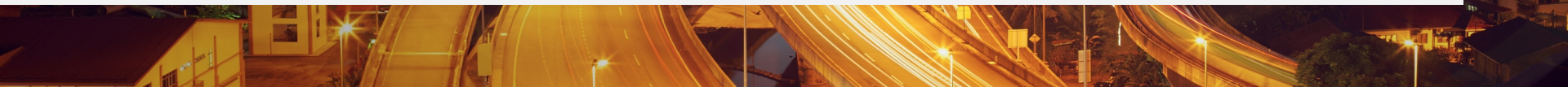
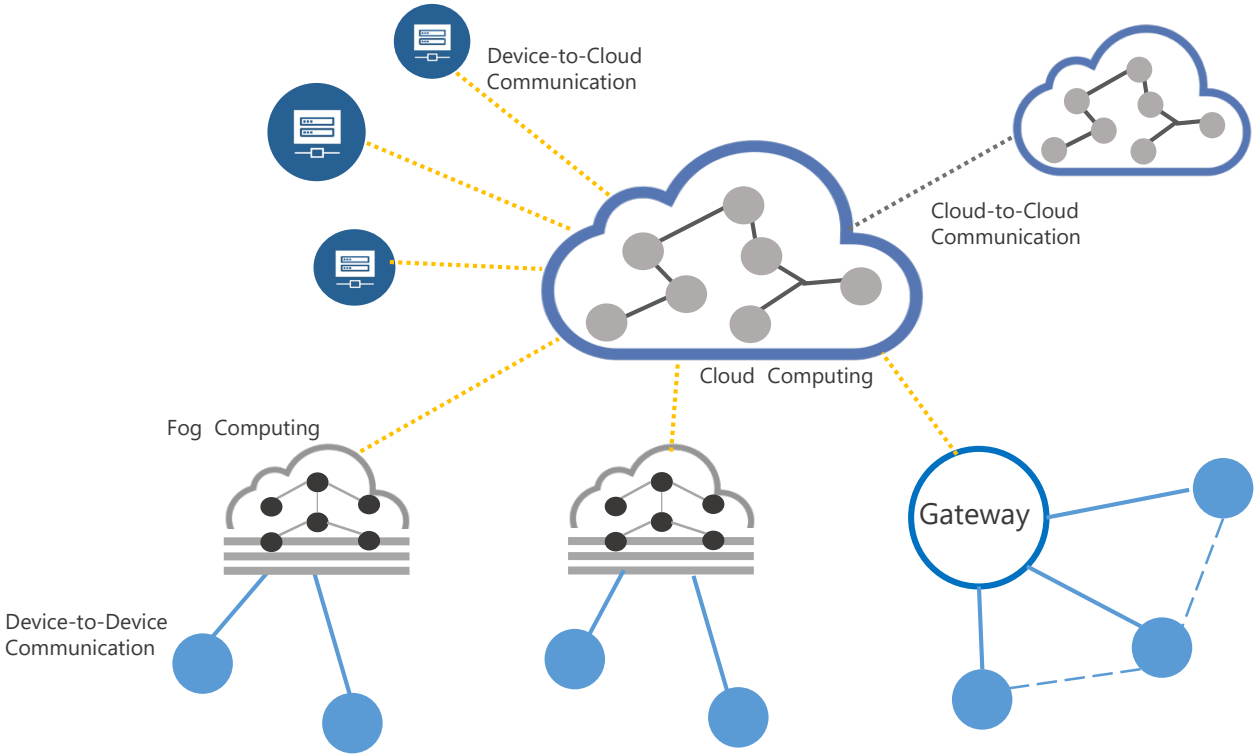
Стандартизованные в РФ протоколы для защиты M2M и IoT

