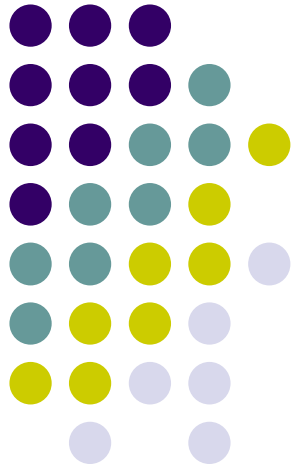
Безопасность протоколов мониторинга индустриальных объектов в концепции Интернета вещей

Беззатеев С.В. (1,2), **Волошина Н.В.** (1,2), **Петряевская И.С.** (3), **Саламатов М.А.** (3)

1 НИУ Информационных технологий, механики и оптики

2 Санкт-Петербургский государственный университет аэрокосмического приборостроения

3 Санкт-Петербургский центр разработок DEL-EMC

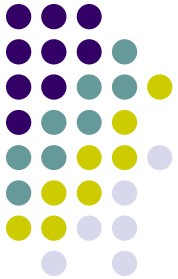


РусКрипто 2017

Постановка задачи

- Построить систему мониторинга параметров окружающий среды для Умных Городов
- Основные свойства:
- Контроль различных параметров (экологический, индустриальный мониторинг)
- Легкость развертывания и масштабирования
- Плотность покрытия территории (контроль текущей обстановки)
- Безопасность

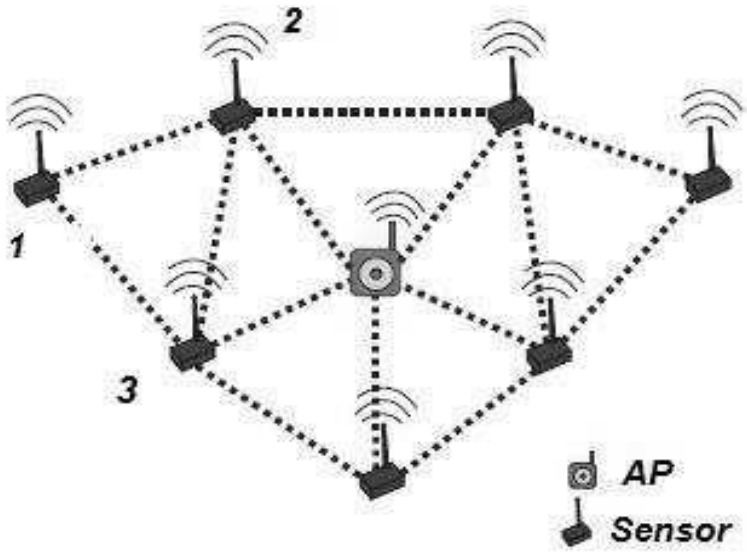
Эко-мониторинг городской среды



- К основным проблемам относят:
  - сложность начальной инициализации сети, состоящей из большого числа устройств,
  - подключения нового датчика к существующей сети,
  - проблемы масштабирования сети,
  - возможность использования доверенного датчика в месте сети отличном от места легальной установки, возможность подключения нелегального устройства (датчика)

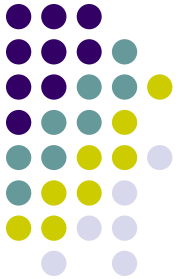
Выбранный подход Самоорганизующаяся сеть

- Wi-Fi сеть
- AP – точка доступа для сбора и ретрансляции данных мониторинга
- Sensor – датчик, осуществляющий сбор данных с сенсоров в отдельной точке сети



- **РусКрипто 2017**

Этапы работы сети



- Инициализация датчика в сети (подключение сенсора к сети):
  - Начальная инициализация сети
  - Добавление нового датчика к сети
- Режим стабильной работы
- Удаление датчика из сети:
  - Удаление из сети с дальнейшим использование только при инициализации новой сети
  - Перенос датчика в другой сегмент сети (переконфигурация)

Мастер ключ для аутентификации в сети

- Мастер ключ хранится в защищенной области памяти датчика (E. Unsal1, M. Milli, Y. Cebi, ”Low cost wireless sensor networks for environment monitoring”, The Online Journal of Science and Technology, v. 6, i.2, 2016, p.61-67)

