Белорусский государственный университет

Защита информации в беспроводных сенсорных сетях

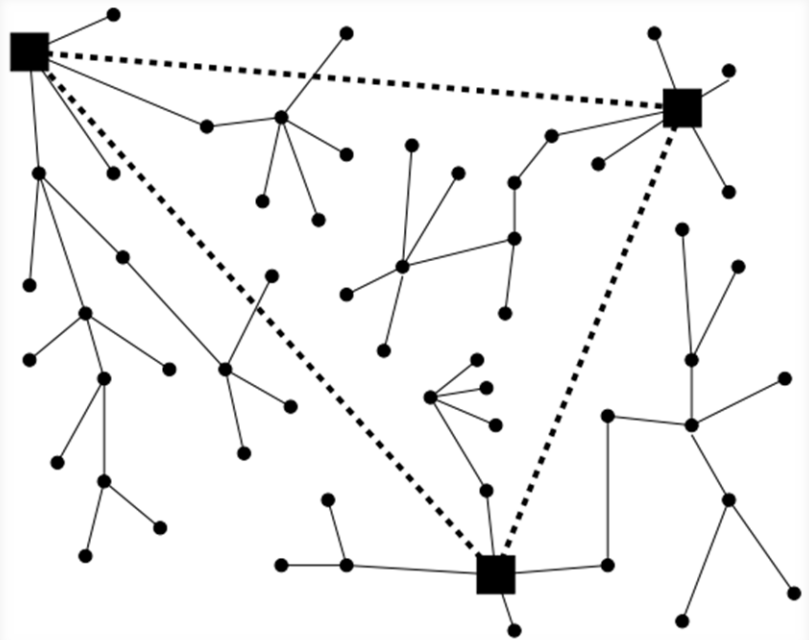
Мулярчик К.С., к.т.н., доцент кафедры телекоммуникаций и информационных технологий

2015

Что такое беспроводная сенсорная сеть?

Ключевые характеристики:

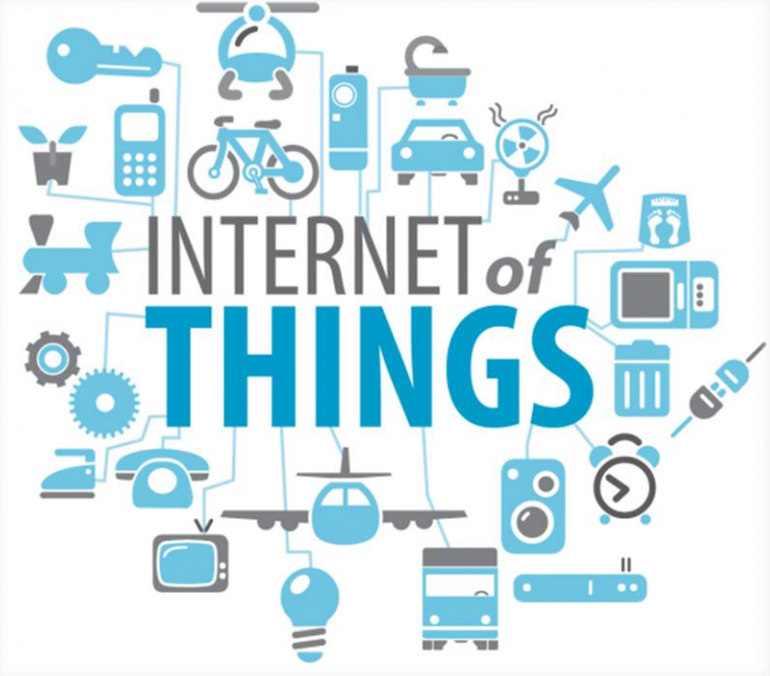
1. Большое количество узлов, распределенных в пространстве
2. Миниатюрные автономные узлы
3. Ограниченная вычислительная возможность узла
4. Одноранговая топология
5. Самоорганизация



Области применения и перспективы

1. Промышленность
2. Инженерия
3. Транспорт
4. Медицина
5. Экология
6. Сельское хозяйство

и т.д.



