Секція 1

РОЗРОБЛЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМУНІКАЦІЇ РОЮ ДРОНІВ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Васильєв О. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Клюшніков І. М.

Актуальність. В наш час для виконання комплексних завдань, де можуть застосовуватися безпілотні літальні апарати (БПЛА) як, наприклад, для проведення військової розвідки, або моніторингу об'єктів критичної інфраструктури є доцільним використання не одного, а рою БПЛА для підвищення гарантоздатності виконання завдань [1]. Проте збільшення кількості БПЛА для виконання завдання суттєво збільшує ризик бути атакованим, що в свою чергу підвищує актуальність питань пов'язаних з безпекою, надійністю та гарантоздатністю як всього рою, так і окремих БПЛА, що його формують.

Метою даної роботи є розробка програмно-апаратного комплексу для забезпечення безпеки комунікації БПЛА між собою та стацією керування, а також створення системи виявлення та запобігання вторгнень на основі технологій штучного інтелекту, розміщених на станції керування та на борту БПЛА для ефективної протидії атакам різного типу, наприклад: Denial of Service attack (DoS); Packet sniffing attack; Man-in-the-middle attack; Spoofing (GPS spoofing) attack; Jamming attack, і Wormhole attack [2]. І у разі загрози втрати зв'язку з оператором, навчити систему приймати рішення в умовах автономності БПЛА для продовження виконання завдань та проведення процедур на відновлення зв'язку з оператором.

Основні положення. Якщо проаналізувати існуючі рішення, то можна зробити висновок, що одні з них можуть добре працювати проти одних видів атак, але бути недієвими проти інших видів атак [2]. Наприклад, використання протоколу WPA2 може захисти канал зв'язку від перехоплення інформації, наприклад логіну та паролю від БПЛА [3], проте цей протокол не захистить від таких атак як Jamming які можуть створювати завади на будь-які радіочастоті, що робить неможливим комунікації з БПЛА, який потрапив в зону дії радіоелектронної боротьби (РЕБ) [4]. Слід зазначити, що атаки можуть комбінуватися, наприклад, після проведення атаки Jamming яка змусить БПЛА увімкнути режим «Return to home» - функція повернення додому, буде задіяна атака GPS spoofing, за допомогою якої зловмисник може коректувати траєкторію польоту БПЛА, який буде намагатися рухатися у напрямку станції керування за сигналами системи супутникової навігації [2].

Висновки. Тому виникає задача створення та розгортання апаратно-програмного комплексу з інтелектуальною системою виявлення та запобігання атак як на станції керування так і на БПЛА з застосуванням засобів штучного інтелекту – системи прийняття рішень, що забезпечить адаптивну автономність БПЛА у разі втрати зв'язку з станцією керування. Та для підвищення ефективності протидії атакам на рій БПЛА планується розроблення БПЛА-приманок [5], які будуть мати визначені точки вразливості та задачею цих БПЛА є навмисне ініціювання кібератаки, з метою визначення методів атаки та викриття порушника.

Список літератури

1. Securing Against DoS/DDoS Attacks in Internet of Flying Things using Experience-based Deep Learning Algorithm. *Researchgate*. URL – https://www.researchgate.net/publication/350171510_Securing_Against_DoSDDoS_Attacks_in_Internet_of_Flying_Things_using_Experience-based_Deep_Learning_Algorithm (дата звернення: 29.04.2023);
2. Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey.*Researchgate*.URL:https://www.researchgate.net/publication/353212475_Fast_Reliable_and_Secure_Drone_Communication_A_Comprehensive_Survey (дата звернення: 30.04.2023);
3. Defense Techniques Against Cyber Attacks on Unmanned Aerial Vehicles. *Researchgate*.URL: https://www.researchgate.net/publication/328135272_Defense_Techniques_Against_Cyber_Attacks_on_Unmanned_Aerial_Vehicles (дата звернення: 30.04.2023);
4. A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception. *MDPI*. URL: https://www.mdpi.com/2079-9292/11/19/3025 (дата звернення: 29.04.2023);
5. HoneyDrone: A medium-interaction unmanned aerial vehicle honeypot.*Researchgate*. URL: https://www.researchgate.net/publication/326280510HoneyDrone_A_mediuminteraction_unmanned_aerial_vehicle_honeypot (дата звернення: 15.04.2023).

Відомості про авторів

Васильєв Олексій Вадимович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», o.v.vasyliev@student.csn.khai.edu

Клюшніков Ігор Миколайович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., старший науковий співробітник, i.kliushnikov@csh.khai.edu