6. Smith E. LILLIE: Information extraction and database integration using linguistics and learning–based algorithms / E. Smith, D. Papadopoulos, M. Braschler, K. Stockinger // Information Systems, 2022. – Vol. 105. – DOI: 10.1016/j.is.2021.101938.
7. Golikov V. A. Issledovanie klyuchevyh arhitekturnyh patternov mikroservisov: teoreticheskij analiz ih roli v postroenii otkazoustojchivoj informacionnoj sistemy / V. A. Golikov, M. V. Yanaeva, N. T. Rudnik. – SPb: Informacionno-upravlyayushchie sistemy, 2023. – No 4. – Pp. 28–37.
8. Abrosimov L. I. Metody proektirovaniya i analiza proizvoditel'nosti raspredelennyh vychislitel'nyh setej / L. I. Abrosimov // M.: Universitetskaya kniga, 2023. – P. 256.
9. Qiang S. The Nonlinear Mathematical Modeling and Optimization of Distributed Control in Complex Systems / S. Qiang // Journal of Advances in Engineering and Technology, 2025. – Vol. 2. – Pp. 34–42. – DOI: 10.62177/jaet.v2i1.152.
10. Wang Y., et al. A multi-level action coupling reinforcement learning approach for online two-stage flexible assembly flow shop scheduling // Journal of Manufacturing Systems, 2024. – Vol. 76. – Pp. 351– 370.
11. Liu C. A Survey on Workflow Management and Scheduling in Cloud Computing. / C. Liu, C. Yang, X. Fan [et al.] // IEEE Transactions on Services Computing, 2022. – Vol. 15. – No 4. – Pp. 2178–2197. – DOI: 10.1109/TSC.2020.3047462.
12. Calheiros R. N. CloudSim: A Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms / R. N. Calheiros, R. Ranjan, A. Beloglazov [et al.] // Software: Practice and Experience, 2011. – Vol. 41. – No 1. – Pp. 23–50. – DOI: 10.1002/spe.995.
13. Sun S. Integrated data-driven topology reconstruction and risk-aware reconfiguration for resilient power distribution systems under incomplete observability / S. Sun, N. Li, L. Zhang, D. Zhao, D. Lun, L. Feng // Scientific Reports, 2025. – Vol. 15. – P. 30661. – DOI: 10.1038/s41598–025–15440–8.
14. Sahu A. ARM–IRL: Adaptive Resilience Metric Quantification Using Inverse Reinforcement Learning / A. Sahu, V. Venkataramanan, R. Macwan // AI, 2025. – Vol. 6. – No 5. – P. 103. – DOI: 10.3390/ai6050103.
15. Meylahn J. M. Quantifying the Likelihood of Learning Collusive Strategy Equilibria / J. M. Meylahn // Chaos: An Interdisciplinary Journal of Nonlinear Science, 2025. – Vol. 35. – No 8. – P. 083106. – DOI: 10.1063/5.0281443.
16. Sheluhin O. I. Modeli i metody upravleniya v mnogoagentnyh sistemah / O. I. Sheluhin, A. V. Osin. – M.: FIZMATLIT, 2018. – P. 288.

МЕТОД КОНТЕКСТНОЙ ВЕРИФИКАЦИИ СОБЫТИЙ ПРИ КОНТРОЛЕ БЕЗОПАСНОСТИ РАСПРЕДЕЛЁННОЙ IoT-ПОДСИСТЕМЫ

Андреев И. А.[1], Липатников В. А.[2], Тарасенко С. Е.[3]

DOI:10.21681/3034-4050-2026-3-29-39

Ключевые слова: *интернет вещей, IoT, ESP32, MQTT, контроль безопасности, контекстная верификация событий, периферийные узлы, серверная обработка данных, виртуальный помощник, адаптивный режим контроля.*

Аннотация

Цель работы: *повышение защищённости распределённой IoT-подсистемы контроля безопасности за счёт разработки метода контекстной верификации событий и адаптивного выбора режима контроля безопасности при взаимодействии периферийных узлов на базе ESP32 с сервером виртуального помощника.*

Метод исследования: *использованы методы формализации событийного контура распределённой IoT-подсистемы, построения показателя доверия к событию на основе идентификационных, временных, процессных, состоянийных и ресурсных факторов, а также накопительной оценки аномальности событийного потока. Для проверки предложенного подхода применён модельный вычислительный эксперимент, основанный на генерации последовательностей событий доступа, телеметрии и управляющих воздействий. Сравнительная оценка выполнена по отношению к базовым статическим и пороговым методам контроля безопасности.*

Результаты исследования: *предложен метод контекстной верификации событий, основанный на совместном учёте идентификационных, временных, процессных и ресурсных факторов; разработано правило накопительной оценки аномальности и адаптивного выбора режима контроля безопасности; сформирован и исследован прикладной сценарий распределённой IoT-подсистемы с двумя узлами ESP32 и серверной обработкой данных; показано, что предложенный подход превосходит базовые статические и пороговые методы по вероятности ложного допуска и полноте выявления некорректных событий, особенно при распределённой во времени аномальной активности.*

Научная новизна *заключается в разработке метода контекстной верификации событий при контроле безопасности распределённой IoT-подсистемы, учитывающего контекст возникновения события, накопительную оценку аномальности и адаптивный выбор режима контроля безопасности в условиях ограниченных ресурсов периферийных узлов и серверно-периферийной архитектуры обработки данных.*

Введение

Интернет вещей является одним из наиболее динамично развивающихся направлений современной цифровой инфраструктуры. Рост числа подключённых устройств, их гетерогенность, распределённый характер взаимодействия и тесная связь с физической средой формируют новые классы киберугроз. В документах NIST подчёркивается, что IoT-системы требуют специальных подходов к обеспечению безопасности, поскольку сочетают сетевую связность, ограниченные ресурсы и высокую вариативность сценариев применения [1–2].

