Известия СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 10. С. 89–97
LETI Transactions on Electrical Engineering & Computer Science. 2024. Vol. 17, no. 10. P. 89–97

УДК 004. 032.26 Научная статья

https://doi.org/10.32603/2071-8985-2024-17-10-89-97

Метод проактивной диагностики в робототехнических системах

Э. А. Лазарев✉, И. И. Викснин, М. С. Беляков,
Н. О. Турсуков, Р. И. Гатауллин, М. С. Куприянов

Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В. И. Ульянова (Ленина), Санкт-Петербург, Россия

✉ lzrveduard@gmail.com

Аннотация. Рассматривается решение задачи выявления неисправных модулей в беспилотных транспортных средствах (БТС), которые рассматриваются как частный случай мультиагентной системы, с использованием метода доверия и репутации. Каждый модуль системы оценивается на основе его надежности и результатов функционирования, что позволяет оперативно обнаруживать неисправности и предотвращать аварийные ситуации, давая возможность адаптироваться к изменениям в окружающей среде. Модель информационного взаимодействия реализована с применением мультиагентного подхода, а эффективность предложенного метода подтверждается компьютерным моделированием.

Ключевые слова: беспилотные транспортные средства, диагностика модулей, методы репутации и доверия, мультиагентная система, автономные транспортные системы, надежность, прогнозирование отказов, мониторинг в реальном времени

Для цитирования: Метод проактивной диагностики в робототехнических системах / Э. А. Лазарев, И. И. Викснин, М. С. Беляков, Н. О. Турсуков, Р. И. Гатауллин, М. С. Куприянов // Изв. СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 10. С. 89–97. doi: 10.32603/2071-8985-2024-17-10-89-97.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Финансирование. Работа выполнена при поддержке Министерства науки и высшего образования Российской Федерации «Госзадание» (проект FSEE-2024-0011).

Original article

Method of Proactive Diagnostics in Robotic Systems

E. A. Lazarev✉, I. I. Viksnin, M. S. Belyakov,
N. O. Tursukov, R. I. Gataullin, M. S. Kupriyanov

Saint Petersburg Electrotechnical University, Saint Petersburg, Russia

✉ lzrveduard@gmail.com

Abstract. This paper addresses the problem of identifying faulty modules in unmanned vehicles (UVs), which are considered as a special case of a multi-agent system, through the use of a trust and reputation method. Each module of the system is evaluated on the basis of its reliability and performance, which allows for rapid fault detection and prevention of emergency situations, which allows for adaptation to changes in the environment. The model of information interaction is implemented using a multi-agent approach, and the effectiveness of the proposed method is confirmed by computer simulation.

Keywords: unmanned vehicles, module diagnostics, trust reputation, multi-agent system, autonomous transport systems, reliability, failure prediction, real-time monitoring

For citation: Method of Proactive Diagnostics in Robotic Systems / E. A. Lazarev, I. I. Viksnin, M. S. Belyakov, N. O. Tursukov, R. I. Gataullin, M. S. Kupriyanov // LETI Transactions on Electrical Engineering & Computer Science. 2024. Vol. 17, no. 10. P. 89–97. doi: 10.32603/2071-8985-2024-17-10-89-97.

Conflict of interest. The authors declare no conflicts of interest.

Acknowledgement. This research was funded by the Ministry of Science and Higher Education of the Russian Science Foundation «Goszadanie» (Project FSEE-2024-0011).

Введение. Мультиагентные системы (МАС) представляют собой системы, в которых несколько автономных и интеллектуальных агентов взаимодействуют друг с другом для достижения общих целей. Агенты в таких системах обладают способностью самостоятельно принимать решения, основываясь на доступной информации и их взаимодействии с другими агентами. Механизм репутации и доверия относится к ключевым механизмам, обеспечивающим успешное взаимодействие агентов в МАС. Этот механизм позволяет агентам оценивать поведение друг друга на основе прошлых взаимодействий и использовать накопленный опыт для повышения эффективности совместной работы.

Часть мультиагентных систем представлена робототехническими системами (РТС), в которых каждая составная часть, будь то отдельный робот, датчик или программный модуль, может быть рассмотрена как независимый интеллектуальный агент.