Ольга Шемякина, системный аналитик



Особенности M2M и IoT/IIoT протоколов

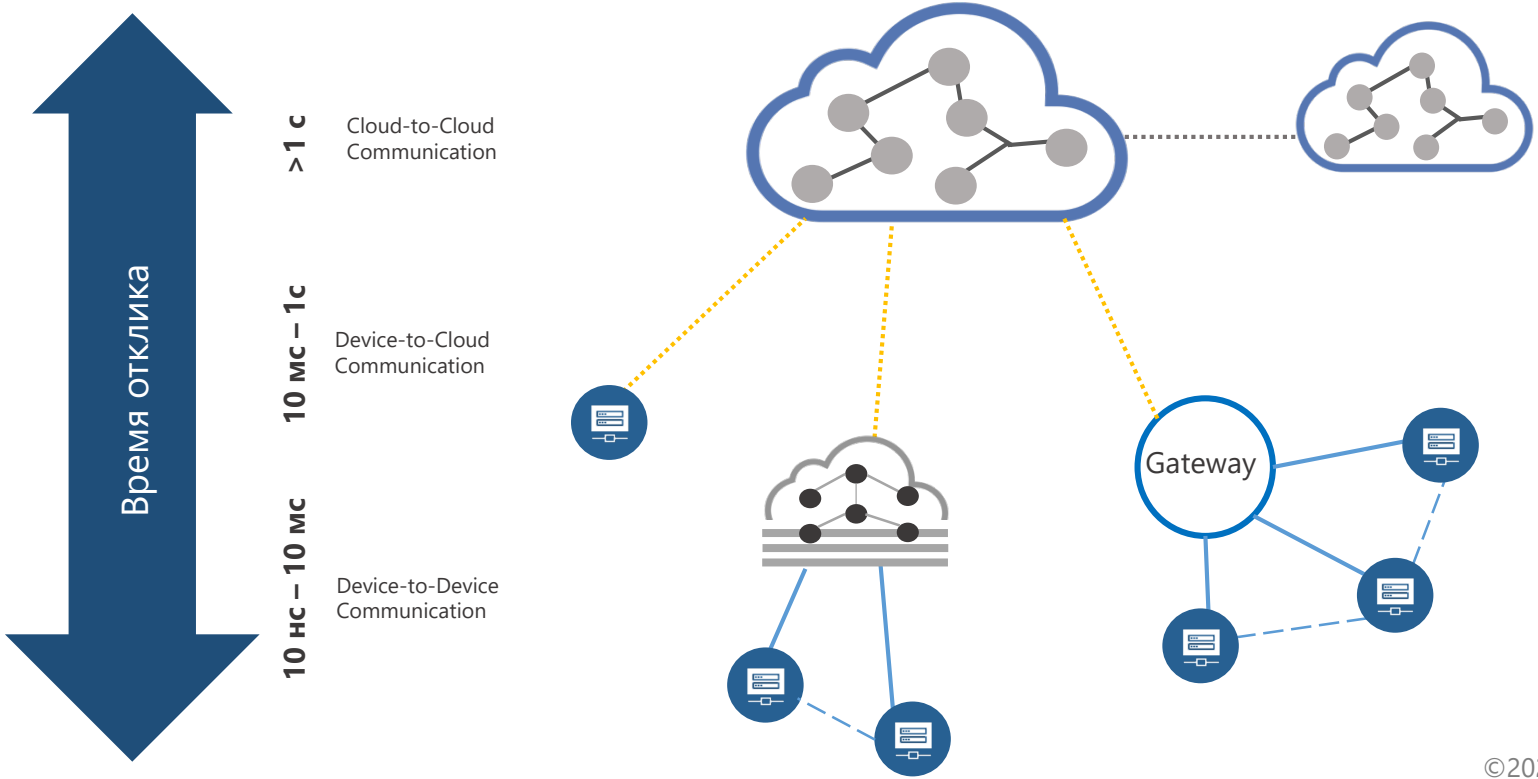
M2M и IoT коммуникации



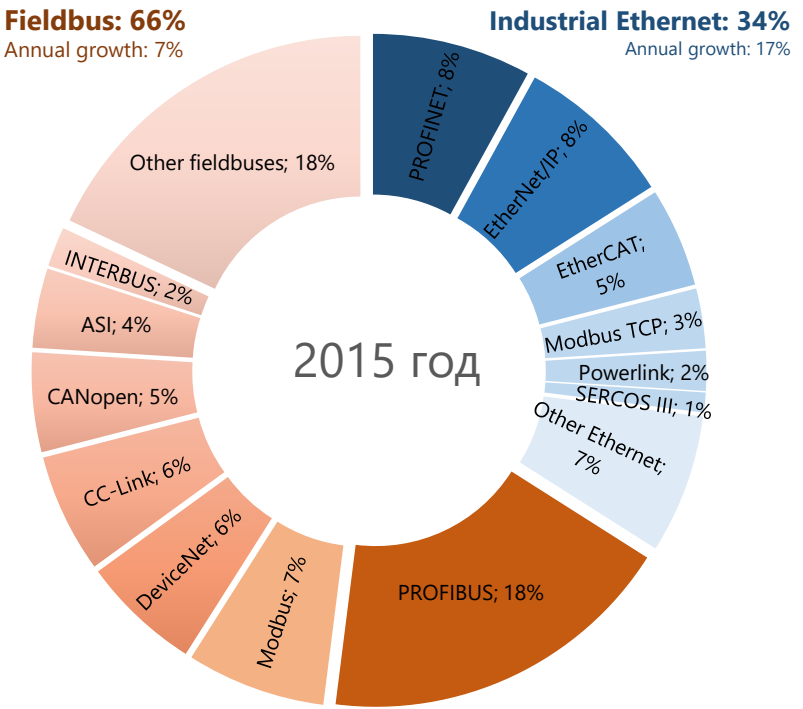
IoT/IIoT коммуникации

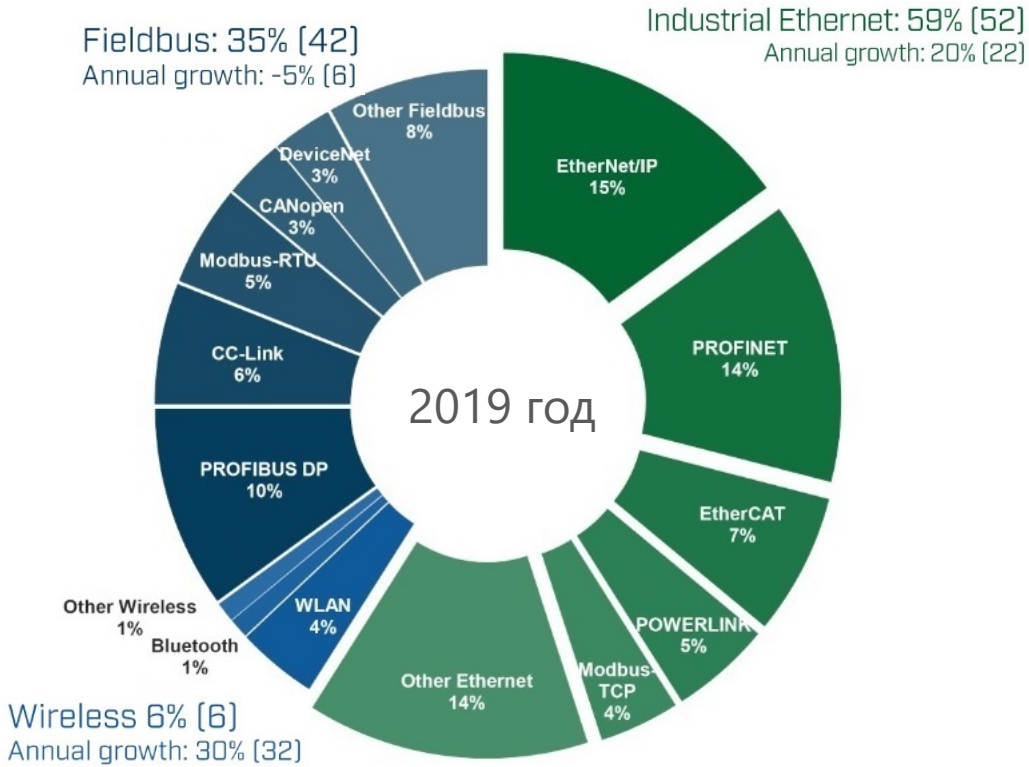
M2M коммуникации

