УДК 003.26.004.056

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В СЕНСОРНИХ МЕРЕЖАХ

Гетьман М.В., Тимошенко Л.М.
Тернопільський національний економічний університет

Основу забезпечення безпеки в сенсорних мережах складають криптографічні методи та засоби захисту інформації. Слід врахувати, що найбільш надійний захист можна забезпечити тільки за допомогою комплексного підходу, тобто рішення задачі має представляти собою сукупність організаційно-технічних та криптографічних заходів.

Рішення проблеми безпеки для бездротових сенсорних мереж. Сенсорні мережі часто розгортаються в агресивних середовищах, уразливих для атак і збоїв. Заходи безпеки повинні бути здійснені з метою запобігання несанкціонованого доступу до мережі і шкідливих атак. Аутентифікація і Anti-Повтор - протокол безпеки являють собою поєднання двох легких механізмів, які забезпечують аутентифікацію, анти-повтор і виявлення вторгнень.

Бездротові сенсорні мережі (WSN) складаються з великої кількості сенсорних пристроїв і характеризуються скороченням розмірності, низькою вартістю і низьким енергоспоживанням, які в змозі організувати себе в мережі, спілкуючись через бездротове середовище і співпрацюючи під час збору даних із зовнішнього середовища з метою виконання спільного завдання.

Датчики вузлів володіють унікальними характеристиками і обмеженнями, які відрізняють їх від стільникових систем, а саме: важка енергія, розрахунок і зберігання обмежень, ненадійність, надмірність даних, самоконфігурація, нестабільна топологія і схема руху багато-до-одного. Ці характеристики і стримують приведення до серйозних проблем в Дизайн WSNs. Тому WSNs мають ту перевагу, що їх розгортають в негостинних областях, таких як битви, космічному просторі, атмосфері і глибинах океанів, вони настійно рекомендується в військовому застосуванні, екологічному моніторингу, безпеки та нагляду, виробничому процесі, для контролю та охорони здоров'я.

Забезпечення WSNs виправдане, коли вони використовуються в критично важливих додатках, таких як спостереження поля бою і національна безпека. Це складне завдання із-за кількох обмежень, таких як бездротові канали і частоти, громадські протоколи, що стримує наявність ресурсів в агресивних середовищах. Оскільки бездротове середовище відкрите, будь-хто може перехоплювати трафік і ввести підробку.

Введемо TinySec. Це механізм рівня шифрування посилання, який призначений для першої частини в набір рішень для забезпечення безпеки крихітних пристроїв. Ядро TinySec є ефективний блоковий шифр і маніпуляційний механізм, який тісно пов'язаний з TinyOS радіо Берклі стека. TinySec в даний час використовує один симетричний ключ, який є спільним для колекції вузлів мережі датчиків. Перед передачею пакетів кожен вузол перший шифрує дані і застосовує Message Authentication Code (MAC), криптостійкі непідробні хеш-функції для захисту цілісності даних. Приймач перевіряє, що пакет не був змінений в дорозі використанням MAC, а потім розшифровує повідомлення.

Існують чотири основні мети TinySec:

• Контроль доступу. Тільки уповноважені вузли повинні мати змогу брати участь в мережі. Уповноваженими вважаються ті вузли, які мають загальний груповий ключ.

• Чесність. Повідомлення приймається тільки в тому випадку, якщо воно не було змінене при транспортуванні. Це запобігає підслуховуванню та зміні ретрансльованого повідомлення.

• Конфіденційність. Несанкціоновані сторони не можуть мати доступу до змісту повідомлення.

• Простота у використанні. Нарешті TinySec повинні бути зручними в експлуатації, беручи до уваги різноманітність користувачів сенсорних мереж.

TinySec працює як в симуляторі TOSSIM, а також і Mica2 порошинки.

Встановлення TinySec

TinySec тепер включений у стандартну поставку TinyOS. (TinyOS - компонентна операційна система з відкритим вихідним кодом і призначена для бездротових сенсорних мереж.) Будівництво TinySec додатків використовує сучок ключ сценарій. Переконайтеся, що цей скрипт на вашому шляху.

