УДК 004.822 *Научная статья* DOI: 10.18287/2223-9537-2024-14-2-243-255

Построение онтологии для систематизации характеристик сети Интернета вещей

© 2024, О.С. Исаева

Институт вычислительного моделирования Сибирского отделения РАН (ИВМ СО РАН), Красноярск, Россия

Аннотация

Представлена формализация модели сети Интернета вещей, предназначенной для мониторинга технологических помещений с телекоммуникационным оборудованием в Федеральном исследовательском центре «Красноярский научный центр СО РАН». Сеть включает измерительные устройства, телекоммуникационную среду, серверы для сбора данных и прикладное программное обеспечение. Для информационного взаимодействия используется схема «издатель-подписчик» и облегчённый протокол с невысокой нагрузкой на каналы связи. Создана онтология, описывающая архитектуру сети и свойства устройств, которые собирают, передают, хранят и обрабатывают данные. Онтология содержит классы, представляющие понятия предметной области, отношения, свойства данных, диапазоны их изменения, критические значения, ограничивающие атрибуты элементов онтологии. Объекты онтологии имеют собственное цифровое представление в базах данных, включая результаты измерений, получаемые датчиками сети Интернета вещей, прецеденты аномальных данных, их статистические и частотные характеристики. Формализация позволила выявить неявные зависимости между объектами, связать их с характеристиками процессов, наблюдаемых устройствами сети Интернета вещей, и решать практические задачи. Рассмотрена задача выбора характеристик, влияющих на изменение схем информационного взаимодействия. Выполнен опрос экспертов и построена модель Кано для приоритизации характеристик, влияющих на принятие решений об организации схемы информационного взаимодействия в сети Интернета вещей.

Ключевые слова: *Интернет вещей, издатель, брокер, подписчик, онтология, анализ задержек, частотный анализ, модель Кано, реинжиниринг сети.*

Цитирование: *Исаева О.С.* Построение онтологии для систематизации характеристик сети Интернета вещей // *Онтология проектирования*. 2024. Т.14, №2(52). С. 243-255. DOI:10.18287/2223-9537-2024-14-2-243-255.

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.

Введение

Интернет вещей (*Internet of Things, IoT*) – это современная сетевая парадигма, обеспечивающая коммуникации между разнородными физическими и виртуальными системами. Международным союзом электросвязи для стандартизации Интернета вещей разработан стандарт (*Internet of Things Global Standards Initiative, IoT-GSI*), в котором определена иерархическая архитектура *IoT*-сетей [1, 2], включающая следующие уровни [3]:

- *сенсорный* (уровень устройств, выполняющих сбор информации о состоянии наблюдаемых объектов, настройка их энергосбережения, поддержка сетевых протоколов);
- *сетевой* (маршрутизация, передача информации – аналог сетевого и транспортного уровней эталонной модели взаимодействия открытых систем);
- *сервисный* (обработка и хранение данных);
- *прикладной* (услуги на основе данных *IoT*-устройств).

Дополнительно определены два вертикальных уровня – *управление* и *безопасность* [4]. Стабильность такой многоуровневой архитектуры обеспечивается специальными инстру-

ментами получения, хранения, обработки и анализа данных. Для обнаружения и смягчения последствий кибератак проводится ряд работ:

- строятся модельные сценарии сетевого поведения *IoT*-устройств [5];
- в системы безопасности интегрируются методы анализа временных рядов [6];
- для поиска аномалий создаются и используются публичные наборы данных [7];
- к структурированным записям сеансов связи добавляются сведения из неструктурированных журналов обращений [8, 9], статистические характеристики, параметры интенсивности и продолжительности передачи пакетов данных и пр., для анализа которых применяются методы машинного обучения [10].

Такие работы включают решения задач сетевого администрирования, обеспечения кибербезопасности, анализа данных и обнаружения сетевых аномалий [11].

Для учёта мобильности и разнородности устройств, разнотипности протоколов сетевого взаимодействия и обеспечения работы с большими объёмами данных в *IoT*-сети требуется структурирование и систематизация характеристик входящих в неё элементов [12]. Для многоуровневых моделей сложных объектов сокращение размерности достигается построением и анализом онтологий, извлечением существенных признаков из определений понятий, разделением их на группы обобщённых свойств, характеризующихся сопоставимыми отношениями с внешней средой, и определением родовидовой связи между существенными признаками [13]. Семантическая связность таких исследований обеспечивается созданием унифицированного словаря концептов и формальным описанием структуры их взаимосвязей. Такие онтологии позволяют обмениваться данными о киберугрозах, улучшая уровень защиты, ускоряют работу моделей машинного обучения, используемых в антивирусных «движках». На их основе строятся векторы атаки, для которых выявляются характерные виды уязвимостей и выбираются соответствующие средства защиты и системные обновления, необходимые для предотвращения инцидентов [14]. Онтологии позволяют решать задачи проектирования и развития телекоммуникационных сетей, обеспечивая включение в них новых сегментов на основе моделей, расширяющих доменную онтологию телекоммуникационных услуг специфичными характеристиками гибридных телекоммуникационных сетей и функциями операторов связи [15].

Целью данной работы является построение онтологии, в которой формализованы основные понятия технологии Интернета вещей и систематизированы характеристики элементов *IoT*-сети, реализованной в Федеральном исследовательском центре «Красноярский научный центр Сибирского отделения РАН». Исследование проводится на базе сети Интернета вещей, выполняющей мониторинг технологических помещений с телекоммуникационным оборудованием [16]. Онтология содержит как фактические, так и расчётные параметры, что позволяет выявлять взаимосвязи понятий и рассматривать характеристики работы устройств. Построенная онтология применяется для выбора настроек брокеров, собирающих и распределяющих данные в *IoT*-сети.

