Метод слияния данных и фильтрации аномалий на основе расстояния Махаланобиса для обеспечения целостности информации в группах автономных транспортных средств

Ю.А. Павелина, И.Ю. Попов

***Аннотация* — В работе рассматривается проблема обеспечения целостности информации в сетях V2X при информационном взаимодействии групп автономных транспортных средств (АТС). В условиях динамичной среды и наличия диверсантов, реализующих атаки типа False Data Injection (FDI), в которых классические методы линейного усреднения сенсорных данных приводят к критическим ошибкам управления. Предлагается метод слияния данных с адаптивным взвешиванием и фильтрацией выбросов на основе расстояния Махаланобиса. Проведен сравнительный эксперимент предложенного метода с подходами на базе евклидова расстояния и одномерной Z-оценки. Результаты показывают, что предложенный метод сохраняет высокую точность оценки состояния и устойчивость траектории при компрометации до 20% узлов группы.**

***Ключевые слова* — мультиагентные системы, автономные транспортные средства, целостность, обнаружение аномалий.**

I. Введение

Переход от изолированных автоматизированных систем к кооперативным группам автономных транспортных средств (уровни автоматизации 3 и 4) требует надежного обмена данными через сети V2X (Vehicle-to-Everything) [1]. В условиях плотного городского трафика агенты вынуждены объединять данные от собственных с информацией, получаемой от соседних АТС, для расширения возможности планирования и принятия решений. В связи с этим была предложена модель внешней среды [2], описывающая дорожную сцену и допустимые состояния объектов.

Однако проблемы искажения данных [3], такие как атаки False Data Injection (FDI), или деградация сенсоров легальных узлов создают прямую угрозу функциональной и информационной безопасности. При получении множества сообщений об одном и том же параметре среды (например, координатах препятствия) возникает задача слияния данных. Традиционные методы консенсуса, применяемые в VANET (Vehicular Ad-hoc Network) [4], уязвимы к скоординированным атакам смещения. Целью данной работы является разработка и экспериментальное исследование метода слияния данных, устойчивого к многомерным аномалиям в пространстве состояний АТС.

Следует отметить, что в реальных V2X-сценариях вектор состояния агента не ограничивается координатами и скоростью. На практике для кооперативной оценки обстановки используются также ускорение, ориентация кузова, угловые скорости, статусы исполнительных подсистем и иные телеметрические параметры. Поэтому, помимо базовой трехмерной постановки (x,y,v), в настоящей работе рассматривается расширенный сценарий с шестимерным вектором признаков $(x, y, v, a, \psi, \omega)$, что позволяет оценить масштабируемость метода при увеличении размерности пространства наблюдений.

II. Анализ подходов к выявлению многомерных выбросов

Процесс фильтрации искаженных данных требует использования метрик расстояния для отделения валидных данных от скомпрометированных. В контексте пространственно-кинематических данных АТС (координаты x, y скорость v) были проанализированы следующие подходы [5], применяемые в задачах обнаружения аномалий.

1. Евклидово расстояние. Метрика предполагает сферическое распределение данных. Ее главный недостаток – игнорирование корреляции между признаками. В навигационных задачах ошибки распределены эллиптически (продольная ошибка скорости коррелирует с продольным смещением координаты). Евклидова метрика часто помечает валидные данные на краях эллипса как аномалии (False Positives) и пропускает реальные атаки, направленные вдоль малых осей дисперсии.

2. Манхэттенское расстояние (L1) и Косинусное расстояние. L1-норма формирует ромбические области допустимых значений, которые сложно коррелируются с физическим описанием движения. Косинусное расстояние учитывает лишь направление вектора ошибки, игнорируя ее абсолютный модуль, что является сложно применимым для оценки метрических координат.

3. Z-оценка (стандартная оценка). Применение Z-оценки для каждой координаты независимо деформирует

реальные связи между признаками, разрушая структуру многомерного облака данных.

При росте размерности пространства признаков недостатки независимых одномерных критериев становятся ещё более выраженными. Если часть параметров кинематически и физически связана между собой, например пары (v, a) и (ψ, ω), то игнорирование ковариационной структуры приводит либо к росту ложных тревог, либо к пропуску согласованных атакующих смещений, распределённых по нескольким координатам пространства состояний. По этой причине многомерная робастная метрика в рассматриваемом классе задач является более естественным инструментом, чем семейство независимых пороговых тестов по отдельным координатам.

