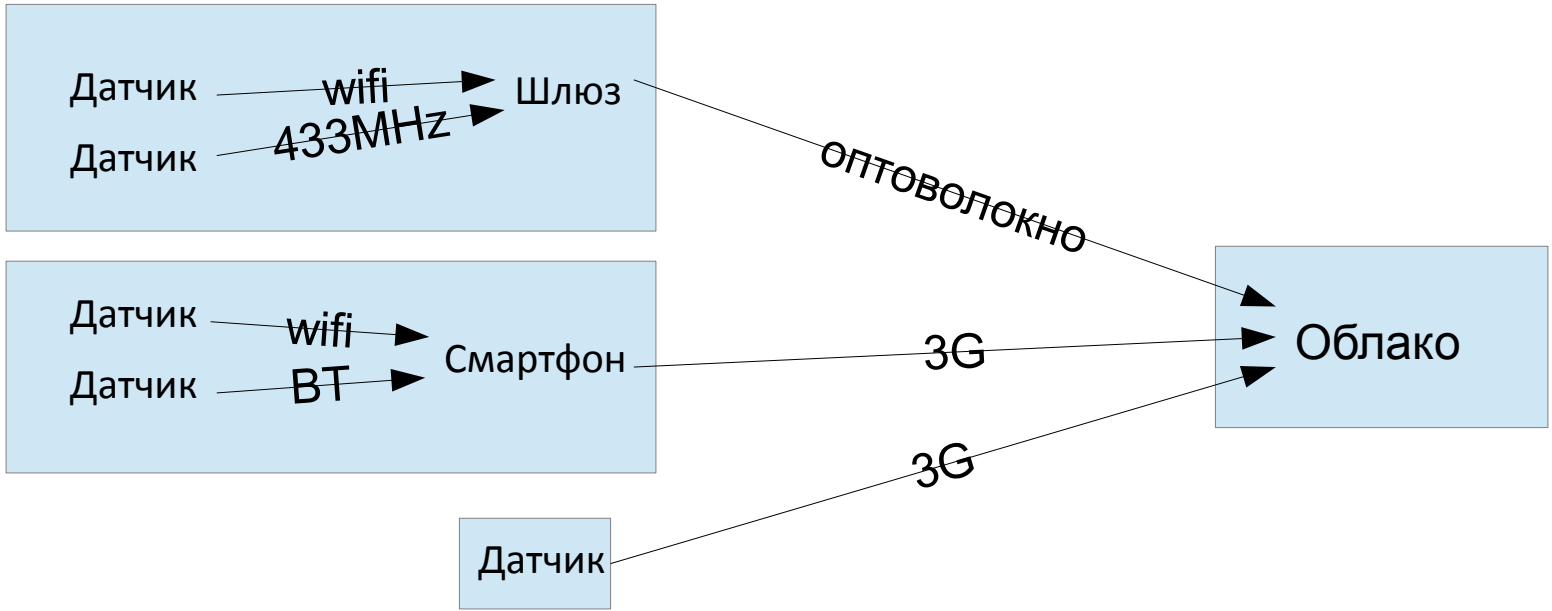
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Кафедра 54 «Технологий защиты информации»

2015-11-02

К.А. Жиданов

Элементы, участвующие в интернете вещей



Элементы, участвующие в интернете вещей

- Датчики/устройства (например, iBeacon, Intel Curie, arduino, любые микроконтроллеры и т.д.)
- Шлюзы (например, Open WRT, Raspberry Pi, Intel Moon island и т.д.)
- Каналы связи (например, bluetooth, zigbee, 3G/4G, wifi, IrDA)
- Средства мониторинга (например, смартфоны, ПК)
- Серверы

Проблемы датчиков/устройств

- Малая ёмкость батарей
- Малая вычислительная мощность
- Малая дальность связи
- Устройство может быть легко украдено
- Отсутствуют средства ввода-вывода для аутентификации (нет клавиатуры для ввода пина/пароля)

  На устройствах должна использоваться lightweight cryptography и нетривиальные алгоритмы распределения ключей

