УДК 681.3

В.М. Сокіл
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

СИСТЕМА АУТЕНТИФІКАЦІЇ ВУЗЛІВ МОБІЛЬНИХ МЕРЕЖ ДОВІЛЬНОЇ СТРУКТУРИ

Розглянуто децентралізовану систему аутентифікації вузлів мобільних мереж довільної структури, побудована на базі концепції довіри Джерка. Показано основні результати досліджень запропонованої системи.

The decentralized authentication system for mobile ad-hoc networks, based on trust conception of Gerck, is considered. Main results of proposed system investigations are shown.

Вступ

Поява малогабаритних і достатньо продуктивних обчислювальних та вимірювальних засобів з низьким рівнем енергоспоживання спричинила початок активних досліджень можливості застосування мобільних мереж для вирішення різного типу завдань [1]. Стрімкий розвиток бездротових технологій передавання даних за останній час, своєю чергою, дає можливість реального розгортання та використання мобільних мереж довільної структури (ММДС). Основними галузями застосування ММДС, окрім традиційно військової, є рятувальні роботи у зонах стихійних та техногенних лих, екологічний моніторинг за допомогою мереж сенсорів, забезпечення зв'язку між транспортними засобами або людьми у випадку відсутності інших засобів комунікації.

Специфіка вищеперерахованих галузей робить вимогу безпеки інформаційного обміну однією з основних під час проектування та розгортання ММДС. Враховуючи те, що доведена автентичність є обов'язковою умовою початку передавання інформації у захищеній мережі, проблема аутентифікації вузлів ММДС є достатньо актуальною.

Аналіз останніх публікацій

Ідеологічним центром функціонування системи аутентифікації є модель довіри, побудована за тією чи іншою концепцією довіри. У 1998 році професором Едом Джерком було запропоновано нову, найближчу до інформаційних технологій, концепцію довіри [2, 3].

У роботі [4] автор навів модель довіри у мобільних мережах довільної структури, розроблену за цією концепцією. Ця стаття присвячена дослідженню реалізації системи аутентифікації вузлів ММДС, побудованої на основі децентралізованої моделі аутентифікації, запропонованої автором у роботі [5].

Постановка завдання

Метою досліджень є отримання характеристик запропонованої системи аутентифікації. На основі цих характеристик можна буде робити висновки щодо можливостей практичного використання системи аутентифікації вузлів мобільних мереж довільної структури за концепцією довіри Джерка.

Для виконання поставленого завдання необхідно:

- розробити апаратну платформу вузла тестової мережі довільної структури;
- розробити та реалізувати систему аутентифікації на базі запропонованої моделі;
- отримати характеристики взаємодії двох вузлів ММДС у межах процесу аутентифікації.

Перелік основних позначень

M – множина мереж, що функціонують в межах одної території. $m \in M$ – ММДС з множини M.

N^m – множина вузлів мережі m. $n \in N^m$ – вузол мережі m.

P_n^m – множина вузлів мережі m, з якими може взаємодіяти вузол n, $P_n^m \subset N^m$.

P_n – загальна множина вузлів всіх мереж множини M, з якими може взаємодіяти вузол n,

$$P_n = P_n^{m_0} \cup P_n^{m_1} \cup \cdots \cup P_n^{m_k},\ m_0, m_1, \cdots m_k \in M;$$

p_n – вузол, з яким взаємодіє вузол n, $p_n \in P_n$;

$S\{A\} : selection\_rule$ – операція відбору елемента з множини A за правилом $selection\_rule$;

$VT(n, p_n, tc, t)$ – рівень довіри вузла n до вузла p_n в категорії tc на момент часу t;

АДЕ – автономне джерело електроенергії;
АКС – асиметрична криптосистема;
ГВЧ – генератор випадкових чисел;
МБПД – модуль бездротової передачі даних;
МКД – модуль керування довірою;
МКК – мікроконтролер керування;
СКС – симетрична криптосистема;
ХФ – хеш функція.

