При финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (Соглашение о предоставлении субсидии № 14.575.21.0100 от 14.11.2014).

Выявление инцидентов безопасности в Интернете Вещей

ФГАОУ ВО
«Санкт-Петербургский государственный политехнический университет»

Лаврова Дарья

Концепция Интернета Вещей и его функциональные и технические проявления

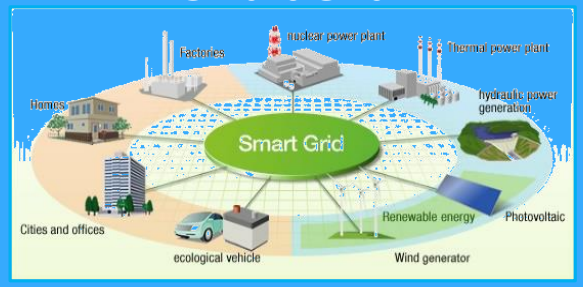
Функциональное проявление

Техническое проявление

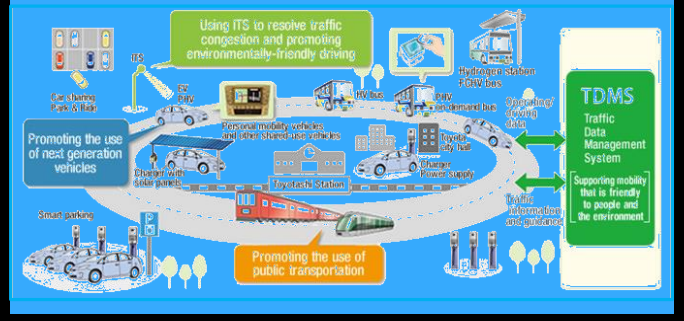
Интернет Вещей

SCADA

Smart Grid



Транспортные системы



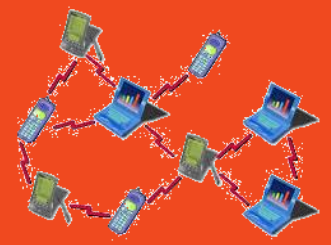
Умный дом

WSN сети

MESH сети

VANET сети

MANET сети



Угрозы безопасности в Интернете Вещей

Сферы применения и особенности Интернета Вещей

Сферы применения:
- Транспорт
- Медицина
- Строительство и промышленность
- Электроэнергия
- «Умные» дома
- Продажи и потребительские услуги

Особенности:
- Многообразие устройств, входящих в состав IoT
- Малая мощность устройств
- Физическая доступность большинства устройств
- Возможность считывания параметров на расстоянии
- Влияние устройств друг на друга

Следствия:
- Сложность обработки разнородных данных
- Наличие у злоумышленника множества точек входа
- Необходимость модификации существующих криптографических алгоритмов
- Сложность ограничения доступа к устройствам
- Возможность нарушения конфиденциальности информации
- Неполнота знаний при мониторинге устройств IoT по отдельности

Угрозы Безопасности в Интернете Вещей

Выход/вывод устройства из строя, вызванный ошибками реализации или атакой, порождающий прекращение работы устройства или нарушение его корректного функционирования

Декабрь 2013 – январь 2014 – первый в мире ботнет с использованием smart-устройств

APT-атаки на устройство или сеть устройств, нацеленные на причинение ущерба конкретному лицу или кругу лиц

Получение несанкционированного удаленного доступа к кардиостимулятору через уязвимый интерфейс и подача смертельного заряда

Кибертерроризм – нарушение функционирования Интернета Вещей, влияющее на физическую безопасность большого числа людей

Угроза получения злоумышленниками контроля над транспортными сетями

Цель и задачи

Цель

Выявление инцидентов безопасности в Интернете Вещей посредством корреляционного анализа подпотоков потока управления и потока данных

Задачи

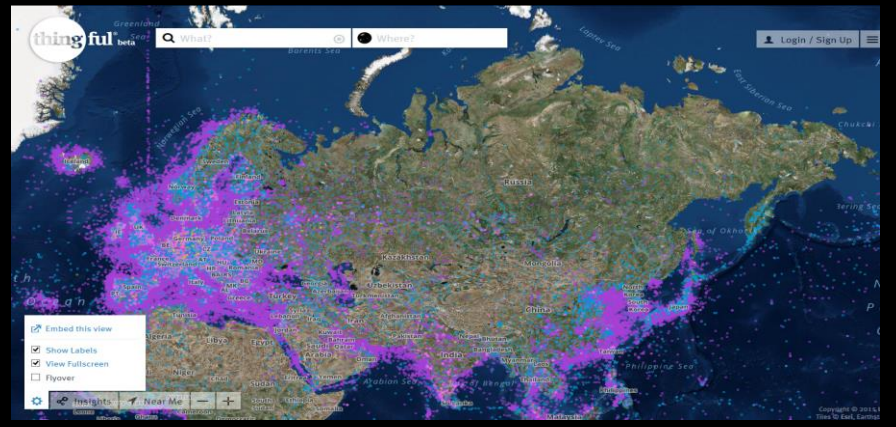
- Сбор и анализ данных от устройств Интернета Вещей
- Обнаружение потенциальных инцидентов безопасности
- Определение точки сбоя при расследовании инцидентов безопасности в Интернете Вещей

