УДК 621.396
DOI https://doi.org/10.32782/2663-5941/2024.5.1/10

Мустафаєв О.В.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

СУЧАСНІ ТЕХНОЛОГІЇ ЗАХИСТУ ВІД GPS СПУФІНГУ У СИСТЕМАХ НАВІГАЦІЇ

У сучасних умовах активного використання безпілотних літальних апаратів (далі – БПЛА) у різних сферах життя, включаючи військову, цивільну авіацію та морську навігацію, питання захисту від загроз, пов'язаних з GPS спуфінгом, набуває особливої актуальності. GPS спуфінг – це технологія створення і передачі підроблених GPS сигналів з метою введення в оману приймачів навігаційних систем. Такі атаки можуть мати серйозні наслідки, зокрема втрату контролю над БПЛА або відхилення від заданого маршруту, що може призвести до катастрофічних подій.

Стаття аналізує сучасні технології захисту від GPS спуфінгу, які використовуються для забезпечення безпеки та надійності навігаційних систем. Зокрема, розглянуто основні підходи до виявлення та запобігання атакам спуфінгу, такі як аналіз сили сигналу, використання диференційного GPS (DGPS), мультичастотних та багатосистемних приймачів, а також аутентифікація сигналів.

Окремо висвітлено перспективи застосування методів машинного навчання для аналізу GPS сигналів та виявлення аномалій, які можуть вказувати на спуфінгові атаки. Зокрема, розглянуто використання нейронних мереж для розпізнавання підроблених сигналів, що підвищує ефективність захисту та знижує кількість помилкових тривог. Також розглянуто інтеграцію інерційних навігаційних систем (INS) з GPS для виявлення невідповідностей між даними навігації з різних джерел, що дозволяє забезпечити автономну навігацію під час атаки.

У статті представлено аналіз сучасних досягнень у сфері захисту від GPS спуфінгу, що підкреслює важливість безперервного розвитку методів протидії, зокрема в критичних сферах, таких як військові операції, авіація та автономні транспортні засоби. Висновки роботи спрямовані на необхідність впровадження новітніх технологічних рішень для забезпечення надійності та безпеки навігаційних систем у сучасних умовах.

Ключові слова: *системи навігації, супутник, GPS спуфінг, сигнали завад, безпілотний літальний апарат, кібербезпека.*

Постановка проблеми. Сучасні БПЛА оснащені новітніми технологіями, камерами, радарами тощо. Однак, попри їхню значимість, використання БПЛА супроводжується низкою викликів, серед яких особливо виділяється проблема GPS спуфінгу [1].

Техніка GPS спуфінгу (GPS spoofing) полягає у створенні та передачі підроблених сигналів GPS, з метою введення в оману приймачів навігаційних систем. Такі атаки можуть призводити до серйозних наслідків, особливо у військовій сфері, авіації, морській навігації та для безпілотних транспортних засобів. Наприклад, якщо приймач не має жодного захисту, БПЛА реагуватиме на будь-яку спробу підміни сигналу, через що автопілот намагатиметься компенсувати зміни фальшивого положення. Це може призвести до того, що БПЛА залишить межі підконтрольної зони. З огляду на це, дослідження захисту від GPS спуфінгу є актуальним завданням, яке вимагає впровадження сучасних технологічних рішень.

Аналіз останніх досліджень і публікацій. З розвитком навігаційних систем і збільшенням їх залежності від GPS, проблема спуфінгу стає дедалі актуальнішою. Останні дослідження та публікації у цій сфері фокусуються на розробці нових технологій і підходів до захисту від таких атак. Отримані нові результати у цьому достатньо прогресивному напрямі представлені у роботах таких вчених, як: Бульба С.С., Волошин Д.Г., Кузьменко Н.С., Остроумов І.В., Петровський А.В., Харченко В.П., Afary A., Broumandan A., Bhatti J., Gonzalez R., Li X., Mojaradi B., Oligeri G., Sun C. та багато інших [2–4].

У наукових працях групи дослідників Корнельського університету, а саме: M. Psiaki, S. Powell, R. Mitch було запропоновано алгоритм для виявлення спуфінгу, який ґрунтується на апріорних знаннях про розташування супутників групами. Для реалізації алгоритму використовується нейронна мережа, що базується на класифікаторах MLP [5].

Варто зазначити, що більшість успішних результатів протидії спуфінгу розраховані на досить великі бюджети для їх реалізації (автоматизовані антени із специфічним програмним забезпеченням, новітні технології із залученням елементів штучного інтелекту тощо).

