# Спосіб перехоплення керування безпілотними літаючими апаратами у межах контрольованої зони

Самойленко Д.М., Нечуєв Д. О.
кафедра електрообладнання суден та інформаційної безпеки,
Національний університет кораблебудування імені адмірала Макарова
Миколаїв, Україна
dnechuyev@gmail.com

# Interceptioning control of unmanned aerial vehicle in the controlled area

D. Samoylenko, D. Nechuyev
Department of electrical equipment of ships and information security
Admiral Makarov National University of Shipbuilding
Mykolaiv, Ukraine,
dnechuyev@gmail.com

***Анотація*—Запропоновано спосіб перехоплення БПЛА (безпілотних літаючих апаратів), які керуються за допомогою протоколу DSMX, у межах контрольованої зони. Основою способу перехоплення є атака за часом та атака перебором. Досліджено властивості протоколу DSMX та мікросхеми CYFR6936.Запропоновано технічне забезпечення для виконання даного способу перехоплення.**

***Abstract*—Method to intercept control of unmanned aerial vehicle, that uses DSMX protocol, in the controlled area. This method bases on timing attack and brute force to intercept control. Properties of DSMX protocol and CYFR6936 chip are investigated. Technical equipment for interception control of unmanned aerial vehicle are offered.**

***Ключові слова—перехоплення БПЛА; протокол DSMX; атака за часом; атака перебором***

***Keywords—interception control; unmanned aerial vehicle; DSMX protocol; timing attack, brute force***

## I.Вступ

Сьогодні однією з найбільш актуальних проблем є захист повітряного простору над контрольованою зоною від безпілотних літальних апаратів (БПЛА). Попит на БПЛА зростає з кожним роком, від аматорських дронів з невеликою дальністю та тривалістю польоту призначених для фото та відео зйомки до БПЛА військового призначення призначених для розвідки та наведення артилерійських розрахунків. Проблема боротьби з БПЛА постійно ускладнюється через захист каналів зв'язку з дроном за допомогою криптоалгоритмів та використання протоколів стійких до радіоперешкод. Таким чином постає необхідність у дослідженні методів виявлення та перехоплення БПЛА, що порушують кордони контрольованих зон. В межах даної роботи ми будемо розглядати протокол передачі пакетів DSMX та спосіб перехоплення дрону, що використовує дану пакетну технологію за допомогою атаки за часом.

Метою даної роботи є розгляд технології передачі пакетів за допомогою протоколу DSMX та способу перехоплення керування БПЛА, що використовують протокол DSMX.

- Для досягнення поставленої мети необхідно розв'язати наступні задачі:
- проаналізувати сферу використання протоколу DSMX;
- розглянути особливості роботи протоколу передачі пакетів DSMX;
- визначити спосіб перехоплення керування БПЛА, що використовує технологію DSMX.

## II.Теоретичний базис для методу перехоплення БПЛА під керуванням DSMX

DSMX протокол – це один з протоколів передачі даних по радіоканалу, використовується при передачі на частоті 2,4 ГГц. Переваги даної технології у великій кількості каналів передачі даних та у прогресивному алгоритмі кодування та зміни каналів. У разі завади на певній частоті даний алгоритм роботи протоколу швидко змінить частоту передачі, що дозволить не втрачати зв'язку між передавачем та приймачем. Даний протокол використовується у апаратурі марки Spekrum, в

основному це лінійка недорогих, але високо функціональних приладів радіо керування. Даний протокол працює на основі мікросхеми CYRF6936. При формуванні радіосигналу використовуються псевдовипадкове перестроювання робочої частоти (FHSS), множинний доступ з кодовим розділенням каналів (CDMA), метод прямої послідовності для розширення спектру (DSSS) та Гаусівська частотна маніпуляція (GFSK).

При перехопленні керування БПЛА необхідно перехопити керуючий сигнал від основного приладу керування для цього необхідно мати програмно-визначальну радіосистему (SDR). SDR – система радіозв'язку, в якій програмне забезпечення використовується як для модуляції, так і для демодуляції радіосигналів. При використанні SDR персональний компьютер стає ядром любительської радіостанції, завдяки чому весь обсяг робіт із обробки сигналу перекладається на програмне забезпечення. Таке обладнання дозволяє гнучко обробляти радіосигнал, модифікувати його та ретранслювати.

Для перехоплення пакетів DSMX можна використовувати плату Nuand BladeRF у якості SDR. Дана плата має у своєму складі тактовий генератор з можливістю програмування Silicon Labs Si5338, мікроконтроллер Cypress CYUSB3014 FX3, над велика інтегральна схема Altera Cyclone IV E FPGA, радіочастотний трансівер Lime Microsystems LMS6002D. Для кодування сигналу в бітовій формі використовується манчестерський код. Для DSSS використовується операція XOR з бітами псевдовипадкового шуму.

