наявним у доступі обчислювальних ресурсів. Більш детально дана система буде розглянута в наступному розділі.

Під грід системою (від англ. Grid - сітка) або мета комп'ютером розуміють мережу гетерогенних обчислювальних ресурсів, географічно розподілених, використовуваних для паралельної обробки обчислювальних завдань.

Грід являє собою програмно-апаратну інфраструктуру для розділяється використання обчислювальних вузлів, мереж, баз даних та інших ресурсів, які знаходяться в юрисдикції різних географічно розподілених організацій.

Для управління ресурсами використовується проміжне ПЗ, причому управління як правило - децентралізоване.

УДК 004.7 : 004.9

Морозюк Р. – ст.гр. СІм-51
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ СИСТЕМИ ЗАХИСТУ БЕЗДРОТОВИХ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ НА ОСНОВІ СТАНДАРТУ IEEE 802.15

Науковий керівник: к.т.н., доцент Баран І. О.

Moroziuk R.
Ternopil Ivan Pul'uj National Technical University

RESEARCH OF WIRELESS DATA NETWORKS PROTECTION BASED ON THE STANDARD IEEE 802.15

Supervisor: Ph.D., as.prof. Baran I.

Ключові слова: стандарт IEEE 802.15, аутентифікація, шифрування
Keywords: standard IEEE 802.15, authentication, encrypting

EEE 802.15 - стандарт, який визначає фізичний шар і керування доступом до середовища для бездротових персональних мереж з низьким рівнем швидкості. Стандарт підтримується робочою групою IEEE 802.15. Є базовою основою для протоколів ZigBee, WirelessHART та MiWi, кожен з яких, у свою чергу, пропонує рішення для побудови мереж за допомогою побудови верхніх шарів, які не регламентуються стандартом. В якості альтернативи він може бути використаний спільно зі стандартом 6LoWPAN і стандартними протоколами Інтернету для побудови вбудованого бездротового Інтернету.

Існує кілька видів атак на Bluetooth-пристрої: від цілком нешкідливих - типу BlueSnarf, до повноцінних DoS-атак і міжнародних дзвінків без відома власника телефону, або "просто" викрадення СМС-повідомлень. Крім того, існують віруси, що поширюються за допомогою Bluetooth.

Основні заходи захисту систем передачі даних на базі протоколу 802.15: організація безпечних каналів аутентифікації в Bluetooth (використання алгоритму аутентифікації E1 на основі алгоритму шифрування SAFER+ (Secure And Fast Encryption Routine); шифрування даних на основі алгоритму E0 (SAFER +), управління з використанням ключів). Алгоритми, що здійснюють шифрування і аутентифікацію, використовують наступні параметри: адресу модуля - загальновідому 48-бітову адресу

пристрою; секретний ключ аутентифікації – секретний 128-бітовий ключ; секретний приватний ключ довжиною від 4 до 128 біт; випадкове 128-бітове число, яке згенеровано в пристрої Bluetooth. Аутентифікація пристроїв відбувається за складною на програмному рівні і водночас непомітною для користувача схемою. Це є першим кроком до безпечного захисту даних. Алгоритм E0 реалізується на лінійному регістрі зсуву з зворотним зв'язком LFSR (Linear Feedback Shift Register), який ініціалізується ключем корисного навантаження.

Шифрування даних у технології 802.15 в загальному випадку складається із чотирьох операцій: заміна першого підключа, нелінійна оборобка заміни, підміна другого підключа й лінійне перетворення. При цьому використовуються тільки байтові операції, що робить цей шифр особливо зручним для реалізації на мікропроцесорах малої розрядності. При шифруванні та розшифровуванні використовується одна унімодулярна матриця розміром 16x16. Пропонується при шифруванні використати різні матриці розміром 16x16 та 32x32. При цьому матриця може виступати елементом ключа.

Основою, на якій базується безпека Bluetooth, є генерація ключів, яка виробляється на основі PIN-коду. Довжина PIN-коду може бути від 1 до 16 байт. В даний час більшість пристроїв використовує 4-байтовий код. Спочатку на основі PIN-коду за алгоритмом E2 генерується 16-байтовий Link Key, після чого за алгоритмом E3 на базі Link Key обчислюється Encryption Key. Перший ключ використовується для аутентифікації, а другий для шифрування.

Для забезпечення конфіденційності, цілісності та доступності даних необхідно провести аудит безпеки. Для аудиту інформаційної безпеки системи передачі даних стандарту 802.15 можна використати будь-яку із спеціалізованих утиліт для виявлення та унеможливлювання спроб несанкціонованого доступу: Bluesnarfing, BlueSnarf++, BlueBug, Bluestab, BlueBump, BlueSpooof, BlueDump і т.п.

За матеріалами проведеного досліження можна надати наступні рекомендації, щодо захисту мереж передачі даних на базі протоколу 802.15: завжди вимикати Bluetooth після завершення передачі даних; ставити захисний код на ініціалізацію з'єднання; вмикати обов'язкову авторизацію; використовувати нестандартні (відсутні в словниках, різні регістри) і достатньо довгі за кількістю символів паролі; відхиляти будь-які запити на під’єднання з невідомими пристроями; встановити невидимий режим для будь-яких користувачів; без потреби не вмикати Bluetooth-пристрій в людних місцях; з’єднання встановлювати тільки з відомими пристроями; не використовувати технологію в комерційних цілях; при можливості «перепрошити» програмне забезпечення пристроїв до новіших версій.