Латентность для IoT и M2M коммуникаций



Промышленные M2M протоколы



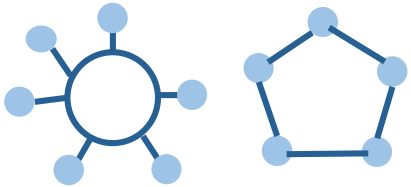


Source: HMS Industrial Networks

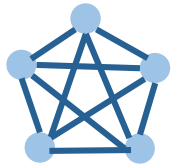
Топология M2M протоколов

Общая шина

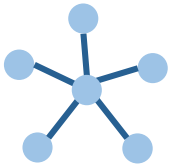
Кольцо



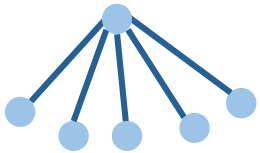
Полносвязная



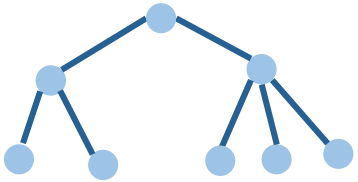
Звезда



Звезда-Иерархия



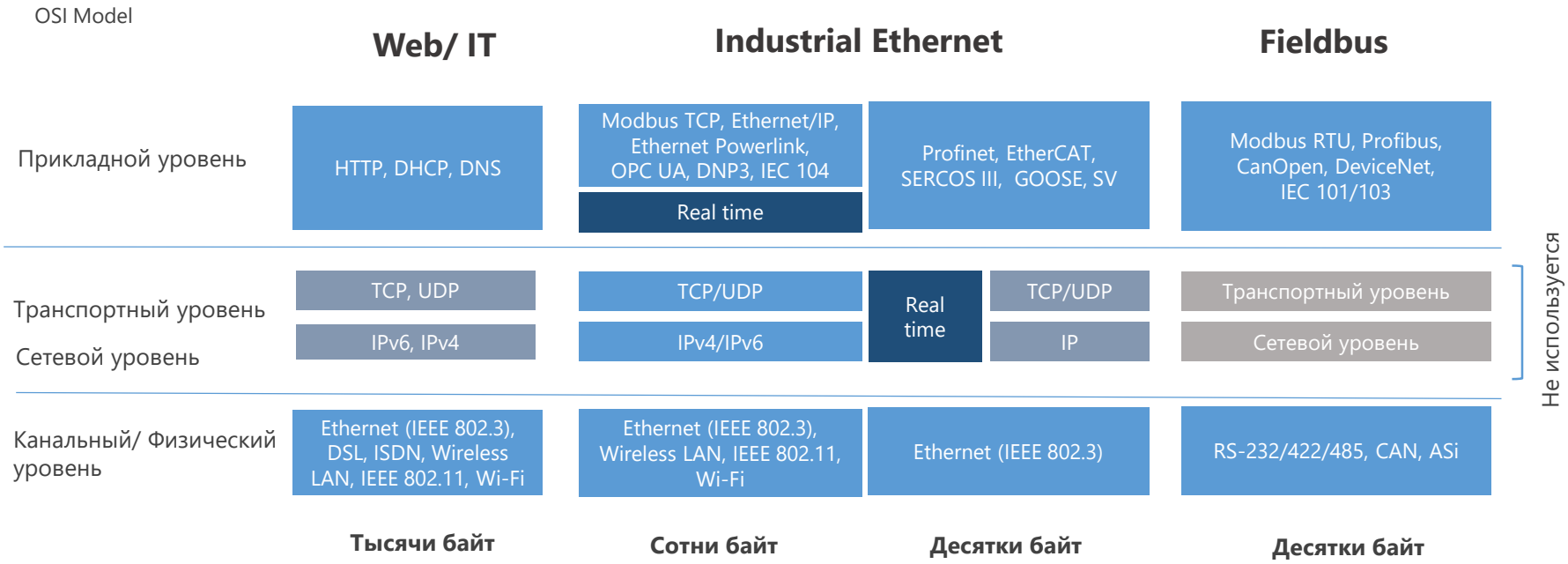
Дерево



Модель взаимодействия

- Точка-точка
- Широковещательная
- Мультикаст
- Подписочная модель
- Запрос / Ответ

