The Access Control System Reader Implementation Based on Radio Frequency Identification Using Lightweight Encryption

Petro Pulya

Information Security Department,
Lviv Polytechnic National University,
UKRAINE, Lviv, S. Bandery street 12,
E-mail: pulya.pa@gmail.com

The aim of the paper is to survey, analyse and compare different radio-frequency identification systems in the data protection fields, choose the method of lightweight encryption for RFID-tags, to define the main drawbacks and methods for their solution.

Modern transponders have a weak cryptographic protection or do not have it at all. That why the development of budget reader control system with an efficient lightweight encryption algorithm is a very actual problem.

Radio-frequency identification is a method of automatic object identification, in which data stored in the transponders (RFID tags) are read or written using radio signal.

Any RFID-system consists of two parts: readers and transponders. According to the standards, the information is transferred by the pulse-phase modulation. Most RFID tags contain at least two parts. One is an integrated circuit for storing and processing information, modulating and demodulating a radio-frequency signal, and other functions. The second is an antenna for receiving and transmitting the signal.

The objects are identified by the unique digital code, read from electronic tag memory attached to the identification object.

The Reader contains a transmitter and an antenna whitch help to emit the electromagnetic field of certain frequency. The tags in the readable field area respond with their own information signal (product identification code, user data, etc.). Reader's antenna receives the signal; the information is decoded and transmitted for processing.

The paper also deals with tags application for object identification, access monitoring, etc. Notwithstanding the wide range of application, there are a lot of drawbacks in the radio tags. The paper discusses the main drawbacks of RFID tags (weak crypto protection and chip content scanning at a distance) and offers possible methods of protection against unauthorized reading or falsification of RFID tags, the modification method of the existing block symmetric lightweight encryption protocol is using for better data protection during the transmission between the tag and the reader.

Keywords - radio frequency identification, RFID-tag, system protection, lightweight encryption.

Реалізація зчитувача системи контролю доступом на основі радіочастотної ідентифікації з використанням легковагового шифрування

Петро Пуля

Кафедра захисту інформації,
Національний університет "Львівська політехніка",
УКРАЇНА, м. Львів, вул. С. Бандери, 12,
E-mail: pulya.pa@gmail.com

В статті здійснюється аналіз основних видів та способів застосування радіочастотної ідентифікації з використанням активних і пасивних транспондерів, огляд та вибір методу легковагового шифрування для захисту каналу передачі даних між зчитувачем та радіоміткою.

Ключові слова – радіочастотна ідентифікація, RFID-мітка, система захисту інформації, легковагове шифрування.

I. Вступ

Сучасні досягнення науки за останні декілька років здійснили революцію в інформаційному світі. Введення систем автоматизації управління змінює наше життя. Бурхливий розвиток технологій збільшує ризик витоку інформації та несанкціонованого доступу, отже, виникає необхідність її захисту. Для запобігання несанкціонованого доступу на контрольовані об'єкти використовуються системи контролю доступом, тобто сукупність програмно-технічних засобів та організаційних заходів, які ускладнюють витік інформації з контрольованого об'єкту. Все більшого поширення в наш час набувають системи контролю доступом на основі технології радіочастотної ідентифікації (RFID – Radio Frequency Identification) [1, 2]. Ідентифікація користувача в таких системах здійснюється за допомогою спеціальних rfid-міток.

Основними сферами застосування RFID технологій є: поштова система та логістика, системи контролю та управління доступом (СКУД), банківські платіжні системи, паспортні біометричні системи, системи захисту інформації.

II. Основна частина

Актуальність роботи. Дослідні роботи в галузі радіочастотної ідентифікації є перспективними, оскільки саме поняття ідентифікації є ключовим в сучасних захищених системах і мережах. Сучасні транспондери мають слабкий крипто-захист або не мають його взагалі, тому розробка бюджетного зчитувача системи контролю з ефективним легковаговим алгоритмом шифрування значно зменшить ймовірність витоку інформації через радіоканал в процесі передавання її від rfid-мітки до зчитувача [3-5].