Множество данных от устройств Интернета Вещей

Типы данных в Интернете Вещей

- **Численные измеримые данные**
- **Численные неизмеримые данные**
- **Текстовые данные**
- **Данные мультимедиа**

Система ThingFul



Домашняя автоматизация

Численные измеримые:
- Температура в помещении
- Свободная память на домашних серверах
- Количество входящих сообщений на почтовом сервере

Численные неизмеримые:
- Координаты местоположения
- IP-адреса

Текстовые
- Имя владельца
- IP-адреса

Транспорт

Численные измеримые:
- Высота полета
- Скорость движения
- Время полета

Численные неизмеримые:
- Координаты
- Сквок-коды

Текстовые
- Модель самолета
- Название грузоперевозчика

Мультимедиа
- Видео дорожного трафика
- Картинка с флагом страны

Медицина и здоровье

Численные измеримые:
- Концентрация вредных веществ в воздухе (%)
- Пульс
- Сердцебиение

Численные неизмеримые:
- Координаты местоположения
- IP-адреса

Текстовые
- Имя владельца
- Ссылки на профиль владельца в социальной сети Twitter
- Модель устройства

Энергетика

Численные измеримые:
- Температура
- Давление
- Влажность
- Освещенность

Численные неизмеримые:
- Координаты лаборатории
- IP-адреса

Текстовые
- Название лаборатории

Мультимедиа
- Видео движения

Окружающая среда

Численные измеримые:
- Температура
- Давление
- Влажность
- Освещенность
- Возраст животного

Численные неизмеримые:
- Координаты метеостанции или животного
- IP-адреса

Текстовые
- Название лаборатории
- Имя животного

Способы сбора данных и их предобработка с целью сокращения размерности

Способы сбора

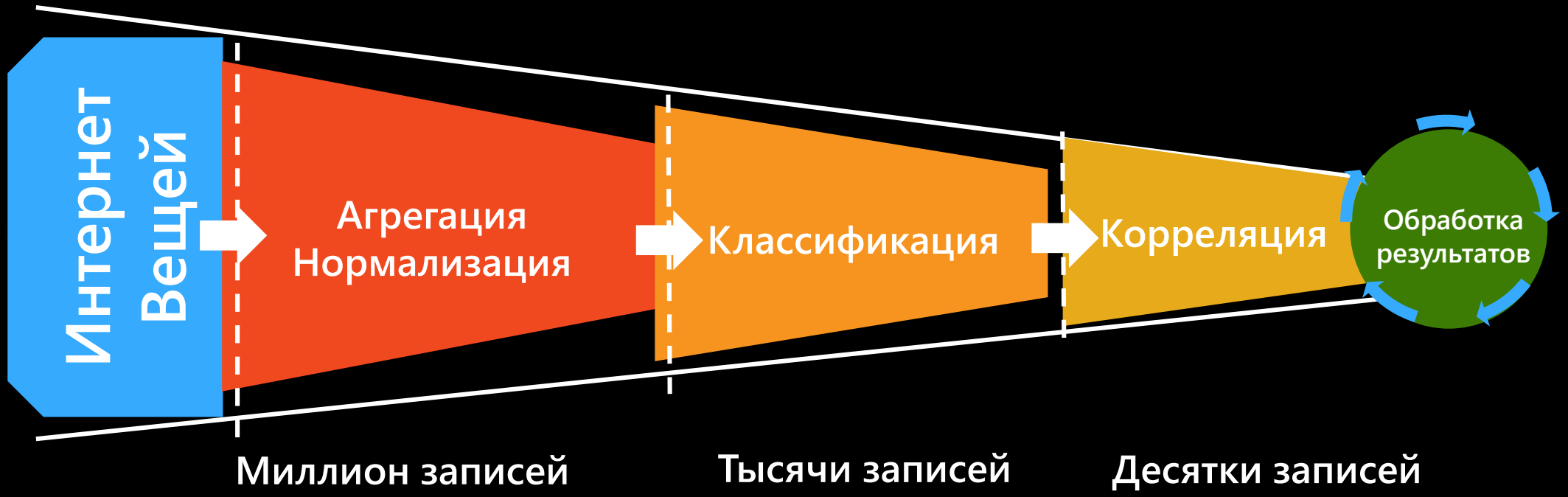
Сбор данных напрямую с конечного устройства