Критические ситуации требуют оперативного выявления неисправных модулей для предотвращения аварий и снижения рисков. Однако традиционные методы диагностики, основанные на периодических проверках или тестировании, могут оказаться недостаточно эффективными в условиях реального времени, особенно агентов, работающих в динамичной среде.

Для выявления неисправных модулей перспективно использование *метода репутации и доверия* [1]. В этом методе каждый модуль рассматривается как независимый агент, которому присваивается определенная репутация на основе его поведения и работоспособности в процессе эксплуатации. Для этого подхода важно следующее:

– мониторинг в реальном времени: система постоянно отслеживает работу модулей и анализирует их эффективность на основе заранее заданных параметров;

– оценка степени доверия к действиям модуля: при обнаружении отклонений от нормального поведения репутация модуля понижается. Например, если сенсор передает некорректные данные или связь с коммуникационным модулем регулярно прерывается, уровень доверия к нему снижается;

– адаптация и реакция: если репутация какого-либо модуля падает ниже критического уровня, система может принять решение об отключении данного модуля, использовании резервного устройства или переходе в безопасный режим.

Такой подход позволяет не только оперативно выявлять неисправные модули, но и предсказывать их возможные отказы на основе накопленных данных о репутации. Это значительно повышает надежность системы и снижает вероятность возникновения критических ситуаций.

В данной статье будет рассмотрено применение метода репутации и доверия для диагностики модулей в мультиагентных системах, а также предложены алгоритмы интеграции этого метода в компьютерную (имитационную) модель работы такой мультиагентной системы.

Постановка задачи. Рассматривается нарушение функциональности агента из-за неисправности устройств, отвечающих за получение данных от окружающей среды.

Согласно ГОСТ 27.002–2015 [2], неисправность – это состояние объекта, в котором он не соответствует хотя бы одному из требований, установленных в документации на него.

Предлагается рассмотреть датчик (или сенсор как устройство, получающее данные из окружающей среды) в качестве элемента мультиагентной системы. В постановке задачи были описаны следующие допущения о выходе датчиков из строя:

– изначально все датчики исправны;

– каждый датчик выходит из строя независимо от других;

– каждый датчик имеет ограниченный ресурс работы.

Управление элементами мультиагентной системы делится на различные типы согласно выбранной стратегии. Так, существуют два типа стратегий группового управления [3], представленные на рис. 1. Так как сенсоры – это интеллектуальные агенты с ограниченными возможностями по принятию решений, выбрана централизованная стратегия с единоначальным управлением.

Полетный контроллер (FC) здесь рассматривается как центральный элемент, с помощью которого осуществляется управление системой в целом по аналогии с устройством беспилотных аппаратов, автономное управление которых осуществляется с помощью такого контроллера [4]. Функционирова-

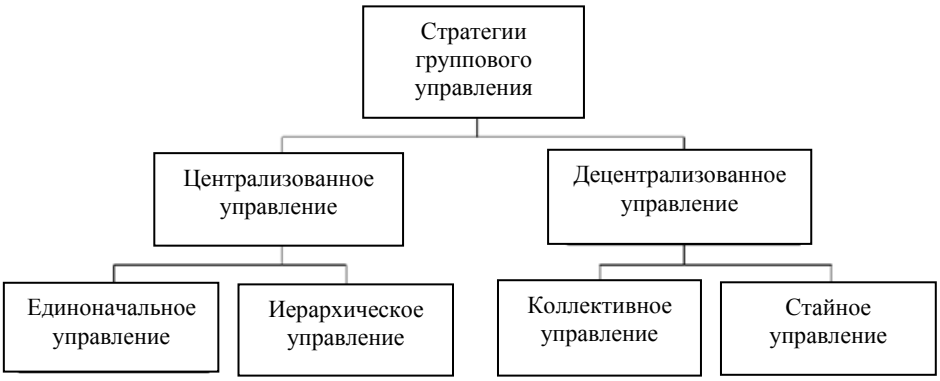

Рис. 1. Стратегии группового управления
Fig. 1. Group Management Strategies

ние агента осуществляется на местности. Положение агента в момент времени t задается вектором **pos**(t) = (x, y, z, r, p, u), где (x, y, z) – координаты центра масс агента в пространстве, (r, p, u) – ориентация агента в пространстве (r – отклонение по горизонтали, p – отклонение по вертикали, u – отклонение по своей оси).

