СПОСОБИ ПРИХОВАНОГО ЗВ'ЯЗКУ ТА ЗАХИСТ ВІД РАДІОМОНІТОРИНГУ

Бердник Ю. В., Шпилька О. О., к. т. н
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна

Система прихованого зв'язку — це система, роботу якої важко виявити методами радіомоніторингу. Одним із варіантів побудови такої системи зв'язку, є використання широкосмугових сигналів, детектування яких можливе навіть у випадку коли, рівень електромагнітного випромінювання радіотехнічної системи нижче рівня шуму. Цього можна досягти за допомогою широкосмугових сигналів, використовуючи хаотичні радіоімпульси, лінійно-частотну модуляцію або пряме розширення спектру. Суть такого підходу зводиться до рівномірного розподілу енергії сигналу по спектру і його ширина може сягати 500 МГц. Але системи побудовані за таким підходом, теоретично можуть бути запеленговані більш чутливими системами радіопеленгу або набором статистику ефіру і дослідженням місцевої електромагнітного становища.

Другий спосіб створити систему прихованого зв'язку — заховати сигнал серед стандартних радіотехнічних систем. Наприклад для GSM, уже існують такі технології як NB-IoT, EC-GSM-IoT і eMTC. Стандарт eMTC (enhanced Machine-Type Communication) розгортається на основі мобільних мереж LTE, а EC-GSM-IoT (Extended Coverage - GSM - Internet of Things) працює поверх мережі GSM. Але найбільш популярний — стандарт NB-IoT (Narrowband IoT). Його особливість полягає в тому, що він може бути розгорнутий, як в мережах GSM або LTE, так і незалежно, окремою мережею. Спектрально сигнал такої системи як NB-IoT неможливо відрізнити від GSM (рис. 1), отже можна використати цю технології для передачі даних.

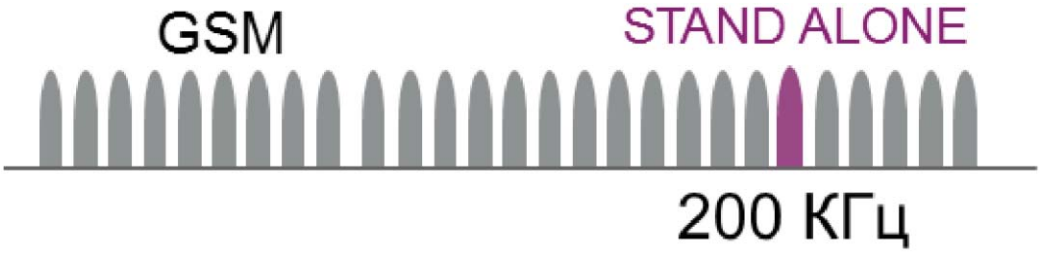

Рисунок 1. Розташування спектру NB-IoT Standalone — розташування поза межами разом з каналами GSM або замість них з будь-якою налаштованою потужністю

Таким чином, при моніторингу ефіру не буде видно, що якась система використовується для передачі скритої інформації. Конфіденційність цієї інформації забезпечується пропрієтарним шифруванням, прийнятим у стандарті NB-IoT. Таким чином, можна організувати зв'язок з десятками і сотнями [2] таких пристроїв, на всій території покриття мобільних операторів,

і забезпечити низьку ймовірність виявлення окремих пристроїв і перешкоджанню їх роботи.

У NB-IoT є важливий недолік — не підтримується процедура handover. Для використання схеми у повній мірі для рухомого зв'язку можливо використати технологію LTE-M для передачі, наприклад, інформації про стан людини на відстані до декількох кілометрів. Недоліком цієї технології є необхідність підтримки стандарту LTE мобільної мережею. Передачу інформації за цим методом можливо сховати за WCDMA або серед спектру LTE, при використанні LTE Cat M1 (eMTC). Таким чином можлива передача навіть відеоінформації, оскільки швидкість передачі даних може сягати 1 Мбіт/с [3].

Таким чином, організовується система що на локальній відкритій місцевості здатна проводити обмін інформації, роботу такої системи важко помітити і майже неможливо аналізувати, окрім як статистичними методами.