1 Описание онтологии

Используется редактор *Protégé*, в котором под онтологией понимается формальное описания понятий (классов), образцов классов, их свойств (функций и атрибутов) и ограничений на свойства [17]. Этот инструмент позволяет строить категорированную иерархическую структуру элементов и предоставляет методы мониторинга зависимостей, реконструкции скрытых знаний, а также создания и выполнения семантических запросов к данным. Формальная семантика используемого языка онтологии представляет логические следствия из фактов, как непосредственно заданных, так и полученных в результате логического вывода.

Для построения онтологии рассмотрена архитектура *IoT*-сети Красноярского научного центра СО РАН и данные сетевого трафика. Элементы сети распределены между перечисленными в стандарте *IoT-GSI* уровнями. Иерархическая структура классов приведена на рисунке 1.

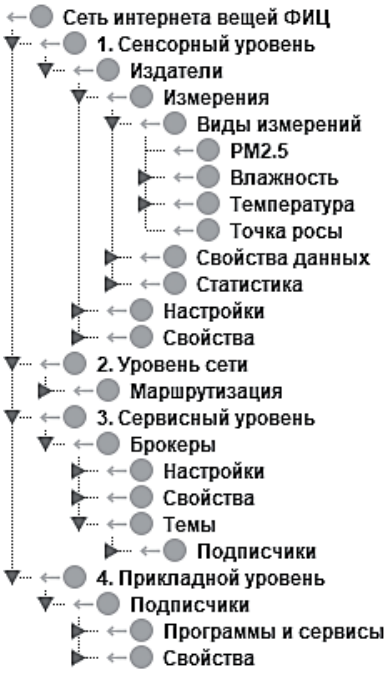

Рисунок 1 – Иерархическая структура классов

На рисунке 1 содержатся сенсорный, сервисный и прикладной уровни, а также уровень сети. К каждому уровню отнесены типы устройств и их характеристики. Информационное взаимодействие между сенсорным и прикладным уровнями организовано по схеме, заданной шаблоном «издатель-подписчик». Используются следующие понятия [18]:

Издатель – устройство, генерирующее данные о состоянии контролируемых объектов. В данном случае - это датчики температуры, влажности и т.д., которые отправляют брокерам сообщения по определённым темам.

Брокер – это сервер и программное обеспечение, которое получает все данные от издателей, а затем распределяет сообщения соответствующим подписчикам.

Подписчик – клиент (приложение или устройство), получающий и потребляющий данные в соответствии с заданными тематическими подписками.

Тема – семантика, определяющая издателя и вид информации и позволяющая подписчику получать необходимые данные.

В такой схеме *IoT*-устройства, являющиеся отправителями сообщений, не связаны с их потребителями. Данные абстрагированы от подписчиков и распределяются через посредника-брокера в соответствии с темами. Это обеспечивает масштабируемость и динамичную топологию сети.

В качестве протокола обмена данными выбран облегчённый протокол с невысокой нагрузкой на каналы связи (*Message Queuing Telemetry Transport*, *MQTT*) [19]. Основные элементы сети: издатели – устройства *CL*-210-*E ICP DAS*[1], имеющие функции измерения температуры, влажности и концентрации мелкодисперсной пыли в окружающей среде, брокеры *Eclipse Mosquitto* [20], развёрнутые на кластере *Kubernetes* (*K8s*)[2], объединяющем физические серверы и виртуальные машины.

Фрагмент графического представления онтологии, описывающего основные характеристики издателей, приведён на рисунке 2.

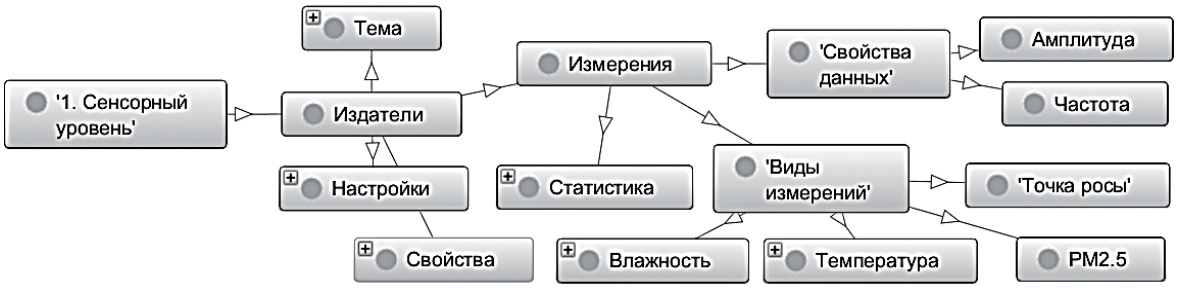

Рисунок 2 – Фрагмент графического представления классов в онтологии

[1] *CL-210-E ICP DAS*. См. например. https://insat.ru/prices/info.php?pid=139924&yclid=13744516879505686527.
[2] *Production-Grade Container Orchestration*. https://kubernetes.io/.

На рисунке 2 показаны значимые характеристики издателей, расположенных на сенсорном уровне: измерения (их виды, статистика и свойства данных), свойства устройств, настройки и публикуемые темы.

Элементы *IoT*-сети представлены в виде экземпляров классов онтологии. На рисунке 3 приведён пример описания издателей, данные которых собираются брокерами и контролируются приложениями-подписчиками.