Пусть $S=\{S_i\}$, где $i=\overline{1,N}$ – множество датчиков, установленных в системе.

Для каждого S_i справедливо существование вектора свойств $\mathbf{s}_i(t)=<s_i^1(t),\ldots,s_i^6(t)>$, состоящего из следующих элементов:

– $s_i^1(t)$ – идентификатор устройства;

– $s_i^2(t)$ – тип датчика;

– $\mathbf{s}_i^3(t)=<x, y, z, r, p, u>$ – положение датчика в системе координат относительно положения агента;

– $\mathbf{s}_i^4(t)$ – вектор с показаниями, полученными датчиком в момент времени t. Длина вектора и его наполнение зависят от типа датчика, задаваемое $s_i^2(t)$;

– $s_i^5(t)$, $0<s_i^5(t)$ – частота, с которой обновляются значения датчика;

– $s_i^6(t)$ – диапазон допустимых значений для свойства $\mathbf{s}_i^4$.

S_i считается исправным в моменты времени t, когда $\mathbf{s}_i^4(t)-\mathbf{real}_v(t)<\boldsymbol{\varepsilon}$, где $\mathbf{real}_v$ – истинные значения; $\boldsymbol{\varepsilon}$ – допустимое значение ошибки датчика.

Показания датчиков одного типа могут быть сравнены с использованием функции, возвращающее число принадлежит интервалу $(-\infty,+\infty)$:

$$d\left[\mathbf{s}_i^4(t),\mathbf{s}_j^4(t),\mathbf{w}\right]=\left|\mathbf{w}\circ\left[\mathbf{s}_i^4(t)-\mathbf{s}_j^4(t)\right]\right|, \quad (*)$$

где $\mathbf{s}_i^4(t)$ и $\mathbf{s}_j^4(t)$ – векторы показаний с двух датчиков; $\mathbf{w}$ – вектор весов, показывающий значимость каждого значения из вектора показаний, определяется для каждого датчика отдельно, задается эмпирически (на основе дополнительных экспериментов); $\circ$ – оператор произведения Адамара, выполняющий поэлементное умножение векторов $(\mathbf{A}\circ\mathbf{B})_i=\mathbf{A}_i\cdot\mathbf{B}_i$.

Пусть FC – контроллер, установленный на агенте. FC обладает отдельным выделенным каналом связи с каждым S_i.

Введем показатель $\alpha_{i(t)}\in\{0,1\}$, отражающий состояние S_i в момент времени t, где $\alpha_i(t)=0$ означает неисправное состояние, $\alpha_i(t)=1$ – исправное. При этом будем считать, что если $\alpha_i(t)=0$, то $\alpha_i(\hat{t})=0,\ \forall\hat{t}\geq t$.

Пусть в начальный момент времени все датчики исправны $\alpha_i(0)=1,\ \forall i$.

Состояние каждого S_i не зависит от состояний остальных датчиков в системе $\alpha_i(t)=0\Leftrightarrow$ $\Leftrightarrow\alpha_j(t)=0,\ \forall j\neq i$.

Каждый датчик имеет ограниченный временной ресурс работы до выхода из строя $\lim\limits_{t\to N}\alpha_i(t)=0$. При этом время $\hat{t}$, когда произойдет отказ, $\alpha_i(\hat{t})=0$, $\alpha_i(\hat{t}-1)=1$, заранее неизвестно.

Также введем показатель $\beta_i(t)\in\{0,1\}$, отражающий информацию FC о состоянии S_i в момент времени t, где $\beta_i(t)=0$ означает, что FC считает S_i неисправным. При этом FC не обладает информацией о значении $\alpha_i(t)$.

Таким образом, общая цель функционирования системы применительно к обеспечению функциональной безопасности может быть представлена согласно формуле

$$\begin{cases} \sum\limits_{i=1}^{N} \left|\beta_i(t) - \alpha_i(t)\right| \to 0; \\ \sum\limits_{i=1}^{N} \alpha_i(t) = \sum\limits_{i=1}^{N} \alpha_i(\hat{t}); \\ t - \hat{t} \to 0, \end{cases}$$

где $\hat{t}$ используется для поиска неисправного датчика.

