Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

Безопасность LoRaWAN RU

Шемякина Ольга,
Системный аналитик, ОАО «ИнфоТеКС»

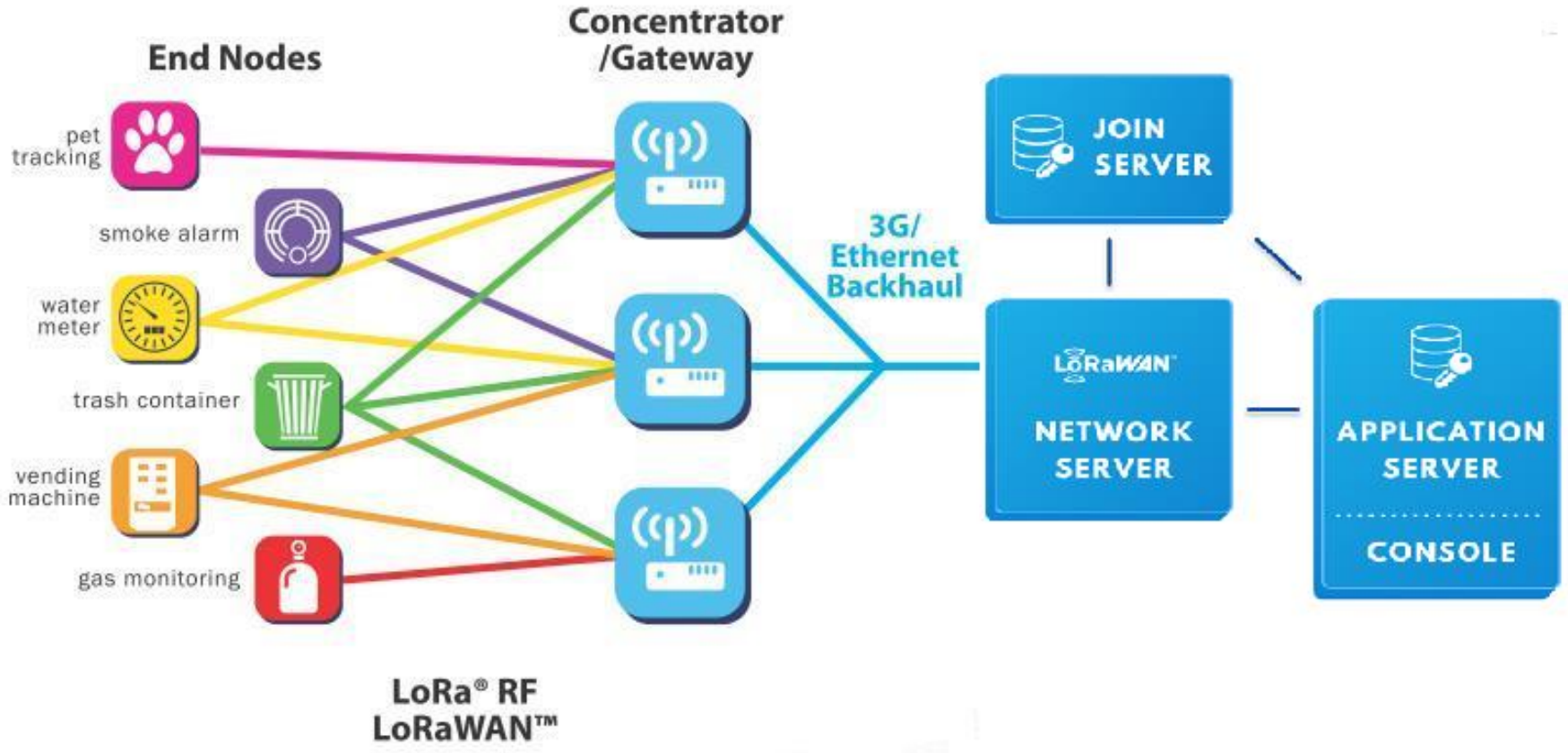
LoRaWAN RU

- В 2019 ТК194 «Кибер-физические системы» представил ПНСТ «Протокол обмена для высокоемких сетей с большим радиусом действия и низким энергопореблением»
- ПНСТ является адаптацией для России протокола LoRaWAN 1.1
- ПНСТ имеет статус региональной спецификации LoRaWAN - LoRaWAN RU
- Был передан для рассмотрения в ТК26 и получил достаточно большое количество замечаний, в результате появилась доработанная версия

НИР «Циферблат»

- Академией криптографии РФ в 2019 году была поставлена научно-исследовательская работа (НИР) «Циферблат», часть которой посвящена криптографической защите информации в LoRaWAN RU

