УДК 004.6
doi:10.31799/1684-8853-2022-5-23-31
EDN: DNOSCW

Научные статьи
Articles

# Формирование адаптивных рассылок брокера данных интернета вещей

***О. С. Исаева***[a]***,*** *канд. техн. наук, старший научный сотрудник, orcid.org/0000-0002-5061-6765, isaeva@icm.krasn.ru*
***С. В. Исаев***[a]***,*** *канд. техн. наук, доцент, orcid.org/0000-0002-6678-0084*
***Н. В. Кулясов***[a]***,*** *программист, orcid.org/0000-0001-5582-9498*
[a]*Институт вычислительного моделирования СО РАН, Академгородок, 50/44, Красноярск, 660036, РФ*

***Введение:*** *возможности взаимодействия с физическим миром через сетевые инфраструктуры пространственно-распределенных узлов интернета вещей несмотря на неоспоримые преимущества технологии вызывают существенные нагрузки на потребителей информации. В этой связи актуальным является создание методов, обеспечивающих сокращение передаваемых объемов данных за счет адаптивной синхронизации систем мониторинга со временем протекания реальных процессов.* ***Цель:*** *разработать подход к формированию адаптивных рассылок брокера данных на основе исследования цикличности наблюдений устройств интернета вещей.* ***Результаты:*** *в рамках корпоративной сети Красноярского научного центра развернута инфраструктура устройств и приложений интернета вещей для мониторинга показателей температуры, влажности и PM2.5 в специализированных технологических помещениях с телекоммуникационным оборудованием. К собираемым данным применен метод дискретного преобразования Фурье. На основании рассчитанных параметров гармонического ряда сделан вывод о частотных характеристиках данных. Выбраны основные пики, описывающие периодичность данных, определены точки колебаний и по теореме Котельникова выбрана частота дискретизации, обеспечивающая достаточную интенсивность наблюдений. Анализ показал, что для различных помещений данные имеют периодический характер, но их гармонические профили не совпадают. Выбор значений гармоник, амплитуда колебания которых определяет динамику изменений в наблюдаемых данных, следует проводить периодически для каждого наблюдаемого устройства. Этот подход реализован в программном обеспечении брокера, который выдает данные по подпискам от каждого из устройств в соответствии с частотой их изменений.* ***Практическая значимость:*** *анализ частотных характеристик данных определяет настройки брокера, которые сокращают потоки выдаваемой информации, что является одним из аспектов обеспечения надежности инфраструктуры интернета вещей. Кроме того, наблюдение за изменениями характера данных позволяет выявлять неполадки в работе охлаждающих систем, которые могут приводить к выходу из строя сложного дорогостоящего оборудования, обладающего повышенной теплоотдачей.*

***Ключевые слова*** *— интернет вещей, протокол обмена сообщениями, Message Queuing Telemetry Transport, дискретное преобразование Фурье, теорема Котельникова.*

**Для цитирования:** Исаева О. С., Исаев С. В., Кулясов Н. В. Формирование адаптивных рассылок брокера данных интернета вещей. *Информационно-управляющие системы*, 2022, № 5, с. 23–31. doi:10.31799/1684-8853-2022-5-23-31, EDN: DNOSCW
**For citation:** Isaeva O. S., Isaev S. V., Kulyasov N. V. Formation of adaptive publications from the Internet of Things data broker. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 5, pp. 23–31 (In Russian). doi:10.31799/1684-8853-2022-5-23-31, EDN: DNOSCW

## Введение

Концепция интернета вещей (Internet of Things, IoT) как обобщающего ключевого понятия для «вещь-ориентированных», «интернет-ориентированных» и «семантико-ориентированных» технологий обеспечивает расширение базовых основ Интернета в физическую сферу [1, 2]. Возможность взаимодействия с физическим миром осуществляется благодаря наличию устройств, способных ощущать физические явления и преобразовывать их в поток информации, а также способных запускать действия, влияющие на физические устройства через исполнительные механизмы. Таким образом, IoT представляет собой динамическую глобальную сетевую инфраструктуру пространственно-распределенных узлов, оснащенных встроенными средствами для взаимодействия друг с другом или с внешней средой и способных измерять, понимать и даже изменять свое окружение [3].

По разным оценкам международных аналитических агентств, количество активных устройств IoT в ближайшее время в мире достигнет от 30 до 60 млрд [4]. Такие цифры предполагают, что IoT станет одним из основных источников больших данных [5], что влечет за собой необходимость переосмысления традиционных подходов к организации вычислительных ресурсов и услуг. Решения проблем надежности, производительности, безопасности и конфиденциальности взаимодействия всех уровней сетевой архитектуры поставщиков или потребителей информации лежат на стыке таких областей знаний, как телекоммуникации, информатика, электроника и др. [6]. И такое решение основывается на детальном исследовании архитектуры IoT и протоколов передачи данных.

