УДК 004.056 EDN VJWCAA

Метод адаптивного подавления ложных тревог детектора аномалий в зонах гарантированных радиопомех

В.И. Пронин*, Д.А. Диканский, К.А. Неборачек, Н. Дибров, С.А. Горяйнов

Северо-Кавказский федеральный университет, Ставрополь, Россия

*E-mail: vladinfotech23@gmail.com

Аннотация. Предложен метод адаптивного подавления ложных тревог детектора аномалий для роя БПЛА в зоне радиопомех. Порог изменяется пропорционально уровню помех. Предусмотрены ограничение максимального порога и его экстренное снижение при подтверждении атаки. Экспериментально ложные тревоги снижены с 41% до 9% при полноте обнаружения 0,78-0,82. Метод не требует переобучения.

Ключевые слова: детектор аномалий, ложные тревоги, радиопомехи, адаптивный порог, рой БПЛА, робастность, подавление помех.

Method of adaptive suppression of false alarms of an anomaly detector in guaranteed radio interference zones

V.I. Pronin*, D.A. Dikansky, K.A. Neborachek, N. Dibrov, S.A. Goryainov

North-Caucasus Federal University, Stavropol, Russia

*E-mail: vladinfotech23@gmail.com

Abstract. A method for adaptive false alarm suppression of an anomaly detector for a UAV swarm in a radio interference zone is proposed. The threshold is adjusted proportionally to the interference level. Two mechanisms are provided: a maximum threshold cap and its emergency reduction upon attack confirmation. Experiments show false alarms reduced from 41% to 9% with attack detection recall of 0.78-0.82. The method requires no retraining.

Keywords: anomaly detector, false alarms, radio interference, adaptive threshold, UAV swarm, robustness, interference suppression.

1. Введение

В реальной эксплуатации рои БПЛА попадают в зоны с гарантированно высоким уровнем радиопомех – районы работы средств РЭБ, промышленные площадки с мощным электромагнитным фоном, грозовые фронты, плотную городскую застройку. Штатный детектор аномалий, настроенный на типовой уровень шума, в таких условиях начинает генерировать лавину ложных тревог. Телеметрия искажается, пакеты бьются, показания датчиков плывут, и детектор принимает эти артефакты за аномалии.

Проблема усугубляется тем, что оператор или автоматическая система реагирования, столкнувшись с потоком ложных срабатываний, перестаёт на них реагировать. Реальная атака, происходящая в зоне помех, легко пропускается.

Классические методы адаптации порога – CUSUM, EWMA, скользящее среднее – не учитывают внешний фактор «зона гарантированных помех». Они реагируют на сами отклонения, а не на их причину. Повышение чувствительности детектора при помехах только ухудшает картину, а полное отключение детектора недопустимо.

Мы предлагаем метод, который не снижает чувствительности детектора, а корректирует его порог срабатывания по измеренному уровню помех. Способность замечать реальные атаки сохраняется за счёт независимого канала верификации.

2. Обзор литературы

Проблеме ложных тревог в обнаружении аномалий посвящено много работ. Классические схемы CUSUM и EWMA адаптируют порог по истории ошибок [1], но не различают природу аномалии – помеха это или атака.

Робастное обнаружение аномалий в условиях шума исследуется в [2], однако без механизма привязки к известным зонам деградации канала. Методы обнаружения аномалий в каналах связи при радиопомехах исследуются в [3], но работают они независимо от детектора аномалий.

Современные подходы к обнаружению радиопомех с использованием глубокого обучения демонстрируют высокую точность [4]. Интеграция информации об уровне помех в решающее правило детектора в явном виде встречается редко.

В данной работе предпринята попытка связать уровень радиопомех с порогом детектора аномалий и оценить эффективность такого подхода в симуляции.

3. Постановка задачи

Рассматривается рой из N БПЛА, движущийся в двумерном пространстве. Каждый агент оснащён детектором аномалий, который на каждом такте t вычисляет статистику $\xi(t)$ (отклонение от прогноза, взаимная информация действий, невязка телеметрии). При превышении порога τ фиксируется аномалия.

Известна карта зон гарантированных помех, либо уровень помех оценивается в реальном времени по метрикам канала – BER, SNR, RSSI. Уровень помех в момент t обозначим $J(t)$. При $J(t) > J_{thr}$ среда считается «зоной помех».