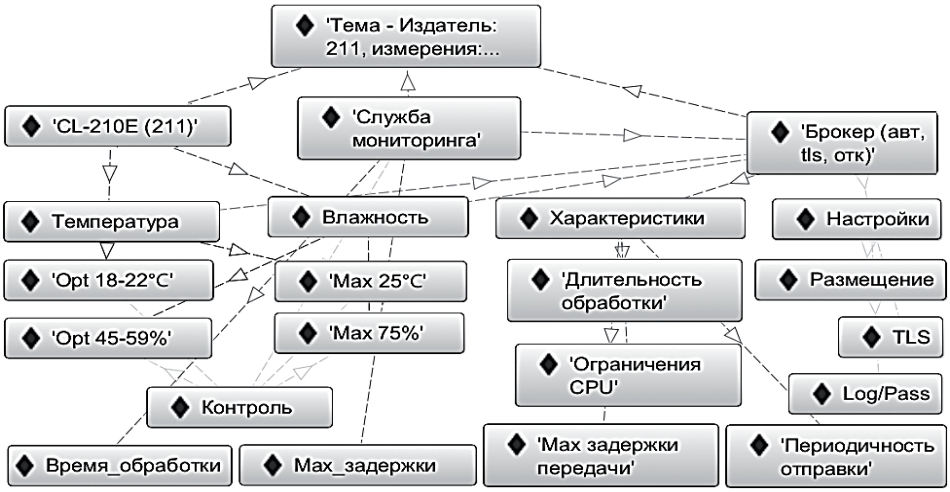

Рисунок 3 – Фрагмент графического представления экземпляров классов

На рисунке 3 показаны взаимосвязи элементов сети и их характеристики. В представленном фрагменте онтологии издатель с именем «CL-210E (211)» связан с брокером, имеющим настройки политик безопасности: доступ по авторизации (Log/Pass), шифрование (TLS[3]) и размещение в открытой сети. Характеристиками брокера являются: периодичность отправки данных издателем; ограничения, установленные сервером, на котором он размещён; задержки передачи; длительность обработки пакетов данных. Для измеряемых показателей температуры и влажности заданы оптимальные и максимальные значения. В зависимости от имени издателя и типа измерения у брокера формируется тема, на которую подписано программное обеспечение «Службы мониторинга», которое выполняет контроль измеряемых показателей по заданным ограничениям. В онтологию включены технические параметры устройств, необходимые для настройки их функционирования, и расчётные, построенные на основе собираемой статистики.

Машина вывода в редакторе *Protégé* позволяет выявлять зависимости и выполнять контроль структуры и связей между экземплярами данных. Выполненное семантическое моделирование позволяет обобщать и структурировать понятия предметной области (ПрО), быстро извлекать знания об элементах *IoT*-сети и может использоваться для решения задач её настройки и сопровождения.

2 Построение характеристик оценки *IoT*-сети

Рассматриваемая *IoT*-сеть выполняет мониторинг технологических помещений, снабжённых системами кондиционирования, в которых размещено коммуникационное и вычислительное оборудование, обладающее повышенной теплоотдачей. Данные о состоянии окружающей среды в помещениях поступают подписчикам от издателей (*IoT*-датчиков) че-

[3] *TLS* от англ. *Transport Layer Security* - протокол защиты транспортного уровня.

рез брокеров. Одна и та же информация может проходить через разные брокеры. Из онтологии выбираются подписчики, брокеры и издатели, связанные общими темами.

На рисунке 4 приведён фрагмент онтологии, содержащей набор издателей, подписчиков и брокеров, связанных темой. Задачи реинжиниринга сети включают выбор наиболее подходящих брокеров, с которыми взаимодействуют потребители информации, и изменение свойств подписки. На рисунке показан пример выбора брокера, который публикует данные по заданной теме. Название темы формирует издатель «CL-210E (211)» (его характеристики представлены на рисунке 3). Выбранная тема публикуется двумя брокерами, имеющими разные настройки безопасности (указаны в их наименованиях).

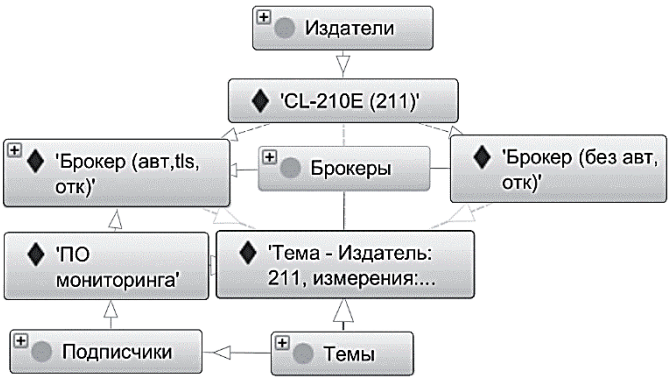

Рисунок 4 – Фрагмент онтологии для выбора брокеров по заданной теме

Выполняя фильтрацию записей в базах данных, собираемых от брокеров, можно получить статистику их работы и рассмотреть её зависимость от размещения и настроек. Анализ полученной статистики позволяет специалистам ПрО выбирать брокеров, обладающих значимыми для функционирования сети характеристиками. Для выполнения такого многокритериального выбора применяются различные подходы. В [21] решение задачи построения оптимального маршрута в сети, зависящего от условий её функционирования (задержка передачи пакетов, коэффициент потери данный, пропускная способность, загруженность буферов, длина маршрута), выполняется на основе нечёткой логики. Все рассматриваемые характеристики входят в нечёткие правила равнозначно и учитываются при их свёртке с одинаковым весом. Проблема выбора конкретных характеристик, которые необходимо учитывать, и определения весовых коэффициентов для построения обобщённой оценки остаётся не решённой.

Для поддержки решения этой задачи в данной работе построена модель Кано [22]. Характеристики, которые по оценкам экспертов попадают в категории базовых, конкурентных, привлекательных или нежелательных, включаются в онтологию и используются для выбора брокеров. Весовые коэффициенты устанавливаются в зависимости от типа категории. Параметры, попавшие в класс нейтральных, влияние на выбор не оказывают.

Чтобы путь от отправки данных до их получения конечным пользователем был наилучшим, требуется учитывать сквозную задержку или время ответа. В статье [23] сквозная задержка определяется как задержка времени ответа от издателя подписчику через брокера. Эта задержка рассчитывается как сумма задержек публикации сообщения брокеру, времени обработки брокером и получения сообщения подписчиком:

$$R(b)_{p\to s} = R_{p\to b} + R_b + R_{b\to s}, \quad (1)$$

где $R(b)_{p\to s}$ – сквозная задержка, p – издатель, b – брокер, s – подписчик; $R_{p\to b}$ – задержка, вызванная сетью передачи между b и p; R_b – среднее время обработки данных брокером; $R_{b\to s}$ – задержка, вызванная сетью передачи между b и s.