Одной из ключевых проблем является обеспечение защищённости распределённых IoT-подсистем контроля безопасности, в которых события доступа, телеметрии и управляющих воздействий обрабатываются в реальном времени. Для таких подсистем недостаточно только сетевой фильтрации или статической проверки идентификаторов, поскольку допустимость события определяется временным контекстом, контекстом развития процесса и текущим состоянием системы. Современные исследования показывают, что жёстко заданные модели авторизации плохо адаптируются к динамичным и гетерогенным IoT-средам, а развитие access control идёт в сторону гибридных и адаптивных подходов [3–5]. Дополнительную сложность создаёт широкое распространение MQTT, где атаки могут быть связаны не только с сетевыми аномалиями, но и с нарушением логики прикладного процесса [6–7].

В связи с этим актуальна разработка метода контроля безопасности, объединяющего

1 ***Андреев Илья Андреевич***, оператор научной роты, Военная академия связи им. Маршала Советского Союза С. М. Будённого. Санкт-Петербург, Россия. E-mail: andreev.ilia.1984@mail.ru

2 ***Липатников Валерий Алексеевич***, заслуженный деятель науки РФ, доктор технических наук, профессор, старший научный сотрудник научно-исследовательского центра, Военная академия связи им. Маршала Советского Союза С. М. Будённого. Санкт-Петербург, Россия. E-mail: lipatnikovanl@mail.ru

3 ***Тарасенко Станислав Евгеньевич***, старший научный сотрудник научно-исследовательского центра, Военная академия связи им. Маршала Советского Союза С. М. Будённого. Санкт-Петербург, Россия. E-mail: s.tar.my@mail.ru

контекстную верификацию событий, накопительный анализ аномальности и адаптивный выбор режима контроля безопасности.

Целью работы является повышение защищённости распределённой IoT-подсистемы управления за счёт разработки метода контекстной верификации событий и адаптивного выбора режима контроля безопасности.

Для достижения цели в статье решаются следующие задачи: анализ существующих подходов к контролю доступа и выявлению аномалий в IoT-среде; формализация событийного контура; разработка показателя доверия к событию; разработка правила накопительной оценки аномальности; разработка правила выбора режима контроля безопасности; проведение экспериментальной оценки предложенного подхода.

Анализ существующих подходов и обзор литературы

Проблематика контроля доступа и защиты ресурсов в IoT подробно рассмотрена в обзорных работах последних лет. В частности, в исследовании S. Ravidas и соавт. показано, что для IoT-систем требования к механизмам авторизации формируются под влиянием масштабируемости, интероперабельности, малых вычислительных затрат, динамичности и необходимости учитывать специфику конкретного приложения. Авторы подчёркивают, что не существует единственного универсального решения для всех IoT-сценариев, а выбор механизма авторизации должен опираться на свойства конкретной архитектуры и среды функционирования [3].

В обзоре M. S. Ahsan и A.-S. K. Pathan доступ к ресурсам в IoT рассматривается как одна из центральных проблем безопасности, а сами модели доступа делятся на conventional и advanced. Авторы отмечают, что классические модели, основанные на ролях, атрибутах, доверии или отношениях, нередко оказываются недостаточно гибкими в условиях высокой динамичности и гетерогенности IoT-среды, тогда как новые подходы всё чаще используют гибридные механизмы, машинное обучение и иные способы адаптации к изменяющимся условиям [5].

Среди работ, наиболее близких к рассматриваемой тематике, следует выделить исследования по context-aware access control. В обзоре A. S. M. Kayes и соавт. показано, что в распределённых cloud/fog-средах решения о доступе должны учитывать не только статические атрибуты субъектов и объектов, но и релевантные контекстные условия [8]. Развивая этот подход, R. Kalaria и соавт. предложили fog-based adaptive context-aware access control framework, в котором принятие решений переносится ближе к конечным узлам сети, а сами политики адаптируются к изменениям контекста и поведения доступа. Показано, что использование fog-узлов позволяет сократить задержку обработки и уменьшить зависимость от централизованного облачного контура [9].

Одновременно с этим в исследованиях по IoT security отмечается, что edge/fog-уровень должен рассматриваться не только как вычислительное расширение облака, но и как самостоятельный уровень защиты. В работе I. Butun и соавт. подчёркивается, что fog computing может выступать промежуточным security layer, обеспечивающим обработку и защиту данных до их передачи в облачную инфраструктуру [10]. Это особенно важно для систем, в которых задержка реакции и доступность критичны для безопасного функционирования.

Отдельное направление исследований связано с выявлением аномалий и вторжений в MQTT-ориентированных IoT-сетях. В статье M. A. Khan и соавт. предложена DNN-модель для intrusion detection в MQTT-based IoT, а также проведено сравнение с классическими ML-моделями на публичных MQTT-датасетах. Авторы показывают, что MQTT-брокер и связанные с ним публикации/подписки являются мишенью для DoS, MitM, intrusion и других атак [6].

Для воспроизводимых исследований важную роль играют специализированные наборы данных. Работа H. Hindy и соавт. посвящена MQTT-IoT-IDS2020 и показывает полезность packet-based, uni-flow и bi-flow признаков для выявления атак в MQTT-сетях. Авторы подчёркивают, что для MQTT-based IDS требуется учитывать особенности самого протокола и структуры потока, а не только общие сетевые признаки [11]. В свою очередь, I. Vaccari и соавт. представили MQTTset – специализированный датасет, включающий как легитимный, так и вредоносный MQTT-трафик, опубликованный в форматах PCAP и CSV. Авторы указывают на ограниченность ранее доступных IoT-датасетов и обосновывают необходимость именно MQTT-ориентированного корпуса данных [12].