Фахівці з кібербезпеки зазначають, що головна проблема GPS систем полягає в слабких сигналах, які передаються з висоти приблизно 20 тисяч кілометрів над Землею, що призводить до перехоплення їх зловмисниками. Наприклад, дослідження в галузі криптографічного підписування сигналів і сертифікації з метою підтвердження їхньої достовірності стають все більш популярними. Ці методи передбачають використання спеціальних ключів для перевірки істинності сигналів.

Крім цього, досить складним завданням є створення спуфінгового поля в умовах міської забудови, де будівлі створюють перешкоди для відображення сигналу. До того ж радіоантени мають різну конфігурацію для справжніх сигналів, що надходять від супутників, і для сигналів перешкод, що ускладнює точне відтворення підроблених сигналів [6].

На основі аналізу наукових та практичних досягнень, в рамках тематики даної статті, виникає необхідність у розробці нових засобів радіоелектронної боротьби, засновані на фазочастотних методах вимірювання та обробки радіосигналів, оскільки, сучасні системи протидії часто характеризуються низькою енергоефективністю, обмеженим радіусом дії та високими витратами на виробництво. Представляє дослідницький інтерес розробка мобільних систем радіоелектронної боротьби, які могли б ефективно працювати із сучасними типами радіозв'язку, здійснювати вимірювання і генерацію радіосигналів, а також підтримувати канали для керування та передачі відеоінформації.

Постановка завдання. Мета статті – дослідження передових технологій захисту від GPS спуфінгу у системах навігації.

Виклад основного матеріалу. Під час вирішення практичних задач із участю БПЛА виникає необхідність у використанні GPS/GNSS для забезпечення високого рівня точності отриманих даних. Global Navigation Satellite System (GNSS) – це супутникова навігаційна система, призначена для визначення позиції об'єктів у просторі, тобто їхніх координат, напрямку руху, швидкості тощо. На сьогодні, близько 200 організацій, які збирають GNSS-дані з базових станцій по всьому світу, об'єднані в IGS (Міжнародну службу GNSS), що входить до складу Міжнародної асоціації геодезії. Найбільш ключовими та перспективними є такі GNSS системи: GPS (США), GELILEO (Євросоюз), BeiDou (Китай), QZSS (Японія).

Для забезпечення надійного захисту навігаційних систем від потенційних загроз необхідне створення ефективної системи протидії спуфінгу. Розглянемо загальний алгоритм моделювання протидії спуфінгу:

1) аналіз вимог і визначення цілей (визначаються основні вимоги до системи захисту, зокрема, які загрози необхідно нейтралізувати, якими повинні бути параметри захищеності та точності);

2) розробка математичної моделі сценарію атаки (модель має містити параметри супутникових сигналів, алгоритми обробки сигналів у приймачі, а також методи виявлення аномалій, які можуть свідчити про спуфінгову атаку);

3) розробка та впровадження алгоритмів виявлення спуфінгу (розробляються алгоритми, до яких можуть входити аналіз потужності та характеристик сигналу, використання криптографічних методів для аутентифікації сигналів, інтеграція інерційних навігаційних систем для порівняння даних з незалежними джерелами тощо);

4) моделювання та симуляція сценаріїв спуфінгу (моделювання роботи навігаційної системи під впливом підроблених сигналів і перевірка роботи розроблених алгоритмів виявлення і захисту);

5) аналіз результатів та оптимізація (визначається ефективність алгоритмів виявлення спуфінгу, оцінюються їх точність, швидкість і надійність та, за необхідності, проводиться оптимізація параметрів системи та алгоритмів для покращення її продуктивності);

6) реалізація в реальних умовах і тестування (перевірка роботи системи у реальних умовах експлуатації, щоб оцінити її ефективність і надійність при реальних атаках спуфінгу).

В цілому результати моделювання GPS спуфінгу можуть буті взяті за основу для розробки та вдосконалення існуючих стандартів та рекомендацій щодо безпеки навігаційних систем. Це сприяє встановленню єдиних вимог і підходів до захисту від спуфінгу на міжнародному рівні.

Крім цього, моделювання дозволяє створювати реалістичні сценарії атак для навчання фахівців з кібербезпеки та операторів систем навігації.

Методи протидії спуфінговим атакам спрямовані на виявлення спровокованих сигналів завад. Вони можуть бути ідентифіковані за допомогою різних підходів, таких як:

– аналіз потужності вхідного сигналу (здійснюється контроль вхідної потужності сигналу, оскільки під час атаки вона може значно зрости через високу потужність сигналів перешкод і досягається шляхом спостереження за коефіцієнтом підсилення в модулі автоматичного регулювання підсилення);

– структурний аналіз потужності сигналів (використовуються циклостаціонарні властивості сигналів GNSS для виявлення підозрілих збільшень потужності структурованих сигналів, таких як коди розширення у прийнятих даних);

– оцінка співвідношення сигнал/шум (для кожного приймача визначають граничну верхню межу значення сигнал/шум, надмірне відхилення від якої вказує на спуфінгову атаку);

– моніторинг якості сигналу SQM (здійснюється ідентифікація асиметричних, аномально різких або підвищених піків кореляції);

– контроль часу прибуття сигналів (необхідно здіснювати моніторинг показники відстані між антенами спуфера і атакованого приймача, тому що такі відхилення провокують змінне зміщення годинника приймача, що дає змогу ідентифікувати спуфінгову атаку).