В практических случаях время сквозной задержки связано со всеми возможными коммуникациями между издателями и подписчиками. Время изменяется в зависимости от их местоположения в общей структуре сети. Вычисляется наихудший случай, связанный с темой и брокером, следующим образом:

$$R(b)_{p\to s} = \sum R(b,\ th)_{p\to s}, \tag{2}$$

где $R(b,\ th)_{p\to s}$ – сквозная задержка для брокера b и всех тем th в b.

$$R(b,\ th)_{p\to s} = \max(R_{pi\to b}) + R_b(th) + \max(R_{b\to sj}), \tag{3}$$

где $R_{pi\to b}$ – задержка, вызванная сетью передачи между брокером b и всеми взаимодействующими с ним по заданной теме th подписчиками p_i; $R_b(th)$ – среднее время обработки результатов измерений, собираемых по теме th; $R_{b\to sj}$ – задержка между брокером b и всеми его подписчиками s_j.

Кроме того, необходимо учитывать загруженность каждого брокера в существующей конфигурации. В простом случае это определяется количеством обрабатываемых тем:

$$S(b) = |\{th_l \in b\}|, \tag{4}$$

где th_l – темы брокера b, $l=\overline{1,\ L}$, L – количество тем, операция $|\ \ |$ – мощность множества.

Периодичность поступления данных от издателей указывается в их настройках и зависит от характеристик устройств. Для каждого брокера можно рассчитать P_{pub} – максимальную периодичность поступления данных (период дискретизации данных).

В общем случае брокер распределяет данные по подписчикам с такой же периодичностью, что и происходит их получение. Для того, чтобы сократить объём рассылок, уменьшить нагрузку на каналы связи и на ограниченные ресурсы подписчиков при сохранении адекватности представления процессов, за которыми выполняется мониторинг, необходимо обеспечить режим выдачи данных с частотой их обновления, не превышающей скорость протекания событий [24]. В [25] представлен способ определения периодичности публикации данных. Минимальный период дискретизации, отражающий частоту изменения данных, вычисляется по формуле:

$$P_{\min} = 1/F_{\max}, \tag{5}$$

где $F_{\max}$ – максимальная частота по каждому измерению (температура, влажность), рассчитанная для каждого издателя.

Период дискретизации, учитывающий скорость изменения данных, вычисляется на основе статистики, полученной при имитации критических состояний. Для этого вычисляется максимальная скорость изменения показателей:

$$S_{\max} = \max_k (|\ x(t_k) - x(t_{k-1})|\ /\ \Delta t\ ), \tag{6}$$

где $k=\overline{1,\ N}$, N – количество наблюдений, $x(t)$ – результат в момент времени t, $\Delta t=(t_k - t_{k\text{-}1})$.

Для каждого наблюдаемого показателя в онтологии задана величина его допустимого изменения. Эта информация определяется из эксплуатационных требований к технологическим помещениям (например, скорость изменения влажности не должна превышать 6% в час). Период дискретизации вычисляется на основе полученной скорости протекания процессов:

$$P_S = X_{\min}\ /\ S_{\max}, \tag{7}$$

где $X_{\min}$ – величина изменения в единицу времени, $S_{\max}$ – максимальная скорость.

Результирующий период дискретизации определяется из (5) и (7):

$$P_d = \min\ (P_S,\ P_{\min}). \tag{8}$$

Полученный период дискретизации устанавливается в настройках брокера.

Характеристика брокера безопасность определяется через количество нелегитимных запросов из различных источников. Брокеры имеют различные варианты настройки (признаки C):

- способы доступа (признак C_A – видимость только из внутренней корпоративной сети или из Интернета);

- аутентификации (признак C_L – с авторизацией или без авторизации);
- признак C_E – наличие или отсутствие шифрования данных.

Пример визуализации статистики обращений для выбранного брокера приведён на рисунке 5, величина метки отражает интенсивность запросов в сутки. Из примера видно, что с некоторых адресов идёт большое число попыток доступа, а некоторые адреса осуществляют такие обращения с выраженной периодичностью, что позволяет выявить характер источника и сравнить по этому параметру брокеры с различными настройками.

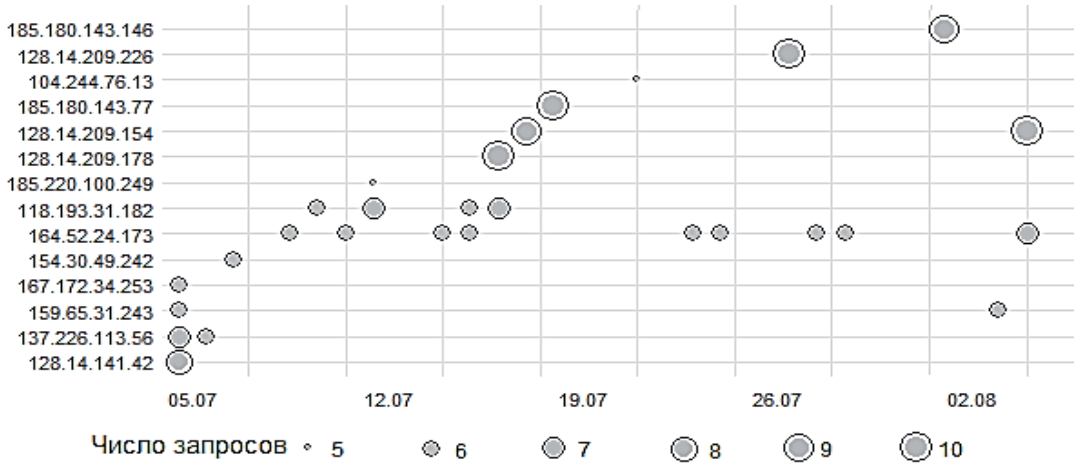

Рисунок 5 – Пример статистики нелигитимных обращений (оси: дата, *ip*-адрес источника обращения)

Выбор данных за разные периоды времени позволяет определять коэффициент безопасности брокера через частоту нелигитимных обращений:

$$F_{IR}(b) = m(b) / M, \tag{9}$$

где $m(b)$ – количество зафиксированных нелигитимных обращений к брокеру b, M – количество внешних запросов.