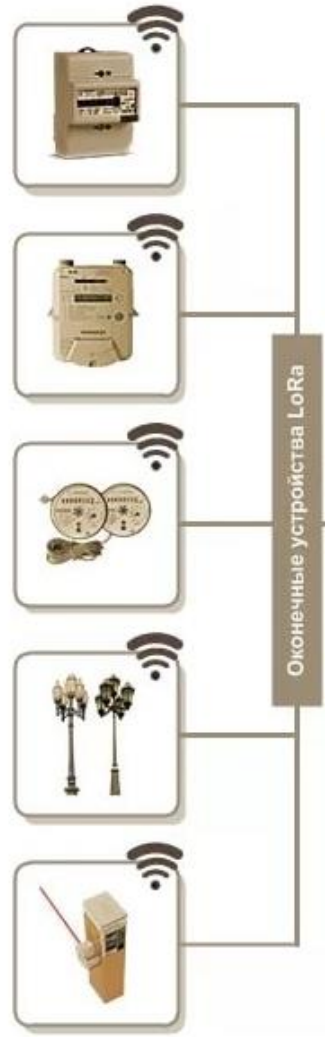
Архитектура LoRaWAN



Оконечные устройства

- Предназначены для осуществления управляющих или измерительных функций

- Класс А – прием нисходящих сообщений возможен только сразу после передачи. Минимальное энергопотребление
- Класс В – возможен прием нисходящих сообщений по расписанию. Возможно получение многоадресных сообщений
- Класс С – постоянная готовность принимать нисходящие сообщения. Возможно получение многоадресных сообщений



Шлюз

- Принимает восходящие сообщения от оконечных устройств по радиоканалу
- Передает восходящие сообщения на сетевой сервер
- Осуществляет доставку нисходящих сообщений на оконечные устройства
- Шлюз и оконечные устройства образуют топологию «звезда»

Базовая станция LoRaWAN

Сетевой сервер

- Управляет радиосетью
- Контролирует радиосеть
- Маршрутизирует сообщения между оконечными устройствами и сервером приложений

Сервер приложений

- Выполняет обработку данных
- Управляет оконечными устройствами на прикладном уровне

Сервер присоединения

- Проводит активацию оконечных устройств по воздуху
- Вырабатывает сеансовые ключи в случае активации оконечных устройств по воздуху

Особенности LoRaWAN RU

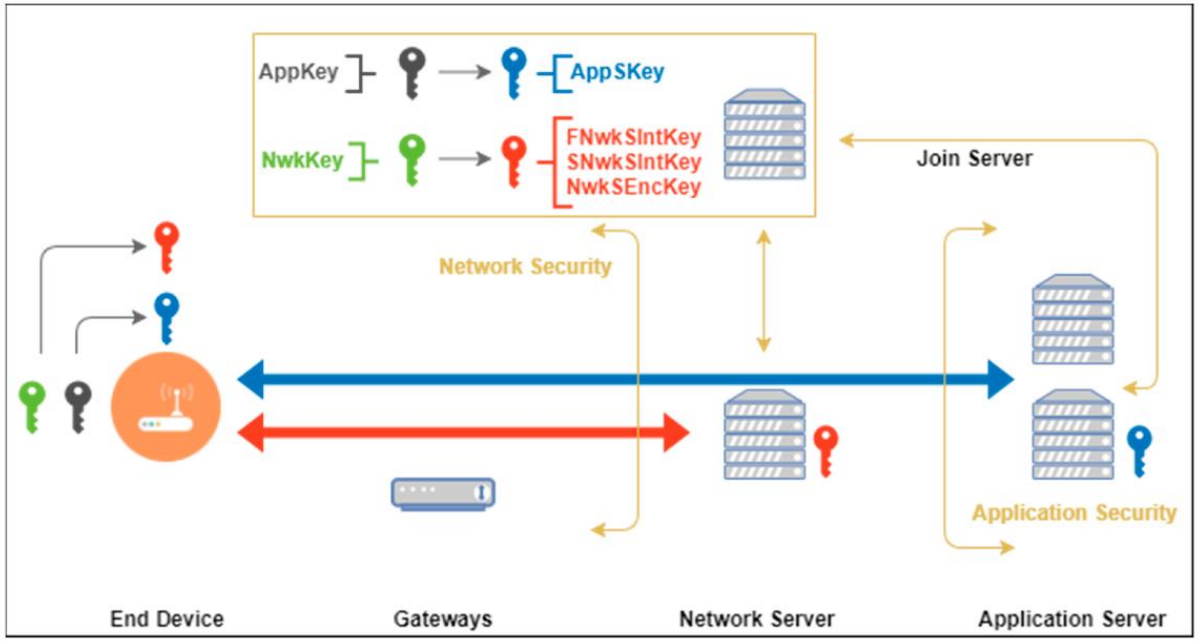
- Сетевой сервер, сервер присоединения, сервер приложений расположены на одном физическом устройстве
- Предусматривает обратную совместимость с протоколом LoRaWAN 1.0