Радіочастотна ідентифікація – технологія, що дозволяє передавати та отримувати інформацію, яка записана на вбудований в об'єкт носій через радіоканал. Загалом RFID система складається з двох базових компонентів: зчитувача та rfid-мітки. Зчитувач містить у своєму складі передавач і антену, за допомогою яких випромінюється електромагнітне поле встановленої частоти. Під час наближення мітки до зчитувача, вона активується, здійснюється передача інформації, що зберігалася на ній до зчитувача. Інформаційний сигнал з даними мітки поступає на зчитувач системи контролю, який, після порівняння бази даних і отриманого сигналу, приймає рішення про належність об'єкту системі [6].

Характеристики радіочастотної ідентифікації визначаються типом мітки. Rfid-мітки поділяються за наступними ознаками: наявність джерела живлення (активні, пасивні); тип зберігання даних (пам'ять, яка використовується); способом запису інформації (робочою частотою). Більшість rfid-міток складається з двох частин інтегральної схеми для зберігання і обробки інформації, модуляції і демодуляції радіочастотного сигналу, деяких інших функцій та антени для прийому-передавання сигналу. Ідентифікація об'єктів здійснюється за унікальним цифровим кодом, який зчитується з пам'яті електронної мітки, що міститься на об'єкті ідентифікації.

Інтегрована мікросхема мітки зберігає дані про об'єкт маркування і забезпечує їх необмежену кількість запису та зчитування. Швидкість роботи систем RFID сягає сотень міток на секунду. Використання RFID-міток є досить актуальним і перспективним на цей час [7].

Незважаючи на широке використання, деякі типи міток мають слабкий криптографічний захист, або не мають його взагалі, що дає можливість зловмиснику несанкціоновано отримувати необхідні дані, або підробити rfid-мітку в цілому. У зв'язку з цим виникає необхідність використання шифрування для захисту каналу передачі.

Зазвичай, канал передачі даних від зчитувача до контролера доступу (сервера) є захищений, тому актуальною проблемою є захист каналу передачі між міткою і зчитувачем. Запропонований зчитувач працює з пасивними мітками. Складність завдання полягає в тому щоб забезпечити відповідний рівень захисту при обмежених ресурсах системи. Криптографічні алгоритми потребують значних об'ємів пам'яті, та енергозатрат. Тому використаємо легковагове шифрування (Lightweight (LW) encryption).

Основою будь-якої LW-криптосистеми є симетричні алгоритми. Це зумовлено, перш за все, високою, у порівнянні з асиметричними шифрами швидкістю виконання, що є критичним параметром у даній системі. Легковагові алгоритми бувають як блочними так і поточними. На даний момент відомо тільки 3 описаних поточних шифра, які мають відповідні характеристики. Це алгоритми MICKEY, Trivium і GRAIN [8]. Однак, вони не придатні для пасивних RFID-міток. Trivium потребує розміру пам'яті на чіпі, що перевищує допустиму більше ніж в 1,5 рази [1 з bit_1]. Шифр GAIN вразливий для атак на зв'язаних ключах [3 з bit_1]. Розробники MICKEY перевірили його стійкість лише на певні види атак, але цього недостатньо для забезпечення впевненості у його надійності. До блочних шифрів належать DESL, PRESENT, KATAN, AES, IDEA та ін. DESL використовує відносно малий ключ – 56 біт і застосовується, зазвичай, для апаратної реалізації. PRESENT використовує 80-бітний ключ, але також є орієнтований на апаратну реалізацію. У роботі [8], здійснено аналіз блокових симетричних алгоритмів за критеріями продуктивність - пам'ять. Результати досліджень підтвердили високу ефективність алгоритмів AES та SASI, які випередили усіх конкурентів. Дані алгоритм є ефективними та зручними при програмній реалізації. Але через обмежені можливості мікропроцесорів, для збільшення швидкодії, використаємо модифікований алгоритм SASI, який базується на побітових операціях І, АБО, додавання за модулем 2 та повороту (Rot(x,y)). У модифікованій схемі поворот здійснюється завдяки циклічному зсуву на величину x (y mod N) позицій вліво для одержання необхідного значення N (у нашому випадку 128) [9]. Генерація випадкових чисел, необхідна для оновлення протоколу - досить складна операція, тому виконується зчитувачем. Щоб підвищити захищеність протоколу додано спеціально розроблену легковагову функцію MixBits. У роботі [10] детально описується принцип виконання функції, яка базується, в основному, на композиції операндів за допомогою генетичного програмування для отримання високої нелінійності функції. MixBits є легковаговою, оскільки в ній виконуються лише операції порозрядного зсуву праворуч та додавання.

```
Z = MixBits(X,Y)
Z = X
for(i=0; i<32; i++) {
Z = (Z>>1) + Z + Z + Y ;}
```
(1)