На выбор брокера может оказывать влияние наличие у него ресурсов, выделенных на хранение данных $Q_S(b)$, и характеристики, такие как быстродействие $Q_W(b)$, возможность обеспечения бесперебойной работы $Q_{UnI}(b)$, наличие альтернативных вариантов подключения к сети $Q_{NC}(b)$, поддержка нескольких протоколов $Q_{Pr}(b)$. Эти показатели могут быть оценены экспертами для каждого брокера.

Для оценки характеристик брокера, наличие или отсутствие которых влияет на его выбор, используется модель пользовательских предпочтений Кано. В настоящий момент применимость модели Кано расширена, и она выведена из сферы потребительской оценки качества производимых товаров в экономические, экологические, организационные области [26].

3 Выбор значимых характеристик оценки *IoT*-сети

Модель Кано позволяет оценивать как объективные так субъективные качества, улучшение которых влияет на экспертный выбор, и используется для того, чтобы получить пользовательский приоритет функций. Объективные качества определяются как необходимые свойства, без которых невозможно выполнение функций брокера. Их выбор основывается на субъективных атрибутах, ценность которых для экспертов сопоставима с объективными качествами.

Для выбора значимых характеристик в соответствии с методом Кано выполнен опрос группы экспертов. В качестве респондентов выбраны специалисты по кибербезопасности, анализу данных и системному администрированию, участвующие в построении *IoT*-сети. Та-

кая выборка оправдана объективной ограниченностью области применимости характеристик, включаемых в онтологию. Категорирование выполняется по следующим вопросам:

1) наличие характеристики или положительность её свойства;
2) отсутствие характеристики или её отрицательное значение.

Первый тип вопросов называют функциональным, второй – дисфункциональным. На каждый из них выбираются ответы, отражающие отношение к наличию свойства и его отсутствию по следующим вариантам: нравится, ожидаемо, безразлично, допустимо (могу смириться), не нравится. Детально метод Кано описан в работах [22, 26].

Для оценки значимости критериев используется матрица классификации Кано, объединяющая функциональные и дисфункциональные вопросы для приоритизации характеристик. Рассматриваются следующие классы:

- обязательно, должно быть (*Basic requirement*, B);
- желательно, относится к основным свойствам (*One-dimensional requirement*, O);
- дополнительно, влечёт преимущества (*Attractive requirement*, A);
- безразлично (*Indifferent requirement*, I);
- нежелательно, свойство обратно, противоположно (*Reverse requirement*, R);
- сомнительно, противоречиво (*Questionable requirement*, Q).

Распределение приоритетов в матрице классификации приведено в таблице 1.

Таблица 1 – Матрица классификации Кано

		Дисфункциональные				
		нравится	*ожидаемо*	*безразлично*	*допустимо*	*не нравится*
Функциональные	*нравится*	Q	A	A	A	O
	ожидаемо	R	Q	I	I	B
	безразлично	R	I	I	I	B
	допустимо	R	I	I	Q	B
	не нравится	R	R	R	R	Q

Перечень характеристик, которые были предложены экспертам для проведения оценивания, и результат классификации приведены в таблице 2. Полученные классы сгруппированы для каждой характеристики и выбрана основная категория, набравшая наибольшее число голосов. В результате категорирования характеристикам присвоены весовые коэффициенты, определяющие принадлежность к каждому из классов.

Часть характеристик попала в категорию I, они либо пересекались с другими параметрами, влияние которых эксперты оценили как существенное (классы B, O, A, R), либо их наличие или отсутствие не оказывало влияние на выбор экспертов. Характеристики, имеющие противоречивую оценку, отнесены к классу Q и их значимость для данной задачи выбора оценена как сомнительная. Обязательные B, желательные O, дополнительные A и нежелательные R характеристики необходимо учитывать с различными (заданными в таблице) весовыми коэффициентами. Эта информация используется для построения комплексной оценки брокера.

Для реинжиниринга функционирующей сети или добавления в схему нового издателя или подписчика рекомендуется выбирать брокера, имеющего лучшие показатели времени обработки данных (min R_b), обеспечивающего минимальную сквозную задержку (min $R_{p\to s}$), с небольшим числом нелигитимных обращений (min F_{IR}), имеющего бо̀льший выделенный ресурс (max Q_S). К факторам, которые не имеют критического значения при выборе, но их наличие даёт потенциальные преимущества, относятся характеристики, свидетельствующие о загруженности брокеров, и признаки настройки политик безопасности. Наличие характери-

стик: скорость изменения данных (min S_{max}), период их выдачи (max P_d), поддержка аутентификации (C_L) и шифрования (C_E) могут оказать преимущества при выборе конкретной реализации схемы информационного взаимодействия.