Модель информационного взаимодействия. Для построения модели информационного взаимодействия необходимо определить отдельные элементы, функционирующие в рамках модели.

Целью диагностики всей системы служит определение неисправных датчиков S_i и устранение их из системы.

В связи с данными ограничениями предлагается использовать метод расчета репутационных оценок, предложенный в [1].

Этот метод вводит показатель доверия $\mathrm{Trust}_i(t)$, отражающий отношение всех элементов системы к *i*-тому элементу в момент времени *t*.

Полетный контроллер *FC* вычисляет этот показатель на основе показаний каждого датчика S_i.

Если значение доверия к S_i в момент времени *t* опускается ниже заданного порога $\mathrm{Trust}_i(t) \le \le \mathrm{Threshold}_{\mathrm{Trust}}$, то в этот момент времени *FC* считает датчик неисправным ($\beta_i(\hat{t}) = 0$, $\hat{t} \ge t$) и перестает учитывать его данные.

Оценка доверия выполняется среди датчиков одного типа $s_i^2(t)$, так как датчики с разными функциями не могут корректно оценивать правильность показаний друг друга.

Для надежной работы метода доверия и репутации важно, чтобы количество исправных датчиков превышало количество неисправных. Если остаются только два устройства одного типа и их показания противоречат друг другу, *FC* не может продолжать выполнять поставленные перед ним задачи и принимается решение о выполнении посадки.

Обновление показателей выполняется с частотой, равной минимальной частоте обновления датчика данного типа:

$$\mathrm{freq}_M = \min_{S_i \in M} s_i^5(t),$$

где M – множество датчиков одного типа $\forall i$, $\forall j, S_i \in M, S_j \in M, s_i^2(t) = s_j^2(t)$.

После получения данных от всех датчиков этого типа выполняется проверка истинности их показаний.

Каждый $S_i \in M$ сравнивает показания других $\mathbf{s}_j^4(t)$ датчиков того же типа со своими показаниями $\mathbf{s}_i^4(t)$ для выявления их истинности согласно

$$\mathrm{Truth}_{i_j}(t) = \begin{cases} 1, \ d\left[\mathbf{s}_j^4(t), \mathbf{s}_i^4(t), \mathbf{w}\right] > \mathrm{Threshold}_d \\ 0, \ d\left[\mathbf{s}_j^4(t), \mathbf{s}_i^4(t), \mathbf{w}\right] \le \mathrm{Threshold}_d \end{cases},$$

где d – функция сравнения показаний датчиков, объявленная в (*); $\mathrm{Threshold}_d$ – пороговое значение для определения того, принимает ли S_i показания датчика S_j, пределы изменения индексов i, j определяются как $i \ne S$, $i, j \in \{1, S_i\}$.

Далее вычисляется истинность высказывания S_i в рамках всей системы согласно

$$\mathrm{Truth}_i(t) = \frac{\sum_{S_i}^{|M|} \mathrm{Truth}_{j\_i}}{|M|}.$$

Показатель истинности выявляет противоречивость значений одного датчика другим элементам системы в данный момент времени.

Так как по одному отличающемуся значению невозможно судить об исправности элемента, необходимо ввести еще один показатель, содержащий в себе исторические данные – репутацию, предложенную в [1]. Предлагается изменить формулы для расчета степени исправности элемента в контексте использования алгоритмов репутации следующим образом:

$$R_i^S(t) = \begin{cases} \sum\limits_{k=1}^{K} R_i(t-k) + \mathrm{Truth}_i(t), \\ \mathrm{Truth}_i(t) \ge \mathrm{Threshold}_{\mathrm{Truth}}; \\ \sum\limits_{k=1}^{K} R_i(t-k) - \gamma(t), \\ \mathrm{Truth}_i(t) < \mathrm{Threshold}_{\mathrm{Truth}}, \end{cases}$$

$$\gamma(t) = \left(\frac{\sum_{k=1}^{K} R_i(t-k)}{K} - e^{-\left(1-\mathrm{Truth}_i(t)\right)\left(t-\hat{t}\right)} \right),$$

где K – количество исторических данных о репутации, используемые при расчете текущей репутации; k – отдельное значение исторических дан-

ных о репутации, входящее в состав K; $\text{Threshold}_{\text{Truth}}$ – пороговое значение для определения необходимости повышать или понижать значение репутации; $\hat{t}$ – последний момент времени, когда $\text{Truth}_i(\hat{t}) \geq \text{Threshold}_{\text{Truth}}$.