Класифікацію основних методів захисту від GPS спуфінгу наведено у Таблиці 1.

Попри потенційні переваги перелічених методів і підходів захисту, їх ефективність знижується через певні недоліки. Зокрема, інерційні навігаційні системи потребують постійного калібрування, що ускладнює їх використання. Також складність аналізу підроблених фреймів на комбінованих виходах GPS/INS та можливі проблеми з доступом до стільникового зв'язку і Wi-Fi у віддалених або важкодоступних районах значно ускладнюють точне виявлення спуфінгу. Крім того, допоміжні системи позиціонування, які синхронізуються за часом за допомогою GPS, потребують додаткового резервування даних для забезпечення надійності.

Окрему увагу варто приділити методам, що використовують додаткову інформацію з візуальної одометрії (альтернативний метод для визначення позиції та переміщення об'єкта) та візуальної картографії в системах позиціонування. Проте, висока потреба в обчислювальних ресурсах і значні витрати обмежують практичне застосування цього методу.

У свою чергу, технічні засоби візуальної одометрії використовуються як додатковий інструмент у захисті від спуфінгу. Вони працюють незалежно від GPS та інших радіочастотних сигналів, що робить їх ефективним засобом в умовах радіочастотних завад.

Беручи до уваги опис значної кількості наявних технологій для захисту від GPS спуфінгу, які наведені у Таблиці 1, можна констатувати, що жодна з них не є абсолютно надійною та стабільною у сучасних реаліях стрімкого розвитку нанотехнологій. Зловмисники постійно розробляють нові методи атак, що змушує науковців і інженерів шукати вдосконалені рішення. Перспектив-

Таблиця 1

Методи захисту від GPS спуфінгу

Назва методу	Опис
Аналіз потужності сигналу та його характеристик	Один із простих методів захисту від спуфінгу полягає у моніторингу сили сигналу GPS. У випадку атаки спуфінгом, підроблені сигнали можуть мати значно вищу або нижчу силу порівняно з реальними сигналами супутників. Аналіз таких відхилень дозволяє виявляти спроби спуфінгу. Крім того, можна відслідковувати час приходу сигналів, їх частоту та фазу, щоб виявляти несумісності з реальними супутниковими сигналами.
Використання диференційного GPS (DGPS)	Технологія DGPS базується на використанні стаціонарних референцних станцій, які приймають сигнали GPS і передають корекційні дані мобільним приймачам. У разі спуфінгу, підроблений сигнал не буде узгоджуватися з корекційними даними від референцних станцій, що дозволить ідентифікувати загрозу. DGPS може значно підвищити точність і надійність навігації, знижуючи ймовірність успішної атаки.
Мультичастотні та багатосистемні приймачі	Сучасні навігаційні приймачі здатні працювати з сигналами від кількох супутникових систем, таких як GPS, ГЛОНАСС, Galileo та BeiDou, і приймати сигнали на різних частотах. Використання мультичастотних та багатосистемних приймачів підвищує стійкість до спуфінгу, оскільки для успішної атаки необхідно підробити сигнали всіх систем і частот, що є значно складнішим завданням.
Аутентифікація сигналів	Для захисту від спуфінгу можуть використовуватись криптографічні методи аутентифікації сигналів. Наприклад, у системі Galileo введено службу Open Service Navigation Message Authentication (OS-NMA), яка забезпечує перевірку автентичності сигналів, що передаються. Такі методи аутентифікації ускладнюють підробку сигналів, оскільки зловмисникам необхідно не тільки згенерувати правильний сигнал, але й правильно його підписати.
Фільтрація на основі машинного навчання	Застосування алгоритмів машинного навчання для аналізу сигналів GPS дозволяє розпізнавати аномалії, що можуть вказувати на спуфінг. Наприклад, нейронні мережі можуть навчатися розпізнавати типові характеристики підроблених сигналів, що дозволить виявляти атаки навіть за невеликих відхилень від норми. Цей підхід дозволяє підвищити ефективність захисту та зменшити кількість помилкових тривог.
Інтеграція з інерційними навігаційними системами (INS)	Інерційні навігаційні системи працюють на основі даних від акселерометрів і гіроскопів, які не залежать від супутникових сигналів. Інтеграція INS з GPS дозволяє виявляти невідповідності між даними навігації з різних джерел. У разі спуфінгу INS може забезпечувати автономну навігацію, поки не буде відновлено довіру до GPS-сигналів.