Таблица 2 – Результат классификации характеристик

№	Наименование характеристики (свойства, признака)	Обозначение	Класс	Результат
1.	Задержка от издателя до брокера	$R_{p\to b}$	I	0
2.	Задержка от брокера до подписчика	$R_{b\to s}$	I	0
3.	Время обработки данных брокером	R_b	R	-2
4.	Сквозная задержка	$R_{p\to s}$	R	-2
5.	Количество тем	S	I	0
6.	Скорость изменения данных	S_{max}	A	1
7.	Частота изменения данных	P_{min}	I	0
8.	Период поступления данных	P_{pub}	I	0
9.	Период выдачи данных	P_d	A	1
10.	Частота нелигитимных обращений	F_{IR}	R	-2
11.	Выделенный ресурс	Q_S	B	2
12.	Оценка быстродействия	Q_W	I	0
13.	Обеспечение бесперебойной работы	Q_{UnI}	O	0,5
14.	Наличие альтернативных способов подключения	Q_{NC}	Q	0
15.	Поддержка нескольких протоколов	Q_{Pr}	Q	0
16.	Обеспечение внешнего доступа	C_A	I	0
17.	Поддержка аутентификации	C_L	A	1
18.	Признак шифрования	C_E	O	0,5

Заключение

Проведённое исследование позволило формализовать описание сети Интернета вещей, функционирующей в Красноярском научном центре СО РАН. В построенной онтологии объединены обобщённые понятия ПрО и характеристики, связанные с реализацией *IoT*-сети. Описана архитектура сети и схема информационного взаимодействия «издатель-подписчик» при различных настройках политик безопасности брокеров данных. Онтология консолидирует знания и представляет объекты, экземпляры объектов, свойства данных: диапазоны их изменения, граничные условия, статистические характеристики, показатели периодичности процессов, контролируемых датчиками; свойства элементов сети - критерии сетевой активности и выделенные ресурсы на хранение и обработку данных. Каждый из экземпляров объектов имеет своё цифровое представление в базах данных.

Выполнена систематизация характеристик *IoT*-сети и экспертный анализ их влияния на выбор брокеров, оказывающих услуги по получению данных от издателей и распределению их подписчикам. Показано, что для реинжиниринга сети и настройки брокеров следует учитывать не только статистику сетевых журналов, но и характеристики, получаемые из анализа наблюдаемых *IoT*-устройствами процессов. Это важно, поскольку устройства Интернета вещей имеют ограниченные возможности по энергопотреблению, использованию памяти, пропускной способности и контролю безопасности. Выбор связанных характеристик, необходимых для расчёта, выполняется запросами в онтологии.

Собранная статистика по брокерам с различными настройками безопасности, типами и источниками нелегитимных обращений, а также прецедентами типичного и аномального поведения может быть учтена не только при выборе брокера, но и при его настройке. Например, используя характеристики, полученные в результате анализа наблюдаемых процессов и

выбора периода выдачи данных, учитывающего скорость их изменения, объём передаваемых данных сокращается без потери сведений о динамике событий. Такой подход применим для настройки энергонезависимых издателей, где снижение частоты передачи данных приведёт к увеличению времени их автономной работы.

Список источников

[1] *Internet of Things Global Standards Initiative* [Электронный ресурс]. https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

[2] ***Росляков А.В., Ваняшин С.В., Гребешков А.Ю.*** Интернет вещей. Самара: Поволжский государственный университет телекоммуникаций и информатики, 2015. 200 с.

[3] ***Лоднева, О.Н., Ромасевич Е.П.*** Анализ трафика устройств Интернета вещей. *Современные информационные технологии и ИТ-образование*. 2018. Т.14, №1. С.149-169. DOI: 10.25559/SITITO.14.201801.149-169.

[4] ***Javed A., Heljanko K., Buda A., Främling K.*** CEFIoT: A Fault-Tolerant IoT Architecture for Edge and Cloud // 2018 IEEE 4th World Forum on Internet of Things. 2018. P. 813-818. DOI: 10.1109/WF-IoT.2018.8355149.

[5] ***Haripriya A., Kulothungan K.*** Secure-MQTT: An efficient fuzzy logic-based approach to detect dos attack in MQTT protocol for Internet of Things. *EURASIP Journal on Wireless Communications and Networking*. 2019, N90. DOI: 10.1186/s13638-019-1402-8.

[6] ***Cook A.A., Mısırlı G., Fan Z.*** Anomaly detection for IoT time-series data: a survey. *IEEE Internet of Things Journal*. 2020. Vol. 7. P.6481-6494. DOI:10.1109/JIOT.2019.2958185.

[7] ***Vaccari I., Chiola G., Aiello M., Mongelli M.*** MQTTset, a New Dataset for Machine Learning Techniques on MQTT. *Sensors*. 2020. Vol. 20(22). P.6578. DOI: 10.3390/s20226578.

[8] ***Isaev S.V., Kononov D.D.*** Analysis of the dynamics of Internet threats for corporate network web services. *CEUR Workshop Proceedings*. 2021. Vol. 3047. P.71-78.

[9] ***Кононов Д.Д., Исаев С.В.*** Анализ киберугроз корпоративной сети на основе параллельной обработки данных Netflow. *Сибирский аэрокосмический журнал*. 2023. Т. 24, № 4. С.663-672. DOI: 10.31772/2712-8970-2023- 24-4-663-672.

[10] ***Bhattacharyya D.K., Kalita J.K.*** Network anomaly detection: A machine learning perspective. Boca Raton: CRC Press, 2013. 376 p.

[11] ***Nassif A.B., Talib M.A., Nasir Q., Dakalbab F.M.*** Machine learning for anomaly detection: A systematic review. *IEEE Access*. 2021. Vol. 9. P.78658-78700. DOI: 10.1109/ACCESS.2021.3083060.

[12] ***Omar S., Ngadi A., Jebur H.*** Machine learning techniques for anomaly detection: an overview. *International Journal of Computer Applications*. 2013. Vol.79(2). P.32-41. DOI: 10.5120/13715-1478.

[13] ***Микони С.В.*** Методика построения многоуровневой модели оценивания сложного объекта. *Онтология проектирования*. 2022. Т.12(3). С.380-392. DOI: 10.18287/2223-9537-2022-12-3-380-392.

[14] ***Моисеев А.*** Онтологии в информационной безопасности [Электронный ресурс]. https://www.kaspersky.ru/blog/cybersecurity-ontology/30977.