С практической точки зрения существенна не только точность выявления угроз, но и применимость метода на периферийных узлах. В работе A. Mudgerikar и соавт. предложена device-edge split IDS, где сбор системных признаков осуществляется на устройстве, а основные вычисления выносятся на edge-server, что позволяет снизить накладные расходы на IoT-устройство [13]. Аналогичная линия прослеживается и в исследовании B. Asulba и соавт., где classical one-class ML

algorithms оцениваются по detection performance, execution time и memory на Raspberry Pi как репрезентативной edge-платформе [14].

Особый интерес представляет работа P. Empl и соавт., в которой предложен process-aware подход к intrusion detection в MQTT networks. Авторы обосновывают, что IoT application layer protocols несут дополнительную contextual information, а значит, могут использоваться для восстановления и анализа процессов, лежащих за отдельными сообщениями. Предложенный framework MISSION объединяет distributed tracing, aggregation of MQTT flows и process mining, позволяя выявлять аномалии уже на уровне отклонения от допустимого процесса, а не только на уровне отдельных пакетов или статистических признаков [7].

Подход к динамическому обнаружению киберугроз в распределённых системах Интернета вещей с использованием генеративных моделей представлен в [15], а методы обеспечения и повышения защищённости сетей при прогнозировании стратегий вторжений и многоэтапных атаках рассмотрены в [16–17].

Таким образом, анализ литературы показывает наличие трёх взаимосвязанных исследовательских направлений: моделей доступа и контекстно-зависимой авторизации в IoT; методов выявления аномалий и вторжений в MQTT-ориентированных сетях; edge/fog-подходов, ориентированных на снижение накладных расходов и повышение оперативности реакции. Однако существующие работы обычно концентрируются либо на доступе, либо на intrusion detection, либо на resource-aware deployment. При этом в меньшей степени исследован подход, который объединяет контекстную допустимость события, накопительную оценку аномальности и адаптивный выбор режима контроля безопасности в рамках единого метода для распределённой IoT-подсистемы мониторинга и управления. Именно этот пробел и определяет постановку задачи настоящей работы.

Постановка задачи

Рассмотрим распределённую IoT-подсистему мониторинга и управления, состоящую из множества периферийных узлов, сенсоров, исполнительных устройств, коммуникационного брокера и серверного контура обработки событий. Такое представление согласуется с подходом NIST, в котором IoT-система трактуется как совокупность сетевых компонентов, обладающих интерфейсами, возможностями восприятия и воздействия на физическую среду, обработки и передачи данных [1, 2].

Структура исследуемой распределённой IoT-подсистемы мониторинга и управления, соответствующая рассматриваемому прикладному сценарию, представлена на рисунке 1.

В прикладной реализации исследуемая распределённая IoT-подсистема включала два периферийных узла на базе ESP32 и серверный контур виртуального помощника. Первый узел

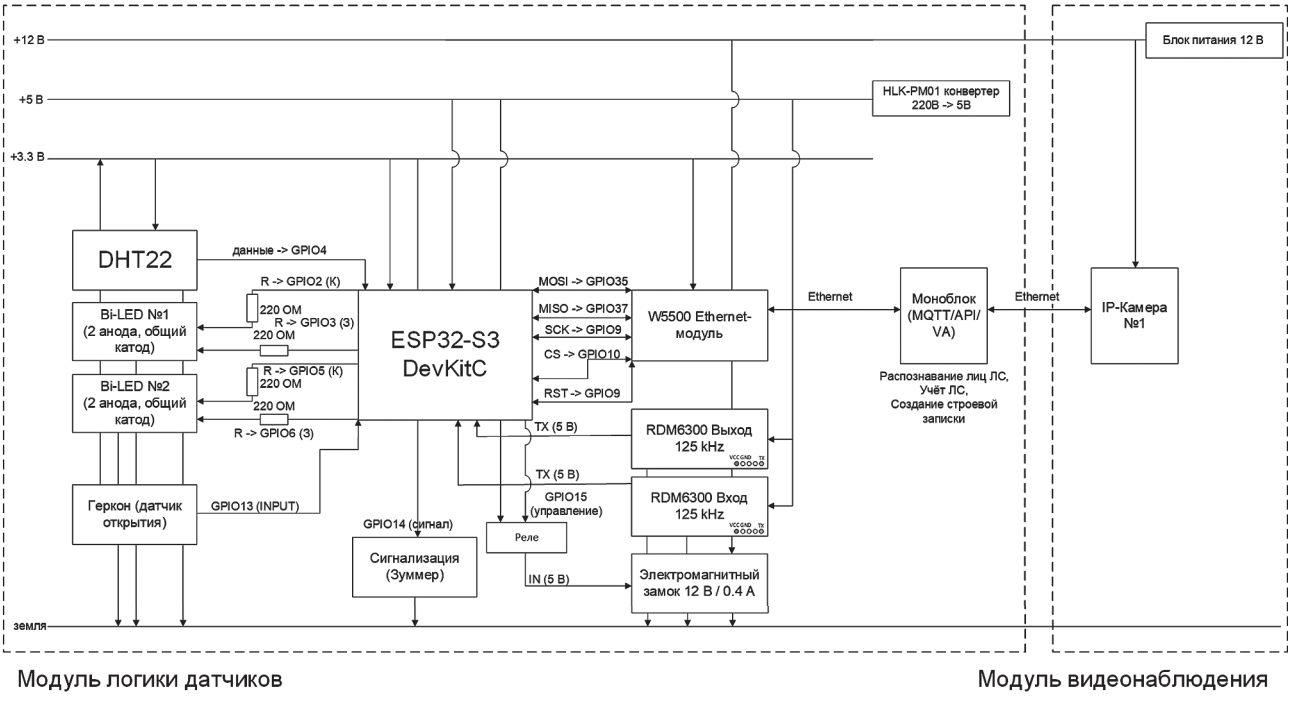

Рис. 1. Структурная схема исследуемой распределённой IoT-подсистемы мониторинга и управления

обеспечивал обработку событий доступа и состояния исполнительных устройств, второй – обработку телеметрических и управляющих сообщений. Сервер виртуального помощника выполнял агрегацию поступающих данных, журналирование событий и поддержку принятия решений в соответствии с реализуемой логикой контроля безопасности.