- Мастер ключ удаляется через некоторое время после инициализации датчика в сети (J. Jang, T. Kwon and J. Song, ”A Time-Based Key Management Protocol for Wireless Sensor Networks”, Proceedings of ISPEC, 2007, LNCS 4464, pp. 314-328)

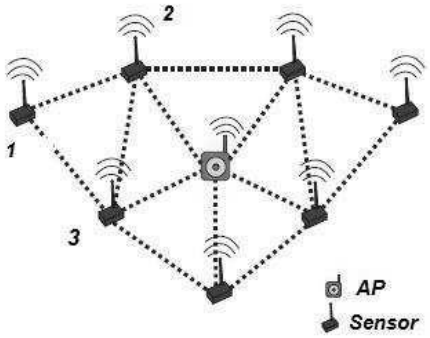
Инициализация сети
Формирование парных ключей

- Мастер ключ MK предустанавливается для новой сенсорной сети.
  Каждый датчик i который должен быть подключен к сети должен иметь свой уникальный идентификационный номер ID_i
  ID_i ($ID_i > ID_j$ для $i > j$).
- Датчики обмениваются Идентификаторами с ближайшими датчиками
- Каждый датчик использует информацию о полученных идентификаторах других датчиков и мастер ключ для вычисления парных ключей для взаимной аутентификации

Например, датчик 1 вычисляет парные ключи для датчиков 2, 3:

$$K_{1,2} = H(ID_1||ID_2||MK),$$

$$K_{1,3} = H(ID_1||ID_3||MK),$$

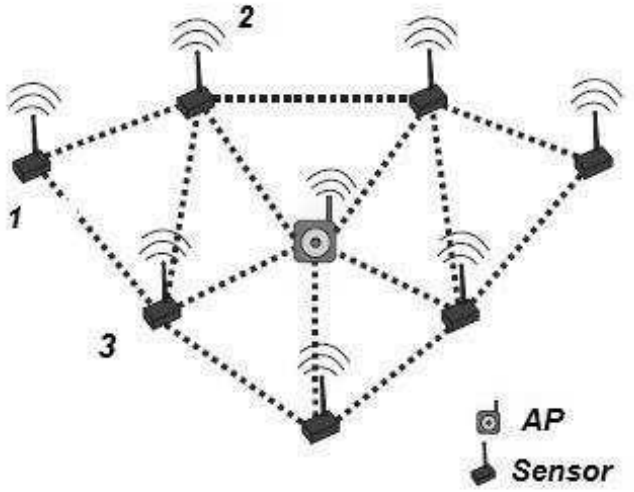


- Также для обеспечения масштабируемости каждый датчик вычисляет вспомогательный ключ
  $K_{i,i} = H(ID_i||MK)$
- После завершения вычисления ключей каждый сенсор уничтожает свой мастер ключ после предустановленного времени **T**kill

- **РусКрипто 2017**

Режим стабильной работы

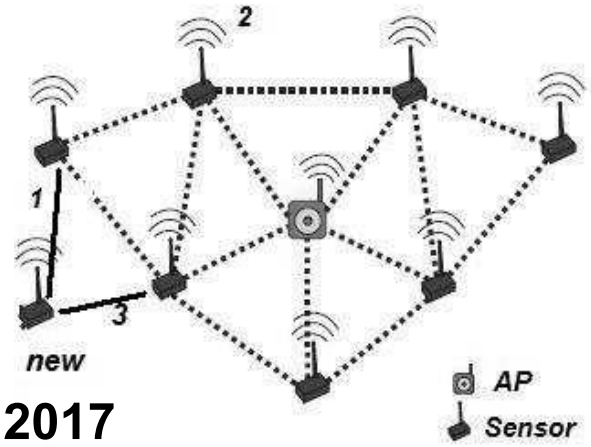
- Датчики используют выработанные парные ключи для взаимной аутентификации.
- Например, датчики 1 и 2 используют парные ключи $K_{1,2}$ и $K_{2,1}$, соответственно.