Пакет технології DSMX складається з преамбули (P), початок пакету 1 (SOP1), початок пакету 2 (SOP2), довжини пакету (L), інформаційної частини (Data) та циклічного надлишкового коду (CRC16). Преамбула – послідовність, що транслюється на початку пакету, її головна задача синхронізувати приймач з кадром, що надходить. SOP1 та SOP2 (Start of Packet) – передають інформацію про режим передачі даних. Data – дана частина пакету місить керуючу інформацію, можлива нульова довжина пакету, максимальна довжина 40 байтів, для режиму передачі 64-chip DDR максимальна довжина 16 байтів. CRC16 існує для перевірки на наявність помилок при передачі, дане поле створюється на основі довжини інформаційного поля.

Першим кроком необхідно просканувати ефір у пошуках певної преамбули необхідного пакету та передати прийнятий пакет в програмне забезпечення для обробки сигналів. Далі зважаючи на швидкість передачі пакету та довжини SOP за таблицями визначимо режим передачі даних в нашому випадку 64-chip 8DR. Кожний пристрій має свій унікальний SOP-код, за цим кодом приймачі визначають кому призначається пакет. Наступним полем, що необхідно проаналізувати є поле довжини пакету. Дане поле довжиною в один байт зашифроване за допомогою DSSS з використанням бітової послідовності псевдовипадкового шуму (PN-код). Поле даних також зашифровано у режимі передачі 8DR кожний символ представляє вісім бітів незашифрованих даних. 128 послідовностей PN-коду згенеровано на основі файлу DATA_CODE_ADR з регістром 0x23. Дані послідовності та стан коду (нормальний чи інвертований) використано для шифрування восьми бітів інформації. Однак, при цьому PN-коди обмежені дев'ятьма кодами на канал, а це вже можна зламати звичайним перебором у реальному часі. Маючи PN-код можна легко розшифрувати усе повідомлення.

Послідовність частотних стрибків можна вирахувати простим спостереженням за сигналом. Після складання таблиці стрибків можна починати атаку на БПЛА. Знаючи SOP та PN-код можна створити і відправити на БПЛА пакет, який переведе управління на новий пульт керування.

Перевага даного методу у тому, що не потрібно глушити сигнал основного пристрою керування. Крім того обладнання для атаки коштує трохи менше 100 доларів. Знання даного алгоритму дозволяє захистити власних дронів додатковими криптоалгоритмами. При одночасному використанні власних БПЛА та даного методу перехоплення БПЛА супротивника необхідно скласти списки SOP послідовностей власних дронів. Також БПЛА перехоплений даним методом можна перехопити повторно за допомогою такого ж комплекту обладнання.

## III. Висновки

Технологія пакетної передачі DSMX має серйозну вразливість до атаки за часом, спосіб реалізації якої розкрито у даній роботі. Ключовим для реалізації даної атаки є відсутність криптографічного шифрування пакетів даних. Програмно-визначальна радіосистема дозволяє реалізувати даний спосіб атаки для будь-якої пакетної технології, що не має достатнього рівня захисту.

## Література References


[1] Протоколи в передавачах та приймачах: PWM, PPM, SBus, DSM2, DSMX, SUMD// Блог RCdetails. URL:https://blog.rcdetails.info/ protokoly-v-priemnikah-i-peredatchikah-pwm-ppm-sbus-dsm2-dsmx-sumd/ (Дата оновлення: 07.2017, дата звернення 30.09.2017).

[2] Опис пристрою bladeRF – the USB 3.0 Superspeed Software Defined Radio// Офіційний сайт компанії Nuand URL:https://www.nuand.com/ (Дата звернення: 30.09.2017)

[3] Software defined radio // інформаційний ресурс: Вікіпедія URL: https://uk.wikipedia.org/wiki/Software_Defined_Radio (Дата оновлення 31.10.2016, дата звернення: 28.09.2017)

[4] Обговорення: SOP in WirelessUSB LP // офіційний сайт компанії Cypress embedded in tomorrow URL: https://community.cypress.com/docs/DOC-12472. (Дата модифікації 24.12.2011, дата перегляду 28.09.2017)

[5] Специфікація для плати WirelessUSB LP 2,4 GHz Radio SoC // офіційний сайт компанії Cypress URL:www.cypress.com/ file/126466/download (Дата звернення: 30.09.2017)