Лекция 6. Функции шлюза IoT

Цель лекции – ознакомить магистрантов с ключевыми функциями шлюзов IoT, их ролью в архитектуре Интернета вещей и значением для эффективного взаимодействия между устройствами.

Введение

Сегодня мы обсудим одну из ключевых составляющих архитектуры Интернета вещей (IoT) – шлюзы IoT. Эти устройства играют центральную роль в обеспечении эффективного взаимодействия между разными устройствами, сетями и облачными сервисами. Понимание функций шлюза поможет лучше осознать, как формируется экосистема IoT и как оптимизировать ее работу.

Шлюз IoT – это устройство, которое обеспечивает связь между различными сенсорами, устройствами и облачными сервисами. Он служит «мостом», позволяющим устройствам, использующим разные протоколы и технологии, обмениваться данными и управлять друг другом.

Шлюз на уровне адаптации данных имеет несколько функций. Это конфиденциальность данных, безопасность данных, обогащение данных, консолидация данных, преобразование и управление устройствами. На рисунке 2.7 показан шлюз IoT, состоящий из обогащения данных, консолидации и управления устройствами, а также коммуникационных фреймворков.

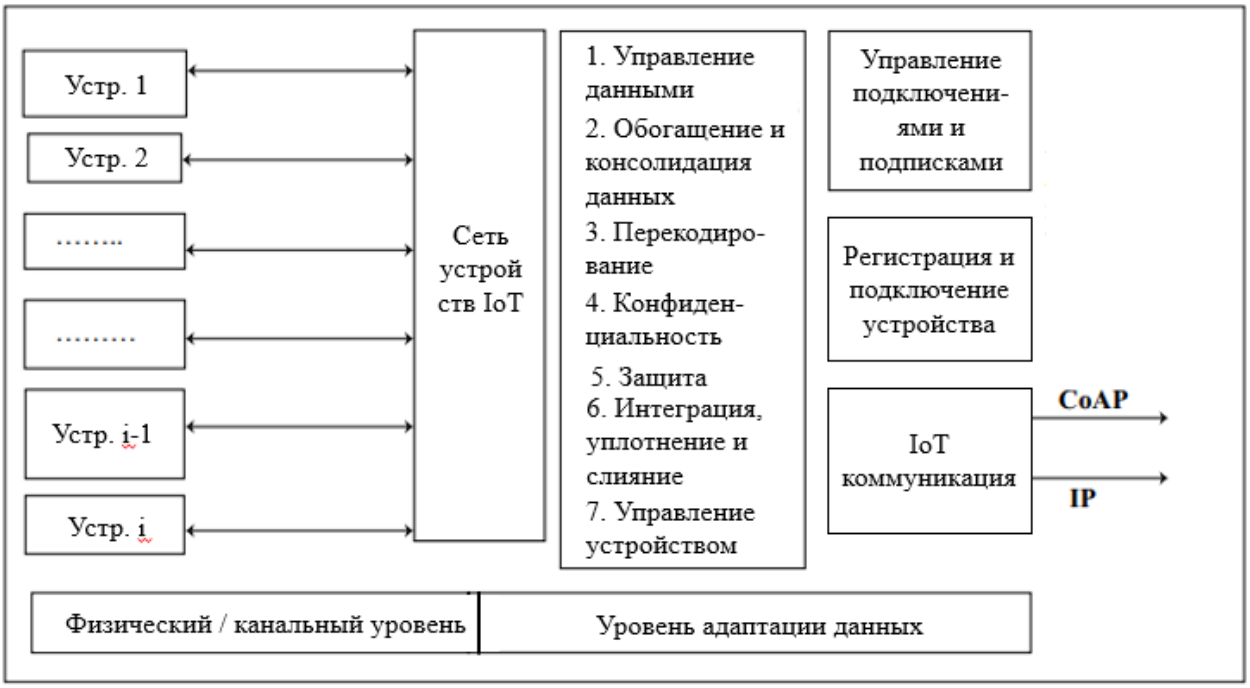

Рисунок 6.1. Шлюз IoT, состоящий из фреймворков обогащения и консолидации данных, управления устройствами и связи на уровне адаптации

Шлюз состоит из фреймворков обогащения данных, консолидации и коммуникации IoT. Шлюз связи позволяет устройствам взаимодействовать и взаимодействовать с сетью Интернет. Шлюз связи использует протоколы передачи сообщений и протоколы веб-коммуникации для Интернета. Шлюз включает в себя две функции, а именно: управление данными и консолидацию, а также управление подключенными устройствами.