Активация оконечных устройств

- Активация по воздуху
- Активация через персонализацию

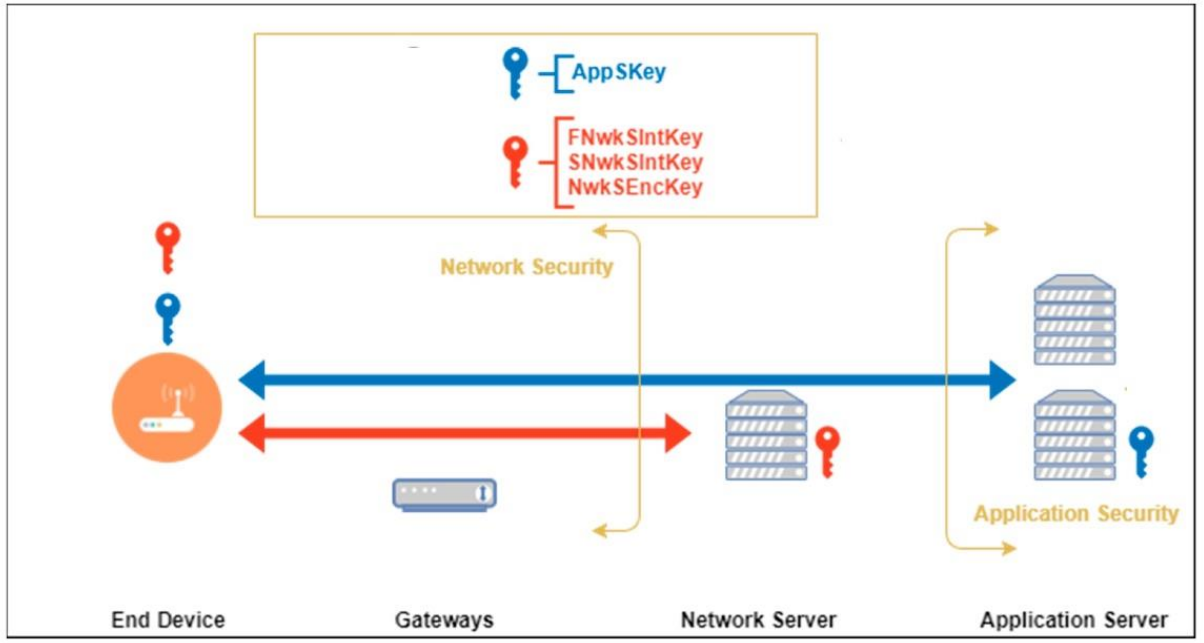
Активация по воздуху

- Оконечное устройство направляет запрос на присоедение к сети на сервер присоединения
- В результате из базовых ключей вырабатываются сеансовые ключи
- Возможно повторное присоединение к сети при потере информации о сеансе или для обновления сеансовых ключей

