УДК 546.261
Хабаров П.О., Семенюк В.Я.
Луцький національний технічний університет

Дослідження та аналіз методів захисту інформації в безпровідних мережах стандарту IEEE 802.16

В даній науковій роботі, мною досліджено новітній мережевий стандарт IEEE 802.16 та розроблено порівняльну характеристику між Wi-Fi і WiMAX.
Ключові слова: *Wi-Fi, WiMAX, SA, EAP, ECB.*

Постановка проблеми

На даний момент питання безпеки безпровідних мереж є досить актуальним. Тому розглянемо та проаналізуємо всі плюси та мінуси мереж стандарту IEEE 802.16.

Вступ

Технологія WiMAX (стандарт IEEE 802.16) являє собою стандарт безпровідового зв'язку, що забезпечує широкосмуговий доступ на великих відстанях. В порівнянні з кабельними лініями зв'язку та супутниковим доступом до мережі інтернет WiMAX є економічнішою та більш простою в експлуатації мережею.

Технологія WiMAX дозволяє вирішувати проблеми розповсюдження мережі інтернет в місця, позбавлені проводової інфраструктури. Використання WiMAX є вигідним як в умовах мегаполісу, так і в позаміських зонах, адже однієї базової станції вистачає для покриття великої території, причому стабільна робота забезпечується навіть за відсутності прямої видимості базової станції. Окрім цього, стандарт WiMAX має високий рівень безпеки передачі даних. Метою подальшої роботи є дослідження методів захисту інформаціїї стандарту IEEE 802.16.

Побоювання багатьох системних адміністраторів з приводу інформаційної безпеки WiMAX є одним з основних перешкод на шляху їх розповсюдження. У зв'язку з цим важливо відзначити, що в специфікації MAC-рівня стандарту 802.16 передбачені надійні захисні механізми. Багато виробників бездротового обладнання будуть випускати продукти стандарту 802.16 з підтримкою методів шифрування 3DES (128-бітовий ключ), RSA (1024-бітовий ключ) і AES. Для аутентифікації користувачів пристроїв при встановленні бездротового з'єднання в даному стандарті передбачено обмін сертифікатами, що завадить підключати до мережі "нелегальні" пристрої. Загалом мережа стандарту 802.16 значно безпечніша мережі стандарту 802.11.

Рішення питань

Консорціум WiMAX розраховує на те, що технологія WiMAX отримає широке розповсюдження на підприємствах. Підтримуваний ним стандарт 802.16 виключно важливий для того, щоб стандартизовані WiMAX стали реальністю.

Захищений зв'язок (Security Association, SA) - одностороннє підключення для забезпечення захищеної передачі даних між пристроями мережі. SA бувають двох типів:

- Data Security Association, захищений зв'язок для даних.
- Authorization Security Association, захищений зв'язок для авторизації.

Захищений зв'язок для даних буває трьох типів:

- Первиннй (основний) (Primary SA);
- Статичний (Static SA);
- Динамічний (Dynamic SA).

Первинний захищений зв'язок встановлюється абонентською станцією на час процесу ініціалізації. Базова станція потім надає статичний захищений зв'язок. Що стосується динамічних захищених зв'язків, то вони встановлюються та ліквідуються у міру необхідності для сервісних потоків. Як статичний, так і динамічний захищений зв'язок може бути одним для декількох абонентських станцій.

Захищений зв'язок для даних визначається:

- 16-бітним ідентифікатором зв'язку.
- Методом шифрування, що застосовується для захисту даних в з'єднанні.
- Двома Traffic Encryption Key (TEK, ключ шифрування трафіку), поточний і той, який буде використовуватися, коли у поточного TEK закінчиться термін життя.
- Двома двухбітними ідентифікаторами, по одному на кожен TEK.

- Часом життя TEK. Може мати значення від 30 хвилин до 7 днів. Значення за замовчуванням 12 годин.

- Двома 64-бітними векторами ініціалізації, по одному на TEK (потрібно для алгоритму шифрування DES).

