УДК 004.056.53

МЕТОДИ ВИЯВЛЕННЯ АТАК НА СИСТЕМУ НАВІГАЦІЇ БПЛА. Частина 2

Головко М. А.
Науковий керівник – к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки, каф. МІРЕС
м. Харків, Україна
e-mail: maksym.holovko@nure.ua

This paper discusses the implementation of methods for protecting unmanned aerial vehicles from global positioning system spoofing attacks. A new self-diagnosis method is proposed, which allows the UAV to independently assess the presence of changes in its subsystems and identify signs of a cyber attack.

В результаті проведеного аналізу поточного стану досліджень в сфері виявлення атак на навігаційну систему БПЛА можна зробити висновок, що задача детектування та запобігання атакам на систему навігації БПЛА досить актуальна і не вирішена досі.

Можливим варіантом вирішення цієї проблеми є алгоритм виявлення атаки на систему GPS БПЛА на основі його кібер-фізичних параметрів:

1) завантаженість центрального процесору (ЦП);

2) висота польоту БПЛА (h);

3) стан фіксації за супутниками (Gs);

4) невизначеність GPS (Gu);

5) шум GPS (Gn);

З урахуванням цих параметрів алгоритм виявлення аномалій можна подати у вигляді наступних кроків:

1. Фіксація «сирих» значень аналізованих кібер-фізичних параметрів протягом певного проміжку часу.

2. Побудова відповідного типу розподілу для зібраних кібер-фізичних параметрів.

3. З використанням ковзного вікна здійснити вибірку попередніх значень та доповнити їх зібраними в новий момент часу, побудувати часовий ряд значень.

4. Побудова нового розподілу для нових значень за тим самим законом розподілу.

5. Обчислення значення дивергенції Кульбака-Лейблера [14] двох аналізованих функцій розподілу.

6. Чим вище отримане значення дивергенції Кульбака-Лейблера, тим більша ймовірність, що на БПЛА впливає атака або зовнішній деструктивний вплив (наприклад, швидкість двигунів та висота польоту можуть бути не пов'язані з атакою, а можуть змінюватися через пориви вітру). Зазвичай таке значення має перевищувати чи дорівнювати 2 [15].

7. Повторити алгоритм для наступних нових значень кіберфізичних параметрів, починаючи з пункту 3 (зсув вікна).

8. В якості допоміжного параметру пропонується використовувати ентропію зібраних значень кібер-фізичних параметрів. Чим вище значення ентропії, тим більша ймовірність, що зміна кіберфізичного параметру говорить про наявність аномальної поведінки.

Перевагою запропонованого методу є його обчислювальна «легкість» та енергоефективність. Також, оскільки метод дозволяє аналізувати будь-які параметри і може працювати з будь-якими доступними даними, немає значення, якими датчиками оснащений БПЛА.

За допомогою розробленого методу можна як виявляти аномалії, так і оцінювати зміну закономірностей поведінки БПЛА, зміну його станів. Якщо значення ентропії не надто високі, і має місце одноразове збільшення, то це може вказувати на зміну режиму польоту. Співвідношення аналізованих параметрів дозволяє однозначно виявити атаку та визначити її тип. Кожна атака стосується певного набору підсистем, тому тип атаки можна охарактеризувати за результуючими параметрами, на які вона впливає. Дані, зібрані у вигляді часових рядів, можуть бути використані для навчання нейронних мереж щодо виявлення атаки та використання захисних мір.

Список використаних джерел

1. Semanjski S., Semanjski I., Wilde W.D., Gautama S. Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data – Part II. Sensors. 2020. № 20(7):1806. pp. 1-15.

2. Kwon K.-C., Shim D.-S. Performance analysis of direct GPS spoofing detection method with AHRS/Accelerometer. Sensors. 2020. № 20(4):954.

3. Wan W., Kim H., Hovakimyan N., Sha L., Voulgaris P.G. A Safety Constrained Control Framework for UAVs in GPS Denied Environment. 59-th IEEE Conference on Decision and Control (CDC). Korea (South). 2020. pp. 214-219.

4. Seo S.-H., Lee B.-H., Im S.-H., Jee G. Effect of spoofing on unmanned aerial vehicle using counterfeited GPS signal. Journal of Positioning Navigation and Timing. 2015. № 6. pp. 57-65.

5. Shepard D., Humphreys T., Fansler A. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. International Journal of Critical Infrastructure Protection. 2012. № 5(3-4). pp. 146-153

6. Jansen K., Schäfer M., Moser D., Lenders V., Pöpper C., Schmitt J. Crowd-GPS-sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks. Proc. IEEE Symp. Security Privacy (SP). San Francisco. CA. USA: IEEE. 2018. pp. 1018-1031.

7. Montgomery P.Y., Humphreys T.E., Ledvina B.M. Receiver-