Загальний опис системи аутентифікації вузлів ММДС

Структура запропонованої системи аутентифікації показана на рис. 1.

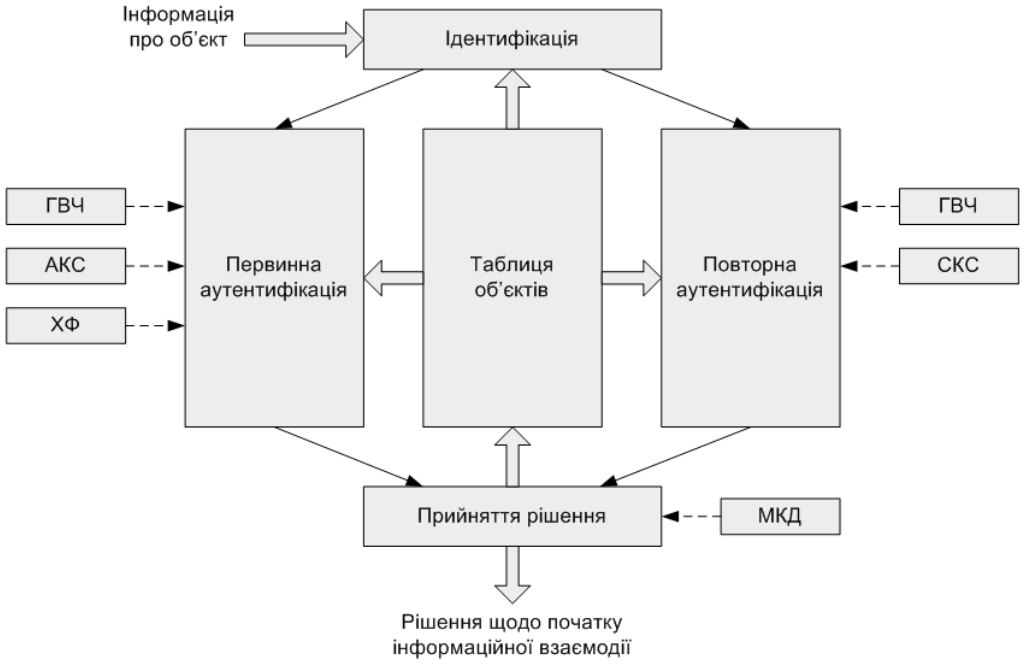

Рис. 1. Структура системи аутентифікації

Запропонована система складається з п'яти основних частин:

- таблиці об'єктів,
- підсистеми ідентифікації,
- підсистеми первинної аутентифікації,
- підсистеми повторної аутентифікації,
- підсистеми прийняття рішень.

Таблиця об'єктів – це "пам'ять" вузла. В ній міститься інформація про об'єкти, з якими в минулому взаємодіяв вузол: ідентифікатор об'єкта, час останньої взаємодії, рівень довіри до цього об'єкта на той час та цифровий сертифікат цього об'єкта. Як ідентифікатор об'єкта використовують ідентифікатор відкритого ключа, що міститься у сертифікаті.

Підсистема ідентифікації визначає з множини P_n, вузол p_n для подальшої взаємодії. Відбір здійснюється за такою схемою:

$$p_n = S\{P_n\} : \max\left(VT(n, p_n, tc, t_{lio})\right) \wedge \min\left(t_{lio}\right).$$

Тобто, з множини P_n спочатку вибирають вузли з найвищими рівнями довіри. А вже з них як p_n вибирають вузол з мінімальним часом останньої взаємодії (вузол, з яким "давно не бачились").

Залежно від того, чи в таблиці об'єктів є інформація про p_n (об'єкт „знайомий" чи ні) проводять первинну або повторну аутентифікацію. Підсистема первинної аутентифікації використовує три криптографічні модулі: ГВЧ, АКС та ХФ; підсистема повторної аутентифікації – два: ГВЧ та СКС.