Пусть в дискретные моменты времени $t = 1,2,\ldots$ в систему поступают события:

$$e_t = \langle id_t, \tau_t, d_t, s_t, r_t, h_t \rangle, \quad (1)$$

где id_t – идентификатор источника события; τ_t – временная метка; d_t – тип события или направление действия; s_t – текущее логическое состояние системы; r_t – вектор ресурсных параметров узла; h_t – информация о предшествующей последовательности событий.

Практическая реализация исследуемой распределённой IoT-подсистемы в двух вариантах размещения периферийных узлов представлена на рисунке 2.

Рис. 2. Практическая реализация распределённой IoT-подсистемы контроля безопасности: слева – вариант установки в роте; справа – вариант установки в технопарке

В рассматриваемой постановке события могут соответствовать операциям доступа, публикациям в MQTT-темы, командам управления исполнительными устройствами, телеметрическим сообщениям и иным действиям, значимым для функционирования подсистемы.

Традиционный подход к принятию решения о допустимости события может быть представлен в виде функции:

$$u_t = F(id_t), \quad (2)$$

где решение определяется, по существу, только фактом наличия идентификатора в разрешённом множестве или удовлетворением простому набору статических правил. Такой подход прост в реализации, но не учитывает ни временную согласованность события, ни допустимость его появления в текущем процессе, ни изменение состояния системы, ни ресурсные ограничения узла. В результате он может приводить как к ложным допускам, так и к ложным блокировкам. Для устранения указанного недостатка требуется перейти от статической проверки отдельных событий к их контекстной верификации. Для этого вводится показатель доверия к событию:

$$T_t = w_1 f_{id}(e_t) + w_2 f_{time}(e_t) + w_3 f_{seq}(e_t) + \\ + w_4 f_{state}(e_t) + w_5 f_{res}(e_t), \quad (3)$$

где f_{id} характеризует корректность идентификатора источника; f_{time} – временную допустимость события; f_{seq} – согласованность с предшествующей последовательностью; f_{state} – соответствие текущему состоянию системы; f_{res} – учёт ресурсного состояния узла; w_i – весовые коэффициенты, удовлетворяющие условию

$$\sum_{i=1}^{5} w_i = 1,\ w_i \geq 0. \quad (4)$$

Одного только значения T_t недостаточно, если вредоносная активность проявляется не единичным отклонением, а устойчивой последовательностью пограничных или слабо аномальных событий. Поэтому дополнительно вводится накопительная оценка аномальности:

$$A_t = max\{0, \lambda A_{t-1} + (1 - T_t) - v\}, \quad (5)$$

где $\lambda \in [0,1]$ – коэффициент памяти, v – параметр отсечения фоновых отклонений.

На основе значения A_t формируется режим контроля безопасности:

$$M_t = \begin{cases} M_1, A_t < \theta_1 \\ M_2, \theta_1 \leq A_t < \theta_2, \\ M_3, A_t \geq \theta_2 \end{cases} \quad (6)$$

где M_1 – нормальный режим; M_2 – усиленный контроль; M_3 – ограничительный режим; θ_1, θ_2 – пороговые значения, $\theta_1 < \theta_2$.

Тогда итоговое решение о допустимости события определяется уже не только самим событием, но и текущим режимом контроля:

$$u_t = G(e_t, T_t, A_t, M_t). \quad (7)$$

Таким образом, задача исследования заключается в разработке метода контекстной верификации событий и адаптивного выбора режима контроля безопасности, обеспечивающего снижение вероятности ложного допуска некорректных событий и повышение полноты их выявления при сохранении допустимой задержки принятия решения и приемлемой вычислительной стоимости. В качестве критерия эффективности принимается достижение превосходства

предложенного метода над базовыми статическими правилами по совокупности показателей:

- вероятности ложного допуска;
- вероятности ложной блокировки;
- полноты выявления некорректных событий;
- средней задержки принятия решения;
- вычислительной стоимости.

Метод контекстной верификации событий

Предлагаемый метод предназначен для принятия решения о допустимости событий в распределённой IoT-подсистеме мониторинга и управления на основе совместного учёта идентификационных, временных, процессных, состоянийных и ресурсных факторов. В отличие от статических правил, ориентированных преимущественно на проверку принадлежности источника разрешённому множеству, предлагаемый подход рассматривает событие как элемент развивающегося событийного процесса. Такая постановка соответствует современным представлениям о необходимости context-aware и process-aware анализа в IoT-средах [5, 7–9].

1. Общая схема метода

Метод включает три основных этапа: нормализацию события, вычисление контекстных признаков и формирование интегрального показателя доверия с последующей передачей результата в модуль накопительной оценки аномальности и выбора режима контроля безопасности. Нормализация позволяет привести различные типы входных сообщений к единому представлению, что особенно важно для MQTT-ориентированного обмена, где в общем потоке совместно присутствуют события доступа, телеметрии и управления. Такой переход от отдельных сообщений к интерпретируемым событиям согласуется с подходами, ориентированными на MQTT flow analysis и process-aware detection [7, 11–12].

2. Контекстные признаки события

Для каждого события формируется набор частных признаков допустимости. Идентификационный признак $f_{id}(e_t) \in [0,1]$ характеризует корректность источника события. Максимальные значения соответствуют зарегистрированным и согласованным с политикой системы источникам. Значимость контроля идентификации и логического доступа к интерфейсам соответствует базовым IoT cybersecurity capabilities, выделяемым NIST [2].