Проблемы шлюзов

- Шлюз может не быть доверенным устройством (датчики должны иметь возможность связываться с облаком в любом месте, где настроена соответствующая инфраструктура)
- Шлюз не может хранить аутентификационные данные устройств
- Шлюз должен авторизовать устройства, чтобы противостоять DoS атакам и спаму

Шлюзы должны реализовывать алгоритмы типа zero-knowledge, на них должно осуществляться end-to-end шифрование

Проблемы каналов связи

- Любой из каналов является мерцающим (связь может эпизодически пропадать даже внутри квартиры)
- Беспроводные каналы могут быть заглушёны помехой (jammers доступны на чёрном рынке)
- Каналы могут быть прослушаны (сниферы доступны на чёрном рынке)
- На каналы может быть произведена атака “человек посередине”

Никакая информация не может передаваться в открытом виде, любое устройство должно иметь возможность связаться со своими соседями (смартфоном, другими датчиками) напрямую. В некоторых случаях наличие связи с облаком вообще не предполагается, либо такая связь планируется эпизодической.

Проблемы серверов

- Возможность построения децентрализованной системы, состоящей из нескольких кластеров

Проблемы устройств мониторинга

- Возможность peer-to-peer подключения к конечным устройствам

Конфиденциальность, целостность и доступность

- В IoT необходимо решить все проблемы ИБ
- Проблемы конфиденциальности подразделяются на категории
  - Реализация Lightweight шифрования
  - Создание схемы распределения ключей с возможностью работы без центра сертификации

Добавление, удаление устройств, делегирование прав

- Все операции с устройствами должны иметь возможность происходить в отсутствие связи с сервером
- Устройство добавленое/удаленное децентрализованно, при появлении связи с сервером должно быть успешно на нём зарегистрировано
- При удалении устройства из группы должно происходить обновление ключей группы (т.е. даже если устройство сохранит аутентификационные данные после процедуры отвязки, оно не должно проходить взаимную аутентификацию с валидными членами группы)

Требования к протоколу аутентификации

- Если операция совершается в отсутствие связи с сервером, то при появлении связи сервер должен принять новые датчики/устройства в Интернет вещей данного пользователя
- аутентификационные данные каждого из датчиков/устройств должны храниться только на самом датчике/устройстве, во избежание компрометации
- протоколы аутентификации и распределения ключей должны быть вычислительно простыми, чтобы они могли выполниться маломощными датчиками/устройствами

Проблемы аутентификации

- Главная проблема – атака типа “человек посередине”
- Решение PKI не подходит, т.к. по условиям задачи нет постоянной связи с центром

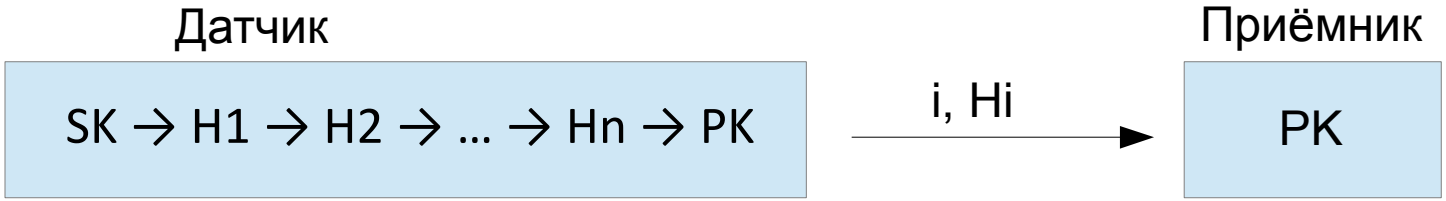
Проблемы, возникающие при краже устройств

- При краже датчика, устройства компрометируются исключительно данные самого датчика/устройства. При этом не должно быть возможности создать другой датчик/устройство, который будет корректно воспринято Интернетом вещей пострадавшего пользователя, используя украденный датчик/устройство
- при краже шлюза не должны быть скомпрометированы секретные ключи датчиков/ устройств пользователя