- Індикатором типу зв'язку (первинний, статичний чи динамічний).

Абонентські станції зазвичай мають один захищений зв'язок для даних та вторинного частотного каналу керування (secondary management channel), або один захищений зв'язок для даних та з'єднання в обидві сторони (uplink і downlink), або один захищений зв'язок для даних та з'єднання від базової станції до абонентської і один - для зворотнього зв'язку.

Захищений зв'язок для авторизації

Абонентська станція і базова станція розділяють один захищений зв'язок для авторизації. Базова станція використовує захищений зв'язок для авторизації та конфігурування захищеного зв'язку для даних.

Захищений зв'язок для авторизації визначається:

- сертифікатом X.509, що ідентифікує абонентську станцію, а також сертифікатом X.509, що ідентифікує виробника абонентської станції.

- 160-бітовим ключем авторизації (authorization key, AK). Використовується для аутентифікації під час обміну ключами TEK.

- 4-бітовим ідентифікатором ключа авторизації.

- Часом життя ключа авторизації. Може приймати значення від 1 дня до 70 днів. Значення за замовчуванням 7 днів.

- 128-бітовим ключем шифрування ключа (Key encryption key, KEK). Використовується для шифрування й розподілу ключів TEK.

- Ключем HMAC для вхідних повідомлень (downlink) при обміні ключами TEK.

- Ключем HMAC для вихідних повідомлень (uplink) при обміні ключами TEK.

- Списком data SA, до якого ця абонентська станція авторизована.

KEK обчислюється наступним чином:

1. Проводиться конкатенація шістнадцятирічного числа 0x53 із самим собою 64 рази. Виходять 512 біт.
2. Справа приписується ключ авторизації.
3. Обчислюється хеш-функція SHA-1 від цього числа. Виходять 160 біт на виході.
4. Перші 128 біт беруться як KEK, решта відкидається.

Ключі HMAC обчислюються наступним чином:

1. Проводиться конкатенація шістнадцятирічного числа 0x3A (uplink) або 0x5C (downlink) із самим собою 64 рази.
2. Справа приписується ключ авторизації.
3. Обчислюється хеш-функція SHA-1 від цього числа. Виходять 160 біт на виході. Це і є ключ HMAC.

Розширюваний протокол аутентифікації .

Extensible Authentication Protocol (EAP, розширюваний протокол аутентифікації) - це протокол, що описує більш гнучку схему аутентифікації в порівнянні з сертифікатами X.509. Вона була введена в додаток до стандарту IEEE 802.16e. EAP-повідомлення кодуються прямо в кадри управління. У зв'язку з цим до протоколу PKM (Privacy and Key Management Protocol - це протокол для отримання авторизації і ключів шифрування трафіку TEK) були додані два нових повідомлення PKM EAP request (EAP-запит) і PKM EAP response (EAP-відповідь). Стандарт IEEE 802.16e не встановлює який-небудь певний метод аутентифікації EAP, ця галузь зараз активно досліджується.

Авторизація

Абонентська станція починає обмін, посилаючи повідомлення, що містить X.509 сертифікат виробника абонентської станції. Зазвичай цей сертифікат ніяк не використовується базовою станцією, хоча можливо налаштувати базову станцію так, що авторизуовуватися будуть тільки абонентські станції від довірних виробників.

Відразу після першого повідомлення, абонентська станція відправляє повідомлення, що містить X.509 сертифікат самої абонентської станції, її криптографічні можливості та ідентифікатор первинної SA (Primary SA).

Базова станція за сертифікатом абонента визначає чи він авторизований. Якщо він авторизований, вона посилає повідомлення, що містить зашифрований ключ авторизації,

послідовний номер цього ключа авторизації, його час життя, а також список ідентифікаторів статичних SA, в яких абонент авторизований. Ключ авторизації шифрується алгоритмом RSA з публічним ключем, що одержуються з сертифіката абонентської станції.