ними напрямками є поєднання кількох технологій одночасно, використання квантової криптографії для аутентифікації сигналів, а також розробка глобальних стандартів захисту навігаційних систем.

Висновки. Захист від GPS спуфінгу є важливою складовою забезпечення безпеки сучасних навігаційних систем. Різноманітні технології, такі як аналіз сигналів, диференційний GPS, мультичастотні приймачі, аутентифікація, машинне навчання та інтеграція з INS, дозволяють підвищити стійкість до атак. Проте постійний розвиток технологій спуфінгу вимагає від дослідників безперервного вдосконалення методів захисту, що забезпечить надійність і безпеку в критичних сферах, таких як авіація, військові операції та автономні транспортні засоби.

Незважаючи на велику кількість наявних методів захисту, жоден з них не є абсолютно надійним, що обумовлює необхідність подальшого вдосконалення технологій захисту. Зокрема, перспективними напрямами є поєднання кількох технологій одночасно, використання квантової криптографії для аутентифікації сигналів, а також розробка глобальних стандартів захисту навігаційних систем.

Список літератури:

1. Матійчик М., Качало І. Тенденції застосування безпілотних повітряних суден в цивільній авіації. Матеріали XI міжнародної наук.-техн. конфер. “ABIA 2013”. 2013. С. 97.

2. Milaat F.A. and Liu H. Decentralized Detection of GPS Spoofing. IEEE Commun. Lett. № 22. 2018. P. 1256–1259

3. Ostroumov I.V., Marais K., Kuzmenko N.S. Aircraft positioning using multiple distance measurements and spline prediction. Aviation. 2022. № 26(1). P. 1–10 doi: 10.3846/aviation.2022.16589.

4. Sun C., Cheong J.W., Dempster A.G., Zhao H., Demicheli L., Fen W. A. New Signal Quality Monitoring Method for Anti-spoofing. China Satellite Navigation Conference (CSNC) Proceedings, Springer. Singapore. 2018. P. 221–231.

5. Varshosaz M., Afary A., Mojaradi B., Saadatseresht M. Spoofing Detection of Civilian UAVs Using Visual Odometry. ISPRS International Journal of Geo-Information № 9. Ebadat. 2019. doi: https://doi.org/10.3390/ijgi9010006.

6. Wildemeersch, M. and Fortuny-Guasch, J. Radio Frequency Interference Impact Assess-ment on Global Navigation Satellite Systems. Ispra (VA), Italy. 2010. doi: 10.2788/6033.

Mustafaiev O.V. MODERN TECHNOLOGIES OF PROTECTION AGAINST GPS SPOOFING IN NAVIGATION SYSTEMS

In today's conditions of active use of unmanned aerial vehicles in various spheres of life, including military, civil aviation and maritime navigation, the issue of protection against threats related to GPS spoofing becomes especially relevant. GPS spoofing is a technology for creating and transmitting fake GPS signals in order to mislead receivers of navigation systems. Such attacks can have serious consequences, including loss of control of the UAV or deviation from the given route, which can lead to catastrophic events.

The article analyzes modern protection technologies against GPS spoofing, which are used to ensure the safety and reliability of navigation systems. In particular, the main approaches to detecting and preventing spoofing attacks are considered, such as signal strength analysis, the use of differential GPS (DGPS), multi-frequency and multi-system receivers, as well as signal authentication.

The prospects of using machine learning methods for analyzing GPS signals and detecting anomalies that may indicate spoofing attacks are highlighted separately. In particular, the use of neural networks to recognize fake signals is considered, which increases the effectiveness of protection and reduces the number of false alarms. Also considered is the integration of inertial navigation systems (INS) with GPS to detect inconsistencies between navigation data from different sources, allowing for autonomous navigation during an attack.

Despite the large number of available protection methods, none of them is absolutely reliable, which determines the need for further improvement of protection technologies. In particular, promising directions are the combination of several technologies at the same time, the use of quantum cryptography for the authentication of signals, as well as the development of global standards for the protection of navigation systems.

The article presents an analysis of current advances in GPS spoofing protection, highlighting the importance of continuous development of countermeasures, particularly in critical areas such as military operations, aviation, and autonomous vehicles. The conclusions of the work are aimed at the need to implement the latest technological solutions to ensure the reliability and safety of navigation systems in modern conditions.

Key words: *navigation systems, satellite, GPS spoofing, interference signals, unmanned aerial vehicle, cyber security.*