Пример lightweight cryptography

- Дано устройство – одноразовый датчик (например, пожара), который должен единоразово подать одну из нескольких команд
- Устройство должно быть дешёвым и крайне энергоэффективным

Цепочки хешей



Цепочки хешей

Датчик

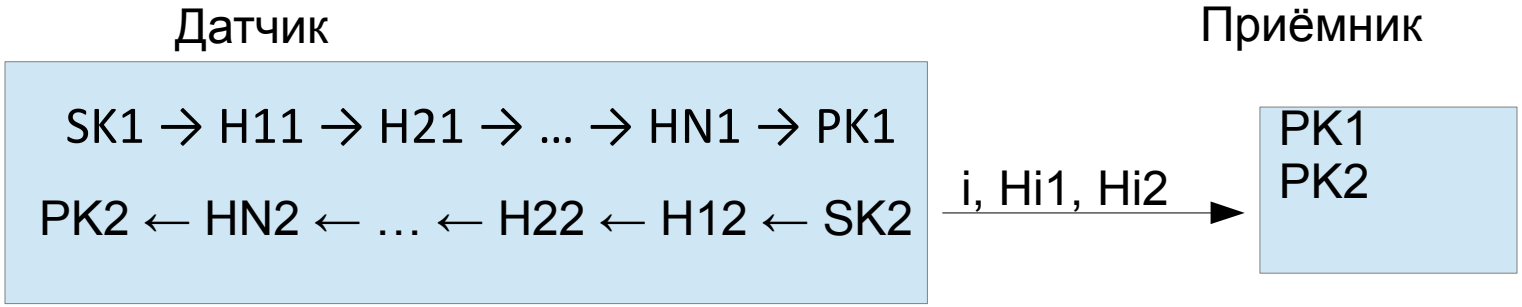
SK → H1 → H2 → … → Hn → PK

Приёмник

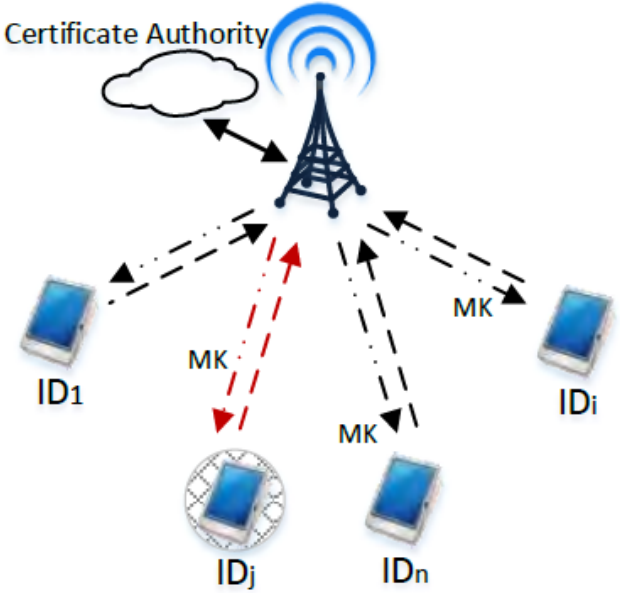
PK

Уязвимость: заставив датчик сгенерировать событие 1, можно будет имитировать остальные события