[15] ***Куликов И.А., Жукова Н.А.*** Интеграция телекоммуникационных сетей в системе мониторинга с использованием доменных онтологий. *Онтология проектирования*. 2022. Т.12(3). С.353-366. DOI:10.18287/2223-9537-2022-12-3-353-366.

[16] ***Исаева О.С., Кулясов Н.В., Исаев С.В***. Создание инструментов сбора данных для анализа аспектов безопасности Интернета вещей. *Информационные и математические технологии в науке и управлении*. 2022. № 3(27). С.113-125. DOI: 10.38028/ESI.2022.27.3.011.

[17] ***Vigo M., Matentzoglu N., Jay C., Stevens R.*** Comparing ontology authoring workflows with Protégé: In the laboratory, in the tutorial and in the 'wild'. *Journal of Web Semantics*. 2019. Vol. 57(12). DOI: 10.1016/j.websem.2018.09.004.

[18] ***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(6). P.1-29. DOI: 10.1145/3292674.

[19] ***Munshi A.*** Improved MQTT secure transmission flags in smart homes. *Sensors*. 2022. Vol. 22(6). P.2-15. DOI: 10.3390/s22062174.

[20] Eclipse Mosquitto. An open source MQTT broker [Электронный ресурс]. https://mosquitto.org.

[21] ***Татаринов В.И., Комашинский В.И., Иванов А.Ю.*** Маршрутизация в гибридных самоорганизующихся беспроводных сетях связи пятого поколения. *Известия ТулГУ. Технические науки*. 2023. № 3. С.283-290. DOI: 10.24412/2071-6168-2023-3-283-290.

[22] ***Marutschke M., Hayashi Y.*** Kano model-based macro and micro shift in feature perception of short-term online courses. *Collaboration Technologies and Social Computing,* 2022. P.112-125. DOI: 10.1007/978-3-031-20218-6_8.
[23] ***Hmissi F., Ouni S***. An MQTT brokers distribution based on mist computing for real-time IoT communications. July 2021. [Preprint]. DOI: 10.21203/rs.3.rs-695717/v1.
[24] ***Исаева О.С., Исаев С.В., Кулясов Н.В.*** Формирование адаптивных рассылок брокера данных Интернета вещей. *Информационно-управляющие системы.* 2022. Т. 5, Вып. 120. С. 23-31. DOI: 10.31799/1684–8853-2022-5–23–31.
[25] ***Исаева О.С.*** Построение цифрового профиля устройств Интернета вещей. *Информационные и математические технологии в науке и управлении*. 2023. № 2(30). С. 36-44. DOI: 10.25729/ESI.2023.30.2.004.
[26] ***Николаева Н.Г., Исмаилова Р.Н.*** Модель Н. Кано: выбор направлений развития испытательной лаборатории. *Компетентность.* 2021. №1. С. 44-51. DOI: 10.24411/1993-8780-2021-10107.

Сведения об авторе

Исаева Ольга Сергеевна, 1976 г. рождения. Окончила Красноярский государственный университет в 1998 г., д.т.н. (2022). Старший научный сотрудник отдела вычислительной механики деформируемых сред Института вычислительного моделирования СО РАН. В списке научных трудов около 100 работ в области ИИ и анализа данных. ORCID: 0000-0002-5061-6765; Author ID (Scopus): 57200530407; Author ID (РИНЦ): 165828. *isaeva@icm.krasn.ru*

Поступила в редакцию 22.04.2024, после рецензирования 22.05.2024. Принята к публикации 7.06.2024.

Scientific article DOI: 10.18287/2223-9537-2024-14-2-243-255

Building an ontology to systematize the characteristics of the Internet of Things network

© 2024, O.S. Isaeva

Institute of Computational Modelling SB RAS, Krasnoyarsk, Russia

Abstract

A formalization of the Internet of Things network model designed for monitoring technological premises with telecommunications equipment at the Federal Research Center "Krasnoyarsk Scientific Center SB RAS" is presented. The network includes measuring devices, a telecommunications environment, data collection servers, and application software. For information interaction, a “publisher-subscriber” scheme and a lightweight protocol with a low load on communication channels are used. An ontology has been created that describes the network architecture and the properties of devices that collect, transmit, store, and process data. The ontology contains classes representing the concepts of the subject area, relationships, data properties, ranges of their changes, and critical values that limit the attributes of ontology elements. Ontology objects have their own digital representation in databases, including measurement results obtained by Internet of Things network sensors, precedents of anomalous data, and their statistical and frequency characteristics. This formalization made it possible to identify implicit dependencies between objects, connect them with the characteristics of processes observed by Internet of Things network devices, and solve practical tasks. The problem of selecting characteristics that influence changes in information interaction patterns is considered. A survey of experts

was carried out, and a Kano model was built to prioritize the characteristics that influence decision-making on the organization of an information interaction scheme in the Internet of Things network.

Keywords: *Internet of Things, publisher, broker, subscriber, ontology, delay analysis, frequency analysis, Kano model, network reengineering.*

Citation: *Isaeva O.S.* Building an ontology to systematize the characteristics of the Internet of Things network [In Russian]. *Ontology of designing*. 2024; 14(2): 243-255. DOI: 10.18287/2223-9537-2024-14-2-243-255.

Conflict of interest: The author declares no conflict of interest.