Для преодоления этих ограничений в работе применяется расстояние Махаланобиса [6], которое способно учитывать различие масштабов параметров и ковариационную структуру данных, приводя распределение к сферическому виду в пространстве главных компонент [7].

III. Метод слияния данных

Рассмотрим группу автономных транспортных средств (АТС), состоящую из n интеллектуальных агентов: $A = \{a_1, \dots, a_n\}$.

Будем считать, что время такой системы дискретно $T = \{0, t_1, \dots, t_q\}$.

В момент времени t каждый агент передаёт соседям вектор наблюдаемого состояния внешнего объекта или собственной кинематики:

$$z_j(t) \in \mathbb{R}^k.$$

Также агент a_i в момент времени t получает от соседних агентов множество сообщений $M_{i,j} = \{m_1, m_2, \dots, m_k\}$, о параметре внешней среды z.

В общем случае агент a_i получает сообщения только от подмножества соседей:

$$N_i(t) = \{a_j \in A: |p_i - p_j| \le R, link_{i,j} = 1\},$$

где R – радиус взаимодействия, $link_{i,j}$ отражает доступность канала связи в текущий момент времени с учётом потерь пакетов и асинхронности доставки. Таким образом, процедура слияния и обнаружения аномалий выполняется локально в динамически меняющемся подграфе взаимодействия

Каждому источнику a_j заранее назначен параметр обеспечения целостности $w_j(t)$, вычисляемый в соответствии с методом вычисления степеней доверия [8] на основе модели социальных сил и истории взаимодействий. Процесс обеспечения целостности включает следующие этапы:

Этап 1. Первичное взвешенное слияние.

Формируется базовая оценка $\hat{z}(t)$ как взвешенное среднее непрерывных параметров:

$$\hat{z}(t) = \frac{\sum_{j=1}^{k} w_j(t) \cdot z_j(t)}{\sum_{j=1}^{k} w_j(t)}.$$

Этап 2. Выявление выбросов (Outlier Detection).

Для каждого наблюдения $z_j(t)$ рассчитывается расстояние Махаланобиса до базовой оценки $\hat{z}(t)$:

$$D_M(z_j) = \sqrt{(z_j - \hat{z})^T \Sigma^{-1} (z_j - \hat{z})},$$

где Σ – ковариационная матрица наблюдений.

Наблюдение признается нарушающим целостность (выбросом), если:

$$D_M(z_j) > \tau_M,$$

где порог τ_M выбирается на основе χ^2-распределения с числом степеней свободы, равным размерности признакового пространства k. Для расстояния Махаланобиса используется критерий:

$$D_M^2 \sim \chi_k^2,$$

поэтому:

$$\tau_M = \sqrt{\chi^2_{k,0.99}}.$$

В частности, для трехмерного вектора (x, y, v) при доверительной вероятности 99% получаем $\tau_M \approx 3{,}37$, а для шестимерного вектора $(x, y, v, a, \psi, \omega)$ – $\tau_M \approx 4{,}10$.

Этап 3. Изоляция и перерасчет параметра обеспечения целостности.

Если наблюдение $z_j(t)$ признано выбросом, оно исключается из итогового слияния, а параметр обеспечения целостности источника снижается по принципу мультипликативного убывания:

$$w_j(t) = \gamma \cdot w_j(t-1),$$

где $\gamma \in (0,1)$ – коэффициент подавления.

При этом итоговая согласованная оценка состояния внешней среды пересчитывается только по валидным источникам информации.

В работе предлагается использовать агрессивное мягкое подавление (Soft Suppression) с $\gamma = 0{,}5$. Выбор этого коэффициента обусловлен необходимостью нейтрализовать скомпрометированный узел за 3-4 такта алгоритма, сохраняя при этом возможность восстановления репутации узла в случае единичного аппаратного сбоя сенсоров (в отличие от стратегии жесткой изоляции).

Пусть $m_i(t) = | N_i(t) |$ – число сообщений, доступных агенту a_i на шаге t, а k – размерность пространства признаков. Тогда вычисление взвешенного среднего требует $O(m_i, k)$ операций, робастная оценка ковариационной матрицы и её регуляризация – порядка $O(m_i, k^2)$ при малом фиксированном k, а вычисление расстояний Махаланобиса для всех входных наблюдений – $O(m_i k^2)$ при переиспользовании обратной матрицы ковариации. Следовательно, при практическом диапазоне $k \in [3{,}6]$ трудоёмкость одного шага алгоритма растёт почти линейно по числу соседей, что делает метод применимым к групповым V2X-сценариям с десятками и сотнями агентов.