Тестування установки. Застосування TestTinySec може бути використана для перевірки вашої TinySec установки. Він періодично посилає пакетну передачу даних при використанні TinySec.

SecureTOSBase є TinySec-Aware аналог TOSBase і буде перемикати червоним, коли він отримує дійсний пакет. Ми повинні використати в програмі дві порошинки, одну з TestTinySec і одну SecureTOSBase:

1 Сторінка 2

$ CD nest/tinyos-1.x/apps/TestTinySec

$ Зробити mica2 установки

$ # Тепер встановіть другий сучок

$ CD nest/tinyos-1.x/apps/SecureTOSBase

$ Зробити mica2 установки

TinySec правильно працює, якщо на сучок SecureTOSBase перемикає його червоний світлодіод періодично. Це вказує, що пакет був переданий з включеною аутентифікацією. Якщо будь-яку програму не побудувати, а потім перевірити, то "сучок ключ" сценарій буде на вашому шляху.

Написання додатків. Включення TinySec до ваших додатків повинно бути простим процесом. Загалом код додатку не потрібно міняти, якщо Ваш Makefile включає Makerules з каталогу tinyos-1.x/apps, нам потрібно тільки додати TINYSEC = вірним програми Makefile нашої, з тим щоб TinySec. Це можна також зробити з командного рядка при виклику: наприклад, зробити mica2 TINYSEC = True.

За замовчуванням, TinySec буде достовірністю всіх повідомлень, а шифрування вимкнено. TinySec дозволяє динамічно змінювати поєднання механізмів безпеки для нашого застосування з TinySecMode інтерфейс. Компонент TinySecC експорт цього інтерфейсу. Є дві команди в TinySecMode - інтерфейс для налаштування прийому і передачі режимів:

Команда result_t setTransmitMode (uint8_t режимі);

Команда result_t setReceiveMode (uint8_t режимі);

setTransmitMode приймає одне з трьох значень як аргумент:

TINYSEC_AUTH_ONLY

TINYSEC_ENCRYPT_AND_AUTH

TINYSEC_DISABLED

Аналогічним чином, setReceiveMode приймає одне з трьох значень як аргумент:

TINYSEC_RECEIVE_AUTHENTICATED

TINYSEC_RECEIVE_CRC

TINYSEC_RECEIVE_ANY

За замовчуванням TINYSEC AUTH тільки для відправлення й TINYSEC ОТРИМАТИ перевірку автентичності для прийому.

TINYSEC шифрування і AUTH посилає шифрування і аутентифікацію повідомлень, і відправляє TINYSEC ІНВАЛІДІВ повідомлення зі стандартним радіо TinyOS стека (КПР тільки, без шифрування або перевірки автентичності).

Коли приймач знаходиться в режимі TINYSEC і проводить перевірку автентичності RECEIVE, то він буде тільки приймати повідомлення від відправника в TINYSEC AUTH ТІЛЬКИ режимі або TINYSEC шифрування і AUTH режимі. Приймач у TINYSEC ОТРИМАТИ КПР.

Режим буде тільки приймати повідомлення від відправника в режимі відключення TINYSEC, і приймач в TINYSEC ОТРИМАННЯ режимі буде приймати повідомлення від відправників, в будь-якому режимі.

Використання програми SecureTOSBase. Інтерфейс комп'ютера з мережею порошинки включений з TinySec. SecureTOSBase буде приймати тільки повідомлення, які були відправлені з MAC, тому він не буде отримувати повідомлення, відправлені з старе радіо стека або з TinySec. Нам потрібно буде змінити застосування SecureTOSBase, якщо ми хотіли б отримати як перевірку справжності і дійсності повідомлень.

Керування ключами. При використанні TinySec ми повинні знати ключі і ключ-файл. Кожен сучок Міка може взаємодіяти тільки з іншими порошинки, які були запрограмовані з тим же ключем. Ключ в даний час встановлений у даній програмі під час складання. Без будь-яких додаткових аргументів для нормального процесу складання, за замовчуванням ключ-файл і ключ за замовчуванням буде використовуватися. За замовчуванням ключ-файл буде створений для нас перший раз TinySec та використовуватися і зберігатися у файлі. Ключовий файл tinyos виглядає таким чином:

TinySec Keyfile. За замовчуванням, перший ключ буде використовуватися.