В общем случае архитектура IoT состоит из следующих функциональных уровней: сенсорного, транспортного, сервисного и прикладного [7]. Уровни и объекты IoT обладают свойством неоднородности и могут содержать дополнительные приложения для обслуживания, управления и использования устройств, включая широкий спектр интеллектуальных систем. Благодаря такой неоднородности IoT становится важным аспектом повседневной жизни [8, 9]. На сенсорном уровне размещаются датчики, обеспечивающие сбор информации о состоянии наблюдаемых объектов. Устройства IoT имеют ограниченные ресурсы, которые не допускают сложной обработки данных на месте. Для их передачи разворачивается транспортная структура, включающая шлюзы и сети передачи данных. Через этот уровень от устройств IoT поступают данные. Они интегрируются на сервисном уровне, где размещается брокер данных, обеспечивающий сбор, интеграцию, хранение и передачу информации в соответствии с используемыми протоколами. На этом уровне консолидируются неструктурированные или полуструктурированные данные, которые характеризуются большим объемом, разнообразием и частотой генерации [10]. Подготовленные данные поступают на прикладной уровень, включающий проблемно-ориентированные приложения, решающие задачи конкретной предметной области [11]. Для обмена данными используются различные протоколы. В нашем исследовании выбран открытый протокол MQTT (Message Queue Telemetry Transport) [12]. Он позволяет работать с удаленными локациями, имеющими ограничения по возможной обработке и пропускной способности каналов связи. Реализация протокола предусматривает взаимодействие логических сущностей со следующими ролями: Издатель (Publisher) — устройство IoT, формирующее сообщение; Брокер (Broker) — специализированное программное обеспечение, получающее и распределяющее сообщения, например Mosquitto MQTT, и Подписчик (Subscriber) — устройства или программное обеспечение, получающее данные от разных издателей по заданным тематическим подпискам [13, 14].

Гетерогенность и иерархичность архитектуры IoT обуславливают необходимость создания специализированных подходов к анализу безопасности, а также к организации механизмов сбора и мониторинга генерируемых данных. В работах [15, 16] показаны подходы к мониторингу и анализу сетевого трафика структурированных данных журналов обращений. В [17, 18] проводится анализ уязвимостей, определяемых особенностями аутентификации в протоколе MQTT схемы Издатель — Брокер — Подписчик, однако полученные в них рекомендации носят общий характер и не предоставляют автоматизированных подходов. В [19, 20] выполнено исследование сетевой архитектуры IoT и предложены универсальные инструменты анализа безопасности различных уровней сети IoT. В их основе лежит подход к построению профилей умных устройств из статистических характеристик сеансов связи: интенсивности и продолжительности передачи пакетов данных. Предложен единый (для всех уровней архитектуры IoT) подход к обнаружению атак, основанный на методах машинного обучения. Проблемы адаптивного доступа к данным на прикладном уровне архитектуры IoT, как правило, остаются за рамками проводимых исследований. Существенное значение эта проблема имеет при использовании конечных устройств, обладающих ограниченными возможностями по обработке данных (мобильных сервисов и приложений). Разумное сокращение передаваемых объемов информации является одним из аспектов защиты от перегрузки сети IoT и способствует обеспечению ее надежности и безопасности. В этом случае требуется автоматизировать анализ поступающих от устройств IoT пакетов, определять скорости протекания наблюдаемых событий и выполнять адаптивную настройку режима выдачи информации от брокера данных потребителям.

Цель исследования — разработать подход к формированию адаптивных рассылок брокера данных на основе исследования данных, собираемых устройствами IoT.

Поскольку большинство процессов как для производственных, так и для бытовых систем имеют периодический характер, то изучение циклических характеристик данных, собираемых устройствами IoT, оправдано и позволит лучше понимать суть происходящих в них явлений. Цикличность — это свойство работы системы, которая стремится сохранить свое состояние в границах равновесия. Для исследования в работе применен метод дискретного преобразования Фурье [21], и на основе рассчитанных параметров гармонического ряда сделан вывод о частотных характеристиках данных. Подобный подход получил свое применение в работах по исследованию частотно-временных характеристик различных последовательностей данных [22].

## Постановка задачи исследования данных IoT

Для проведения исследований в рамках корпоративной сети Красноярского научного центра развернута инфраструктура устройств и приложений IoT. Устройства IoT размещены в специализированных технологических помещениях с теле-

коммуникационным оборудованием и выполняют мониторинг показателей температуры, влажности и PM2.5. Результаты измерений датчиков от устройств IoT по протоколу MQTT поступают брокерам, которые их собирают, обрабатывают, размещают в базах данных и передают в устройства и приложения. Кроме того, брокер собирает сетевые журналы, содержащие сведения о наличии обращений к данным и несанкционированных запросах. У подписчиков (например, мобильных приложений) существуют ограничения на объемы и частоту поступления данных. Задача брокера — обеспечить адаптивность режима выдачи данных, при котором частота их обновления соответствовала бы скорости протекания наблюдаемых событий. Требуется выполнить анализ поступающих данных и создать инструменты для формирования адаптивных рассылок.

Концептуальная схема инфраструктуры IoT (рис. 1) содержит как развернутые в настоящий момент системы и сервисы, так и потенциальные точки расширения и объединяет потоки данных устройств IoT и приложений.