Экспонента, используемая в случае уменьшения репутации, предотвращает резкое падение значения в начальный момент времени, тем самым сглаживая уменьшение репутации и предотвращая ложное понижение значения.

Поскольку в $R_i^S(t)$ также содержится информация за K предыдущих моментов времени, его значение необходимо нормализовать для дальнейшей работы:

$$R_i(t) = \frac{R_i^S(t)}{K+1}.$$

Показатель репутации $R_i(t)$ характеризует накопительную оценку показаний S_i за все время функционирования. При этом данный показатель обладает следующими характеристиками:

– медленный рост значения при отсутствии противоречивости данных;

– значительное уменьшение значения при появлении противоречивости.

Значение показателя доверия к S_i в момент времени t рассчитывается с учетом показателя репутации по формуле

$$\text{Trust}_i(t) = \left\{ \sqrt{R_i(t)^2 + \text{Truth}_i(t)^2} - \right.$$
$$\left. - \sqrt{\left[1 - R_i(t)\right]^2 + \left[1 - \text{Truth}_i(t)\right]^2} \right\} \Big/ \sqrt{2}.$$

Доверие принимает значения в диапазоне [–1, 1].

Этот метод позволяет эффективно выявлять два типа неисправностей:

– датчики, которые временно работают некорректно, но их показания похожи на данные других устройств;

– датчики, которые внезапно начинают выдавать кардинально отличные значения.

С целью определения исправности S_i по полученному значению доверия Trust_i вводится пороговое значение $\text{Threshold}_{\text{Trust}}$. Если значение доверия больше порогового $\text{Trust}_i \geq \text{Threshold}_{\text{Trust}}$, датчик S_i считается исправным. Иначе S_i принимается как неисправный, и показания, полученные с него, перестают учитываться до момента восстановления доверия.

Настройка модели. Для $\text{Threshold}_{\text{Truth}}$ и $\text{Threshold}_{\text{Trust}}$ принимаются значения 0.5 и 0 соответственно, как средние значения в возможном диапазоне.

Значение Threshold_d должно подбираться исходя из специфики установленных датчиков и решаемой задачи.

Значение K влияет на то, сколько прошлых значений репутации влияют на расчет текущего значения репутации. Большее влияние K имеет в случае понижения репутации. Так, если значение слишком мало, репутация будет быстро сходиться к значению 0, а если слишком велико – репутация не будет уменьшаться.

В эталонном случае уменьшение репутации должно происходить по экспоненте $e^{\alpha t}$, где $\alpha = \ln 0.01 \cdot \text{duration}$ соответствует уменьшению значения от 1 до 0.01 за время duration. Значение duration считается, как среднее время неисправности датчика. Для подбора оптимального значения K строятся графики уменьшения репутации

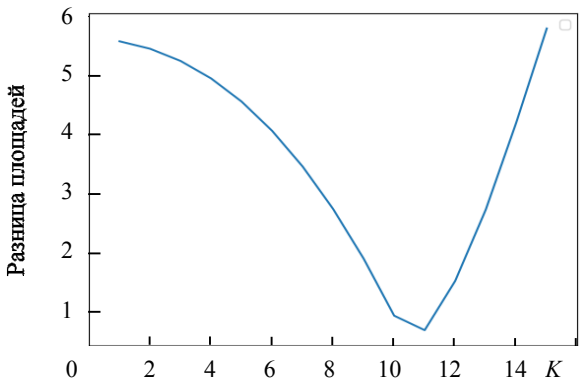

Рис. 2. Разница площадей графика убывания репутации и экспоненты при duration = 30

Fig. 2. Difference in areas of the graph of reputation decay and the exponent at duration = 30