Временной признак $f_{time}(e_t) \in [0,1]$ отражает временную допустимость события и учитывает принадлежность события допустимому временному окну, а также ограничения на межсобытийные интервалы. Признак согласованности последовательности $f_{seq}(e_t) \in [0,1]$ показывает, насколько событие соответствует допустимому порядку развития процесса. Его важность для MQTT-сетей подтверждается исследованиями по process-aware intrusion detection [7]. Признак согласованности состояния $f_{state}(e_t) \in [0,1]$ оценивает совместимость события с текущим состоянием системы. Ресурсный признак $f_{res}(e_t) \in [0,1]$ учитывает состояние узла, канала и доступного вычислительного бюджета. Этот фактор особенно важен для resource-constrained IoT/edge-среды [10, 13–14].

3. Агрегирование частных оценок

Интегральный показатель доверия к событию вычисляется как взвешенная сумма частных функций по выражению (3). Такое представление обеспечивает интерпретируемость метода: снижение итогового доверия можно объяснить вкладом конкретных факторов. Весовые коэффициенты задаются на этапе настройки системы и могут определяться экспертно либо уточняться по результатам модельного эксперимента.

4. Правило первичного решения

По значению T_t формируется первичная оценка допустимости события:

$$\hat{u}_t = \begin{cases} 1, & T_t \geq \delta, \\ 0, & T_t < \delta, \end{cases} \tag{8}$$

где δ – порог базовой контекстной допустимости.

Однако использование только порога δ недостаточно в случае медленно развивающейся вредоносной активности, состоящей из последовательности пограничных событий. Поэтому величина T_t используется не как окончательное решение, а как входной параметр для накопительной оценки аномальности, описанной в разделе 5.

5. Свойства метода

Предлагаемый метод является контекстнозависимым, интерпретируемым и масштабируемым по набору учитываемых признаков. Кроме того, он совместим с edge/fog-развёртыванием, поскольку вычисление отдельных признаков может быть распределено между устройством, брокером и периферийным сервером, что согласуется с device-edge split архитектурой IDS для IoT [13].

Адаптивный выбор режима контроля безопасности

Контекстная верификация отдельного события позволяет оценить его локальную допустимость, однако не всегда обеспечивает выявление устойчивой вредоносной активности. На практике многие атаки в распределённых IoT-средах проявляются как последовательность

частично допустимых или слабо аномальных действий. Поэтому в предлагаемом подходе используется накопительная оценка аномальности и адаптивный выбор режима контроля безопасности.

1. Накопительная оценка аномальности

Для учёта инерции событийного процесса вводится переменная аномальности A_t, вычисляемая по выражению (5). Если текущее событие имеет высокую контекстную допустимость, значение A_t остаётся близким к нулю. При поступлении серии событий с пониженным доверием аномальность накапливается. Это позволяет перейти от реакции на единичное отклонение к выявлению устойчивого аномального паттерна, что более адекватно отражает природу MQTT-ориентированных атак [6–7].

2. Режимы контроля безопасности

Предполагается, что подсистема функционирует в одном из трёх режимов (6). Режим M_1 соответствует штатному функционированию и минимальному набору проверок. Режим M_2 характеризуется усилением контроля и повышением строгости анализа. Режим M_3 является ограничительным и предполагает блокировку низкодоверенных событий, а также применение более консервативной политики принятия решений.

3. Правило адаптации

Итоговое решение о допустимости события определяется функцией (7), где режим M_t задаёт текущую строгость контроля. Это означает, что одинаковое значение T_t может приводить к различным решениям в зависимости от накопленной аномальности процесса. Тем самым механизм является адаптивным и изменяет политику контроля не по фиксированному расписанию, а в зависимости от текущего состояния событийного потока.

4. Учёт ресурсных ограничений

Выбор режима контроля безопасности должен учитывать не только уровень аномальности, но и доступный ресурсный бюджет узла, поскольку усиление контроля не должно вызывать неприемлемую деградацию производительности в IoT- и edge-среде [9–10, 13–14]. Для этого может быть введено ограничение:

$$C(M_t) \le B_t, \tag{9}$$

где $C(M_t)$ – вычислительная стоимость режима, B_t – доступный ресурсный бюджет. В случае дефицита ресурсов система может усиливать только критические проверки, сохраняя приемлемые задержки обработки.

Экспериментальное исследование

Целью экспериментального исследования явилась оценка эффективности предложенного метода контекстной верификации событий и адаптивного выбора режима контроля безопасности по сравнению с базовыми правилами принятия решения в распределённой IoT-подсистеме мониторинга и управления.

В отличие от натурного стендового эксперимента, в данной работе используется модельный вычислительный эксперимент, основанный на генерации и анализе событийных последовательностей, имитирующих функционирование MQTT-ориентированной IoT-подсистемы. Такой подход представляется допустимым для предварительной проверки метода, поскольку в современных исследованиях по безопасности IoT и MQTT широко используются симулированные сетевые сценарии, синтетические и полусинтетические датасеты, а также имитационные модели атак [6, 11, 12, 14]. При этом для MQTT-сетей в литературе уже представлены как специализированные датасеты, так и исследования, ориентированные на packet-based, flow-based и process-aware анализ [7, 11–12].

Серверный контур обработки и визуализации событий, используемый в прикладной реализации исследуемой подсистемы, представлен на рисунке 3.

1. Схема модельного эксперимента

В рамках эксперимента моделировалась распределённая IoT-подсистема с учётом структуры подсистемы, представленной на рисунке 1, включающая:

- источники событий доступа;
- публикации телеметрических и управляющих сообщений;
- события изменения состояния объекта;
- команды исполнительным устройствам;
- ограниченный ресурсный профиль периферийного узла.

Модельный сценарий формировался на основе архитектуры прикладной реализации, в которой два узла ESP32 передавали события в серверный контур виртуального помощника, обеспечивавший централизованную обработку данных и поддержку решений по контролю безопасности.