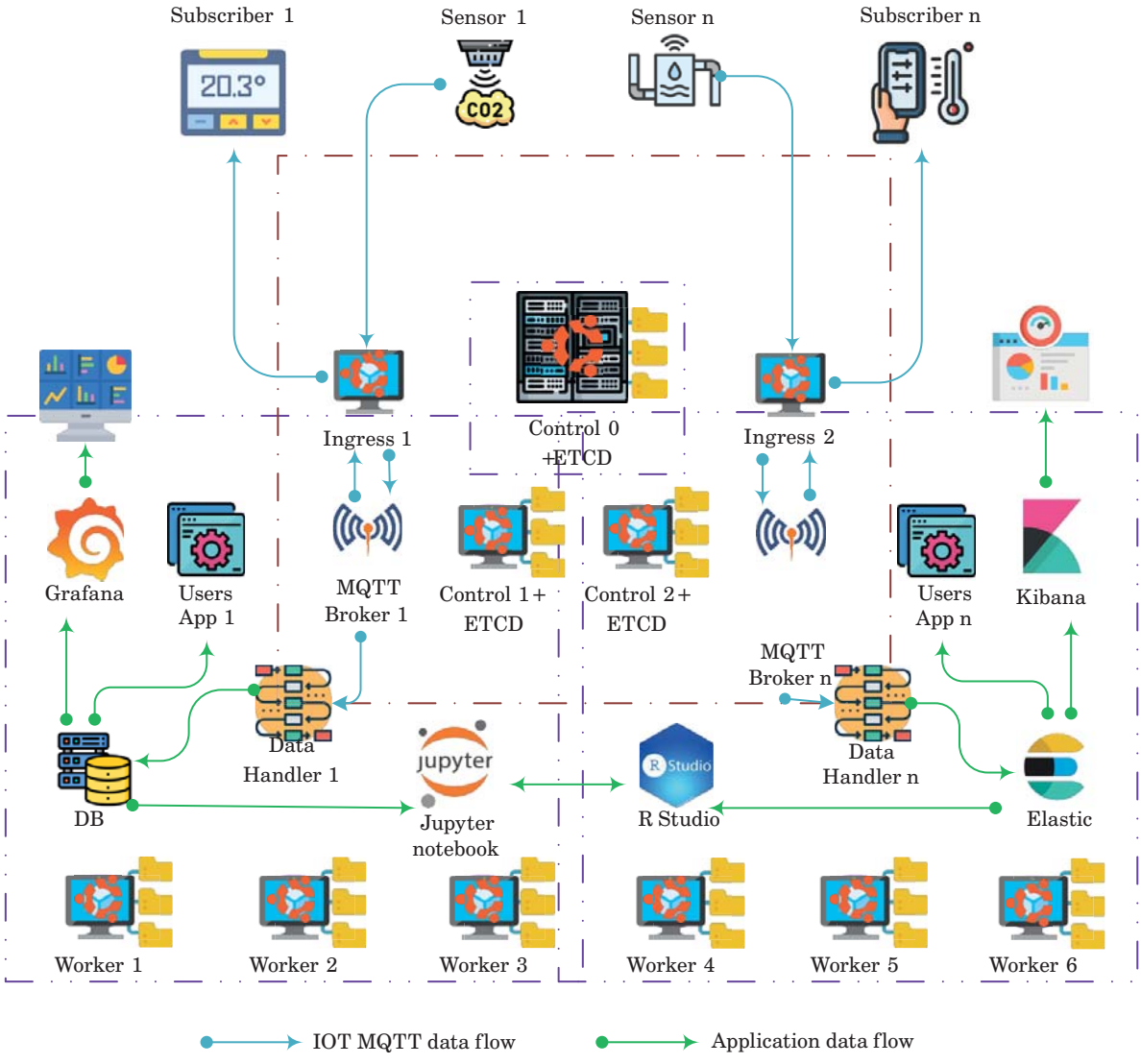
В концептуальной схеме представлены основные устройства и приложения инфраструктуры:

— устройства сенсорного уровня для сбора данных и взаимодействия с окружением по протоколу MQTT (на рисунке обозначены как Sensor);

— маршрутизаторы трафика из внешней сети в кластер (Ingress);

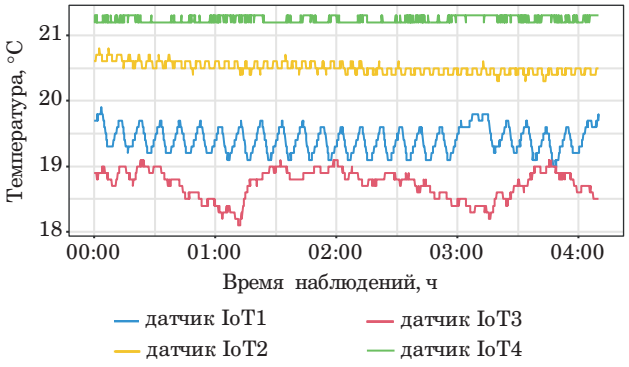
— узлы кластера, предназначенные для развертывания контейнеров с приложениями (Control, Worker);

— брокеры рассылки данных по протоколу MQTT (MQTT Broker);




■ ***Рис. 1.*** Концептуальная схема инфраструктуры IoT

■ ***Fig. 1.*** Conceptual diagram of the IoT infrastructure




■ ***Рис. 2.*** График температуры с датчиков
■ ***Fig. 2.*** Graph of temperature from sensors

— сервисы для анализа данных и настройки рассылок (Data Handler);

— база данных (DB — в нашей реализации MySQL и PhpMyAdmin);

— обработчики данных и приложения, выступающие подписчиками MQTT-брокера (Subskriber);

— средства разработки, графические интерфейсы и компоненты статистического анализа и визуализации (R-Studio, Jupiter, Kibuna, Grafana, Elastik, Users App).

Детали организации и настройки самой инфраструктуры IoT в настоящей статье не рассматриваются.

Из приведенной структуры выделены потоки данных между издателями, брокерами и подписчиками. Устройства IoT собирают данные с датчиков (температуры, влажности и PM2.5), на рис. 2 показан фрагмент графика результатов измерений, получаемых брокером данных от устройств IoT.