Сбор данных через «посредника»:

Сбор данных со шлюза

Сбор данных с сервера

Предобработка данных



Особенности обеспечения безопасности в Интернете Вещей

Интернет

Интернет Вещей

Обнаружение инцидентов безопасности

Анализ поведения ЧЕЛОВЕКА	В Интернете Вещей НЕТ ЧЕЛОВЕКА! Анализ поведения устройств
Анализ потока управления от ЧЕЛОВЕКА	Анализ потока управления от УСТРОЙСТВ; Анализ данных от УСТРОЙСТВ
Поведение человека сложно предсказать	Каждое устройство функционирует в соответствии со строго заданным алгоритмом

Взаимодействие устройств в Интернете Вещей может быть представлено в виде четкого математического описания

Взаимосвязь потока данных и потока управления в Интернете Вещей

Взаимодействие устройств характеризуется их управляющим воздействием друг на друга

- Поток управления – совокупность управляющих воздействий на устройство
- Анализ потока управления первостепенен: в нем будет отражено воздействие злоумышленника на устройство

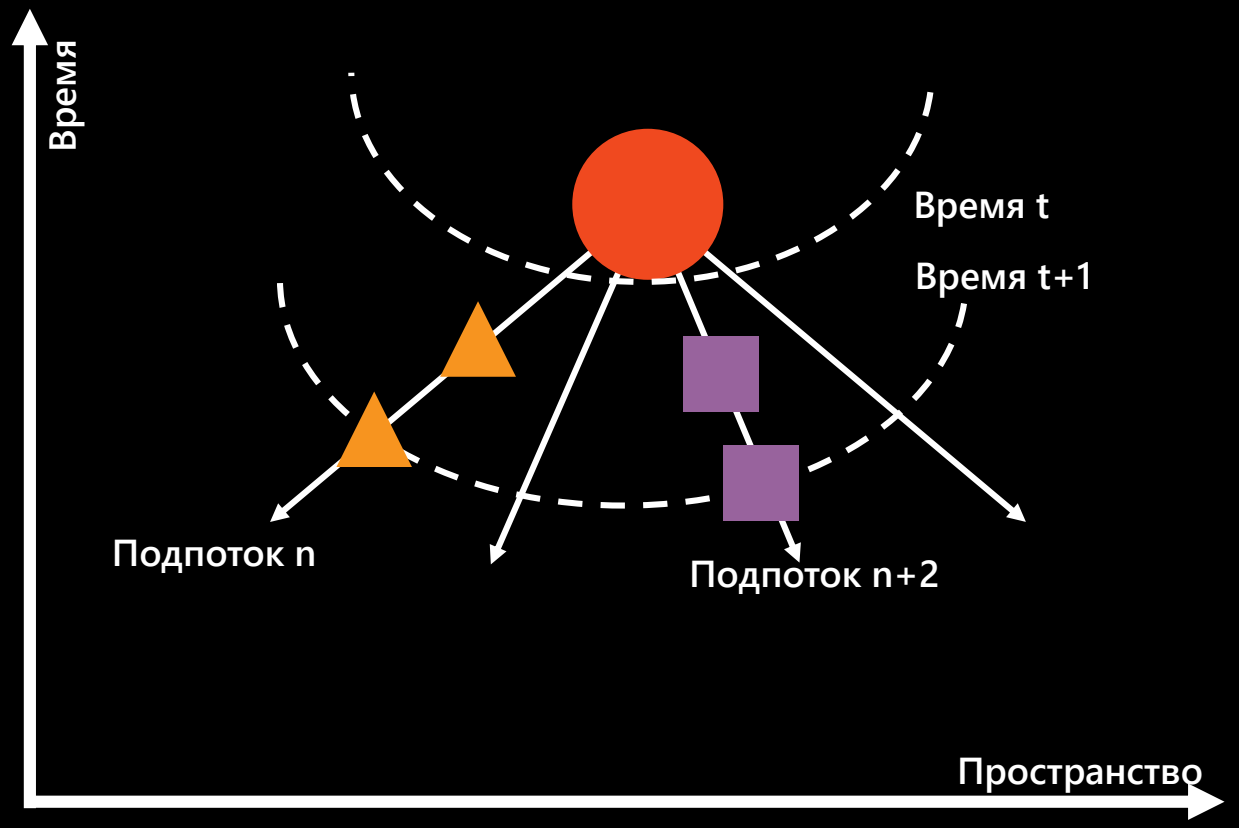
Команды в управляющем потоке и значения показателей в потоке данных могут быть рассмотрены как случайные величины!