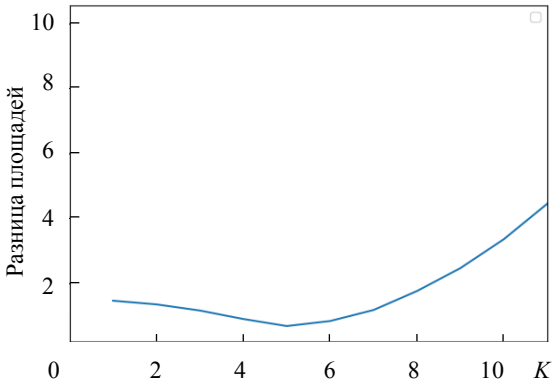

Рис. 3. Разница площадей графика убывания репутации и экспоненты при duration = 5

Fig. 3. Difference in the areas of the graph of reputation decay and the exponent at duration = 5

с различными коэффициентами K и сравниваются площади под полученными кривыми с эталонной кривой. Оптимальное значение K будет соответствовать минимальному отличию площадей.

Примеры для duration = 5; 30 представлены на рис. 2 и 3. При duration = 5 оптимальное K = 5, а при duration = 30 оптимальное K = 11.

Оценка эффективности. Для оценки эффективности разработанной модели информационного взаимодействия элементов с использованием метода доверия и репутации выполнялось моделирование показаний датчиков.

Во время моделирования замерялись взаимодействия двух типов:

– с применением разработанной модели;

– без применения разработанной модели.

В экспериментах без применения разработанной модели датчик считался неисправным, если его показания отличаются от показаний остальных датчиков в системе.

В качестве показаний датчиков в рамках одного эксперимента случайно создавалась функция $f(t)$, равная измеряемому значению в момент времени t:

$$f(t) = A\sin\frac{t}{B} + C\sin\frac{t}{D},$$

где A, B, C, D – случайные коэффициенты, выбираемые для одного эксперимента. Коэффициенты имеют равномерное непрерывное распределение $U(a, b)$. Для A и B – $U(–50, 50)$, для C и D – $U(–5, 5)$.

Так как датчики неидеальны, в их показаниях содержится шум. Таким образом, значения показания датчика S_i могут быть получены согласно формуле

$$f_i(t) = f(t) + N\left[0, \left(\max_t f(t) - \min_t f(t)\cdot 0.1\right)\right],$$

где $N(\mu, \sigma^2)$ – гауссовское распределение случайной величины.

Для работы репутации доверия необходимо определить следующие пороговые значения:

– Threshold_d;

– K;

– $\text{Threshold}_{\text{Truth}}$;

– $\text{Threshold}_{\text{Truth}}$.

Диапазон времени работы датчиков в проводимом исследовании равен 1000 значениям.

В рамках каждого эксперимента существует три различных датчика, один из которых неисправен.

Для описания поведения неисправного датчика использована концепция атаки on-off [5]. При таком поведении элемент с неисправностью может находиться в двух состояниях, сменяющих друг друга в разные моменты времени:

– состояние on – датчик выдает неисправные значения;

– состояние off – датчик выдает исправные значения.

В рамках одного эксперимента датчик может находиться в состоянии on от 30 до 80 % времени измерений. В среднем время, когда датчик находится в состоянии on, составляет 30 таков. В таком случае параметр K = 11.

Главный параметр в работе проверяемых методов – это Threshold_d, обозначающий порог в разности значений, после преодоления которого значения считаются разными. Проводилось сравнение на трех значениях: 20, 30 и 40 % от диапазона значений. Для каждого порогового значения проводилось 100 испытаний.

Результаты экспериментов представлены в таблице. Для таблицы определены следующие параметры:

$\textit{Threshold}_d$ – допустимое пороговое значение (отклонение) модели;

– *использование разработанной модели* – используется ли разработанная модель для проведения эксперимента;

TP – классификатор «true positive» (верноположительный), выявляющий верное определение объекта в составе рассматриваемого класса в процентах;

– *FP* – классификатор «false positive» (неверно-положительный), выявляющий неверное определение объекта не в составе рассматриваемого класса в процентах;

– *TN* – классификатор «true negative» (верноотрицательный), выявляющий верное определение объекта не в составе рассматриваемого класса в процентах;

FN – классификатор «false positive» (неверноотрицательный), выявляющий неверное определение объекта в процентах не в составе рассматриваемого класса;

– *Accuracy* (точность) – параметр точности, определяющий точность работы модели;