Из наблюдений видно, что характеристики цикличности результатов измерений различаются для каждого из устройств.

## Формирование адаптивных рассылок

Устройства IoT установлены в технологических помещениях с оборудованием, обладающим повышенной теплоотдачей. В помещениях установлены системы кондиционирования, выход из строя или изменение режима работы которых повлечет проблемы в работоспособности сложного коммуникационного и вычислительного оборудования. Периодичность поступления данных с устройств IoT в MQTT-брокер настраивается на источниках данных.

Рассмотрим дискретные моменты времени наблюдения $\{t_n\}$, где $n = [0,\ N-1]$, $N$ – количество отсчетов. Время между наблюдениями $\Delta t = (t_{n+1} - t_n) + \tau$, где $\tau$ – задержки передачи данных. Значение $\tau$ столь мало, что период дискретизации можно считать постоянным, равным $T = (t_{n+1} - t_n)$. Длительность наблюдений равна $NT$. Представим последовательность наблюдаемых данных как функцию дискретного аргумента, принимающую произвольные положительные значения в дискретные промежутки времени $nT$: $x(t) = \{x(nT)\}$, где $x(nT)$ — $n$-й результат наблюдений в момент $nT$.

Функция $x(t)$ — периодическая, в общем случае свойство периодичности достигается путем повторения рассматриваемых данных с периодом $NT$. Для периодической функции может быть выполнено спектральное разложение в виде ряда Фурье и получен дискретный спектр $X(k)$, $k \in Z$, состоящий из гармоник, кратных $\Delta\omega = 2\pi/T$. Поскольку исходная функция $x(t)$ — дискретная, достаточно определить спектральные значения для $k = [0,\ N-1]$. Коэффициенты разложения в ряд Фурье могут быть получены по формуле дискретного преобразования, которое зависит только от индекса входного сигнала:

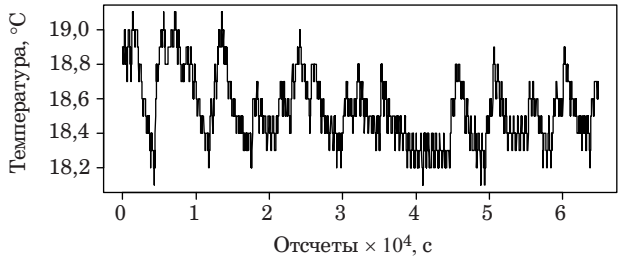
$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-i\frac{2\pi}{N}nk}. \qquad (1)$$

Преобразование позволяет по $N$ измерениям значений $x(t)$ получить $N$ спектральных отсчетов на одном периоде повторения спектра $X(k)$.

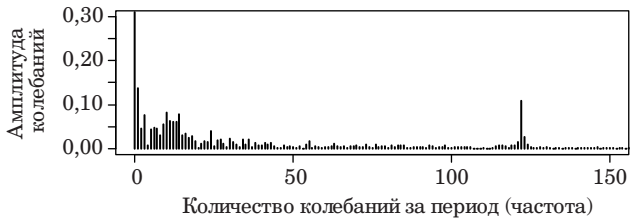
Применим к нашим результатам наблюдений по каждому из источников дискретное преобразование Фурье, рассмотрим модули комплексных чисел полученных коэффициентов. По ним будем делать вывод о значениях амплитуд и частот гармоник. На основе полученного результата сделаем вывод о частоте изменения наблюдаемых событий и сформируем настройки для выдачи данных, которые позволят выбирать значимые события. Такую последовательность действий требуется выполнять для большого набора данных с заданной периодичностью, чтобы оперативно изменять настройки времени событий выдачи данных. Реализация этого подхода позволит автоматически формировать адаптивные подписки.

Поясним подход к формированию адаптивных рассылок на примере. Возьмем выборку данных, являющихся результатом измерений в $N$ отсчетах (рис. 3).

Применим дискретное преобразование Фурье (1) и построим частотный спектр данных. Весовые коэффициенты разложения являются комплексным спектром периодического сигнала (нашей выборки данных). По коэффициентам Фурье построим $\mathrm{mod}(X(k))$, где mod — функция, возвращающая действительную часть комплексного числа. График результатов показан на рис. 4.




■ ***Рис. 3.*** Данные в наблюдаемых отсчетах
■ ***Fig. 3.*** Data in the observed samples




■ ***Рис. 4.*** Частотный спектр данных
■ ***Fig. 4.*** Frequency spectrum of data

Построенный спектр — дискретный и состоит из гармоник, кратных $\Delta\omega$. Его первая гармоника при $k = 0$ является основной частотой сигнала и отражает постоянную составляющую данных. Для настройки адаптивных рассылок ее не учитываем. Остальные частоты дискретного спектра (при $k \geq 1$) являются гармониками сигнала. Требуется найти значения гармоник, амплитуда колебания которых показывает динамику изменений в наблюдаемых данных. Зададим порог $\varepsilon$ для выбора значений амплитуд, которые будем учитывать при анализе. Минимальное $\varepsilon$ может быть определено из характеристик точности используемых датчиков IoT. Выберем коэффициенты разложения $X(k)$ такие, что $\mathrm{Re}(X(k)) > \varepsilon$ и выполнено условие

$$X(k-1) \leq X(k) \geq X(k+1). \quad (2)$$

По $k$ (номеру коэффициента) определим период колебаний, соответствующий выбранным $X(k)$, разделив интервал наблюдений $NT$ на номер отсчета:

$$P(k) = NT/k. \quad (3)$$

Частоту колебаний будем рассчитывать по формуле

$$F(k) = 1/P(k). \quad (4)$$

Выберем для $k$, удовлетворяющих условию (2), максимальную частоту колебаний спектра сигнала, определяющую период дискретизации $Fd$:

$$Fd = \max F(k). \quad (5)$$

Воспользуемся теоремой Котельникова [23, 24], согласно которой если спектр сигнала ограничен частотой $F_{\max}$, то он может быть однозначно восстановлен по его дискретным отсчетам, взятым через интервалы времени с частотой как минимум в два раза превышающей максимальную частоту сигнала, который мы хотим измерить, т. е. на каждое колебание сигнала (изменение измеренных значений) должно приходиться как минимум два отсчета. Отсюда следует, что для наблюдения за данными достаточно выполнять измерения с частотой дискретизации

$$F_{\max} \geq 2Fd. \quad (6)$$

Минимальный период дискретизации определяется обратно максимальной частоте:

$$P_{\min} = 1/F_{\max}. \quad (7)$$

В рассматриваемом примере значения $k \in \{10, 14, 122\}$ удовлетворяют условию (2) коэффициентов разложения (1) с частотами, соответствующими периодам колебаний (3) $P(k) \in \{6480, 4632, 525\}$ секунд соответственно. По (4) определяем частоту. По (5) выбираем максимальную частоту колебаний наблюдаемых данных: $Fd = 1/525$ Гц, и частоту дискретизации можем выбрать из (6): $F_{\max} = Fd \cdot 2 = 2/525$ Гц. Отсюда получаем по (7) период дискретизации $P_{\min} = 262{,}5$ с. Найденный период $P_{\min}$ применяется для настройки брокера, что обеспечивает наблюдение за событиями в соответствии с динамикой их изменений.

## Выбор периода дискретизации данных для устройств IoT

Предложенный подход применим для настройки выдачи данных от устройств IoT, в том числе для энергонезависимых источников. Уменьшение частоты пересылки данных от таких устройств к брокеру и увеличение длительности периодов покоя продлит время их автономного функционирования.

Выбор параметров дискретизации измерений выполняется на основе статистики их работы по формуле (7). Рассматривается длительный интервал наблюдений. Для избежания потери информативности в моменты неактивности устройств IoT при выборе интервала дискретизации следует учитывать минимальный период измерений при максимальной скорости протекания наблюдаемых процессов. В общем случае скорость может быть получена на основе собран-


■ ***Рис. 5.*** Данные для расчета максимальной скорости протекания процессов

■ ***Fig. 5.*** Data for calculating the maximum speed of processes

ной статистики (при имитации критических состояний):

$$S_{\max} = \max_{k=1,N} \frac{|X(k) - X(k-1)|}{\Delta t}. \quad (8)$$

Для каждого наблюдаемого показателя зададим значение $X_{\min}$ его допустимого изменения, тогда период вычисляется на основе скорости протекания процессов:

$$P_S = X_{\min} / S_{\max}. \quad (9)$$

Результирующий период дискретизации для работы устройств IoT определяется из результатов (7) и (9):

$$P_d = \min(P_S, P_{\min}). \quad (10)$$

Рассмотрим пример определения периода дискретизации для датчиков IoT измерения температуры окружающей среды. Устройства IoT выполняют измерения и передают данные брокеру каждые 10 с. Требуется поддерживать температуру технологических помещений в диапазоне 18–24 °C. Покажем, каким должен быть режим выдачи данных при допустимом изменении на 2 °C.

Скорость протекания процессов вычисляется из данных, полученных как при стандартном режиме работы, так и при имитации выхода из строя систем охлаждения и увеличении нагрузки на серверное оборудование. Фрагмент графика исходных данных приведен на рис. 5.

По (8) максимальная скорость изменения температуры составляет 0,04 °C/с, по (9), (10) период дискретизации составляет 50 с. Проведенный расчет позволяет сократить количество передаваемых данных и периодов активности устройств IoT в 5 раз. Перенастройка устройств IoT должна происходить при изменении параметров физического состояния окружения.

## Обсуждение предложенного подхода

Реализация предложенного в работе подхода выполнена в виде сервиса на языке R. Используемый брокер имеет открытый код и модифицирован для получения конфигурационных настроек от сервиса. Получатели данных подписываются на данные брокера без возможности взаимодействовать напрямую с устройствами IoT.

Подход применим для стандартного функционирования, когда необходимо снизить нагрузку на мобильные устройства, выполняющие мониторинг данных. Он позволяет сократить объем рассылок от брокера и уменьшить загрузку каналов связи при сохранении адекватности представления протекающих процессов. Такие рассылки помечаются флагом «0 — at most once» в поле качества обслуживания Quality of Service (QoS) протокола MQTT. Сообщения, выходящие за границы диапазонов безопасного функционирования систем, не фильтруются данным сервисом и помечаются флагом «2 — exactly once», что гарантирует их обязательную доставку подписчикам. В дальнейшем сервисы обработки данных будут модифицированы для обнаружения критических ситуаций и посылки сообщений брокером с измененными флагами QoS.