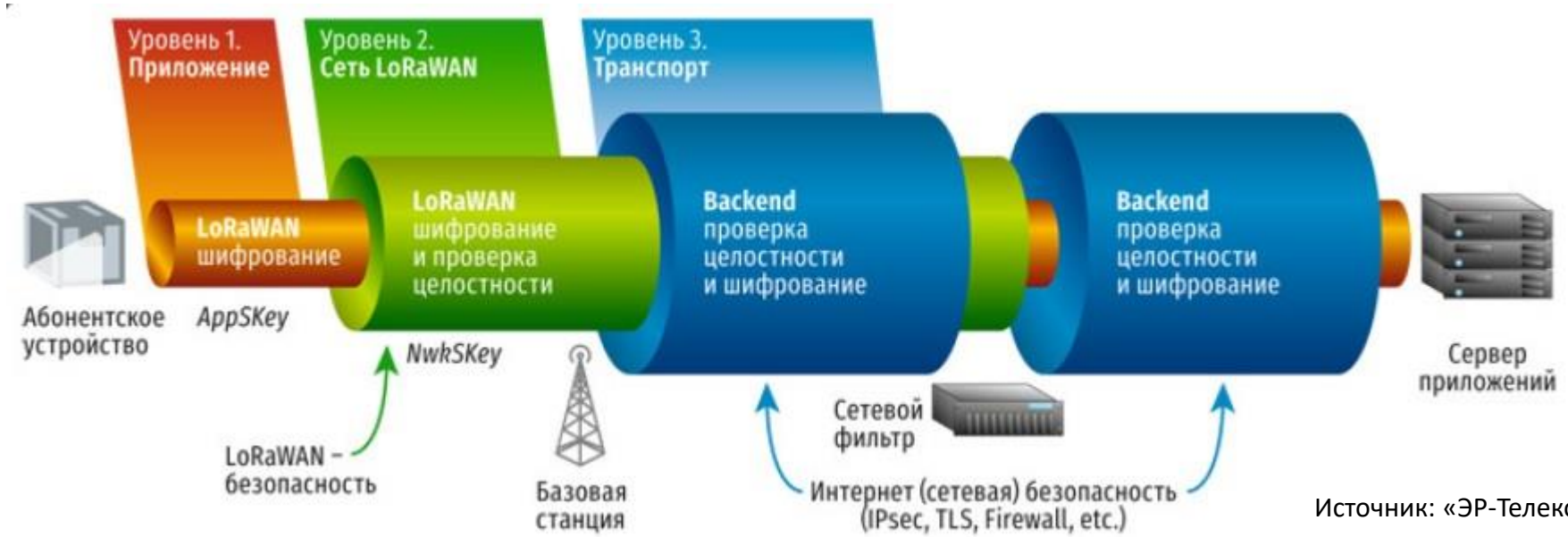


Активация через персонализацию

- Не проводится процедура присоединения
- Оконечное устройство укомплектовано необходимой информацией для работы в конкретной сети (включая сеансовые ключи)



Защита передаваемых данных



Источник: «ЭР-Телеком Холдинг»

- Не обеспечивается целостность данных на прикладном уровне
- Backend защита в LoRaWAN не определена
- В LoRaWAN используется алгоритм AES, в LoRaWAN RU не определен*

Дополнительная защита в LoRaWAN RU

Источник: «ЭР-Телеком Холдинг»

- Возможно дополнительное шифрование и вычисление имитовставки по алгоритму «Кузнечик»

Анализ LoRaWAN 1/4

- Уязвимости в режиме обратной совместимости с LoRaWAN 1.0
  - Использование случайных чисел при передаче данных и при присоединении к сети (они могут повториться)
  - Переполнение или сброс счетчиков сообщений
  - Отсутствие связи сообщения-подтверждения с исходным сообщением или исходным запросом на присоединение к сети
- Эти уязвимости приводят к различным атакам
- Часть атак возможна для одного из направлений связи в режиме обратной совместимости

Анализ LoRaWAN 2/4

- Установка, распределение и хранение первичных ключей
  - Ключи остаются в виде меток на корпусе оконечного устройства
  - Значения ключей по умолчанию не меняются при вводе устройств в эксплуатацию
  - Формирование ключей на основе идентификаторов
  - Дубликаты ключей остаются в технических средствах, использовавших для ввода ключей
  - Файлы с ключами передаются по почте, на флэш-накопителях и т.д.
  - Одинаковые ключи используются для группы устройств
  - Недостаточная защита серверов
  - Недостаточная защита инфраструктуры разработчика

Анализ LoRaWAN 3/4

- Небольшой размер счетчика присоединений может привести к переполнению и блокированию дальнейшей работы устройства
- Не обеспечивается целостность данных между оконечным устройством и сервером приложений. Возможны атаки человека посередине или вредоносного сетевого сервера
- Не определен протокол передачи сеансового ключа от сервера присоединения к серверу приложений
- Длины имитовставки 4 байта может быть недостаточно
- При активации через персонализацию сеансовые ключи не меняются

Анализ LoRaWAN 4/4

Выводы

- Уязвимости относятся к протоколу, а не используемым криптографическим алгоритмам
- Замена AES на ГОСТ не изменит ситуацию с безопасностью

Анализ дополнительного шифрования 1/4

- Декларируется использование режима гаммирования, однако формулы не соответствуют ГОСТ Р 34.13-2015
- Вопрос с достаточностью имитовставки длиной 4 байта
- Ключи шифрования и имитозащиты сообщений постоянные на весь срок службы

Анализ дополнительного шифрования 2/4

- Вызывают большой вопрос требования к счетчикам сообщений:
  - Размер счетчика 4 байта
  - Счетчик циклический
  - Значение счетчика не должно повторяться
  - Рекомендуется использовать каждый раз новое значение счетчика
  - Есть требование по обновлению сеанса до переполнения значения счетчика при активации по воздуху
  - Указанные скорости при сроке службы в 10 лет могут привести к переполнению счетчика при активации через персонализацию