Шлюз управления и консолидации данных

Шлюз включает положения для одной или нескольких из следующих функций: транскодирование и управление данными. Ниже приведены функции управления данными и консолидации:

- Транскодирование (перекодирование);
- Конфиденциальность, безопасность;
- Интеграция;
- Уплотнение и слияние.

Транскодирование означает адаптацию данных, преобразование и изменение протокола, формата или кода с помощью программного обеспечения. Шлюз отображает веб-ответ и сообщения в форматах и представлениях, требуемых и приемлемых на устройстве IoT. Аналогично запросы устройства IoT адаптируются, преобразуются и изменяются в требуемые форматы, приемлемые на сервере с помощью программного обеспечения транскодирования. Например, использование транскодирования позволяет символам запроса сообщения быть в формате ASCII на устройстве и в Unicode на сервере. Оно также позволяет использовать базу данных формата XML на устройстве, в то время как на сервере есть DB2, Oracle или любая другая база данных. Транскодирование включает в себя форматы, данные и преобразование кода с одного конца на другой, когда мультимедийные данные передаются с сервера на мобильное телевидение, интернет-телевидение, телефон VoIP или смартфон в качестве клиентских устройств. Приложения транскодирования также включают в себя фильтрацию, сжатие или декомпрессию. Прокси-сервер транскодирования может выполняться на клиентской системе или сервере приложений. Прокси-сервер транскодирования имеет возможности преобразования, вычисления и анализа, в то время как шлюз имеет только возможности преобразования и вычисления.

Конфиденциальность. Такие данные, как медицинские данные пациентов, данные о поставках товаров в компании из разных мест и в разные места, а также изменения в запасах, могут нуждаться в конфиденциальности и защите от сознательной или бессознательной передачи в ненадежные пункты назначения с использованием Интернета. Конфиденциальность является аспектом управления данными и должна учитываться при разработке приложения. Проект должен обеспечивать конфиденциальность, гарантируя, что данные на принимающей стороне считаются анонимными от отдельного лица или компании. Ниже приведены компоненты модели конфиденциальности:

- Управление идентификацией устройств и приложений;
- Аутентификация;
- Авторизация;
- Доверие;
- Репутация.

Соответствующее шифрование идентификации источника данных обеспечивает конфиденциальность. Управление идентификатором устройства обеспечивает конфиденциальность. Проанализированные расшифрованные данные являются входными данными для приложения, сервиса или процесса. Данные IoT или M2M должны быть предназначены только для бенефициара, отдельного лица или компании. Когда данные передаются из одной точки в другую, необходимо гарантировать, что заинтересованная сторона в будущем не сможет неправильно использовать конечные данные устройства или данные приложения. Эти статические и динамические отношения являются компонентами, которые зависят от доверия и репутации.

Безопасный доступ к данным

Доступ к данным должен быть безопасным. Проект обеспечивает аутентификацию запроса на данные и авторизацию для доступа к ответу или услуге. Он также может включать аудит запросов и доступов к ответам для подотчетности в будущем. Пример 2.4

описывает, как уровень обеспечивает конфиденциальность и авторизацию с использованием AES-128 и CCM. Сквозная безопасность – это еще один аспект, который подразумевает использование протокола безопасности на каждом уровне, физическом, логическом канале и транспортных уровнях во время связи на обоих концах сети..

Сбор и обогащение данных

Приложения IoT/M2M включают такие действия, как сбор данных (приобретение), проверка, хранение, обработка, запоминание (сохранение) и анализ. Сбор данных относится к получению данных из сети устройств/устройств. Существует четыре режима сбора данных:

1. Опрос относится к данным, запрашиваемым с устройства путем обращения к устройству; например, информация о заполнении контейнера для отходов в системе управления отходами.

2. Сбор на основе событий относится к данным, запрашиваемым с устройства при наступлении события; например, когда устройство приближается к точке доступа или карта приближается к считывателю карт или происходит начальный обмен данными для настройки однорангового или главного-подчиненного соединения устройства BT с использованием NFC.

3. Запланированный интервал относится к данным, запрашиваемым с устройства через выбранные интервалы; например, данные об условиях окружающего освещения в Интернете уличных фонарей.

4. Непрерывный мониторинг относится к данным, запрашиваемым с устройства непрерывно; например, данные о наличии дорожного движения в определенных условиях уличного освещения в Интернете уличных фонарей. Обогащение данных относится к добавлению ценности, безопасности и удобства использования данных..