В настоящий момент рассматриваются варианты внедрения функций сервиса в код брокера. Это возможно, поскольку в расчетах используется быстрое дискретное преобразование Фурье, имеющее сложность $O(N*\log N)$, что не приводит к существенным вычислительным затратам, в том числе и при увеличении длительности периода, за который анализируются данные (подтверждено экспериментами). В рассмотренном примере длительность периода выборки данных, превышающая сутки, не актуальна, так как протекающие процессы имеют периодичность несколько десятков секунд. Но этот подход может быть применен для медленно протекающих процессов, где период рассылок может быть существенно увеличен, что потребует увеличения периода выборки анализируемых данных.

При наблюдении нескольких параметров следует выбирать для них минимальный период дискретизации. Например, для показателей влажности технологических помещений существенным критерием является скорость изменения показателя не более 6 % в час для исключения конденсации влаги. Эта оценка устанавливается для расчета периода дискретизации для устройств измерения влажности. К непериодическим процессам или процессам, имеющим мгновенное протекание, предложенный в работе подход не применим.

## Заключение

Интернет вещей определяет новые архитектурные и технологические решения для разнообразных инфокоммуникационных задач. Выполненное исследование по формированию адаптивных рассылок данных устройств IoT является основой функционирования автономных систем сбора данных и независимых сервисов для их анализа. Применение математических методов сокращает объемы передаваемых данных и оптимизирует работу всех элементов инфраструктуры IoT, каждое устройство которой имеет собственные спектральные характеристики. Автоматизация указанных функций позволяет соотносить время наблюдений со временем протекания реальных процессов. Анализ частотных характеристик собранных данных выполняется в заданные промежутки времени и определяет адаптивность персональных настроек брокера данных по всем анализируемым устройствам, что позволяет сократить нагрузку на устройства — потребители информации.

Дальнейшее исследование спектральных характеристик собираемых данных позволит понимать суть наблюдаемых явлений и выявлять нарушения в работе устройств, оказывающих влияние на измеряемые показатели. Вследствие этого применение данного подхода для мониторинга состояния специализированных технологических помещений с телекоммуникационным оборудованием имеет существенное практическое значение. Так, например, изменение спектральных характеристик температурных наблюдений даже в случае нахождения всех значений в допустимых границах свидетельствует о необходимости провести диагностику охлаждающего оборудования, поскольку может быть следствием отключения части устройств или изменения их режима работы. Превентивные меры позволят избежать неконтролируемого превышения температурных значений, которое приведет к выходу из строя сложного дорогостоящего оборудования, обладающего повышенной теплоотдачей.

## Финансовая поддержка

Работа поддержана Красноярским математическим центром, финансируемым Минобрнауки РФ в рамках мероприятий по созданию и развитию региональных НОМЦ (соглашение № 075-02-2022-873).

## Литература


1. **Atzori L., Iera A., Morabito G.** The Internet of Things: A survey. *Computer Networks*, 2010, no. 54, pp. 2787–2805. doi:10.1016/j.comnet.2010.05.010
2. **Korte A., Tiberius V., Potsdam U., Brem A., Stuttgart U.** Internet of Things (IoT) technology research in business and management literature: Results from a co-citation analysis. *Journal of Theoretical and Applied Electronic Commerce Research*, 2021, no. 16(6), pp. 2073–2090. doi:10.3390/jtaer16060116
3. **Rozik A. S., Tolba A. S., El-Dosuky M. A.** Design and implementation of the Sense Egypt platform for real-time analysis of IoT data streams. *Advances in Internet of Things*, 2016, no. 6(4), pp. 66–91.
4. **Alam T.** A reliable communication framework and its use in Internet of Things (IoT). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2018, no. 3(5), pp. 450–456.
5. **Gubbi J., Buyya R., Marusic S., Palaniswami M.** Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 2013, no. 29(7), pp. 1645–1660. doi:10.1016/j.future.2013.01.010
6. **D'Angelo G., Ferretti S., Ghini V.** Simulation of the Internet of Things. *Proc. of the Intern. Conf. on High Performance Computing and Simulation*, 2016, pp. 1–8. doi:10.1109/HPCSim.2016.7568309
7. **Javed A., Heljanko K., Buda A., Främling K.** CEFIoT: A fault-tolerant IoT architecture for edge and cloud. *IEEE World Forum on Internet of Things*, 2018, pp. 813–818. doi:10.1109/WF-IoT.2018.8355149
8. **Botta A., Donato W., Persico V., Pescapé A.** Integration of cloud computing and Internet of Things: A survey. *Future Generation Computer Systems*, 2016, no. 56, pp. 684–700. doi:10.1016/j.future.2015.09.021
9. **Kumar S., Tiwari P., Zymbler M.** Internet of Things is a revolutionary approach for future technology enhancement: A review. *Journal of Big Data*, 2019, no. 6, pp. 1–21. doi:10.1186/s40537-019-0268-2
10. **Azad P., Navimipour N. J., Rahmani A. M.** The role of structured and unstructured data managing mechanisms in the Internet of Things. *Cluster Computing*, 2020, no. 23, pp. 1185–1198. doi:10.1007/s10586-019-02986-2
11. **Sanabria-Russo L., Pubill D., Serra J., Verikoukis C.** IoT data analytics as a network edge service. *IEEE Conf. on Computer Communications Workshops*, 2019, pp. 969–970. doi:10.1109/INFCOMW.2019.8845207
12. **Dizdarević J., Carpio F., Jukan A., Masip-Bruin X.** A survey of communication protocols for Internet of Things and related challenges of fog and cloud computing integration. *ACM Computing Surveys*, 2019, vol. 51, iss. 6, pp. 1–29.
13. *Mosquitto-MQTT-broker.* https://github.com/topics/mosquitto-mqtt-broker (дата обращения: 11.07.2022).