Каждое событие описывалось вектором e_t (1), использованным в разделе 3. Для моделирования были сформированы последовательности событий двух типов:

1. Нормальные последовательности, соответствующие допустимой логике функционирования подсистемы.
2. Аномальные последовательности, содержащие отклонения одного или нескольких видов.

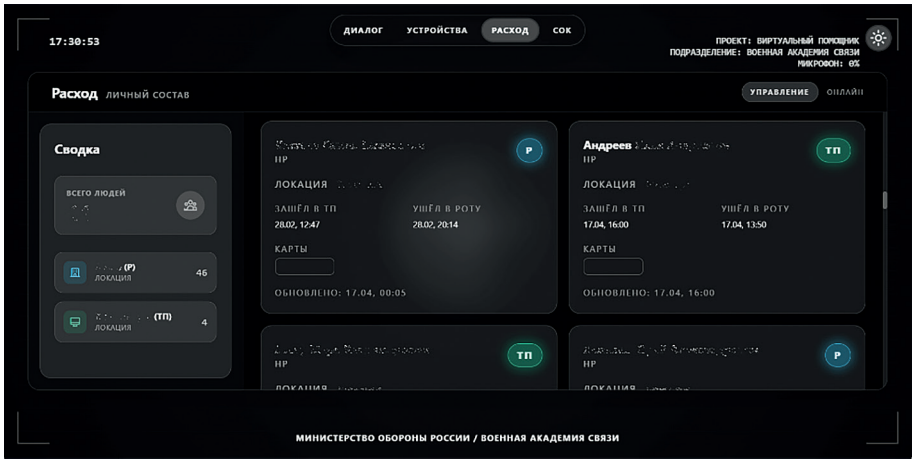

Рис. 3. Интерфейс серверного контура виртуального помощника для обработки и визуализации событий распределённой IoT-подсистемы

В вычислительном эксперименте рассматривались следующие классы аномалий:

- повтор разрешающего события в недопустимом временном окне;
- нарушение допустимой последовательности действий;
- управляющая команда вне корректного состояния системы;
- событие от формально допустимого источника в нетипичном контексте;
- серия пограничных событий, каждое из которых по отдельности не является грубым нарушением, но в совокупности образует устойчивую аномальную активность.

Последний класс особенно важен, поскольку именно он позволяет проверить преимущество предлагаемого накопительного механизма над простыми статическими правилами.

2. Сравниваемые методы

Для оценки были использованы три варианта принятия решения.

Метод 1. Статическая проверка идентификатора (Baseline-1): событие считается допустимым, если идентификатор источника принадлежит разрешённому множеству u_t (1) по выражению (2).

Метод 2. Пороговая контекстная проверка без накопления (Baseline-2): для события вычисляется показатель доверия T_t, однако окончательное решение принимается только по порогу δ, без учёта накопления аномальности: u_t (2) по выражению (8).

Метод 3. Предлагаемый метод: используется показатель доверия T_t, накопительная оценка аномальности A_t и адаптивный выбор режима контроля безопасности u_t (3) по выражению (7).

Таким образом, сравнение позволяет оценить вклад двух элементов:

- контекстной верификации по сравнению со статической проверкой;
- накопительной адаптации по сравнению с разовой пороговой контекстной проверкой.

3. Параметры эксперимента

В рамках модельного исследования было сгенерировано 12000 событий, объединённых в 600 сценариев по 20 событий в каждом. Из них:

- 360 сценариев относились к нормальному функционированию;
- 240 сценариев включали один или несколько типов аномалий.

Доля аномальных сценариев была выбрана повышенной по сравнению с реальной эксплуатационной средой для получения более выраженной сравнительной картины качества методов. Для обеспечения воспроизводимости в каждом сценарии использовались одинаковые правила генерации последовательностей, а варьировались только временные интервалы, текущие состояния и структура допустимых или недопустимых переходов. При моделировании были использованы следующие параметры предложенного метода: $w_1 = 0{,}22$, $w_2 = 0{,}18$, $w_3 = 0{,}24$, $w_4 = 0{,}21$, $w_5 = 0{,}15$; $\delta = 0{,}60$, $\lambda = 0{,}72$, $v = 0{,}08$, $\theta_1 = 0{,}35$, $\theta_2 = 0{,}70$.

Выбор весов отражает более высокую значимость процессной согласованности и состояния системы по сравнению с ресурсным фактором, что соответствует характеру исследуемой задачи.

4. Метрики оценки

Для оценки эффективности использовались следующие показатели:

- FAR – вероятность ложного допуска некорректного события;
- FRR – вероятность ложной блокировки корректного события;

- $Recall$ – полнота выявления некорректных событий;
- $Precision$ – точность выявления некорректных событий;
- F_1 – гармоническое среднее точности и полноты;
- t_{avg} – средняя задержка принятия решения на одно событие;
- c_{rel} – относительная вычислительная стоимость метода.

Использование не только quality-метрик, но и временных/ресурсных показателей согласуется с современными исследованиями по edge-ориентированным IoT-методам, где эффективность должна рассматриваться совместно с вычислительной стоимостью [13–14].

5. Результаты сравнения методов

Результаты модельного вычислительного эксперимента приведены в таблице 1.

Из таблицы 1 следует, что простой статический подход характеризуется наименьшими вычислительными затратами, однако имеет наибольшую вероятность ложного допуска. Это означает, что проверка только по идентификатору не обеспечивает требуемого уровня защищённости в условиях контекстно-зависимых нарушений.

Переход к пороговой контекстной проверке без накопления аномальности приводит к заметному снижению FAR и росту полноты выявления. Однако этот вариант по-прежнему недостаточно устойчив к сериям пограничных событий, поскольку не учитывает их накопительный эффект. Предлагаемый метод показывает наилучшие значения $Recall$ и F_1, а также минимальный FAR. Это указывает на более высокую способность выявлять некорректные события при меньшем числе опасных пропусков. При этом наблюдается умеренный рост FRR и вычислительной стоимости по сравнению с более простыми подходами, что является ожидаемой платой за повышение защищённости.