В зоне помех штатный детектор с фиксированным порогом τ_0 выдаёт ложные тревоги с частотой FAR_{high}, а реальные атаки продолжают происходить.

Требуется построить правило адаптации порога $\tau(t)$, при котором: в зоне помех частота ложных тревог существенно снижается, полнота обнаружения реальных атак не падает ниже заданного уровня, метод не требует переобучения детектора, после выхода из зоны помех штатный режим восстанавливается автоматически.

4. Предлагаемый метод

Метод состоит из четырёх основных механизмов: оценка уровня помех, адаптивное изменение порога, гистерезисное переключение режимов и экстренное снижение порога при верификации атаки.

Оценка уровня помех. Уровень помех J(t) оценивается по частоте битовых ошибок BER, отношению сигнал/шум SNR или уровню принимаемого сигнала RSSI.

Выбор BER обусловлен тем, что при фиксированном пороге детектора рост BER напрямую коррелирует с увеличением числа ложных тревог, что подтверждено предварительными экспериментами.

Для практики достаточно любого из этих параметров, приведённого к диапазону [0,1], где 0 – отсутствие помех, 1 – полная деградация связи.

Адаптивное изменение порога. В штатном режиме ($J(t) \leq J_{thr}$) порог равен базовому значению τ_0.

При входе в зону помех ($J(t) > J_{thr}$) порог увеличивается по линейному закону:

$$\tau(t) = \tau_0 \cdot \left(1 + k \cdot \frac{J(t) - J_{thr}}{1 - J_{thr}}\right), \quad k \in [0, k_{max}],$$

где k – коэффициент адаптации, k_{max} – максимально допустимое повышение порога, определяемое экспериментально так, чтобы не пропускать реальные атаки.

Повышение порога означает, что детектор срабатывает только на более сильные отклонения. Это не ослабление защиты, а отсев помехового шума.

Защитные механизмы. Чтобы порог не рос неоправданно, введены два ограничения:

1. Ограничение максимального порога: $\tau(t) \leq \tau_{max}$. Значение τ_{max} подбирается как наименьший порог, при котором частота ложных тревог в зоне помех не превышает 5–10%, а полнота обнаружения реальной атаки остаётся не ниже 0,75.

2. Ограничение длительности повышенного порога: если детектор находится в режиме подавления дольше T_{max} тактов, порог постепенно снижается к τ_0, даже если помехи не уменьшились. Это предотвращает «привыкание» и пропуск медленных атак.

Экстренное снижение порога при верификации атаки. В зоне помех детектор с повышенным порогом может не заметить реальную атаку. Для подстраховки работает независимый контур верификации: анализ данных от независимых датчиков (например, инерциальная система против GPS), сравнение показаний соседних БПЛА (консенсус), сигнал от внешнего источника – оператора или наземной станции.

При получении подтверждения атаки порог временно снижается до τ_0 (или ниже) на T_{boost} тактов, чтобы детектор зафиксировал аномалию и запустил ответные действия.

Гистерезис. Для устранения дребезга на границе зоны помех введён гистерезис: - режим подавления включается после того, как $J(t) > J_{thr}$ в течение T_{enter} тактов подряд, - выключается после T_{exit} тактов, когда $J(t) < J_{thr}$.

Типичные значения: $T_{enter} = 5–10$, $T_{exit} = 10–20$ тактов.

5. Экспериментальная среда

Эксперименты проводились в симуляторе движения роя на сетке 20×20. Рой состоял из 6 агентов, задача – следование маршруту с обходом препятствий.

В качестве штатного детектора использовался пороговый детектор, построенный на невязке между предсказанным (линейная экстраполяция) и фактическим положением агента. Базовый порог $\tau_0 = 0{,}15$ (нормированная ошибка).

Зоны помех задавались прямоугольными областями с уровнем $J = 0{,}7$. При нахождении в зоне к телеметрии добавлялся гауссовский шум с дисперсией, пропорциональной $J(t)$.

Рассмотрены три сценария:

1. Сценарий А (только помехи): рой входит в зону помех, реальных атак нет. Оценивается частота ложных тревог (FAR).

2. Сценарий Б (помехи + атака): в зоне помех происходит подмена телеметрии одного агента (линейный дрейф координат). Оценивается полнота обнаружения атаки (Recall).