Завдяки вище перерахованим діям, значно знижується ймовірність проведення атак, які базуються на підміні та підстановці нових повідомлень.

Протокол охоплює три стадії: ідентифікація мітки, взаємну авторизацію і фазу оновлення ключів.

Ідентифікація мітки. Зчитувач вперше посилає сигнал для мітки, яка у відповідь надсилає свій наступний ідентифікаційний код (IDS). Зчитувач порівнює ідентифікаційний номер картки з відповідними записами у базі даних. Якщо даний запис існує, то наступає стадія взаємної авторизації, тобто повторюється ідентифікація, але зі старими IDS, які передаються карткою під час відповіді.

Стадія взаємної перевірки автентичності. Разом із ідентифікатором мітки зчитувач отримує конфіденційну інформацію яка звіряється із базою даних. Транспондер генерує значення n1 та n2, і передає до мітки повідомлення (A||B||C).

$$R \to T : A \| B \| C \quad (2)$$

Зчитувач генерує повідомлення n1 та n2 для побудови суб повідомлень:

$$A = Rot((IDS + k_1 + 128 + n_1, k_2) + k_1, k_1) \quad (3)$$

$$B = Rot((Rot(IDS + k_2 + 128 + n_2, k_1) + k_2 \quad (4)$$

$$\text{де } n_3 = MixBits(n_1, n_2) \quad (5)$$

$$k_1^* = Rot((Rot(n_2 + k_1 + 128 + n_3, n_2) + k_2, n_1) \quad (5)$$

$$k_2^* = Rot((Rot(n_1 + k_2 + 128 + n_3, n_2) + n_3 \quad (6)$$

$$\text{де } n_1^1 = MixBits(n_3, n_2) \quad (7)$$

$$C = Rot((Rot(n_3 + k_1^* + 128 + n_1^{'}, n_3) + k_2^*, n_2) \quad (8)$$

Із повідомлень A і B мітка дістає значення n1 та n2, обчислює n3/n1, k1*/k2* і будує свою версію суб повідомлення C. Результат порівнюється із отриманим. Якщо дане значення проходить перевірку – зчитувач автентифікований. Нарешті, rfid-мітка посилає повідомлення D для зчитувача. Дане значення порівнюється із власним обчисленим еквівалентом. При співпаданні повідомлень відбувається автентифікація мітки, в іншому випадку-розрив з'єднання.

Індексація та оновлення ключів. Після успішної автентифікації мітка та зчитувач оновлюють IDS та ключі (k1,k2). Субповідомлення C, D дозволяють провести взаємну автентифікацію. Більше того, використання повідомлень C та D для підтвердження синхронізації для внутрішніх таємних значень (n3/n01 та k1*/k2*) що використовуються на стадії оновлення, запобігає прямим активним атакам на систему.