Одного разу авторизувавшись, абонентська станція буде періодично переавторизовуватися.

Шифрування даних

Стандарт IEEE 802.16 використовує алгоритм DES у режимі зчеплення блоку шифрів для шифрування даних. В даний час DES вважається небезпечним, тому в додаток до стандарту IEEE 802.16e для шифрування даних був доданий алгоритм AES.

DES (Data Encryption Standard) - симетричний алгоритм шифрування, в якому один ключ використовується як для шифрування, так і для розшифрування даних. DES має блоки по 64 біт і 16 циклову структуру мережі Фейстеля, для шифрування використовує ключ довжиною 56 біт. Алгоритм використовує комбінацію нелінійних (S-блоки) та лінійних (перестановки E, IP, IP-1) перетворень. Для DES рекомендовано кілька режимів:

- режим електронної кодової книги (ECB - Electronic Code Book),
- режим зчеплення блоків (CBC - Cipher Block Chaining),
- режим зворотнього зв'язку по шифротексту (CFB - Cipher Feed Back),
- режим зворотнього зв'язку по виході (OFB - Output Feed Back).

Шифрування даних проходить наступним чином. Вектор ініціалізації з даного data SA і поле синхронізації проходять побітову операцію АБО і подаються як ініціалізуючий вектор алгоритму DES в режимі зчеплення блоку шифрів (CBC, cipher block chaining). Також на вхід схеми подається TEK ключ для шифрування і відкритий текст повідомлення. Алгоритм видає зашифрований текст. Заголовок Generic MAC header (GMH) не змінюється за винятком бітового поля EC, а кінцевик CRC, якщо він є, змінюється під зашифрований текст.

Цей алгоритм шифрування раніше використовувавсь в США як національний стандарт. Зараз його використовують тільни на застарілих системах, а на нових використовують Triple DES (3DES), котрий є більш стійким.

Advanced Encryption Standard (AES) - симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт). Має чотири режими:

- Cipher Block Chaining (CBC, режим зчеплення блоку шифрів)
- Counter Encryption (CTR, шифрування лічильника)
- Counter Encryption with Cipher Block Chaining message authentication code (CCM, лічильникове шифрування з message authentication code, отриманим зчепленням блоку шифрів). Додає можливість перевірки аутентичності зашифрованого повідомлення до режиму CTR.

- Electronic Code Book (ECB, режим електронної кодової книги). Використовується для шифрування ключів TEK.

У режимі CCM, для шифрування корисної інформації передавальна станція генерує на кожен пакет nonce - байтову послідовність, перші 5 байт якої являють собою початок Generic MAC Header. Далі йдуть 4 зарезервованих байти, що мають нульові значення. Потім слідує 4-байтовий номер пакету Packet Number (PN) в даному data SA. Значення Packet Number ставиться в 1 при встановленні нового data SA чи нового TEK.

Блок CBC складається з однобайтового флагу, що має значення 00011001, послідовності nonce і поля, яке містить довжину інформаційної частини повідомлення.

Блок Counter складається з однобайтового флагу, що має значення 00000001, послідовності nonce і поля, яке містить номер і Counter-блоку. Число і може змінюватися від нуля до n, де n - кількість Counter-блоків, необхідних для покриття всього повідомлення та коду message authentication code.

При створенні message authentication code використовується модифікований режим CBC, у якому замість ініціалізуючого вектору IV, до початку інформаційної частини повідомлення приєднується початковий (нульовий) блок CBC. Далі ця пара зашифровується алгоритмом AES в режимі CBC з ключем TEK. Останні 128 біт зашифрованого тексту беруться як message authentication code (коди аутентичності). Далі message authentication code шифрується побітовим складанням за модулем два вихідного message authentication code і зашифрованого за допомогою алгоритму AES в режимі CTR початкового (нульового) Counter-блоку.