Добавление нового датчика в сеть

$$K_{new,1} = H(ID_1||MK) = K_{1,1}$$
$$K_{new,3} = H(ID_3||MK) = K_{3,3}$$

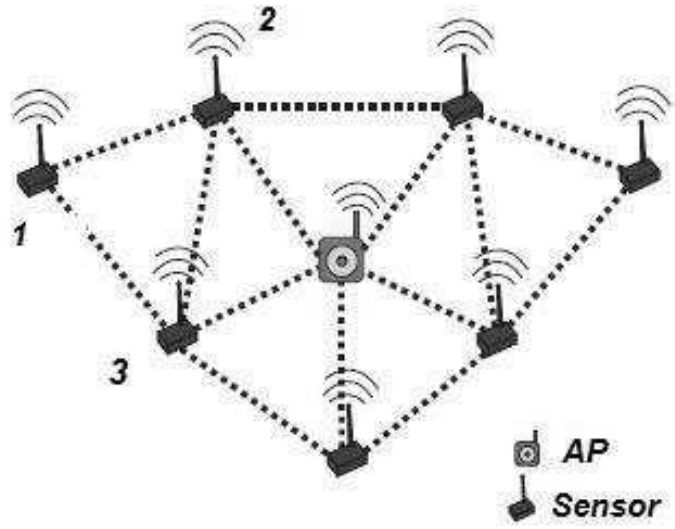
- Перед удалением мастер ключа специальный ключ $K_{new,new}$ должен быть создан для нового датчика.
- В результате новый датчик хранит следующую последовательность ключей $\{K_{new,new}, K_{new,1}, K_{new,3}\}$

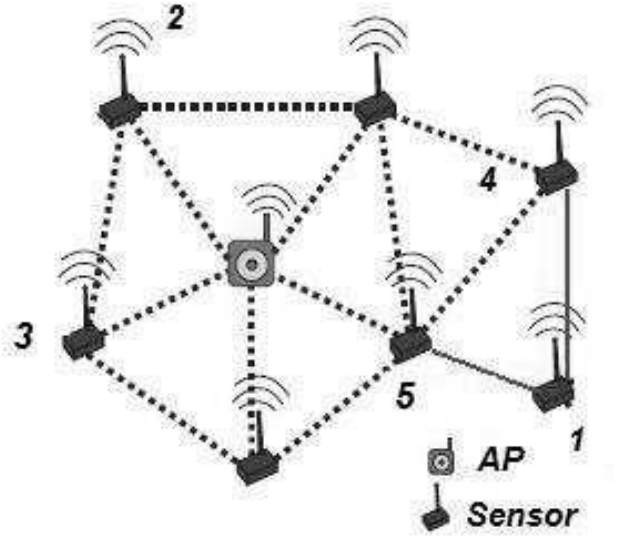


- **РусКрипто 2017**

Нелегальное перемещение датчика

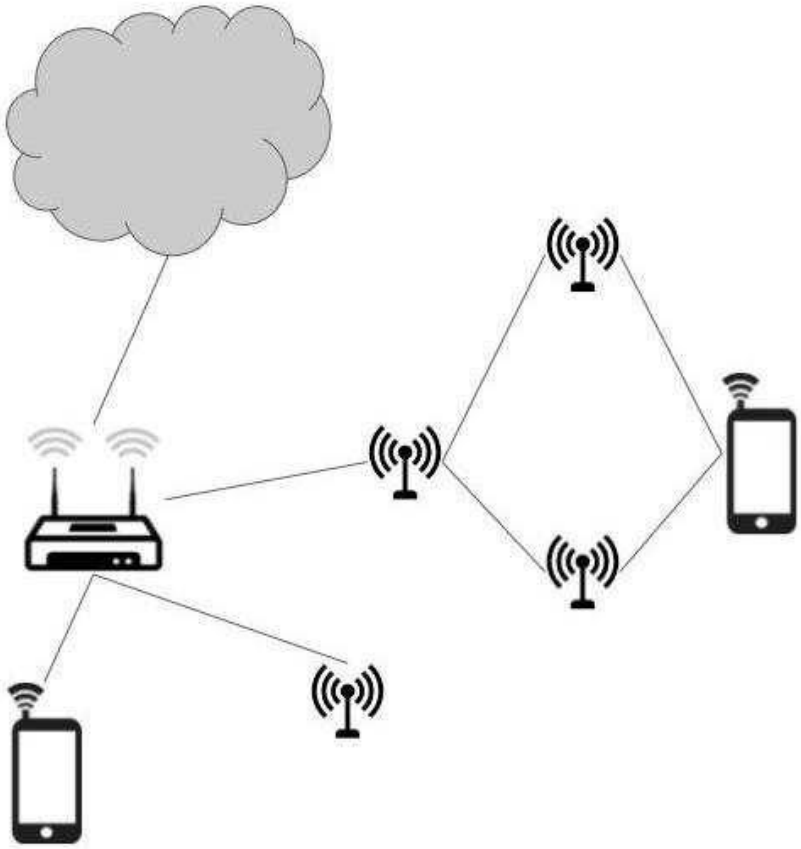
- В случае нелегального перемещения датчика в другой сегмент сети процедура аутентификации завершится ошибкой. Для перемещения нужна перезапись МК на датчике.