Ми можемо імпортувати інші ключі шляхом додавання їх у файл.

замовчуванням 6D524D67F24F178B0A69933FDD6C6F7B.

Звернемо увагу, що наше ключове значення не буде таким же, як зазначено вище. Кожен рядок списку включає ім'я та ключове значення. Коли ми викликаємо зробити mica2, перший ключ в ключ за замовчуванням файл буде встановлений. Це означає, що за замовчуванням, якщо ми встановимо програму на один сучок з нашого ноутбука, і встановимо програми на інший сучок на робочому столі, вони не зможуть взаємодіяти. Це відбувається тому, що вони будуть використовувати різні ключі. Таким чином, нам необхідно виконати одну з таких дій:

• використовувати той же ключ-файл на обох комп'ютерах

• скопіюйте ключовий файл з вашого ноутбука на робочому столі, перейменування файлів на "ноутбук-файл ключа". Тоді, при створенні на робочому столі, використання нових ключовий файл, якщо ви хочете створити порошинки, що "Інтер- працювати з порошинки запрограмований з ноутбуком:

зробити mica2 KEYFILE = ноутбук-Keyfile

• копія лінії від ключового файлу в якому йдеться "за замовчуванням 6D524 ..." з ноутбука на робочому столі ключового файлу (. ключовий файл). Крім того, перейменувати ярлик ключ від "за умовчанням" на "ноутбук". Потім, коли Будівля на робочому столі, використовуйте новий ключовий файл, якщо ви хочете створити порошинки, які взаємодіють з порошинками запрограмованими з ноутбуком:

зробити mica2 KeyName = ноутбук

Оновлення ключів. Інтерфейс TinySecControl експортує компоненти TinySecC, що дозволяє оновлювати ключі TinySec і запити і скидання вектором ініціалізації (IV). Інтерфейс TinySecControl має шість команд:

Команда result_t updateMACKey (uint8_t * Маккі);

Команда result_t getMACKey (uint8_t результат *);

Команда result_t updateEncryptionKey (uint8_t encryptionKey *);

Команда result_t getEncryptionKey (uint8_t результат *);

Команда result_t resetIV ();

Команда result_t getIV (uint8_t результат *)

Ці команди повернення будуть успішними, якщо ключ оновлено успішно.

Список використаних джерел

1. Романюк В.А. Мобильные радиосети-перспективы беспроводных технологий //Сети и телекоммуникации. –2003. – № 12. – С. 53 – 58.

2. J. Campbell, P.B. Gibbons, S. Nath, P. Pillai, S. Seshan,R. Sukthankar, IrisNet: an Internet-scale architecture for multimedia sensors, in: Proc. of the ACM Multimedia Conference, 2005.

3. P. Kulkarni, D. Ganesan, P. Shenoy, Q. Lu, Sens Eye: a multi-tier camera sensor network, in: Proc. of ACM Multimedia, Singapore, November 2005.

УДК 681.3.06

ПРОГРАМНЕ СЕРЕДОВИЩЕ ТА АПАРАТНІ ЗАСОБИ ОРГАНІЗАЦІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ СТІЙКОЇ ДО АТАК ТИПУ DOS/DDOS

Гончар Л.І., Сикотинська І.В.
Тернопільський національний економічний університет

Атаки відмови послуг становлять одну з найбільших загроз в мережі Інтернет. На сьогодні відсутній результативний та універсальний метод цілковитого запобігання цього типу атакам. Додатково, для здійснення атаки DoS/DdoS не треба володіти ґрунтовними знаннями в цій галузі. Це зумовлює виробників до створення щораз сучасніших технологій та засобів захисту комп'ютерних мереж (КМ) [3].

Найчастіше використовуються такі засоби захисту КМ:

- списки контролю доступу ACL (Access Control List);
- firewall;
- системи викриття зловмисників IDS (Intrusion Detection Systems) – NIDS, HIDS, NNIDS;
- система запобігання взломам IPS (Intrusion Prevention Systems) – In-Line IDS, інтегрований IDS із firewall).