Аналіз захищеності. Відкриті повідомлення містять у собі три секретні величини, якими можуть обмінюватись лише авторизовані мітки та зчитувачі. Зауважимо, що конфіденційними вважаються значення ідентифікатора мітки та ключі (ID, K1, K2), випадкові числа (n1,n2) і локально обчислені значення (n3, n01, n02, k1*,k2*). Отже значно зменшується ймовірність перехоплення статичного ідентифікатора та ключів. Кожна rfid-мітка оновлює свій IDS та секретні ключі відразу після успішної автентифікації. Цей процес включає в себе оновлення випадково згенерованих значень (n3, n01, n02). Якщо повторно надіслати запит для мітки, то буде згенероване нове значення IDS. Крім того, всі відкриті суб повідомлення (B, C і D) є анонімними при використанні випадкових чисел (n1,n2,n3,n01), тобто анонімність мітки ускладнює пошук її власника. Завдяки взаємній перевірці достовірності та цілісності даних протокол забезпечує взаємну перевірку автентичності. Тільки законний зчитувач може згенерувати ключі (k1,k2) та побудувати належним чином повідомлення A||B||C. Так само лише автентифікована мітка може виділити із запиту значення (n1, n2) та на їх основі обчислити і згенерувати повідомлення D. Завдяки повідомленням C і D, в яких містяться таємні значення (n3,n01,k1*,k2*,n1,n2) забезпечується перевірка цілісності даних. Навіть при розкритті таємних значень (ID, k1, k2) при успішному перехопленні та дешифруванні повідомлення зловмисник не зможе визначити секретні значення (n1,n2) та (k1*,k2*,n3, n02), що локально обчислюються у мікроконтролері мітки і зчитувача відповідно, та беруть участь у взаємній автентифікації. Отже завдяки перехопленим даним неможливо визначити структуру наступних згенерованих повідомлень. Через наявність завад у радіоканалі існує ймовірність некоректного прийому повідомлення D. Але завдяки подвійному зберіганню кортежу (IDS, k1, k2) у пам'яті rfid-мітки (попереднього та наступного значення) система синхронізується використовуючи попередні значення IDS. Протокол виконує взаємну автентифікацю та захист цілісності даних використовуючи всього чотири повідомлення. Отже, із врахуванням 5 байт необхідних для генерації повідомлення у початковій фазі ідентифікації, в цілому по радіоканалу передаються 424 біт. Основні переваги модифікованого протоколу наведені у таблиці.

	U-MAP сімейство	SSASI	модифіко-ваний протокол
Стійкість до десинхронізо-ваних атак	ні	ні	так
Стійкість до підбору ключа	ні	ні	так
Конфіденцій-ність та анонімність	так	так	так
Взаємна автентифікація	так	так	так
Повідомлень для взаємної автентифікації	4-5L	4L	4L
Об'єм пам'яті міток	6L	7L	7L
Види операцій при шифруванні	$\oplus,\cup,\cap,+$	$\oplus,\cup,\cap,$ $+, Rot^2$	$\cap,+, Rot,$ $MixBit$

Проведене тестування запропонованого зчитувача із Light Weight- шифруванням продемонструвало високу надійність роботи – практична відсутність помилок першого (FAR=0.001) та другого роду (FRR=0.01) із проведених 8000 випробувань. Перевагою розробленого зчитувача є значна економічна ефективність, за технічними характеристиками він не поступається наявним на ринку аналогам, а завдяки криптозахисту значно знижує ризик успішних атак.

Швидкодія, надійність та живучість. Наступним основним параметром системи RFID є швидкодія, яка залежить від застосування та конфігурації системи. Характеризується: швидкістю передачі даних та швидкістю ідентифікації. Швидкість передачі даних є власне швидкістю передачі бітів даних, тоді як швидкість ідентифікації визначається характеристиками антиколізійних алгоритмів при визначенні індивідуального номера мітки.

Швидкість передачі даних в основному залежить від частоти пристрою та періоду повторення бітів

інформації. Чим менший період, тим більша швидкість передавання даних. З точки зору апаратної реалізації можна зазначити, що для даної схеми кодування та модуляція призводить до розширення спектру. З врахуванням обмежень за шириною спектру це призведе до зниження потужності, що надається мітці. З цього спостерігаємо взаємозв'язок між швидкістю передавання даних і дальністю дії.

Швидкодія ідентифікації залежить від використаного антиколізійного протоколу. Антиколізійні протоколи впливають на витрати при проектуванні апаратури, які у свою чергу, помітно впливають на вартість. Існує взаємозв'язок між швидкістю ідентифікації та вартістю. Крім того, протоколи впливають на потужність споживання – чим більше інтенсивність обробки, тим більше споживається потужність [11].