IV. Экспериментальное исследование

Для оценки эффективности разработанного метода был реализован программный симулятор, имитирующий информационное взаимодействие группы АТС в условиях наличия легальных и скомпрометированных узлов. В вычислительном эксперименте рассматриваются базовый трехмерный вектор состояния (x, y, v), а также расширенное шестимерное пространство признаков $(x, y, v, a, \psi, \omega)$, а также сценарии частичной связности, асинхронности сообщений, задержек и потерь пакетов.

Вычислительный эксперимент был реализован на языке программирования Python (версия 3.10). Для реализации метода применялись следующие ключевые программные средства и библиотеки:

- NumPy – применялась для векторных и матричных вычислений, включая генерацию многомерного нормального распределения сенсорного шума с заданными параметрами ковариации, а также для эффективного пересчета весовых коэффициентов агентов.
- SciPy – использовалась для прямого расчета расстояния Махаланобиса и евклидова расстояния между векторами состояний.
- Scikit-Learn – применялась для реализации алгоритма Minimum Covariance Determinant (MCD) через модуль EllipticEnvelope. Данный инструмент позволил робастно оценивать матрицу ковариации Σ без учета выбросов, что критически важно при атаках FDI, когда агенты-диверсанты пытаются исказить саму форму эллипса дисперсии.
- Matplotlib, Plotly – использовались для визуализации двумерных и трехмерных проекций пространства признаков, построения доверительных эллипсоидов, а также для графического отображения динамики метрик точности и RMSE в процессе симуляции.
- Pandas – применялась для сбора, структурирования и агрегации результатов каждого из 100 прогонов симуляции (Run #) с последующим расчетом средних значений и доверительных интервалов для итоговой таблицы метрик.

Архитектура программного комплекса построена на принципах объектно-ориентированного программирования: каждый агент в сети представлен независимым объектом с собственным состоянием, сенсорной моделью, буфером входящих сообщений и модулем расчета индексов надежности соседей. Это позволило корректно имитировать децентрализованную природу информационного обмена в группе АТС.

Были рассмотрены три класса сценариев:

- Базовый сценарий: размерность $k = 3$, синхронный обмен, отсутствие потерь пакетов, радиус взаимодействия $R = 0{,}5$;
- Расширенный кинематический сценарий: размерность $k = 6$, где дополнительно учитываются ускорение a, ориентация ψ и угловая скорость ω;
- Сетевой сценарий повышенной реалистичности: размерность $k = 6$, частичная связность, случайные задержки доставки сообщений, потери пакетов и асинхронность обновлений

В ходе эксперимента для каждого сценария были смоделированы группа из 30 агентов, среди которых 20% выступали в роли диверсантов с пониженной достоверностью сообщений после 50-го временного шага. Атакующие согласованно внедряют в сеть вектор смещения d_{attack}, который на каждом такте плавно уводит передаваемые координаты от истинных (дрейф координат). Сила смещения подбирается таким образом, чтобы каждое отдельное сообщение нарушителя выглядело как правдоподобная сенсорная ошибка (что делает атаку невидимой для базовых фильтров), но за счет скоординированности группы атакующих их вес в линейном усреднении способен нарушить целостность общей оценки.

Все агенты $\Lambda = \{A_1, .., A_n\}$ в симуляторе объединены в систему, где каждый элемент может взаимодействовать друг с другом на некотором радиусе взаимодействия.

Входные параметры моделирования следующие:

- количество агентов: 30, выбрано как репрезентативный размер для плотного городского трафика или колонны АТС, обеспечивающий достаточное число взаимодействий для статистически значимых выводов;
- 20% агентов случайно выбираются как диверсанты – их поведение после определённого момента времени меняется;
- каждый агент имеет начальный параметр обеспечения целостности 1, что соответствует нейтральной позиции;
- радиус взаимодействия агентов: 0,5 нормализованное расстояние, соответствующее типичной дальности связи V2V (Vehicle-to-Vehicle) 200-300 м, в симуляторе пространство нормализовано к единичному квадрату;
- коэффициент снижения параметра обеспечения целостности при обнаружении аномалии $\gamma = 0.5$.