6. Анализ результатов по типам аномалий

Для более детальной оценки были отдельно рассмотрены результаты по различным типам аномальных сценариев. Они приведены в таблице 2.

Наибольшее различие наблюдается для серии пограничных событий. Для данного класса аномалий статическая проверка и даже разовая контекстная верификация демонстрируют ограниченную эффективность, так как отдельные события по отдельности могут не пересекать установленный порог аномальности. Предлагаемый метод, благодаря использованию накопительной переменной A_t, выявляет такие сценарии существенно лучше. Именно этот результат подтверждает целесообразность введения адаптивного режима контроля безопасности: он позволяет учитывать не только локальное качество текущего события, но и характер развития процесса во времени.

7. Влияние накопительного механизма и обсуждение результатов

Дополнительная проверка показала, что рациональные значения коэффициента памяти λ лежат в диапазоне 0,6–0,75: при меньших значениях снижается чувствительность метода

Таблица 1.

Сравнение методов принятия решения по основным показателям

Метод	FAR	FRR	$Recall$	$Precision$	F_1	t_{avg}	c_{rel}
Baseline-1: статическая проверка идентификатора	0,173	0,041	0,781	0,812	0,796	0,19	1,00
Baseline-2: контекстная проверка без накопления	0,091	0,058	0,872	0,884	0,878	0,43	1,84
Предлагаемый метод	0,049	0,064	0,931	0,918	0,924	0,67	2,41

Таблица 2.

Полнота выявления по типам аномальных сценариев

Тип аномалии	Baseline-1	Baseline-2	Предлагаемый метод
Нарушение временного окна	0,69	0,86	0,91
Нарушение последовательности событий	0,62	0,84	0,93
Команда в недопустимом состоянии	0,74	0,88	0,94
Нетипичный контекст при допустимом источнике	0,71	0,82	0,90
Серия пограничных событий	0,55	0,67	0,96

к распределённым во времени аномалиям, а при больших возрастает число ложных блокировок. Это подтверждает целесообразность использования накопительного механизма как средства выявления устойчивых аномальных паттернов.

Результаты эксперимента показывают, что учёт контекстных признаков сам по себе повышает качество принятия решения по сравнению со статической проверкой идентификатора. Наибольший прирост достигается за счёт введения накопительной оценки аномальности и адаптивного режима контроля, что особенно заметно в сценариях, где вредоносная активность распределена во времени и маскируется под последовательность частично допустимых действий. При этом рост вычислительной стоимости остаётся ограниченным и не приводит к неприемлемому увеличению задержки обработки событий, что согласуется с требованиями edge-ориентированных решений [13–17].

8. Вывод по результатам экспериментального исследования

Результаты модельного вычислительного эксперимента показывают, что предложенный метод контекстной верификации событий и адаптивного выбора режима контроля безопасности превосходит базовые статические и пороговые подходы по ключевым показателям защищённости. Наиболее существенное улучшение достигается по вероятности ложного допуска и полноте выявления некорректных событий, особенно в сценариях с распределённой во времени аномальной активностью. Следовательно, цель статьи может считаться достигнутой в рамках проведённого модельного исследования.

Заключение

В статье рассмотрена задача повышения защищённости распределённой IoT-подсистемы специального назначения в условиях киберугроз, нестационарности событийного потока и ограниченных ресурсов периферийных узлов. Показано, что статические правила проверки событий и решения, основанные только на идентификаторе источника, недостаточны для выявления сложных контекстно-зависимых нарушений.

Предложен метод контекстной верификации событий при контроле безопасности, в котором допустимость события определяется на основе идентификационных, временных, процессных, состояний и ресурсных факторов. В развитие этого подхода введён механизм накопительной оценки аномальности и адаптивного выбора режима контроля безопасности, позволяющий учитывать не только текущее событие, но и характер развития событийного процесса во времени.

В рамках модельного вычислительного эксперимента показано, что предложенный метод превосходит базовые статические и пороговые подходы по вероятности ложного допуска и полноте выявления некорректных событий, особенно в сценариях с распределённой во времени аномальной активностью. Полученные результаты позволяют сделать вывод о достижении поставленной цели работы – повышении защищённости распределённой IoT-подсистемы за счёт разработки метода контекстной верификации событий и адаптивного выбора режима контроля безопасности.

Перспективы дальнейших исследований связаны с уточнением процедуры настройки весовых коэффициентов и пороговых параметров, а также с расширением метода на более сложные распределённые IoT/IoRT-сценарии с несколькими взаимосвязанными контурами принятия решений.

Литература

1. Hogan M., Piccarreta B. Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT). Gaithersburg: National Institute of Standards and Technology, 2018. – P. 185. – DOI: 10.6028/NIST.IR.8200.
2. Fagan M., Megas K. N., Scarfone K., Smith M. IoT Device Cybersecurity Capability Core Baseline. Gaithersburg: National Institute of Standards and Technology, 2020. – P. 23. – DOI: 10.6028/NIST.IR.8259A.
3. Ravidas S., Lekidis A., Paci F., Zannone N. Access control in Internet-of-Things: A survey // Journal of Network and Computer Applications, 2019. – Vol. 144. – Pp. 79–101. – DOI: 10.1016/j.jnca.2019.06.017.
4. Ragothaman K., Wang Y., Rimal B., Lawrence M. Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions // Sensors, 2023. – Vol. 23. – No 4. – Art. 1805. – DOI: 10.3390/s23041805.
5. Ahsan M. S., Pathan A.-S. K. A Comprehensive Survey on the Requirements, Applications, and Future Challenges for Access Control Models in IoT: The State of the Art // IoT, 2025. – Vol. 6. – Art. 9. – DOI: 10.3390/iot6010009.
6. Khan M. A., Khan M. A., Jan S. U., Ahmad J., Jamal S. S., Shah A. A., Pitropakis N., Buchanan W. J. A Deep Learning-Based Intrusion Detection System for MQTT Enabled IoT // Sensors, 2021. – Vol. 21. – Art. 7016. – DOI: 10.3390/s21217016.
7. Empl P., Böhm F., Pernul G. Process-Aware Intrusion Detection in MQTT Networks // Proceedings of the Fourteenth ACM Conference on Data and Application Security and Privacy (CODASPY '24). Porto, Portugal, 2024. – Pp. 91–102. – DOI: 10.1145/3626232.3653271.