14. **Patel C., Doshi N.** A novel MQTT security framework in generic IoT model. *Procedia Computer Science*, 2020, no. 171, pp. 1399–1408. doi:10.1016/j.procs.2020.04.150
15. **Isaev S., Kononov D.** Analysis of the dynamics of Internet threats for corporate network web services. *CEUR Workshop Proceedings*, 2021, no. 3047, pp. 71–78. doi:10.47813/sibdata-2-2021-10
16. **Kononov D. D., Isaev S. V.** Development of secure automated management systems based on web technologies. *IOP Conference Series: Materials Science and Engineering*, 2019, no. 537(5). doi:10.1088/1757–899X/537/5/052024
17. **Дикий Д. И., Артемьева В. Д.** Протокол передачи данных MQTT в модели удаленного управления правами доступа для сетей Интернета. *Научно-технический вестник информационных технологий, механики и оптики*, 2019, т. 19, № 1, с. 109–117. doi:10.17586/2226-1494-2019-19-1-109-117
18. **Andy S., Rahardjo B., Hanindhito B.** Attack scenarios and security analysis of MQTT communication protocol in IoT system. *4th Intern. Conf. on Electrical Engineering, Computer Science and Informatics*, 2017, pp. 1–6. doi:10.1109/EECSI. 2017.8239179
19. **Татарникова Т. М., Богданов П. Ю.** Обнаружение атак в сетях интернета вещей методами машинного обучения. *Информационно-управляющие системы*, 2021, № 6, с. 42–52. doi:10.31799/1684-8853-2021-6-42-52
20. **Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Breitenbacher D., Shabtai A., Elovici Y. N.** BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing, Special Issue — Securing the IoT*, 2018, no. 17(3), pp. 12–22.
21. **Duhamel P., Vetterli M.** Fast Fourier transforms: a tutorial review and a state of the art. *Signal Processing*, 1990, no. 19, pp. 259–299.
22. **Кононович Э. В., Миронова И. В., Батурин В. А.** Частотно-временной анализ рядов солнечной активности. *Исследовано в России*, 2006, № 182, с. 1704–1715. http://crydee.sai.msu.ru/~mir/182.pdf (дата обращения: 13.05.2022).
23. **Зиатдинов С. И.** Восстановление сигнала по его выборкам на основе теоремы отсчетов Котельникова. *Изв. вузов. Приборостроение*, 2010, № 53(5), с. 44–47.
24. **Lüke H. D.** The origins of the sampling theorem. *IEEE Communications Magazine*, 1999, no. 37(4), pp. 106–108.



UDC 004.6
doi:10.31799/1684-8853-2022-5-23-31
EDN: DNOSCW


**Formation of adaptive publications from the Internet of Things data broker**


O. S. Isaeva[a], PhD, Tech., Senior Researcher, orcid.org/0000-0002-5061-6765, isaeva@icm.krasn.ru
S. V. Isaev[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-6678-0084
N. V. Kulyasov[a], Programmer, orcid.org/0000-0001-5582-9498
[a]Institute of Computational Modelling SB RAS, 50/44, Akademgorodok St., 660036, Krasnoyarsk, Russian Federation



**Introduction:** The possibility of interaction with the physical world through the network infrastructures of spatially distributed nodes of Internet of Things (IoT), despite the undeniable advantages of the technology, produces significant loads on information consumers. In this regard, the current interest is the creation of methods that provide the reduction of transmitted data due to the adaptive synchronization of monitoring systems with the time of real processes. **Purpose:** To develop an approach to the formation of adaptive data broker publications based on the study of the cyclicity of observations of Internet of Things devices. **Results:** Within the corporate network of Krasnoyarsk Research Center, an infrastructure of devices and applications of the Internet of Things has been deployed to monitor temperature, humidity and PM2.5 in specialized technological rooms with telecommunications equipment. The discrete Fourier transform method was applied to the collected data. Based on the calculated parameters of the harmonic series, a conclusion has been made about the frequency characteristics of the data. The main peaks describing the periodicity of the data have been selected, the oscillation points have been determined, and, according to the Nyquist — Shannon — Kotelnikov theorem, a sampling frequency that provides a sufficient intensity of observations has been chosen. The analysis has shown that for different rooms the data are periodic but their harmonic profiles do not coincide. The choice of harmonic values whose oscillation amplitude determines the dynamics of changes in the data observed should be carried out periodically for each device under observation. This approach is implemented in the broker software which distributes data in subscriptions from each of the devices in accordance with the frequency of their changes. **Practical relevance:** The analysis of the frequency characteristics of data determines the broker settings that reduce output information flows, which is one of the aspects of ensuring the reliability of the IoT infrastructure. In addition, observing data changes allows to detect cooling system operation faults and malfunctions which can lead to the failure of sophisticated and expensive equipment with increased heat irradiation.



**Keywords —** Internet of Things, Message Queuing Telemetry Transport, discrete Fourier transform, Nyquist — Shannon — Kotelnikov sampling theorem.

**For citation:** Isaeva O. S., Isaev S. V., Kulyasov N. V. Formation of adaptive publications from the Internet of Things data broker. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2022, no. 5, pp. 23–31 (In Russian). doi:10.31799/1684-8853-2022-5-23-31, EDN: DNOSCW

**Financial support**

This work is supported by the Krasnoyarsk Mathematical Center and financed by the Ministry of Science and Higher Education of the Russian Federation in the framework of the establishment and development of regional Centers for Mathematics Research and Education (Agreement No. 075-02-2022-873).