List of figures and table

References

[1] Internet of Things Global Standards Initiative. https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.
[2] ***Roslyakov AV, Vanyashin SV, Grebeskov AYu.*** Internet of things [In Russian]. Samara: PGUTI; 2015. 200 p.
[3] ***Lodneva ON, Romasevich EP.*** Analysis of devices traffic of the Internet of Things [In Russian*]. Modern Information Technologies and IT-Education.* 2018; 14(1): 149-169. DOI: 10.25559/SITITO.14.201801.149-169.
[4] ***Javed A, Javed A, Heljanko K, Buda A, Främling K.*** CEFIoT: A Fault-Tolerant IoT Architecture for Edge and Cloud // Proc. of IEEE World Forum on Internet of Things. 2018. P. 813-818. DOI: 10.1109/WF-IoT.2018.8355149.
[5] ***Haripriya A, Kulothungan K.*** Secure-MQTT: An efficient fuzzy logic-based approach to detect dos attack in MQTT protocol for Internet of Things. *EURASIP Journal on Wireless Communications and Networking.* 2019; 90. DOI: 10.1186/s13638-019-1402-8.
[6] ***Cook AA, Mısırlı G, Fan Z.*** Anomaly detection for IoT time-series data: a survey. *IEEE Internet of Things Journal*. 2020; 7: 6481-6494. DOI:10.1109/JIOT.2019.2958185.
[7] ***Vaccari I, Chiola G, Aiello M, Mongelli M.*** MQTTset, a New Dataset for Machine Learning Techniques on MQTT. *Sensors*. 2020; 20(22): 6578. DOI: 10.3390/s20226578.
[8] ***Isaev SV, Kononov DD.*** Analysis of the dynamics of Internet threats for corporate network web services. *CEUR Workshop Proceedings*. 2021; 3047: 71-78.
[9] ***Kononov DD, Isaev SV***. Analysis of corporate network cyber threats based on parallel processing of Netflow data. [In Russian]. *Siberian Aerospace Journal.* 2023; 24(4): 663-672. DOI: 10.31772/2712-8970-2023- 24-4-663-672.
[10] ***Bhattacharyya DK, Kalita JK.*** Network anomaly detection: A machine learning perspective. Boca Raton: CRC Press, 2013. 376 p.
[11] ***Nassif AB, Talib MA, Nasir Q, Dakalbab FM.*** Machine learning for anomaly detection: A systematic review. *IEEE Access*. 2021; 9: 78658-78700. DOI: 10.1109/ACCESS.2021.3083060.
[12] ***Omar S, Ngadi A, Jebur H.*** Machine learning techniques for anomaly detection: an overview. *International Journal of Computer Applications*. 2013; 79(2): 32-41. DOI: 10.5120/13715-1478.
[13] ***Mikoni SV.*** Methodology for creating a multi-level model for evaluating a complex object [In Russian]. *Ontology of designing*. 2022; 12(3): 380-392. DOI: 10.18287/2223-9537-2022-12-3-380-392.
[14] ***Moiseev A***. Ontologies in information security [In Russian]. https://www.kaspersky.ru/blog/cybersecurity-ontology/30977/.
[15] ***Kulikov IA, Zhukova NA***. Integration of telecommunication networks in a monitoring system using domain ontologies [In Russian]. *Ontology of designing*. 2022; 12(3): 353-366. DOI:10.18287/2223-9537-2022-12-3-353-366.
[16] ***Isaeva OS, Kulyasov NV, Isaev SV***. Creating data collection tools to analyze security aspects of Internet of Things [In Russian]. *Information and mathematical technologies in science and management*. 2022; 3(27): 113-125. DOI: 10.38028/ESI.2022.27.3.011.

[17] ***Vigo M, Matentzoglu N, Jay C, Stevens R.*** Comparing ontology authoring workflows with Protégé: In the laboratory, in the tutorial and in the 'wild'. *Journal of Web Semantics*. 2019; 57(12). DOI: 10.1016/j.websem.2018.09.004.
[18] ***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; 51(6): 1-29. DOI: 10.1145/3292674
[19] ***Munshi A.*** Improved MQTT secure transmission flags in smart homes. *Sensors*. 2022; 22(6): 2-15. DOI: 10.3390/s22062174.
[20] Eclipse Mosquitto. An open source MQTT broker. http://mosquitto.org.
[21] ***Tatarinov VI, Komashinsky VI, Ivanov AY***. Routing in hybrid self-organizing wireless communication networks of the fifth generation [In Russian]. News of Tula State University. *Technical science*. 2023; 3: 283-290. DOI: 10.24412/2071-6168-2023-3-283-290.
[22] ***Marutschke DM, Hayashi Y.*** Kano model based macro and micro shift in feature perception of short-term online courses. *Collaboration Technologies and Social Computing.* 2022; 112-125. DOI: 10.1007/978-3-031-20218-6_8.
[23] ***Hmissi F, Ouni S***. An MQTT brokers distribution based on mist computing for real-time IoT communications. July 2021. [Preprint]. DOI: 10.21203/rs.3.rs-695717/v1.
[24] ***Isaeva OS, Isaev SV, Kulyasov NV.*** Formation of adaptive publications from the Internet of things data broker. [In Russian]. *Information and Control Systems*. 2022; 5(120): 23-31. DOI: 10.31799/1684–8853-2022-5–23–31.
[25] ***Isaeva OS.*** Building a digital profile of IoT devices [In Russian]. *Information and mathematical technologies in science and management*. 2023; 2(30): 36-44. DOI: 10.25729/ESI.2023.30.2.004.
[26] ***Nikolaeva NG, Ismailova RN.*** Model N. Kano: selection of directions for development of a testing laboratory [In Russian]. *Competency*. 2021; 1: 44-51. DOI: 10.24411/1993-8780-2021-10107.

About the author

Olga Sergeevna Isaeva (b. 1976) graduated from the Krasnoyarsk State University in 1998, Doctor of Technical Sciences (2022). Senior researcher at the Department of Computational mechanics of deformable media at the Institute of Computational Modelling SB RAS. The list of scientific papers includes about 100 articles in the field of AI and data analysis. ORCID: 0000-0002-5061-6765; Author ID (Scopus): 57200530407; Author ID (RSCI): 165828. *isaeva@icm.krasn.ru*

Received April 22, 2024, Revised May 22, 2024. Accepted June 7, 2024.