Анализ дополнительного шифрования 3/4

- В случае возможного переполнения счетчика:
  - **Нарушается защита от повторов**
  - **Нарушается конфиденциальность** (используется режим гаммирования и синхропосылка определяется значением счетчика)
  - Из-за особенностей формирования имитовставки (имитовставка вычисляется только для значения счетчика и значения прикладных данных) в некоторых ситуациях можно навязать одной из сторон корректное сообщение, таким образом **нарушается целостность** и **аутентификация источника информации**

Анализ дополнительного шифрования 4/4

Выводы

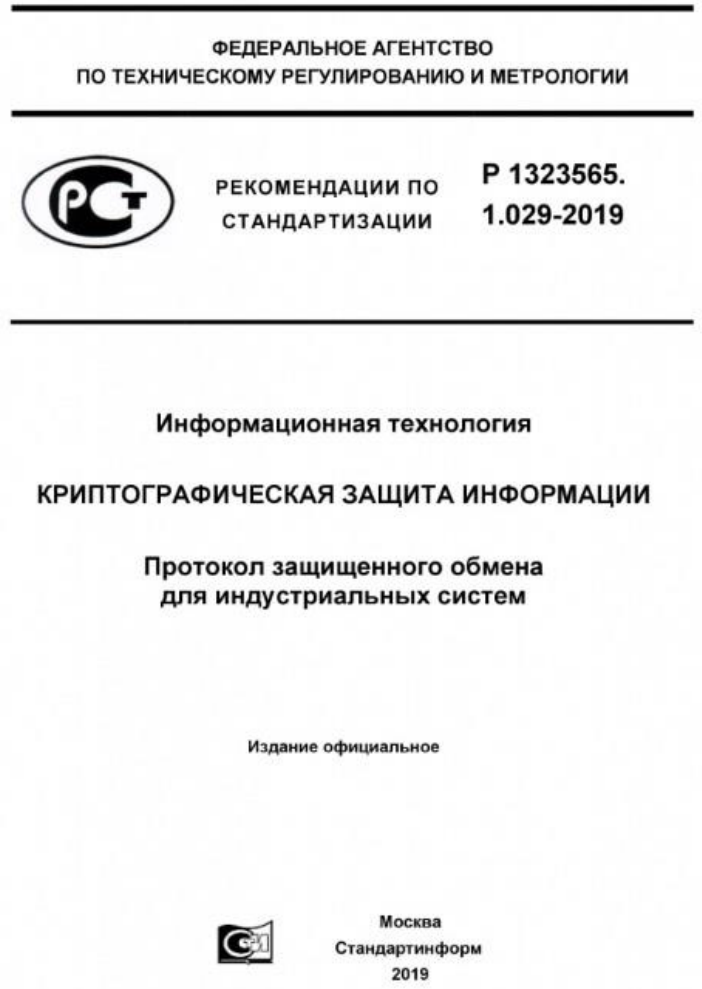
- Проблемы с криптографической стойкостью дополнительного шифрования LoRaWAN RU могут привести к тому, что разные разработчики по-разному будут их устранять и это приведет к несовместимым реализациям

Предложения по защите LoRaWAN RU

- Позиционировать LoRaWAN RU только как протокол передачи данных без упоминания криптографической защиты и свойств безопасности
- Реализовать криптографическую защиту данных на прикладном уровне
- Использовать стандартизованный криптографический протокол (CRISP)
- Формирование рекомендаций по использованию криптографического протокола осуществлять в рамках рабочей группы ТК26 при участии представителей Ассоциации интернета вещей

Свойства протокола CRISP

- Не требует установления сеанса связи
- Использует только симметричные алгоритмы
- Использует минимальный набор алгоритмов
- Использует небольшой объем ключевой информации
- Обеспечивает защиту от повторов
- Шифр «Магма» может быть эффективнее «Кузнечика» для легковесных реализаций
- Позволяет использовать только имитозащиту
- Позволяет работать с многоадресными сообщениями
- Поддерживает сменные криптографические наборы
- Одобрен ТК26 и имеет статус рекомендаций по стандартизации



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.
1.029-2019

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Протокол защищенного обмена
для индустриальных систем

Издание официальное

Москва
Стандартинформ
2019

Вопросы

Контактная информация

Электронная почта:

Olga.Shemyakina@infotecs.ru

Телефон:

+7 812 383-14-28 (доб. 4910)

Сайт:

infotecs.ru

tc26.ru