У разі успішного проходження аутентифікації приймають рішення щодо початку інформаційної взаємодії. Використовуючи інформацію, що міститься у таблиці об'єктів, та, за необхідності, рекомендації від інших вузлів, визначають поточний рівень довіри до потрібного вузла p_n. Якщо значення довіри, отримане від МКД, більше за мінімально необхідне, то дають дозвіл на початок взаємодії. Після проведення взаємодії та аналізу отриманої інформації відбувається модифікація запису про p_n у таблиці об'єктів.

Апаратна платформа вузла тестової ММДС

Основними вимогами під час розроблення апаратної платформи вузла було отримання максимальних обчислювальних та комунікаційних ресурсів за мінімального споживання електроенергії. Апаратна платформа вузла складається з чотирьох основних частин: мікроконтролера керування (МКК), модуля бездротової передачі даних (МБПД), радіоінтерфейсної частини та джерела електроенергії. На рис. 2 показано загальну структуру апаратної платформи вузла.

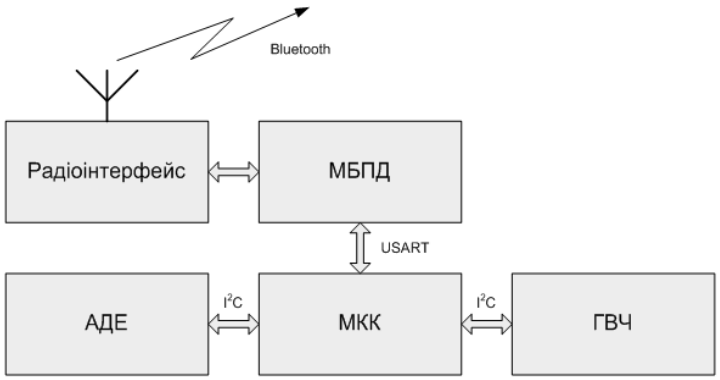

Рис. 2. Структура апаратної платформи вузла

Як МКК використовують 32-бітний RISC мікроконтролер фірми Atmel AT91SAM7S64 з ядром ARM7TDMI [6]. Це є один з найкращих мікроконтролерів за співвідношенням продуктивність – споживання. Ядро ARM7TDMI використовує трисходинковий конвеєр: вибір, декодування та виконання інструкції. Більшість операцій обробки даних виконують за один цикл. Середня продуктивність ядра становить 0,8 MIPS/МГц при споживанні 1,8мВт/МГц. Окрім того, сімейство AT91SAM7S характеризується наявністю достатньо широкого спектра різноманітних інтерфейсів передавання даних.

Для реалізації МБПД було використано Bluetooth модуль фірми National Semiconductor LMX9820A [7]. Це високоінтегрований, готовий для використання модуль класу 2 з реалізованим стеком протоколів за специфікацією Bluetooth 1.1. Він поєднує в собі радіоінтерфейсну частину,

FLASH, RAM пам'ять та 16-бітне процесорне ядро CompactRisc™. Для взаємодії з МКК використовують послідовний інтерфейс з апаратним контролем потоку даних.

Основним критерієм під час вибору автономного джерела електроенергії була така характеристика, як щільність енергії зарядженої батареї. Найкращі показники мають літій–полімерні акумулятори ($150\ldots200 Вт\cdot год/кг$), помітно поступаються їм літій–іонні акумулятори ($100 Вт\cdot год/кг$). Тому як джерело електроенергії для вузла було використано Li-Pol акумулятор. Заряджання та контроль ємності акумулятора здійснює окрема підсистема [8]. Вся необхідна інформація про стан акумулятора передається через I^2C інтерфейс на МКК.

Четвертою складовою апаратної платформи вузла є модуль генератора випадкових чисел, також під'єднаний до I^2C шини МКК. Детальну інформацію щодо реалізації такого генератора наведено у роботі [9].

Загальні характеристики апаратної платформи тестового вузла ММДС наведено у табл. 1.