Кожен з n залишившихся Counter-блоків (нульовий вже був задіяний в шифруванні message authentication code) зашифровують методом AES в режимі CTR з ключем TEK. Потім результат складають побітовим складанням за модулем два з інформаційною частиною повідомлення.

Отриманий зашифрований текст разом з зашифрованих message authentication code, номером пакету даних, заголовком Generic MAC Header і CRC-кінцевиків відправляється на фізичний рівень. При цьому в заголовку GMH поле EC (Encryption Control) встановлюють у одиницю, оскільки дані були зашифровані, а в двохбітовому полі EKS (Encryption Key Sequence) стоїть індекс використаного при цьому ключа TEK (traffic encryption key).

На даний момент цей алгоритм являється національним стандартом в США. Він має багато рівнів захисту і дуже високу криптостійкість.

RSA - криптографічний алгоритм з відкритим ключем. RSA став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису. Алгоритм використовується у великій кількості криптографічних додатків.

Через низьку швидкість шифрування (близько 30 кбіт/с при 512 бітному ключі на процесорі 2 ГГц), повідомлення звичайно шифрують за допомогою більш продуктивних симетричних алгоритмів з випадковим ключем (сеансовий ключ), а за допомогою RSA шифрують лише цей ключ. Такий механізм має потенційні вразливі місця зважаючи на необхідність використовувати криптостійкий генератор випадкових чисел для формування випадкового сеансового ключа симетричного шифрування і ефективно стійкий проти атак симетричний криптоалгоритм.

Який алгоритм шифрування буде вибраний залежить, насамперед, від виробника обладнання.

Якщо говорити про ці алгоритми більш детальніше, то можна побачити також їх негативні риси та не завжди стійку криптосхему.

Криптостійкість алгоритму DES.

Через невелике число можливих ключів (всього 256), з'являється можливість їх повного перебору на швидкодіючій обчислювальній техніці за реальний час. У 1998 році The Electronic Foundation використовуючи спеціальний комп'ютер DES-Cracker, вдалося зламати DES за 3 дні.

В алгоритмі DES існують слабкі і частково-слабкі ключі. Слабкими ключами називається ключі k такі що DESk(DESk (x)) = x, x - блок 64 біт. Частково-слабкі ключі - пари ключів (k1, k2) такі що DESk1 (DESk2(x)) = x

Відомі 4 слабких ключа. Для кожного слабкого ключа існує 232 «постійні точки», тобто таких 64-бітових блоки x, в яких DESk (x) = x.

0101-0101-0101-0101;

FEFE-FEFE-FEFE-FEFE;

1F1F-1F1F-0E0E-0E0E;

E0E0-E0E0-F1F1-F1F1.

Для того, щоб збільшити криптостійкість цього алгоритму був розроблений 3DES (TripleDES).

3DES з різними ключами має довжину ключа рівну 168 біт, але через атаки «зустріч посередині» ефективна крипостійкість становить лише 112 біт. У варіанті DES-EDE, в якому k1 = k3, ефективний ключ має довжину 80 біт. Для успішної атаки на 3DES потрібно близько 232 біт відомого відкритого тексту, 2113 кроків, 290 циклів DES-шифрування і 288 біт пам'яті.

Криптостійкість можливо підвищи за рахунок:

- Метод DESX - посилений варіант DES, підтримуваний інструментарієм RSA Security. DESX відрізняється від DES тим, що кожен біт вхідного відкритого тексту DESX логічно підсумовується за модулем 2 з 64 бітами додаткового ключа, а потім шифрується за алгоритмом DES. Кожен біт результату також логічно підсумовується за модулем 2 з іншими 64 бітами ключа. Головною причиною використання DESX є спосіб значного підвищити стійкість DES до атак повного перебору ключа.