Измерения легальных АТС зашумлены в соответствии с двумерным нормальным распределением $\mathcal{N}(\mu, \Sigma_{\text{sensor}})$. Для имитации реальной работы лидаров и радаров распределение ошибок имеет выраженную ковариацию: дисперсия вдоль продольной оси движения (ошибка определения дальности) больше, чем поперечная (ошибка азимута)

Вычислительный эксперимент выполняется циклически для каждого временного такта $t \in [0, 99]$. Для обеспечения статистической значимости результатов весь сценарий прогоняется 100 раз, после чего метрики усредняются. На каждом такте t алгоритм симуляции выполняет следующие шаги:

Шаг 1. Генерация истинного состояния и измерений (Data Generation).

Истинное состояние объекта задаётся вектором:

$$Z_{true}(t) = (x(t), y(t), v(t), a(t), \psi(t), \omega(t)) .$$

В базовом сценарии используются только первые три компоненты. Движение формируется по кусочно-заданной кинематической модели: участки равномерного движения чередуются с участками разгона, торможения и плавного поворота.

Для каждого честного узла генерируется вектор наблюдения $z_j(t) = Z_{true}(t) + \epsilon_j(t)$, где $\epsilon_j(t)$, – многомерный гауссов шум с ковариационной структурой, отражающей связи между признаками $= (x, y, v, a, \psi, \omega)$.

Шаг 2а. Имитация атаки (Attack Injection).

Для $t < 50$ атакующие узлы ведут себя как честные, генерируя штатный шум.

Для $t \geq 50$ каждый скомпрометированный узел формирует ложное сообщение:

$$z_m(t) = Z_{true}(t) + d_{attack}(t) + \epsilon_m(t).$$

Вектор $d_{attack}(t)$ плавно нарастающий вектор смещения. В отличие от базового случая, в расширенном сценарии смещение распределяется по нескольким физически связанным координатам, например одновременно по (x, v, a) или по (y, ψ, ω), что затрудняет его выявление независимыми одномерными критериями.

Шаг 2б. Моделирование сетевых эффектов.

Для приближения к реальным V2X-условиям на каждом временном шаге формируется динамический граф взаимодействия. Агент получает сообщения только

от тех соседей, которые находятся в пределах радиуса взаимодействия R. Дополнительно для каждого канала моделируются:

- вероятность потери пакета p_{loss};
- случайная задержка доставки $d \in \{0, 1, 2\}$ такта;
- асинхронность обновлений, при которой не каждый сосед передаёт сообщение на каждом шаге. Если сообщение потеряно или задержано, агент либо не использует его, либо использует последнюю доступную версию, если её возраст не превышает допустимого порога устаревания.

Шаг 3. Первичное слияние и оценка параметров (Initial Fusion).

Алгоритм принимает на вход массив из 30 векторов наблюдений $z_1, \dots, z_{30}$.

Рассчитывается первичное взвешенное среднее $\hat{z}_{initial}$ с использованием текущих параметров обеспечения целостности $w_j(t)$.

На основе массива наблюдений вычисляется эмпирическая ковариационная матрица Σ. Для повышения робастности Σ оценивается с использованием алгоритма Minimum Covariance Determinant (MCD), чтобы исключить влияние атакующих на форму самого эллипсоида ошибок.

Шаг 4. Фильтрация аномалий (Anomaly Detection).

Для каждого наблюдения z_j рассчитывается расстояние Махаланобиса $D_M(z_j)$ относительно $\hat{z}_{initial}$ и матрицы Σ.

Наблюдения, для которых выполняется условие $D_M(z_j) > \tau_M = 3.37$, классифицируются как выбросы ($outlier\_flag\_j = 1$).

Шаг 5. Принятие решения и пересчет репутации (Decision & Update).

Формируется итоговая оценка состояния среды $\hat{z}_{final}(t)$. При этом наблюдения, помеченные как выбросы, полностью исключаются из расчета.

Веса источников обновляются:

Если $outlier\_flag\_j = 0$, параметр обеспечения целостности не изменяется: $w_j(t+1) = w_j(t)$.

Если $outlier\_flag\_j = 1$, применяется мягкое подавление: $w_j(t+1) = \gamma \cdot w_j(t)$, где $\gamma = 0{,}5$.

Шаг 6. Сбор метрик (Metrics Collection).