При розгляді характеристик NB-IoT мережі (див. табл. 1) можна звернути увагу на досить низьку швидкість підключення та затримки. Ці недоліки перекриває той факт, що мережа розрахована на нове покоління IoT пристроїв, що будуть здатні проводити розрахунки у собі, а в мережу передавати лише стислі висновки цих розрахунків згідно з налаштуваннями пріоритету пристроїв. До того ж, на відміну від LoRaWAN, система здатна опрацювати тисячі пристроїв в режимі реального часу, тобто будь-який пристрій може без зволікань передати оперативну інформацію [4].

Таблиця 1. Стислий набір характеристик NB-IoT підключення

3GPP Release	**Release 13**
Пропускна спроможність DL, кбіт/с	250
Пропускна спроможність UL, кбіт/с	250
Затримка, с	<10
Кількість антен	1
Режим передачі даних	Напівдуплекс
Ширина смуги, кГц	180
Потужність передавача пристрою, дБм	20/23
Максимальні втрати у радіоканалі, дБ	165
Потужність передавача станції, дБм	43
Максимальна відстань, км	15

Як видно з таблиці, дана технологія забезпечує швидкість передачі 250 кбіт/с, що можливо використати навіть для організації голосового прихованого зв'язку. Оскільки сучасні алгоритми стиснення звукових сигналів, дозволяють передавати розбірливо мову при швидкостях 10 кбіт/с, наприклад ITU G.723, ITU G.729 або інші.

Затримки, що можуть виникати при передачі інформації, як видно з таблиці, можуть становити до 10 секунд. Постає питання про використання голосового зв'язку в таких умовах, проте, така затримка стосується лише передачі даних в найбільш енергозберігаючих режимах, коли забезпечу-

ється робота від акумуляторів до 10 років. Вищезазначені варіанти застосування технологій LTE-M та NB-IoT для прихованого зв'язку передбачають безперервну роботу датчиків до півроку. Оскільки, такого терміну буде достатньо для противника викрити способи обміну даними регулярними спостереженнями та аналізу статистики цих спостережень. В такому разі для повторного застосування системи достатньо переконфігурувати її (змінити місцеположення датчиків, можливо оновити обладнання тощо). Тому, при реалізації голосового зв'язку системою NB-IoT, можливо досягти режиму реального часу.

Перелік посилань

1. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / А.С. Осипов ; под науч. ред. Е.Н. Гарина. — Красноярск : Сиб. федер. ун-т, 2013. — 344 с. — ISBN 978-5-7638-2736-1

2. NB IoT tutorial-features,Spectrum,applications of NB IoT [Електронний ресурс] : RF Wireless World. Режим доступу: http://www.rfwireless-world.com/Tutorials/NB-IoT-tutorial.html — Назва з екрана.

3. eMTC (LTE Cat-M1) [Електронний ресурс] : Halberd Bastion RF Consultancy. Режим доступу: https://halberdbastion.com/technology/iot/iot-protocols/emtc-lte-cat-m1. — Назва з екрана.

4. 3GPP Low Power Wide Area Technologies [Електронний ресурс] : GSMA White Paper // 2016. — 46 с. — Режим доступу: https://www.gsma.com/iot/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf. — Назва з екрана.

Анотація

Представлені способи прихованого зв'язку та захисту від радіомоніторингу. Розглянуті можливості стільникових технологій NB-IoT та LTE-M для забезпечення роботи прихованого зв'язку для нерухомих давачів та рухомих підрозділів. Розглянуті здатності цих систем до передачі голосових та відео даних. Розглянута можливість створення цілісної системи прихованого IoT-зв'язку.

Ключові слова: прихований зв'язок, NB-IoT, IoT, LTE-M, стільниковий зв'язок.

Аннотация

Представлены способы скрытой связи и защиты от радиомониторинга. Рассмотрены возможности сотовых технологий NB-IoT и LTE-M для обеспечения работы скрытой связи для неподвижных датчиков, подвижных подразделений. Рассмотрены возможности этих систем передавать голосовые и видео данные. Рассмотрена возможность создания целостной системы скрытой IoT-связи.

Ключевые слова: скрытая связь, NB-IoT, IoT, LTE-M, сотовая связь.

Abstract

The methods of covert communication and protection from radio monitoring are presented. The capabilities of the NB-IoT and LTE-M cellular technologies to ensure the operation of covert communications for fixed sensors and mobile units are considered. The capabilities of these systems to transmit voice and video data are considered. The possibility of creating an integrated system of hidden IoT-communication is considered.

Keywords: covert communication, NB-IoT, IoT, LTE-M, cellular communication