- Ще інший варіант DES використовує незалежні суб-ключі. По-різному від алгоритму DES, в якому на основі 56-бітного секретного ключа користувача алгоритм DES отримує шістнадцять 48-бітових суб-ключів для використання в кожному з 16 раундів, в цьому варіанті використовує 768-бітного ключа (розділеного на 16 48-бітових підключів) замість 16 залежних 48-бітових ключів, що створюються по ключовому алгоритму DES. Хоча очевидно, що використання незалежних суб-ключів значно ускладнить повний пошук ключа, але стійкість до атаки диференціальний або лінійним криптоаналіз не набагато перевищить стійкість звичайного DES.

На основі вище описаного можна зробити висновки, що стандарт IEEE 802.16 є досить захищеним, але з іншого боку він також має ряд вразливих місць.

- Атаки фізичного рівня, такі як глушіння передачі сигналу, що веде до відмови доступу або лавинний наплив кадрів (flooding), який має на меті виснажити батарею станції. Ефективних способів протистояти таким загрозам на сьогодні немає.

- Самозвані базові станції, що пов'язані з відсутністю сертифіката базової станції. У стандарті проявляється явна несиметричність в питаннях аутентифікації. Запропоноване рішення цієї проблеми - інфраструктура управління ключем в безпровідному середовищі (WKMI, wireless key management infrastructure), заснована на стандарті IEEE 802.11i. У цій інфраструктурі є взаємна аутентифікація за допомогою сертифікатів X.509.

- Уразливість, пов'язана з невипадковою генерацією базовою станцією ключів авторизації. Взаємна участь базової і абонентської станції, можливо, вирішило б цю проблему.

- Можливість повторно використовувати ключі TEK, чий термін життя вже закінчився. Це пов'язано з дуже малим розміром поля EKS індексу ключа TEK. Так як найбільший час життя ключа авторизації 70 діб, тобто 100800 хвилин, а найменший час життя ключа TEK 30 хвилин, то необхідне число можливих ідентифікаторів ключа TEK - 3360. А це означає, що кількість необхідних біт для поля EKS - 12.

- Ще одна проблема пов'язана, як уже згадувалося, з небезпечністю використання шифрування DES. При достатньо великому часу життя ключа TEK і інтенсивному обміні повідомленнями можливість злому шифру представляє реальну загрозу безпеці. Ця проблема була усунена з введенням шифрування AES в поправці до стандарту IEEE 802.16e. Однак, велике число користувачів до цих пір має обладнання, що підтримує лише старий стандарт IEEE 802.16.

Ринок широкосмугового доступу однозначно перспективний і буде розвиватися високими темпами, оскільки люди прагнуть обмінюватися інформацією швидше і в більших обсягах. WiMAX всього лише одне з можливих рішень, і у нього є серйозні конкуренти. Є провайдери, що розвивають цей сервіс на мережах з кабельних технологій, і їх чимало. Є мобільні оператори, які, маючи мережі GSM або CDMA з сильними брендами, вже існуючої клієнтської і потужною фінансовою базою, роблять ставку на 3G.

Єдиною поки що перевагою WiMAX - висока швидкість. На ринку практично немає пристроїв, які піідтримують цю технологію. До цих пір не вирішені питання їх сумісності між собою, а також фіксованого (802.16d) та мобільного (802.16e) WiMAX. Я вважаю, що навіть при вдалому збігу обставин WiMAX отримає розвиток не раніше 2010 р.

Багатьом людям, як правило, потрібні висока швидкість передачі даних і мобільність - тут переваги мобільного WiMAX очевидні.

Літератра

1. Панасенко С. Алгоритм шифрования DES и его варианты. // Connect! Мир связи. — 2006 — №№ 3-6
2. В. Вишневский, С. Портной, И. Шахнович. Энциклопедия WiMAX. Путь к 4G. /Техносфера. Москва – 2009, 479 ст..
3. WiMAX Forum. "http://www.wimaxforum.ru/"
4. Advanced Encryption Standard. "http://en.wikipedia.org/wiki/Advanced_Encryption_Standard"
5. Ю. Петлёваная, Сравнение основных характеристик систем Wi-Fi и WiMAX
6. О.А. Мукомелов, Технологія WiMAX та її інтеграція в системи 4G