На каждом такте вычислялись:

- ошибка оценки состояния $RMSE(t) = \left|\left|\hat{z}_{final}(t) - Z_{true}(t)\right|\right|$;
- метрики бинарной классификации атакующих узлов: TPR, FPR, Precision и F1-Score
- среднее число соседей, доступных агенту в условиях частичной связности;
- среднее время выполнения одного шага алгоритма.

Сравниваются предсказанные флаги выбросов с реальным статусом узла (Честный/Диверсант) для вычисления метрик классификации (True Positive Rate, False Positive Rate, F1-Score).

Динамика поведения диверсантов меняется на 50-м временном шаге, после чего они увеличивают число сообщений со смещением данных. Их параметр снижается, и они исключаются из дальнейшего взаимодействия с группой.

Описанный алгоритм выполняется параллельно для четырех сравниваемых методов (без защиты, Евклидово расстояние - Euclidean Filter, стандартизированная оценка - Z-Score Filter и предложенный метод (Mahalanobis Fusion)), при этом для первых трех методов шаг пересчета весов w_j опускается, а критерии фильтрации на Шаге 4 заменяются соответствующими метриками.

Основной целью моделирования была проверка возможности предложенного метода обнаруживать агентов-диверсантов при информационном взаимодействии.

В таблице 1 представлены метрики эффективности алгоритмов за 100 прогонов симуляции. Для итоговых таблиц вычислялись средние значения и стандартные отклонения, а также 95%-ые доверительные интервалы.

Таблица 1. Сравнение эффективности методов слияния данных при 20% атакующих

Метод фильтрации	RMSE, средн. ± std	TPR, средн. ± std	FPR, средн. ± std	F1-Score, средн. ± std
Без защиты	1,84 ± 0,27	–	–	–
Euclidean Filter	0,92 ± 0,11	0,71 ± 0,05	0,14 ± 0,03	0,78 ± 0,04
Z-score Filter	0,88 ± 0,09	0,76 ± 0,04	0,11 ± 0,02	0,81 ± 0,03
Mahalanobis Fusion	0,21 ± 0,03	0,98 ± 0,01	0,02 ± 0,01	0,98 ± 0,01

Представление метрик в виде среднего значения и стандартного отклонения показывает, что выигрыш Mahalanobis Fusion по сравнению с базовыми методами является не случайным эффектом отдельных прогонов, а устойчивой тенденцией. Узкие интервалы разброса при высокой полноте обнаружения указывают на статистическую стабильность метода в рассматриваемом классе сценариев

Как видно из полученных данных, отсутствие защиты (Mean Baseline) приводит к критическому росту ошибки RMSE, так как злоумышленники успешно «отравляют» общую оценку.

Методы на основе евклидова расстояния и Z-оценки показывают высокий процент ложных срабатываний (FPR = 14.2% и 11.5% соответственно). Из-за того, что они не учитывают ковариацию, валидные измерения на краях нормального распределения ошибочно блокируются системой, а аккуратные смещения диверсантов (построенные с учетом независимых дисперсий) проходят фильтр.

Формирование эллипсоидной зоны допустимых значений предложенным методом позволило выявлять аномалии с полнотой 98% при минимальной доле ложных срабатываний (2%). Внедрение механизма штрафования параметра обеспечения целостности w_j привело к тому, что после 3-4 тактов атаки скомпрометированные узлы были полностью изолированы из информационного обмена, а ошибка оценки среды вернулась к уровню нормального сенсорного шума (RMSE = 0.21 м).

При частоте обновления 10 Гц (типичной для систем V2V) 3-4 шага соответствуют 0,3-0,4 секундам. Для автономных транспортных средств, движущихся со скоростью 60 км/ч (≈16,7 м/с), это означает прохождение

дистанции 6,7 метра с момента начала враждебного поведения до изоляции диверсанта. Это время реакции, учитывая необходимость накопления статистически значимого числа несоответствий для уверенного обнаружения аномалий в передаче информации.

В таблице 2 представлены метрики эффективности алгоритмов слияния данных в условиях различных значений размерности признаков.

Таблица 2. Сравнение эффективности методов слияния данных при различных значениях размерности признаков.

