, функції Dot16KDF) повинна забезпечувати максимальний період формованих послідовностей.

Виконання сформульованих вимог дозволить забезпечити потрібні ймовірнісно-часові показники формованих ключів авторизації доступу для підвищення безпеки безпроводових телекомунікаційних систем і технологій. Навпаки, невиконання сформульованих вимог гарантовано призведе до колізії (збігу) формованих ключів авторизації доступу із зниженням рівня забезпечуваної безпеки, так як це створює передумови для порушення авторизації безпроводового доступу.

Перспективним напрямком подальших досліджень є вдосконалення методу авторизації та автентифікації безпроводового доступу, який за рахунок забезпечення потрібних колізійних властивостей формованих ключів авторизації дозволить підвищити безпеку телекомунікаційних систем та мереж.

Список літератури

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

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

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

4. End-to-End (E2E) Security Approach / S. Adibi, G. B. Agnew,T. Tofigh, // WiMAX: Security Technical Overview for Corporate Multimedia Applications, 747-758, Handbook of Research on Wireless Security (2 Volumes) Edited By: Yan Zhang, Jun Zheng, Miao Ma, 2008.

5. Authentication Authorization and Accounting (AAA) Schemes / S. Adibi, B. Lin, P.-H. Ho, G.B. Agnew, S. Erfani // WiMAX, University of Waterloo, Broadband Communication Research Centre (BBCR) , appears in: Electro/information Technology, 2006 IEEE International Conference on 7-10 on pages: 210-215, May 2006.

6. Airspan, "Mobile WiMAX security", Airspan Networks Inc. 2007. [Online]. Available: http://www.airspan.com

7. Taeshik Shon and Wook Choi, "An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions", Lecture Notes in Computer Science, Aug. 2007 – Vol. 4658. – P. 88-97.

8. Прокопович-Ткаченко Д.І. Дослідження протоколів автентифікації та авторизації доступу в безпроводових телекомунікаційних системах та мережах / Д.І. Прокопович-Ткаченко // Системи озброєння і військова техніка, 2013, № 1(33). – С. 119-122.

Надійшла до редколегії 30.01.2013

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

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ АВТОРИЗАЦИИ И АВТЕНТИФИКАЦИИ БЕСПРОВОДНОГО ДОСТУПА В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ

Д.И. Прокопович-Ткаченко

Предлагается математическая модель авторизации и автентификации беспроводного доступа, которая позволяет учесть коллизионные свойства формуемых ключей авторизации для оценки безопасности телекоммуникационных систем и сетей. Обосновываются требования к схеме авторизации и автентификации, выполнение которых позволяет

обеспечить нужные вероятностно-часовые показатели формуемых ключей авторизации доступа для повышения безопасности беспроводных телекоммуникационных систем и технологий.

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

MATHEMATICAL MODEL OF OFF-WIRE ACCESS AUTHORIZING AND AVTENTIFIKATION IN TELECOMMUNICATION SYSTEMS AND NETWORKS

D.I. Prokopovich-Tkachenko

The mathematical model of authorizing and avtentifikation of off-wire access is offered, which allows to take into account collision properties of the mouldable keys of authorizing for the estimation of safety of the telecommunication systems and networks. Grounded requirement to the chart of authorizing and avtentifikation , implementation of which allows to provide the necessary probabilistic-sentinel indexes of the mouldable keys of authorizing of access for the increase of safety of the off-wire telecommunication systems and technologies.

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