Распространение данных

Рассмотрим следующие три шага для обогащения данных перед распространением данных в сети как агрегацию, уплотнение и слияние.

Агрегация относится к процессу объединения текущих и ранее полученных кадров данных после удаления избыточных или дублирующихся данных.

Уплотнение означает сокращение информации без изменения смысла или контекста; например, передача только инкрементных данных, чтобы отправленная информация была короткой.

Слияние означает форматирование информации, полученной по частям, через различные кадры данных и несколько типов данных (или данные из нескольких источников), удаление избыточности в полученных данных и представление отформатированной информации, созданной из частей информации. Слияние данных используется в случаях, когда отдельные записи не требуются и/или не могут быть извлечены позже.

Рассеивание энергии при распространении данных

Потребление энергии при распространении данных является важным фактором во многих устройствах в WPAN и беспроводных сенсорных узлах. Это связано с ограниченным сроком службы батареи. Энергия потребляется при выполнении вычислений и передач. Чем выше скорость передачи данных, тем больше будет потребляться энергии. Чем выше используется радиочастота, тем больше будет потребляться энергии. Чем выше интервал сбора, тем меньше будет потребляться энергии.

Энергоэффективные вычисления могут быть выполнены с использованием концепций агрегации, уплотнения и слияния данных.. Меньшее количество передаваемых байтов данных, большие интервалы сбора и более низкая скорость передачи данных

Источник данных и назначение данных

ID: каждому устройству и каждому ресурсу устройства назначается идентификатор для указания данных источника и отдельный идентификатор для назначения данных.

Адрес: поля заголовка добавляют адрес назначения (например, 48-битный MAC-адрес на канальном уровне, 32-битный адрес IPv4 в сети IP и 128-битный адрес IPv6 в сети IPv6), а также могут добавлять порт (например, порт 80 для приложения HTTP).

Характеристики, форматы и структуры данных

Характеристики данных могут быть в терминах временных данных (зависящих от времени), пространственных данных (зависящих от местоположения), данных в реальном времени (генерируемых непрерывно и получаемых непрерывно в том же темпе), данных реального мира (из физического мира, например, дорожного движения или уличного освещения, условий окружающей среды), проприетарных данных (данные об авторском праве, зарезервированные для распространения уполномоченным предприятиям) и больших данных (неструктурированные объемные данные).

Данные, полученные с устройств, форматируются перед передачей в Интернет. Формат может быть в XML, JSON и TLV. Файл может иметь тип MIME для Интернета..

Шлюз управления устройствами

Управление устройствами означает предоставление идентификатора или адреса устройства, который отличается от других ресурсов, активацию устройства, настройку (управление параметрами и настройками устройства), регистрацию, отмену регистрации, присоединение и отсоединение.

Управление устройствами также означает принятие подписки на его ресурсы. Управление неисправностями устройства означает порядок действий и рекомендации, которым необходимо следовать в случае возникновения неисправности в устройстве. Для управления устройствами используются Open Mobile Alliance (OMA)-DM и несколько стандартов. Модель OMA-DM предполагает использование сервера DM, который взаимодействует с устройствами через шлюз в случае приложений IoT/M2M. Сервер DM – это сервер для назначения идентификатора или адреса устройства, активации, настройки (управления параметрами и настройками устройства), подписки на службы устройства или отказа от служб устройства и настройки режимов устройства. Устройство вместо сервера DM взаимодействует со шлюзом в случае среды с низким уровнем потерь мощности.

Функции шлюза для управления устройствами:

– Выполняет ли функцию пересылки, когда сервер DM и устройство могут взаимодействовать без переформатирования или структурирования.

– Выполняет ли преобразование протоколов, когда устройство и сервер DM используют разные протоколы.

– Выполняет ли функцию прокси, если требуется промежуточная предварительная выборка в среде с потерями или сетевой среде требуется.

Контрольные вопросы:

1. Что такое шлюз IoT и какую роль он играет в архитектуре IoT?
2. Перечислите основные функции, которые выполняет шлюз IoT в управлении данными.
3. Каковы различия между транскодированием и уплотнением данных в контексте функций шлюза?
4. Объясните, что такое сбор данных на основе событий и приведите пример его применения.
5. Как шлюз IoT обеспечивает взаимодействие между устройствами, использующими разные протоколы?
6. В чем заключается значение управления устройствами в контексте работы шлюза IoT?