Метод фильтрации	Раз-мер-ность	RMSE	TPR	FPR	F1-Score
Euclidean Filter	$k = 3$	0,92	0,71	0,14	0,78
Euclidean Filter	$k = 6$	1,05	0,68	0,18	0,74
Z-score Filter	$k = 3$	0,88	0,76	0,11	0,81
Z-score Filter	$k = 6$	0,97	0,72	0,15	0,78
Mahalanobis Fusion	$k = 3$	0,21	0,98	0,02	0,98
Mahalanobis Fusion	$k = 6$	0,25	0,97	0,03	0,97

При увеличении размерности пространства признаков с 3 до 6 наблюдается умеренная деградация всех методов, однако для предложенного метода она существенно меньше, чем для методов на основе евклидова расстояния и Z-оценки. Это объясняется тем, что рост размерности в большей степени влияет на методы, не учитывающие совместную ковариационную структуру признаков.

Таблица 3. Зависимость эффективности обнаружения диверсантов от радиуса взаимодействия.

Радиус взаимод. R	Среднее число соседей	TPR	FPR	F1-Score	RMSE
0,3	6,4	0,93	0,04	0,93	0,31
0,5	11,8	0,97	0,03	0,97	0,25
0,7	17,6	0,98	0,02	0,98	0,23

Полученные результаты показывают, что уменьшение радиуса взаимодействия и, как следствие, локальной наблюдаемости действительно ухудшает качество обнаружения аномалий. Однако даже в условиях разреженного графа взаимодействия предложенный метод сохраняет высокую полноту и низкий уровень ложных срабатываний. Это позволяет считать его устойчивым к умеренной фрагментации связности, характерной для реальных V2X-сетей.

Таблица 4. Среднее время шага для различного числа агентов

Число агентов	Размерность	Среднее время шага, мс	Эквива-лентная частота, Гц
30	6	0,45	222
60	6	0,82	122
100	6	1,35	74

Для группы из 100 агентов и шестимерного пространства признаков среднее время одного шага остаётся существенно ниже 10 мс, что соответствует частоте выше 70 Гц на интерпретируемом прототипе. Следовательно, с учётом более эффективной реализации на бортовом вычислителе или в компилируемой среде можно считать заявленную применимость метода к режиму, близкому к реальному времени, обоснованной.

V. Ограничение исследования

Использованная модель остается упрощенной по отношению к полноразмерным V2X-сценариям. Во-первых, даже шестимерный вектор состояния не охватывает весь набор телеметрических параметров, встречающихся в реальных кооперативных системах, таких как статусы тормозной системы, сигналы поворота, диагностические коды и дискретные режимы исполнительных модулей. Во-вторых, препятствия и сложные коллективные манёвры в работе моделируются лишь опосредованно через изменение кинематических параметров и не представлены как полноценные интерактивные объекты среды. В-третьих, частичная связность рассматривается на уровне геометрического радиуса и вероятностной доступности канала, без детального моделирования протоколов нижних уровней стека связи.

полученные результаты следует трактовать как подтверждение работоспособности метода на уровне статистической фильтрации многомерных аномалий в локальном кооперативном взаимодействии, а не как исчерпывающую оценку поведения всей V2X-инфраструктуры. Полноценная интеграция в реалистичные транспортные симуляторы, учитывающие препятствия, перестроения, неоднородную топологию движения и сетевые протоколы, является направлением дальнейших исследований.

VI. Заключение

Предложенный метод слияния данных, основанный на обнаружении выбросов с помощью расстояния Махалонобиса, повышает безопасность кооперативного управления АТС. Доказано, что использование метрики Махаланобиса для проверки прагматической целостности входящей информации позволяет корректно учитывать многомерную специфику кинематических данных. Экспериментальное сравнение подтвердило, что предложенный подход снижает ошибку оценки в условиях скоординированных FDI-атак почти в 4 раза по сравнению с независимыми одномерными фильтрами и сохраняет связность легального сегмента группы. Данный метод интегрируется в общий контур защиты ИБ автономного транспорта и применим для бортовых вычислителей в режиме реального времени.

Благодарности

Работа выполнена в Университете ИТМО при финансовой поддержке Министерства науки и высшего образования Российской Федерации в рамках проекта № 70-2024-001354 «Разработка технологий и демонстратора комплексной системы группового управления, взаимодействия и организации поведения

группы БВС при выполнении целевых задач».

Библиография

[1] Arena F., Pau G. An overview of vehicular communications //Future internet. – 2019. – Т. 11. – №. 2. – С. 27.

[2] Павелина Ю.А., Мухамеджанов С., Комаров И.И. Метод построения модели пространства автономных транспортных средств // International Journal of Open Information Technologies. – 2024. – Т. 12. – № 7. – С. 38-42.