Цепочки хешей

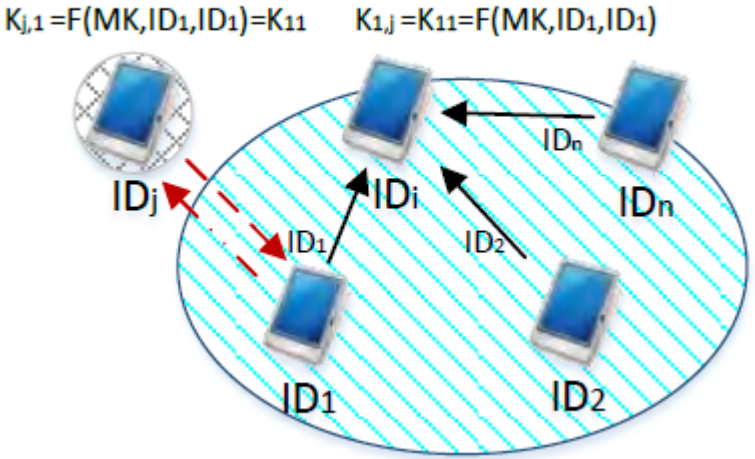


Включение в группу с временно отсутствующим центром сертификации



Включение в группу с временно отсутствующим центром сертификации

Один из способов решить проблему — разрешить k пользователям включать ещё одного



Интерполяционный полином Лагранжа

Пусть есть набор k точек

$$(x_0, y_0), \ldots, (x_j, y_j), \ldots, (x_k, y_k)$$

Тогда, если f(x) — полином степени k-1

$$L(x) := \sum_{j=0}^{k} y_j \ell_j(x)$$

, где

$$\ell_j(x) := \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{x - x_m}{x_j - x_m}$$

Интерполяционный полином Лагранжа

P(x) = y1*[(x-x2)(x-x3)]/[(x1-x2)(x1-x3)] +
y2*[(x-x1)(x-x3)]/[(x2-x1)(x2-x3)] +
Y3*[(x-x1)(x-x2)]/[(x3-x1)(x3-x2)]

$$x_0 = 1 \qquad f(x_0) = 1$$
$$x_1 = 2 \qquad f(x_1) = 4$$
$$x_2 = 3 \qquad f(x_2) = 9.$$

The interpolating polynomial is:

$$L(x) = 1 \cdot \frac{x-2}{1-2} \cdot \frac{x-3}{1-3} + 4 \cdot \frac{x-1}{2-1} \cdot \frac{x-3}{2-3} + 9 \cdot \frac{x-1}{3-1} \cdot \frac{x-2}{3-2}$$

Протокол включения пользователей в группу

Базовая станция

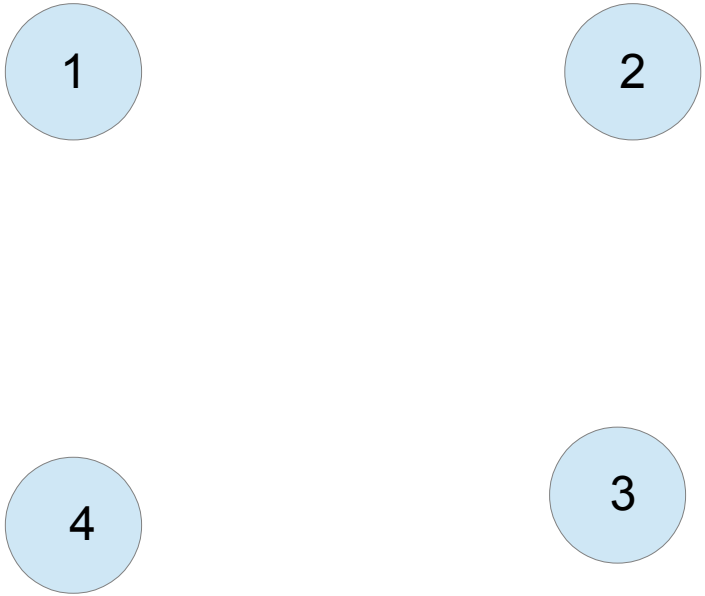
$$f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1 x + SK_c,$$
$$f(0) = SK_c,$$

Устройство 1: ID1, f(ID1)

Устройство 2: ID2, f(ID2)

Устройство N: IDn, f(IDn)

Протокол включения пользователей в группу



P1(ID1)+s1 = C1 → 2
C1 + P2(ID2)+s2 = C2 → 3
C2 + P3(ID3)+s3 = C3 → 4

C3 = P1(ID1) +
P2(ID2)+P3(ID3)+s1+s2+s3

C3 + s4 = C4 → 1
C4 - s1 = C5 → 2
C5 - s2 = C6 → 3
C6 - s3 = C7 → 4

C7 - s4 = P1(ID1) +
P2(ID2)+P3(ID3) = f(ID4)