Таблиця 1

Основні характеристики апаратної платформи вузла ММДС

Продуктивність МКК, MIPS	38,4
Об'єм RAM МКК, кБ	16
Об'єм FLASH МКК, кБ	64
Пропускна здатність МБПД, кбіт/с	230,4
Струм споживання при напрузі 3,3В, мА	50
Ємність акумуляторної батареї, мА*год	1500

Програмне забезпечення вузла тестової ММДС

Програмне забезпечення вузла виконується на МКК та складається з двох основних модулів: системи аутентифікації, що використовує бібліотеку криптографічних алгоритмів, та програмного модуля МБПД.

Програмний модуль МБПД. Окрім нижніх рівнів стеку протоколів Bluetooth модуль LMX9820A містить реалізацію таких профілів: профілю загального доступу GAP (Generic Access Profile), профілю пошуку сервісів SDAP (Service Discovery Application Profile) та профілю послідовного порту SPP (Serial Port Profile). Для роботи з цими профілями програмний модуль МБПД використовує спеціалізований командний інтерфейс [10].

Періодично за допомогою функцій профілю загального доступу формується множина вузлів P_n, що містяться в межах дії каналу передачі даних та рівень сигналу від яких перевищує заданий поріг чутливості. Подальший обмін інформацією між вузлами здійснюється засобами профілю послідовного порту. Після узгодження усіх параметрів послідовного каналу з'єднання з потрібним вузлом переводиться у режим прямого передавання даних між системами аутентифікації ("прозорий" режим).

Реалізація системи аутентифікації. Основними модулями системи аутентифікації є бібліотека криптографічних алгоритмів, модуль керування довірою та таблиця об'єктів. Криптографічна бібліотека містить реалізацію таких класів алгоритмів:

- алгоритмів симетричного блокового шифрування – RC5-32/12/16 та CAST-128;
- алгоритму асиметричного шифрування – ECC;
- алгоритмів хеш-функцій – MD5 та SHA-1.

Доступ до генератора випадкових чисел, реалізованого у вигляді окремого апаратного модуля, здійснюється через буфер за допомогою контролера прямого доступу до пам'яті. У табл. 2 показано характеристики основних модулів системи аутентифікації з використанням різних криптографічних алгоритмів.

Таблицю об'єктів реалізовано у вигляді статичного масиву структур. Розмір масиву визначається наявною вільною оперативною пам'яттю МКК. Отримують та записують інформацію з таблиці за допомогою набору інтерфейсних функцій.

Таблиця 2

Характеристики криптографічних модулів системи аутентифікації вузлів ММДС

Тип модуля	Назва алгоритму	Об'єм RAM, байт	Об'єм ROM, байт	Час виконання, мс
ГВЧ	HRND	14	524	0,64
СКС	RC5-32/12/16	172	716	0,23/0,22(1)
	CAST-128	180	14116	0,26/0,26(1)
АКС	ECC	358	6592	112,6/57,9(1)
ХФ	MD5	21	2512	0,082
	SHA-1	25	6094	0,28

Примітка. (1) – час шифрування/дешифрування.

Модуль керування довірою є "мозком" запропонованої системи аутентифікації. Він містить таблицю таких параметрів всіх можливих типів взаємодії, як мінімальний рівень довіри для початку взаємодії та мінімальний рівень довіри для інтерпретації інформації як коректної. Метод визначення поточного рівня довіри до вузла залежить від того, який з трьох можливих профілів довіри використовують:

- "Оптиміст" – з усіх наявних значень довіри (власних даних та отриманих рекомендацій) як поточний рівень обирають максимальне значення;
- "Реаліст" – як поточний рівень обирають середнє арифметичне усіх значень;
- "Песиміст" – з усіх наявних значень довіри як поточний рівень обирають мінімальне значення.

Для подальших досліджень системи аутентифікації було використано реалізацію на базі модулів з найменшим часом виконання: HRND, RC5-32/12/16, ECC та MD5.