3. Сценарий В (многократное пересечение границ): рой трижды входит и выходит из зоны помех. Оценивается устойчивость к смене условий.

Параметры метода: $J_{thr} = 0{,}5$, $k = 1{,}5$, $k_{max} = 2{,}0$, $\tau_{max} = 2{,}0 \cdot \tau_0$, $T_{enter} = 5$, $T_{exit} = 15$, $T_{max} = 500$ тактов.

6. Полученные результаты

Результаты сведены в таблицу 1.

Таблица 1. Сравнение фиксированного порога и адаптивного метода.

Сценарий	**Метод**	**FAR (ложные тревоги), %**	**Recall (полнота)**
А (только помехи)	Фиксированный порог	41,2	–
А	Адаптивный (предл.)	8,7	–
Б (помехи + атака)	Фиксированный порог	39,8	0,44
Б	Адаптивный (предл.)	9,1	0,78
В (многократные входы)	Фиксированный порог	44,3	–
В	Адаптивный (предл.)	8,2	–

Адаптивный метод снижает частоту ложных тревог в зоне помех в 4-5 раз. Полнота обнаружения реальной атаки растёт с 0,44 до 0,78: оператор перестаёт игнорировать тревоги, а дополнительный контур верификации помогает пробить повышенный порог.

Гистерезис полностью устранил дребезг: при многократном пересечении границ зоны не зафиксировано ни одного лишнего переключения режима.

Ограничение τ_{max} и временное окно T_{max} не дали порогу неоправданно завыситься в длительной миссии (1000 тактов в зоне помех).

Анализ результатов. Предложенный метод устойчив к трём главным проблемам, возникающим у детектора аномалий в зонах помех: лавина ложных тревог, дребезг на границах и потеря чувствительности к реальным атакам.

Чувствительность к параметру k умеренная: при изменении k на ±0,25 FAR меняется не более чем на 2 процентных пункта. Основной вклад в подавление ложных тревог даёт сам факт повышения порога, а не точное значение коэффициента.

Детектор без адаптации при высоком уровне помех даёт около 40% ложных тревог вне зависимости от длительности миссии. Предложенный метод сохраняет ложные тревоги ниже 10% даже при небольших отклонениях параметров симуляции, но требуют калибровки под конкретный детектор и типовой уровень помех.

7. Заключение

Разработан метод адаптивного подавления ложных тревог детектора аномалий для роя БПЛА в зонах гарантированных радиопомех. Порог срабатывания детектора повышается пропорционально уровню помех, но защитные механизмы – ограничение максимального порога и экстренное снижение при верификации реальной атаки – не дают пропустить угрозу.

Эксперименты показали, что частота ложных тревог падает с 41 до 9%, а полнота обнаружения реальных атак увеличивается с 0,44 до 0,78. Метод не требует переобучения детектора, обладает линейной вычислительной сложностью и может быть выполнен как легковесная надстройка.

Список литературы

1. An enhanced CLKAN-RF framework for robust anomaly detection in unmanned aerial vehicle sensor data / Ch. Li, W. Xie, B. Zheng [et al.] // Knowledge-Based Systems. – 2025. – Vol. 319. – P. 113690. – DOI 10.1016/j.knosys.2025.113690. – EDN KYCPYE.

2. Kim, S. Integrating Risk Assessment and Deep-Learning-Based Anomaly Detection for Efficient Risk-Informed Decision Making for Swarm Flight Robot Systems / S. Kim, H. Ahn // IEEE Transactions on Aerospace and Electronic Systems. – 2025. – Vol. 61, No. 5. – P. 13719-13731. – DOI 10.1109/taes.2025.3579483. – EDN CKVLQG.

3. Tariq, U. Tri-stream multi-model architecture for real-time detection of BeiDou signal manipulation in UAV swarms / U. Tariq, T. A. Ahanger, K. Shaukat // Scientific Reports. – 2026. – Vol. 16, No. 1. – DOI 10.1038/s41598-026-46655-y. – EDN VVGBRA.

4. Elyousseph, H. Robustness of Deep-Learning-Based RF UAV Detectors / H. Elyousseph, M. Altamimi // Sensors. – 2024. – Vol. 24, No. 22. – P. 7339. – DOI 10.3390/s24227339. – EDN NWFSGR.