[3] Lu Z., Qu G., Liu Z. A survey on recent advances in vehicular network security, trust, and privacy //IEEE Transactions on Intelligent Transportation Systems. – 2018. – Т. 20. – №. 2. – С. 760-776.

[4] ALASEM R., Mansour M. Decentralized Trust Model for Vehicle Ad-Hoc Networks (VANETs) with 5G Integration: A Blockchain-Based Approach for Enhanced Security and Privacy in Intelligent Transportation Systems. – 2025.

[5] Aggarwal C. C., Sathe S. Which outlier detection algorithm should I use? //Outlier Ensembles: An Introduction. – Cham : Springer International Publishing, 2017. – С. 207-274.

[6] Rousseeuw P. J., Hubert M. Anomaly detection by robust statistics //Wiley interdisciplinary reviews: Data mining and knowledge discovery. – 2018. – Т. 8. – №. 2. – С. e1236.

[7] Wang F. et al. A multivariate time series anomaly detection model based on spatio-temporal dual features //2023 International Conference on Networking and Network Applications (NaNA). – IEEE, 2023. – С. 416-421.

[8] Павелина Ю.А. Метод определения степени репутации автономных транспортных средств на основе социальных сил // International Journal of Open Information Technologies. – 2026. – Т. 14. – № 2. – С. 141-146.

Статья получена 11 марта 2026.

Павелина Юлия Александровна, аспирант факультета Безопасности Информационных Технологий, Национальный исследовательский университет ИТМО (email: lyakhovenko.kam@gmail.com).

Попов Илья Юрьевич, к.т.н., доцент факультета Безопасности Информационных Технологий, Национальный исследовательский университет ИТМО (email: ilyapopov27@gmail.com)

A Mahalanobis-based data fusion and anomaly filtering method for ensuring information integrity in autonomous vehicle populations

J.A. Pavelina, I.Y. Popov

***Abstract* — This paper examines the problem of ensuring information integrity in V2X networks during information exchange between groups of autonomous vehicles (AVs). This problem arises in a dynamic environment and the presence of saboteurs implementing False Data Injection (FDI) attacks, in which classical methods of linear averaging of sensor data lead to critical control errors. A data fusion method with adaptive weighting and outlier filtering based on the Mahalanobis distance is proposed. A comparative experiment of the proposed method with approaches based on Euclidean distance and one-dimensional Z-score is conducted. The results demonstrate that the proposed method maintains high state estimation accuracy and trajectory stability even when up to 20% of the group's nodes are compromised.**

***Keywords* — multi-agent systems, autonomous vehicles, integrity, anomaly detection.**

REFERENCES

[1] Arena F., Pau G. An overview of vehicular communications //Future internet. – 2019. – T. 11. – №. 2. – C. 27.

[2] Pavelina J.A., Mukhamedzhanov S., I.I. Komarov I.I. Method for Building an Environment Model of Autonomous Vehicles // International Journal of Open Information Technologies. – 2024. – T. 12. – № 7. – C. 38-42.

[3] Lu Z., Qu G., Liu Z. A survey on recent advances in vehicular network security, trust, and privacy //IEEE Transactions on Intelligent Transportation Systems. – 2018. – T. 20. – №. 2. – C. 760-776.

[4] ALASEM R., Mansour M. Decentralized Trust Model for Vehicle Ad-Hoc Networks (VANETs) with 5G Integration: A Blockchain-Based Approach for Enhanced Security and Privacy in Intelligent Transportation Systems. – 2025.

[5] Aggarwal C. C., Sathe S. Which outlier detection algorithm should I use? //Outlier Ensembles: An Introduction. – Cham : Springer International Publishing, 2017. – C. 207-274.

[6] Rousseeuw P. J., Hubert M. Anomaly detection by robust statistics //Wiley interdisciplinary reviews: Data mining and knowledge discovery. – 2018. – T. 8. – №. 2. – C. e1236.

[7] Wang F. et al. A multivariate time series anomaly detection model based on spatio-temporal dual features //2023 International Conference on Networking and Network Applications (NaNA). – IEEE, 2023. – C. 416-421.

[8] Pavelina J.A. A method for determining the trustworthiness of autonomous vehicles based on social forces // International Journal of Open Information Technologies. – 2026. – T. 14. – № 2. – C. 141-146.