Литература

О необходимости безопасных прямых соединений в условиях нестабильной работы сотового канала связи в совмещенных сетях «Интернета Вещей»

А.Я. Омётов, Е.А. Кучерявый, К.А. Жиданов, С.В. Беззатеев, С.Д. Андреев

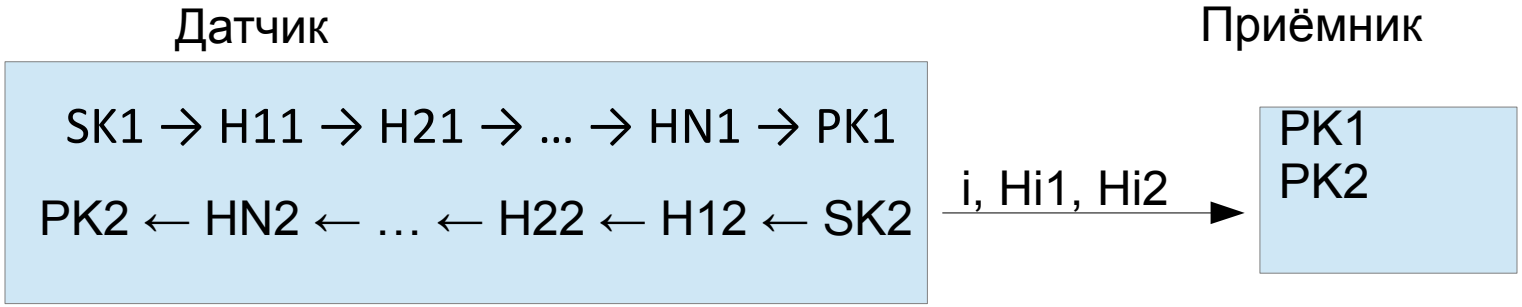
Специфика разработки протокола информационной безопасности для реализации прямых соединений в условиях нестабильной работы сотового канала связи в совмещенных сетях «Интернета Вещей»

А.Я. Омётов, Е.А. Кучерявый, К.А. Жиданов, С.В. Беззатеев, С.Д. Андреев

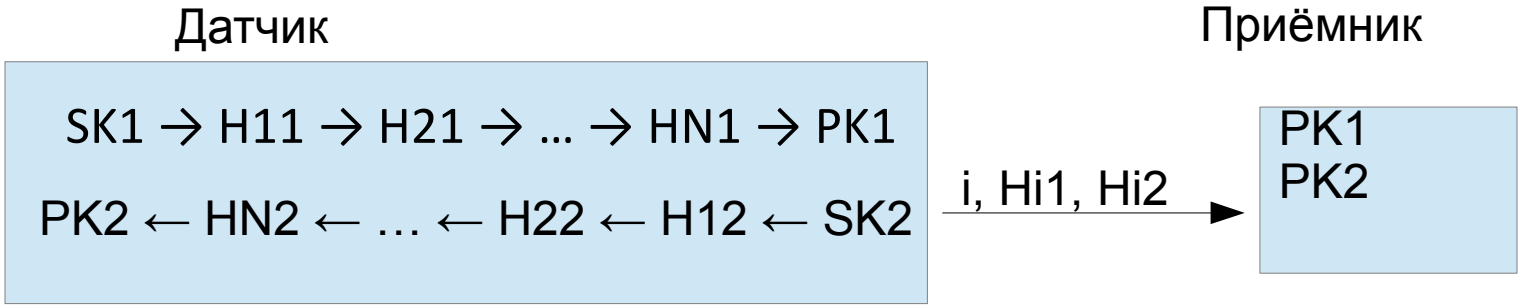
SECURING NETWORK-ASSISTED DIRECT COMMUNICATION: THE CASE OF UNRELIABLE CELLULAR CONNECTIVITY

Aleksandr Ometov, Konstantin Zhidanov, Sergey Bezzateev, Roman Florea, Sergey Andreev, and Yevgeni Koucheryavy

Включение в группу без



Включение в группу без



Жиданов Константин
konstantin.zhidanov@gmail.com
www.guap.ru