Дослідження системи аутентифікації вузлів ММДС

Дослідження роботи системи аутентифікації в межах цілої ММДС вимагає наявності інформації щодо характеристик протоколу аутентифікації вузла мережі. Як такі характеристики використовують такі величини:

- час, що затрачається на проведення аутентифікації;
- об'єм додаткової інформації, що передається між двома вузлами для проведення аутентифікації;
- об'єм пам'яті (FLASH та RAM), необхідний для функціонування системи аутентифікації на одному вузлі мережі.

У табл. 3 показано характеристики протоколів первинної та повторної аутентифікації, а також запропонованої системи загалом.

Таблиця 3

Характеристики системи аутентифікації вузлів ММДС

Тип модуля	Об'єм RAM, байт	Об'єм ROM, байт	Час виконання, мс	Кількість додаткового трафіка, байт
МПрА(1)	3156	31128	679,2	128
МПвА(2)	2278	26452	1,99	32
СА(3)	4564(4)	47816	637,4/4,6 (5)	128/32(5)

Примітки: (1) – МПрА – модуль первинної аутентифікації; (2) – МПвА – модуль повторної аутентифікації; (3) – СА – система аутентифікації; (4) – об'єм RAM без врахування таблиці об'єктів; (5) – середній час виконання процесу аутентифікації та кількість додаткового трафіка залежать від розподілу ймовірностей частоти використання процедури первинної та повторної аутентифікації.

З наведених даних можна зробити висновок, що обчислювальних ресурсів апаратної платформи вузла, описаної вище, достатньо для нормального функціонування розробленої системи аутентифікації.

Аналіз криптографічної стійкості системи аутентифікації вузлів ММДС

Відомо, що криптографічна стійкість системи захисту інформації загалом визначається стійкістю найслабшої її частини. Для того, щоб оцінити стійкість запропонованої системи, розглянемо коротко характеристики стійкості її окремих модулів.

HRND. Як недетерміноване джерело сигналу в апаратному генераторі випадкових чисел HRND використовується "білий шум" в електронній схемі. За результатами імовірнісних та графічних тестів, наведених у [9], бітові послідовності, отримані від генератора, можна вважати випадковими.

RC5-32/12/16. Параметризований алгоритм симетричного блокового шифрування RC5 запропонував Рон Райвест у 1994 році. Він є стійким до диференційного та лінійного криптоаналізу; довжина ключа в 128 біт забезпечує достатню стійкість до атак з перебором ключів.

ECC. Рівень стійкості криптографічних алгоритмів на базі математичного апарату еліптичних кривих визначається складністю розв'язання задачі логарифмування на еліптичних кривих. За сучасними оцінками ключ для ECC завдовжки в 160 біт за стійкістю відповідає 1024-бітовому ключу RSA.

MD5. У 1996 році німецький криптоаналітик Доббертін запропонував підхід, що дає можливість генерувати колізії для одного 512-бітового блоку даних. Проте сьогодні не існує способу узагальнення цього підходу для цілого повідомлення. Алгоритм MD5 використовують для генерації ключів з двох блоків по 512 біт. Таке застосування можна вважати достатньо стійким.

Протоколи аутентифікації. Протокол як первинної, так і повторної аутентифікації забезпечує двосторонню аутентифікацію та використовує механізм "запит–відповідь". Як унікальний ідентифікатор кожного запиту використовують випадкове число розміром 64 біти від генератора HRND.

Протокол первинної аутентифікації перевіряє знання закритого ключа, що відповідає відкритому ключу наданого сертифіката. Тобто, його стійкість визначається стійкістю генератора випадкових чисел та асиметричної криптосистеми. Протокол повторної аутентифікації перевіряє знання попередньо згенерованої пари ключів симетричної криптосистеми. Як такі ключі використовують значення хеш-функцій двох випадкових чисел, тобто ключі також є випадковими числами. Стійкість протоколу повторної аутентифікації визначається стійкістю генератора випадкових чисел та симетричної криптосистеми.

Отже, криптографічна стійкість запропонованої системи аутентифікації відповідає сучасним вимогам.

Висновки

У роботі запропоновано нову децентралізовану систему аутентифікації вузлів мобільних мереж довільної структури, визначено її параметри та характеристики.

