

УДК 004.056.57 + 519.87

Гордієнко А.В.¹, Дубровін В.І.²

¹ студ. гр. КНТ-222 НУ «Запорізька політехніка»

² канд. техн. наук, проф. НУ «Запорізька політехніка»

МУЛЬТИФРАКТАЛИ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК

Розвиток IoT та мобільних мереж вимагає ширшої, швидшої та безпечнішої інфраструктури. Для боротьби зі зловмисними атаками розроблено алгоритм AMDES (система виявлення вторгнень з мультифрактальним аналізом безпілотних літальних апаратів), що поєднує мультифрактальний аналіз та машинне навчання для точного виявлення атак підробки. Методологія успішно застосована для виявлення атак спуфінгу в мережах безпілотних літальних систем (UAS), що підкреслює її ефективність у підтримці безпеки цих систем.

Запропонована методологія виявлення вторгнень – IDS Framework.

Дослідження зосереджено на аналізі корисного навантаження мережеских пакетів замість мережевої статистики, особливо у випадку прихованих атак типу MITM. IDS використовує двоетапний процес: збір мережевої інформації через датчики та обробка даних для виявлення характеристик. Перший крок фокусується на характеристиках трафіку для

визначення сигнальних підписів, а другий - на автоматичній класифікації цих підписів через нейронну мережу для активації оповіщень або протидій.

Запропонована методологія виявлення вторгнень – мультифрактальний аналіз вейвлет-лідера.

Мультифрактальний аналіз вейвлет-лідера (WLM) дозволяє фіксувати різні рівні щільності сингулярностей сигналу в різних часових масштабах, що є ефективним проти атак затоплення в бездротових мережах UAS. Цей метод використовується для аналізу магнітного поля та оцінки спектру магнітного поля точніше за рахунок заміни розмірності Херста на структурну функцію WLM. Аналіз WLM дозволяє оцінити мінливість часових рядів, включаючи геопозиціонування літальних апаратів, та ефективно розрізняти різні типи даних. Інструмент MATLAB WLM забезпечує просте рішення для оцінки спектру магнітного поля шляхом обчислення функції масштабування з використанням лідера вейвлетів.

Запропонована методологія виявлення вторгнень – класифікація підписів машинного навчання

Класифікація підписів машинного навчання в системах виявлення вторгнень є важливою. Дослідження показують, що методи машинного навчання, зокрема LSTM, ефективніше за аналітичні методи, особливо для DoS-атак. LSTM - це модифікована форма рекурентної нейронної мережі, яка зберігає пам'ять протягом тривалого часу та уникає проблеми зникнення градієнта[2]. Запропонована модель використовує двонаправлену структуру мережі LSTM (BiLSTM) з оригінальним та додатковим рівнем LSTM, що підвищує здатність мережі розуміти контекст сигналу.

Застосування до експериментальних даних – моделювання мобільності UAS

Щоб продемонструвати здійсненність такої методології, за відсутності фізично працюючої UAS, дослідники розробили тестовий стенд на основі попередньо записаних мережових записів RADAR. Замість того, щоб застосовувати моделі мобільності випадкової ходьби, які використовувалися в інших дослідженнях, вони вважали, що профілі місії та моделі мобільності сучасних літаків є більш придатними представленнями складної UAS.

Записи RADAR служили відображенням того, що спостерігає наземна станція управління БПЛА у мережі БПЛА через такі причини:

- корисне навантаження. БПЛА повідомляли про своє місцезнаходження для внутрішнього контролю і планування маршруту;
- мобільність. БПЛА могли приєднуватися до мережі та покидати її в будь-який час, і ця поведінка фіксувалась за допомогою RADAR;
- інфраструктура UAS. Система UAS значною мірою залежить від існуючих інфраструктур, подібних до інфраструктури цивільної авіації;

– схеми руху. Схеми руху літаків схожі на моделі робочого стану безпілотних систем.

Застосування до експериментальних даних – евклідова відстань перед обробкою.

Порівнюючи LSTM з SVM для класифікації, виявлено, що LSTM трохи кращий. Проте ефективність обох методів залежить від їх дизайну та оптимізації. Введення SVM допомогло краще зрозуміти можливу продуктивність IDS (системи виявлення вторгнень).

Ми розібрали інноваційний підхід для виявлення мережових атак підробки, який використовує класифікацію нейронних мереж для покращення нашого IDS. Ці експерименти показали обіцяні попередні результати, підтверджуючи ефективність цієї нової конструкції з високою точністю виявлення і мінімальними помилковими позитивними результатами. Цей метод спрямований на специфічні типи вторгнень, особливо у мобільних мережах.