## References

1. Atzori L., Iera A., Morabito G. The Internet of Things: A survey. *Computer Networks*, 2010, no. 54, pp. 2787–2805. doi:10.1016/j.comnet.2010.05.010
2. Korte A., Tiberius V., Potsdam U., Brem A., Stuttgart U. Internet of Things (IoT) technology research in business and management literature: Results from a co-citation analysis. *Journal of Theoretical and Applied Electronic Commerce Research*, 2021, no. 16(6), pp. 2073–2090. doi:10.3390/jtaer16060116
3. Rozik A. S., Tolba A. S., El-Dosuky M. A. Design and implementation of the Sense Egypt platform for real-time analysis of IoT data streams. *Advances in Internet of Things*, 2016, no. 6(4), pp. 66–91.
4. Alam T. A reliable communication framework and its use in Internet of Things (IoT). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2018, no. 3(5), pp. 450–456.
5. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 2013, no. 29(7), pp. 1645–1660. doi:10.1016/j.future.2013.01.010
6. D'Angelo G., Ferretti S., Ghini V. Simulation of the Internet of Things. *Proc. of the Intern. Conf. on High Performance Computing and Simulation*, 2016, pp. 1–8. doi:10.1109/HPCSim.2016.7568309
7. Javed A., Heljanko K., Buda A., Främling K. CEFIoT: A fault-tolerant IoT architecture for edge and cloud. *IEEE World Forum on Internet of Things*, 2018. pp. 813–818. doi:10.1109/WF-IoT.2018.8355149
8. Botta A., Donato W., Persico V., Pescapé A. Integration of cloud computing and internet of things: A survey. *Future Generation Computer Systems*, 2016, no. 56, pp. 684–700. doi:10.1016/j.future.2015.09.021
9. Kumar S., Tiwari P., Zymbler M. Internet of Things is a revolutionary approach for future technology enhancement: A review. *Journal of Big Data*, 2019, no. 6, pp. 1–21. doi:10.1186/s40537-019-0268-2
10. Azad P., Navimipour N. J., Rahmani A. M. The role of structured and unstructured data managing mechanisms in the Internet of Things. *Cluster Computing*, 2020, no. 23, pp. 1185–1198. doi:10.1007/s10586-019-02986-2
11. Sanabria-Russo L., Pubill D., Serra J., Verikoukis C. IoT data analytics as a network edge service. *IEEE Conf. on Computer Communications Workshops*, 2019, pp. 969–970. doi:10.1109/INFCOMW.2019.8845207
12. Dizdarević J., Carpio F., Jukan A., Masip-Bruin X. A survey of communication protocols for Internet of Things and related challenges of fog and cloud computing integration. *ACM Computing Surveys*, 2019, vol. 51, iss. 6, pp. 1–29.
13. *Mosquitto-MQTT-broker*. Available at: https://github.com/topics/mosquitto-mqtt-broker (accessed 11 July 2022).
14. Patel C., Doshi N. A novel MQTT security framework in generic IoT model. *Procedia Computer Science*, 2020, no. 171, pp. 1399–1408. doi:10.1016/j.procs.2020.04.150
15. Isaev S., Kononov D. Analysis of the dynamics of Internet threats for corporate network web services. *CEUR Workshop Proceedings*, 2021, no. 3047, pp. 71–78. doi:10.47813/sibdata-2-2021-10
16. Kononov D. D., Isaev S. V. Development of secure automated management systems based on web technologies. *IOP Conf. Series: Materials Science and Engineering*, 2019, no. 537(5). doi:10.1088/1757–899X/537/5/052024
17. Dikii D. I., Artemeva V. D. MQTT data protocol in remote access control management model for Internet networks. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 1, pp. 109–117 (In Russian). doi:10.17586/2226-1494- 2019-19-1-109-117
18. Andy S., Rahardjo B., Hanindhito B. Attack scenarios and security analysis of MQTT communication protocol in IoT system. *4th Intern. Conf. on Electrical Engineering, Computer Science and Informatics*, 2017, pp. 1–6. doi:10.1109/EECSI. 2017.8239179
19. Tatarnikova T. M., Bogdanov P. Yu. Intrusion detection in internet of things networks based on machine learning methods. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 6, pp. 42–52 (In Russian). doi:10.31799/1684- 8853-2021-6-42-52
20. Meidan Y., Bohadana M., Mathov Y., Mirsky Y., Breitenbacher D., Shabtai A., Elovici Y. N. BaIoT: Network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing, Special Issue — Securing the IoT*, 2018, no. 17(3), pp. 12–22.
21. Duhamel P., Vetterli M. Fast Fourier transforms: a tutorial review and a state of the art. *Signal Processing*, 1990, no. 19, pp. 259–299.
22. Kononovich E. V., Mironova I. V., Baturin V. A. Time-frequency analysis of solar activity series. *Investigated in Russia*, 2006, no. 182, pp. 1704–1715. Available at: (accessed 13 May 2022) (In Russian).
23. Ziatdinov S. I. Reconstruction of signal by its samples on the base of Kotelnikov counts theorem. *Journal of Instrument Engineering*, 2010, no. 53(5), pp. 44–47 (In Russian).
24. Lüke H. D. The origins of the sampling theorem. *IEEE Communications Magazine*, 1999, no. 37(4), pp. 106–108.