– *Precision* (точность, перевод совпадает с Accuracy) – параметр точности, выявляющий верно классифицированные объекты среди всех объектов, которые к этому классу отнес классификатор, в процентах;

Результаты оценки эффективности разработанной модели
Results of the evaluation of the effectiveness of the developed model

Threshold$_d$, %	Использование разработанной модели	TP, %	FP, %	TN, %	FN, %	Accuracy, %	Precision, %	Recall, %	$F_{0.5}$	F_1	F_2
20	Да	18.1	6.3	63.1	12.0	81	74	60	0.70	0.66	0.62
20	Нет	33.3	66.6	0	0	33	33	100	0.38	0.50	0.71
30	Да	12.0	22.3	44.3	21.3	56	34	36	0.35	0.35	0.35
30	Нет	33.3	66.6	0	0	33	33	100	0.38	0.50	0.71
40	Да	14.3	12.0	54.6	19.0	69	54	43	0.51	0.48	0.44
40	Нет	17.0	23.3	43.3	16.3	60	40	50	0.43	0.46	0.49

– *Recall* (полнота) – параметр, определяющий отношение верно классифицированных элементов класса к общему числу элементов этого класса;

– F_x – параметры F-меры, определяющие эффективность работы классификатора через соотношение значений параметров Recall и Precision. Параметр x определяет то, насколько более значимым для подсчета будет значение Recall относительно Precision (при $F_{0.5}$ двойной коэффициент при подсчете получает параметр Precision, при F_2 – Recall, при F_1 – параметры равнозначны).

Как видно из результатов, у сравниваемых методов различна чувствительность к отклонениям в значениях. Так, при 30 %-ном отклонении оба метода работают неудовлетворительно. При 20 %-ном лучше работает модель с использованием репутации доверия, а при 40 %-ном – стандартная модель. Такое поведение связано с сохранением исторических значений датчиков в методе доверия и репутации, что позволяет точнее отделять шумы в значениях от неверных показаний.

С учетом того, что исследуемые модели работают на разных пороговых значениях, доля верно определенных неисправных датчиков больше на 10 % при использовании метода с репутацией доверия.

Заключение. В данной статье были рассмотрены методы применения механизма репутации и доверия для диагностики модулей в мультиагентных системах, включая робототехнические системы. Особое внимание уделено важности мониторинга в реальном времени для своевременного выявления неисправных модулей и повышения надежности всей системы. Предложенный подход позволяет оперативно оценивать поведение модулей на основе их предыдущей деятельности и использовать накопленные данные для повышения точности проактивной диагностики. Это способствует снижению риска возникновения критических ситуаций и увеличивает эффективность работы системы в условиях динамичной и изменяющейся среды. Таким образом, интеграция механизмов репутации и доверия в РТС открывает новые возможности для улучшения их надежности и безопасности, что является важным шагом в развитии автономных и робототехнических систем.

Список литературы

1. Reputation and trust approach for security and safety assurance in intersection management system / S. Chuprov, I. Viksnin, I. Kim, E. Marinenkov // Energies. 2019. Vol. 12. P. 4527.

2. ГОСТ 27.002–2015 «Надежность в технике. Термины и определения». М.: Стандартинформ, 2016.

3. Каляев И. А., Капустян С. Г. Проблемы группового управления роботами // Мехатроника, автоматизация, управление. 2009. № 6. С. 33–40.

4. Design considerations of a small UAV platform carrying medium payloads / J. A. Benito, J. Garrido, R. Ponticelli, G. Gonzalez de Rivera // Design of Circuits and Integrated Systems. IEEE. 2014. P. 1–6.

5. Perrone L., Nelson S. A study of on-off attack models for wireless ad hoc networks // 20061st Workshop on Operator-Assisted (Wireless Mesh) Community Networks. Berlin, 2006. P. 1–10.