8. Kayes A. S. M., Rahayu W., Dillon T., Chang E. A Survey of Context-Aware Access Control Mechanisms for Cloud and Fog Networks: Taxonomy and Open Research Issues // Sensors, 2020. – Vol. 20. – No 9. – Art. 2464. – DOI: 10.3390/s20092464.
9. Kalaria R., Kayes A. S. M., Rahayu W., Pardede E., Shahraki A. S. Adaptive context-aware access control for IoT environments leveraging fog computing // International Journal of Information Security, 2024. – Vol. 23. – Pp. 3089–3107. – DOI: 10.1007/s10207-024-00866-4.
10. Butun I., Sari A., Österberg P. Hardware Security of Fog End-Devices for the Internet of Things // Sensors, 2020. – Vol. 20. – No. 20. – Art. 5729. – DOI: 10.3390/s20205729.
11. Hindy H., Bayne E., Bures M., Atkinson R., Tachtatzis C., Bellekens X. Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset) // arXiv, 2020. arXiv:2006.15340.
12. Vaccari I., Chiola G., Aiello M., Mongelli M., Cambiaso E. MQTTset, a New Dataset for Machine Learning Techniques on MQTT // Sensors, 2020. – Vol. 20. – No 22. – Art. 6578. – DOI: 10.3390/s20226578.
13. Mudgerikar A., Sharma P., Bertino E. Edge-Based Intrusion Detection for IoT devices // ACM Transactions on Management Information Systems, 2020. – Vol. 11. – No. 4. – Art. 18. – DOI: 10.1145/3382159.
14. Asulba B., Souto P. F., Almeida L. Bringing IoT Intrusion Detection to the Edge // Proceedings of the 8th International Conference on Future Networks & Distributed Systems (ICFNDS '24). Marakech, Morocco, 2024. New York: ACM, 2024. – P. 10. – DOI: 10.1145/3726122.3726166.
15. Котенко И. В., Саенко И. Б., Липатников В. А., Андреев И. А. Метод динамического обнаружения киберугроз в распределенных системах Интернета вещей на основе генеративных моделей // Прикладная информатика. – 2026. – Т. 21. – № 2. – С. 102–118. – DOI: 10.37791/2687-0649-2026-21-2-102-118.
16. Липатников В. А., Шевченко А. А., Косолапов В. С., Сокол Д. С. Метод обеспечения информационной безопасности сети VoIP-телефонии с прогнозом стратегии вторжений нарушителя // Информационно-управляющие системы, 2022. – № 1. – С. 54–67. – DOI: 10.31799/1684-8853-2022-1-54-67.
17. Липатников В. А., Шевченко А. А., Мелехов К. В., Ткачев Д. Ф. Методика повышения защищенности сети передачи данных объектов критической информационной инфраструктуры при многоэтапных атаках // Информационно-управляющие системы, 2024. – № 1. – С. 44–55. – DOI: 10.31799/1684-8853-2024-1-44-55.

METHOD OF FIELD VERIFICATION OF EVENTS IN SECURITY CONTROL OF A DISTRIBUTED IoT SUBSYSTEM

Andreev I. A.[4], Lipatnikov V. A.[5], Tarasenko S. E.[6]

Keywords: *Internet of Things, IoT, ESP32, MQTT, security control, field verification of events, edge nodes, server data processing, virtual assistant, adaptive control mode.*

Abstract

The aim of the work *is to improve the security of the distributed IoT security control subsystem by developing a method for field verification of events and adaptive selection of the security control mode when interaction between edge nodes based on ESP32 and the virtual assistant server.*

Research method: *the methods of formalizing the event circuit of the distributed IoT subsystem, constructing an indicator of confidence in an event based on identification, time, process, state and resource factors, as well as cumulative assessment of the anomalousness of the event flow were used. To test the proposed approach, a model computational experiment based on the generation of sequences of access events, telemetry and control actions was used. A comparative assessment was carried out in relation to the basic static and threshold methods of safety control.*

Results of the study: *a method of field verification of events based on the joint consideration of identification, time, process and resource factors is proposed; a rule for cumulative anomaly assessment and adaptive selection of the security control mode is developed; an applied scenario of a distributed IoT subsystem with two ESP32 nodes and server data processing is formed and investigated; it is shown that the proposed approach surpasses the basic static and threshold methods for the probability of false tolerance and completeness of detection of invalid events, especially in the case of anomalous activity distributed over time.*

The scientific novelty *lies in the development of a method for field verification of events in the security control of a distributed IoT subsystem, taking into account the context of the event, cumulative anomaly assessment and adaptive selection of the security control mode in conditions of limited resources of peripheral nodes and server-edge architecture of data processing.*

4 ***Ilya A. Andreev***, Operator of the scientific company, Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny. St. Petersburg, Russia. E-mail: andreev.ilia.1984@mail.ru

5 ***Valery A. Lipatnikov***, Honored Scientist of the Russian Federation, Doctor of Technical Sciences, Professor, Senior Researcher of the Research Center, Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny. St. Petersburg, Russia. E-mail: lipatnikovanl@mail.ru

6 ***Stanislav E. Tarasenko***, Senior Researcher, Research Center, Military Academy of Communications named after Marshal of the Soviet Union S.M. Budyonny. St. Petersburg, Russia. E-mail: s.tar.my@mail.ru