Наведена система забезпечує високу стійкість до відомих криптографічних атак поєднано з помірними вимогами до ресурсів апаратної платформи функціонування.

Отримані результати будуть використані для дослідження ефективності роботи розробленої системи у межах всієї ММДС.

1. Бочкарьов О.Ю., Голембо В.А. Система розподілених контактних вимірювань на основі автономних мобільних інтелектуальних агентів // Вісн. Нац. ун-ту "Львівська політехніка". – 2001. – № 437. – С. 62–66. 2. Gerck E. Generalized Certification theory. – 1998. 3. Gerck E. Toward Real-World Models of Trust: Reliance on Received Information. – 2002 4. Сокіл В.М., Морозов Ю.В. Модель довіри в спеціалізованих мобільних мережах // Вісн. Нац. ун-ту "Львівська політехніка". – 2005. – № 546. – С. 135–139. 5. Сокіл В.М. Модель аутентифікації в спеціалізованих мобільних

мережах // Вісн. ІПМЕ НАНУ. – 2006. – № 34. – С. 108–115. 6. Atmel Corp. Datasheet "AT91 ARM® Thumb® – based Microcontrollers", 2005. 7. LMX9820 Bluetooth™ Serial Port Module, Rev. 0.731, December 2004. 8. Cypress Semiconductor Corp. AN 2294 "Li-Ion/Li-Polymer Battery Charger with Fuel Gauge Function", 2006. 9. Сокіл В.М. Генератор випадкових чисел // Вісн. Нац. ун-ту "Львівська політехніка". – 2004. – № 523. – С. 127–134. 10. LMX9820/LMX9820A Bluetooth Serial Port Module – Software Users Guide, Rev. 1.6.1, November 2004.

УДК 624.941

С.Ю. Спіченков
Національний університет "Львівська політехніка",
кафедра електронних засобів інформаційно-комп'ютерних технологій

МЕТОД ПАСИВНОЇ ЛОКАЦІЇ ДЖЕРЕЛА КВАЗІПЕРІОДИЧНОГО СИГНАЛУ

Запропоновано метод пасивної локації джерела квазіперіодичного сигналу, незалежного від періоду повторення сигналу, його можливої широкосмуговості та наявності випадкової складової з можливістю визначення координат джерела сигналу однозначно та з наперед заданою точністю. Наведено послідовність його реалізації.

A method of quasi-periodic signal passive location is proposed. The method is not dependent on the period of signal, its possible wide bandwidth factor and random component presence. It has a possibility of position data to be determined uniquely or with a preset accuracy. Execution sequence of the method is presented.

Вступ

Методи пасивної локації джерел просторових сигналів, наприклад, звукових коливань, в яких координати джерела сигналу встановлюють як точку перетину пеленгів або геометричних місць точок можливого знаходження джерела сигналу, є досить поширеним. В них визначається кожна точка перетину (геометричне місце) для пари просторово рознесених точок прийому за відомими швидкостями просторового поширення сигналу V, координатами точок приймання сигналу та різницями часів поширення сигналу від джерела до цих точок приймання. Характерною особливістю запропонованого у статті методу є квазіперіодичний часово-просторовий характер сигналу, що надходить від джерела, який є типовим для широкого класу періодично працюючих джерел сигналу, таких як двигуни, маяки, просторові маркери. Такі сигнали характеризуються не тільки періодичністю, але й можливою широкосмуговістю та наявністю випадкової складової системи в реальному масштабі часу. Серед публікацій на цю тему важливо зазначити [1–3].

Мета статті

Метою статті є приведення та обґрунтування методу пасивної локації джерела квазіперіодичного сигналу незалежного від періоду повторення сигналу, його можливої широкосмуговості та наявності випадкової складової з можливістю визначення координат джерела сигналу однозначно та з наперед заданою точністю.

Огляд існуючих методів

Одним із відомих методів пасивної локації джерела квазіперіодичного сигналу є метод, за яким визначають період повторення сигналу $T_П$, коли сигнал приймають та реєструють у парах