1. Корреляционный анализ в рамках управляющего потока для обнаружения инцидента безопасности
2. Корреляционный анализ значений показателей потока данных в точке сбоя

Пространственно-временной корреляционный анализ потоков управления(1)

Пространственное и временное распределение атаки

S – множество сценариев атак на Интернет Вещей, представленных в виде набора управляющих воздействий (команд). Предположим, что имеем набор из m сценариев атаки $S = \{s_1, s_2, \dots, s_m\}$. Управляющие подпотоки главного управляющего потока: O и Q, $O = (o_1, o_2, \dots, o_t)$, $Q = (q_1, q_2, \dots, q_t)$.



Корреляция событий из разных подпотоков без учета времени

Зная априорные вероятности и распределение команд, обусловленных атакой, вычисляем условную вероятность:

$$p(s_j|o_i) = \frac{p(o_i|s_j) \cdot p(s_j)}{p(o_i)}$$

Имея команды из подпотоков O и Q, совместная апостериорная вероятность вычисляется по формуле:

$$p(s_j|o_i, q_k) = \frac{p(o_i, q_k|s_j) \cdot p(s_j)}{p(o_i, q_k)}$$

Пространственно-временной корреляционный анализ потоков управления(2)

Динамический процесс атаки может быть представлен как состояние *X*.
Изменение состояния *X* за период времени t: $x_1, x_2, \dots, x_t$

В каждый момент времени t можно осуществить корреляционный анализ нескольких подпотоков управления с шаблоном атак с учетом времени, если есть апостериорная вероятность $p(s_t|o_{1:t}, q_{1:t})$

В каждый момент времени t для каждого подпотока учитываем время посылки команды и вычисляем $p(s_t|o_{1:t})$ и $p(s_t|q_{1:t})$

Совмещаем подпотоки управления и вычисляем $p(s_t|o_{1:t}, q_{1:t})$

$p(s_t|o_{1:t}, q_{1:t})$ позволяет заменить сразу обе вероятности $p(s_t|o_{1:t})$ и $p(s_t|q_{1:t})$

Если подпотоки управления независимы (исходят от разных устройств Интернета Вещей), можем вычислить $p(s_t|o_{1:t}, q_{1:t})$.

Рассмотренный подход к пространственно-временному корреляционному анализу подпотоков управления в Интернете Вещей позволяет определять степень соответствия последовательности управляющих воздействий шаблонам атак

Определение места сбоя при расследовании инцидентов безопасности

- Поиск взаимосвязей между значениями показателей в потоке данных одного типа (численные измеримые)
- Значения каждого типа в потоке данных в разные временные промежутки рассматриваются как случайная величина
- Совместно случайные величины имеют Нормальное распределение
- Строится ковариационная матрица, позволяющая оценить степень зависимости и направление связи между величинами

N - количество датчиков в сети, каждый датчик обладает M типами измеримых данных. Для каждого типа измеримых данных для одного датчика есть T измеренных значений, собранных в разные моменты времени T: $t_{i,i=1,\dots,T}$

Для одного типа измеримых данных используем матрицу U размером NxT, чтобы выразить измеренные значения, полученные от N датчиков в различное время периода T.

$$U_{N\times T} = (U_1, U_2, \dots, U_T)$$

Для всех типов измеримых данных, имеем M типов данных в один момент времени от N датчиков, которые выражаются через матрицу Q размером NxM

$$Q_{N\times M} = (Q_1, Q_2, \dots, Q_M)$$

$$X_{N\times(M\times T)} = \left(U^{(1)}_{N\times T}, U^{(2)}_{N\times T}, \dots, U^{(M)}_{N\times T}\right) = \left(Q^{(1)}_{N\times M}, Q^{(2)}_{N\times M}, \dots, Q^{(T)}_{N\times M}\right)$$

Определим K как K=M x T Распределение $X_{N\times K}$, где Σ – матрица ковариации, μ – вектор средних значений:

$$p_X(x_1, x_2, \dots, x_K) = \frac{1}{(2\pi)^{K/2}|\Sigma|^{1/2}} \exp\left(\frac{-(x-\mu)^T\Sigma^{-1}(x-\mu)}{2}\right)$$

Результаты и дальнейшее направление работ

Результаты

1. Исследованы и классифицированы данные, которые могут быть получены от устройств Интернета Вещей
2. Предложены подходы к выявлению инцидентов безопасности в Интернете Вещей:
   - Пространственно-временной корреляционный анализ потоков управления
   - Корреляционный анализ потоков данных для исследования выявленных инцидентов безопасности

Направление работ

- Представление взаимодействия устройств в Интернете Вещей как вероятностного конечного автомата
- Построение модели возможных действий нарушителя в Интернете Вещей
- Разработка подхода к корреляционному анализу данных текстового типа и мультимедиа

СПАСИБО ЗА ВНИМАНИЕ!