Информация об авторах

Лазарев Эдуард Артемович – аспирант кафедры вычислительной техники СПбГЭТУ «ЛЭТИ».
Email: lzrveduard@gmail.com
https://orcid.org/0000-0002-3695-7109

Викснин Илья Игоревич – канд. техн. наук, доцент кафедры вычислительной техники СПбГЭТУ «ЛЭТИ».
E-mail: wixnin@mail.ru
https://orcid.org/0000-0001-6240-0390

Беляков Максим Сергеевич – студент гр. 2310 СПбГЭТУ «ЛЭТИ».
E-mail: pitbul_04@mail.ru

Турсуков Никита Олегович – ассистент кафедры вычислительной техники СПбГЭТУ «ЛЭТИ».
E-mail: stepingnik@gmail.com
https://orcid.org/0000-0003-3848-1981

Гатауллин Руслан Ильнурович – аспирант кафедры вычислительной техники СПбГЭТУ «ЛЭТИ»
E-mail: rusfiner@mail.ru
https://orcid.org/0000-0001-5077-9970

Куприянов Михаил Степанович – д-р техн. наук, руководитель перспективных проектов СПбГЭТУ «ЛЭТИ».
E-mail: mskupriyanov@etu.ru

Вклад авторов:
Лазарев Э. А. – разработка имитационной модели информационного взаимодействия.
Викснин И. И. – математическое описание метода проактивной диагностики.
Беляков М. С. – проведение экспериментов с использованием модели информационного взаимодействия.
Турсуков Н. О. –эффективности разработанной модели информационного взаимодействия.
Гатауллин Р. И. – описание процесса настройки модели информационного взаимодействия.
Куприянов М. С. – вклад в работу: постановка задачи.

References

1. Reputation and trust approach for security and safety assurance in intersection management system / S. Chuprov, I. Viksnin, I. Kim, E. Marinenkov // Energies. 2019. Vol. 12. P. 4527.

2. GOST 27.002-2015 «Nadezhnost' v tehnike. Terminy i opredelenija». M.: Standartinform, 2016. (In Russ).

3. Kaljaev I. A., Kapustjan S. G. Problemy gruppovogo upravlenija robotami // Mehatronika, avtomatizacija, upravlenie. 2009. № 6. S. 33–40. (In Russ).

4. Design considerations of a small UAV platform carrying medium payloads / J. A. Benito, J. Garrido, R. Ponticelli, G. Gonzalez de Rivera // Design of Circuits and Integrated Systems. IEEE. 2014. P. 1–6.

5. Perrone L., Nelson S. A study of on-off attack models for wireless ad hoc networks // 20061st Workshop on Operator-Assisted (Wireless Mesh) Community Networks. Berlin, 2006. P. 1–10.

Information about the authors

Eduard A. Lazarev – postgraduate student of the Department of Computer Technology of Saint Petersburg Electrotechnical University.
E-mail: lzrveduard@gmail.com
https://orcid.org/0000-0002-3695-7109

Ilia I. Viksnin – Cand. Sci. (Eng.), associate professor of the Department of Computer Science of Saint Petersburg Electrotechnical University.
E-mail: wixnin@mail.ru
https://orcid.org/0000-0001-6240-0390

Maksim S. Belyakov – student gr. 2310 of the Department of Computer Science of Saint Petersburg Electrotechnical University.
E-mail: pitbul_04@mail.ru

Nikita O. Tursukov – assistant of the Department of Computer Science of Saint Petersburg Electrotechnical University.
E-mail: stepingnik@gmail.com
https://orcid.org/0000-0003-3848-1981

Ruslan I. Gataullin – postgraduate student of the Department of Computer Science of Saint Petersburg Electrotechnical University.
E-mail: rusfiner@mail.ru
https://orcid.org/0000-0001-5077-9970

Mikhail S. Kupriyanov – Dr Sci. (Eng.), Head of Advanced Projects of Saint Petersburg Electrotechnical University.
E-mail: mskupriyanov@mail.ru

Author contribution statement:
Lazarev E. A. – development of a simulation of the information interaction model.
Viksnin I. I. – mathematical description of the method of proactive diagnostics.
Belyakov M. S. – conducting experiments using the information interaction model.
Tursukov N. O. – evaluation of the effectiveness of the developed information interaction model.
Gataullin R. I. – description of the process of setting up an information interaction model.
Kupriyanov M. S. – statement of the problem.

Статья поступила в редакцию 29.11.2024; принята к публикации после рецензирования 05.12.2024; опубликована онлайн 25.12.2024.

Submitted 29.11.2024; accepted 05.12.2024; published online 25.12.2024.