Надійність зв'язку в системах RFID також сильно пов'язана з антиколізійними алгоритмами. Так, в прямому каналі зв'язку надійність є вищою, тому що в ньому простіше забезпечити велике відношення сигнал/шум. Натомість надійність зворотного каналу зв'язку значно нижча, тому більш надійними є протоколи, які вимагають передачі меншого обсягу даних від мітки до зчитувача. Застосування процедур виявлення і корекції помилок призводить до зниження швидкості передавання даних, ускладнює апаратуру, вимагає великих витрат потужності і, отже, зменшує дальність. Як зазначалося раніше, у міру наближення до зчитувача напруженість поля зростає, сигнал стає більш помітним і, отже, зростає надійність зв'язку. Надійність каналів зв'язку пов'язана як з дальністю дії, так і з швидкодією системи [12].

Властивість живучості – це здатність системи виконувати основні функції під час атак, пошкоджень, аварійних ситуацій і швидко відновлювати всі функції. Одним із найефективніших методів підвищення живучості є резервування, тобто введення в систему надлишковості. При використанні запропонованого авторами пристрою живучість системи контролю задовільняє поставлені вимоги. У самій схемі уже є певна надлишковість, оскільки дані зберігаються як в базі даних EEPROM пам'яті, так і в базі даних комп'ютера до якого зчитувач може бути підключений. При виході бази даних комп'ютера з ладу дані залишаться на самому пристрої. Система залишається живучою навіть у випадку пропадання напруги живлення за рахунок вчасного під'єднання апаратного резерву [12].

Висновки

Технологія радіочастотної ідентифікації знаходить широке поширення в різних галузях. Застосування її для систем контролю доступом полегшує процес ідентифікації користувача. Схема запропонованого пристрою жодним чином не поступається аналогам на ринку, в економічному відношенні є ефективнішою в 4 рази та використовує модифікований метод симетричного блочного легковагового шифрування даних із взаємною автентифікацією та перевіркою цілісності даних. Майбутні дослідження пов'язані із розробкою ефективного антиколізійного протоколу та подальшим тестуванням системи на наявність вразливостей.

Література

[1] Ворона В. А. Системы контроля и управления доступом / К. М. Тихонов, В. А. Ворона // Горячая Линия Телеком, 2010. – С. 272.

[2] Парк Дж. Системы контроля и управления доступом / С.Маккей , Е.Райт // «Группа ИДТ», 2007.- С. 102-156.

[3] Yan Zhang. RFID and sensor networks: architectures, protocols, security and integrations / Yan Zhang, Laurence T. Yang, Jiming Chen // «Taylor & Francis Group», 2009. – С. 648.

[4] Keith E. Mayes. Smart cards, tokens, security and applications/Keith E. Mayes Konstantinos Markantonakis // Springer Science+Business Media, 2008. – С. 416

[5] Проблемы и их решения в RFID технологии [Електронний ресурс] режим доступу: http://www.itsec.ru/articles2/Inf_security.

[6] Фролова Г. Технология RFID. Проблемы и решения / Г. Фролова // Журнал «Склад и техника», 2007. – № 1.

[7] Шарфельд Т. Системы RFID низкой стоимости / Т. Шарфельд // Москва 2006. – С. 197

[8] Konidala D. M. RFID Tag-Reader Mutual Authentication Scheme Utilizing Tag's Access Password/. M. Konidala and K. Kim// Auto-ID Labs White Paper WP-HARDWARE-033, Jan 2007. – С 25-86

[9] Poschmann A. New Light-Weight Crypto Algorithms for RFID./ , G. Leander, K. Schramm, C. Paar. // In Proc. of ISCAS'07,2007. – С. 1843–1846

[10] Chien H.Y. Mutual authentication protocol for RFID conforming to EPC Class-1 Generation-2 standards/ H.Y. Chien H.Y., C.H. Chen// in Computer Standards & Interfaces 29:(2). 2007.-С. 254–259

[11] Bogdanov A. PRESENT: An Ultra-Lightweight Block Cipher In Proc. of CHES'07, volume 4727 of LNCS/ A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe.// Springer-Verlag, 2007, - С. 450–466.

[12] Гарасим Ю. Р. Метод загального резервування для забезпечення живучості системи захисту інформації / В. Б. Дудикевич , Ю. Р. Гарасим // Науково-технічний журнал «Захист інформації» №2, 2010 – С. 81-85.