- **РусКрипто 2017**

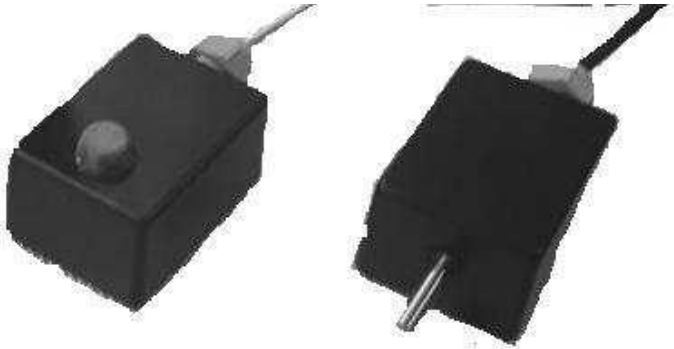
Общая схема системы мониторинга

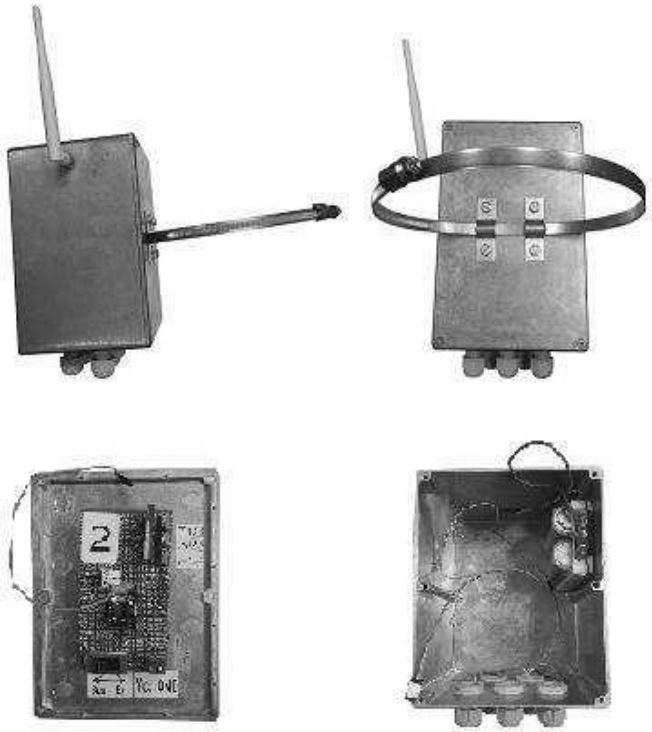


- РусКрипто 2017

Прототип системы эко-мониторинга

- Прототип системы реализован на базе микроконтроллера ESP8266





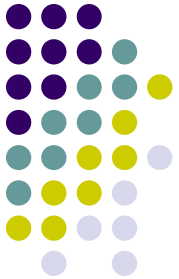
- Датчик (сенсоры CO_2, уровень радиации, уровень шума)

Апробация прототипа

Прототип системы экомониторинга с использованием безопасного протокола был успешно апробирован в г. Санкт-Петербург и Наукограде Кольцово (г. Новосибирск) в рамках программы развития Умных Городов.

- **РусКрипто 2017**

Вопросы?



Спасибо за внимание!

Волошина Наталия
nataliv@ya.ru

- **РусКрипто 2017**