Стек M2M протоколов



Основные IoT/IIoT протоколы

- OPC UA
- MQTT
- AMQP
- CoAP
- REST/HTTP
- LoRaWAN
- LoWPAN
- И многие другие …

Сравнение IoT/IIoT протоколов

	MQTT	OPC UA	AMQP	REST	CoAP	LoRaWAN LoWPAN
Транспорт	TCP/IP	TCP/IP	TCP/IP	TCP/IP	UDP/IP	TCP/IP
Взаимодействие	Publish-Subscr.	Request-Respon	Point-to-point	Request-Respon	Request-Respon	Point-to-point
Применение	Device-to-Cloud Cloud-to-Cloud	Device-to-Cloud Cloud-to-Cloud Device-to-Device	Device-to-Cloud Cloud-to-Cloud Device-to-Device	Device-to-Cloud Cloud-to-Cloud	Device-to-Cloud Cloud-to-Cloud	Device-to-Cloud Cloud-to-Cloud
Латентность	низкая	низкая	низкая	высокая	высокая	низкая
Real-time	условно	Real-time	условно	нет	нет	нет
ИБ	TLS	профиль	TLS	HTTPS	DTLS	TLS/ DTLS На уровне чипа

Архитектура и особенности

- Малые вычислительные ресурсы устройств
- Работа от «батарейки»
- Большая вариативность технологий
- Множество протоколов
- Низкая пропускная способность полевых протоколов
- Чувствительность к размеру добавляемых данных
- Высокая латентность полевых протоколов
- Групповые операции

Особенности ИБ для M2M и IoT

Основные атаки на IIoT/M2M

Навязывание устаревших данных (REPLAY ATTACK)

Подмена IIoT/M2M устройств

Подмена команд (COMMAND INJECTION)

«Перепрошивка» IIoT/M2M устройств

Подача команды аварийного останова

DDOS-атака для отказа в обслуживании

Приоритеты защиты

Web/IT

- Конфиденциальность
- Целостность
- Доступность

M2M
IoT/IIoT

- Доступность
- Целостность
- Аутентичность
- Конфиденциальность

Требования к протоколам защиты M2M и IoT/IIoT коммуникаций

- Работа на прикладном уровне и независимость от протоколов передачи данных
- Отсутствие установления сессии
- Защита от повторов
- Поддержка групповых операций
- Простая ключевая система

Требования к алгоритмам защиты M2M и IoT/IIoT коммуникаций

- Небольшой размер добавляемых данных
- Быстрые алгоритмы
- Энергоэффективные алгоритмы
- Минимальный набор алгоритмов

Симметричные алгоритмы

Защищенные индустриальные протоколы

Защищенные протоколы ТК26

- «Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств» (Р 1323565.1.028–2019)
- «Протокол защищенного обмена для индустриальных систем» (CRISP 1.0) (Р 1323565.1.029–2019)
- «Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS»
- «Протокол безопасности сетевого уровня» (IPlir)

Криптографические механизмы защищенного взаимодействия контрольных и измерительных устройств

- Работает на прикладном уровне, не зависит от протоколов передачи данных
- Требует установления соединения
- Нет защиты от повторов
- Не поддерживаются групповые связи
- Алгоритмы: блочный шифр, хэш-функция, HMAC, вычисление точек эллиптической кривой + опционально: ЭП

CRISP

- Работает на прикладном уровне, не зависит от протоколов передачи данных
- Не требует установления соединения
- Есть защита от повторов
- Поддерживаются групповые связи
- Алгоритмы: блочный шифр в режимах CTR и CMAC
- Предраспределенные ключи

Использование российских криптографических механизмов для реализации обмена данными по протоколу DLMS

- Защита DLMS
- Установление соединения опционально
- Нет защиты от повторов
- Поддерживаются групповые связи
- Алгоритмы: блочный шифр в режимах CTR* и CMAC*, KExp15* / KImp15* + опционально: VKO, ЭП, HMAC
- Предраспределенные ключи или механизмы согласования ключей

IPlir

- Защита IP-трафика
- Может использоваться для построения полноценных VPN
- Не требует установления соединения
- Защита от повторов опциональна
- Не поддерживаются групповые связи
- Алгоритмы: блочный шифр в режимах CTR (MGM) и CMAC
- Предраспределенные ключи


infotecs
Спасибо за внимание!