Стек протоколов в беспроводных сенсорных сетях

Приложений (APP)

Сетевой (NWK)

Канальный (MAC)

Физический (PHY)

Канальный уровень

Основные задачи:

1. Реализация режима функционирования узла
   - регулярный
   - событийный
2. Предоставление доступа к среде
   - произвольный доступ (конкурентные методы)
   - доступ по расписанию (неконкурентные методы)
3. Разрешение коллизий
4. Синхронизация времени

Сетевой уровень

Основные задачи:

1. Маршрутизация трафика
   - обеспечение отказоустойчивости
   - балансировка нагрузки
   - увеличение пропускной способности

Ограничения:

1. Уровень энергии узла и время жизни всей сети
   - “энергетические дыры”
2. Мобильность узлов
3. Предварительная обработка данных
   - необходима «общая картина»
   - необходимы данные от каждого узла

Инструменты (дополнительные сервисы)

1. Кластеризация узлов
2. Локализация узлов
3. Шифрование и аутентификация

и др.

Кластеризация

1. Маршрутизация и балансировка нагрузки:
   - уменьшение потребления энергии (увеличение времени жизни сети),
   - уменьшение задержки, избежание коллизий, устранение «энергетических дыр»

2. Масштабируемость
   узлам необходимо знать только о других узлах в пределах кластера

3. Предварительная обработка данных

4. Устойчивость
   добавление узла, подвижность сенсоров, вывод узла из строя – справиться с этими задачами локально внутри отдельного кластера проще, чем в масштабах всей сети

Кластеризация

1. Характеристики кластеров
   - количество кластеров: фиксированное / переменное
   - размер кластеров: одинаковый / разный
   - внутри- и межкластерная маршрутизация: single-hop / multi-hop
2. Главы кластеров
   - наличие / отсутствие
   - физическое устройство: то же / с расширенными возможностями
   - роль: ретранслятор сообщений, обработчик информации, «базовая станция»
3. Процесс кластеризации
   - хранение сведений о всей сети централизовано / распределено
   - распределение ролей узлов: вероятностное или итерационное (по очереди)
   - выбор главы кластера: предопределённый, адаптивный (определение какой-либо метрики), случайный

Недостатки существующих алгоритмов кластеризации

1. Не учитывается уровень энергии при выборе главы кластера
2. Избыточный расход энергии при выборе/смене главы кластера
3. Большое или непредсказуемое количество итераций при выборе/смене главы кластера
4. Неравномерное распределение кластеров
5. Проблема «энергетических дыр»
6. Избыточные главы кластеров
7. Нет поддержки мобильности узлов и/или глав кластеров
8. **Необходимость наличия полной информации о сети (таблицы маршрутизации)**
9. **Централизованное управление кластерами**
10. Невозможность реактивного функционирования (только периодическая трансляция сообщений)
11. Single-hop протоколы. Ограниченная область действия сети

Области научных исследований

1. Физическая передача данных и доступ к среде
2. Оптимальная маршрутизация сетевого трафика
3. Кластеризация и агрегация трафика
4. Обеспечение качества обслуживания
5. Защита трафика и узлов сети
6. Разработка приемо-передающих устройств – узлов сети

Области научных исследований

1. Физическая передача данных и доступ к среде
2. **Оптимальная маршрутизация сетевого трафика**
3. Кластеризация и агрегация трафика
4. Обеспечение качества обслуживания
5. **Защита трафика и узлов сети**
6. Разработка приемо-передающих устройств – узлов сети

Защита трафика и узлов

Направления исследований:

1. Шифрование трафика, передаваемого между узлами сети
2. Аутентификация узлов сети
3. Аутентификация трафика

Шифрование трафика между узлами сети

Направления исследования:

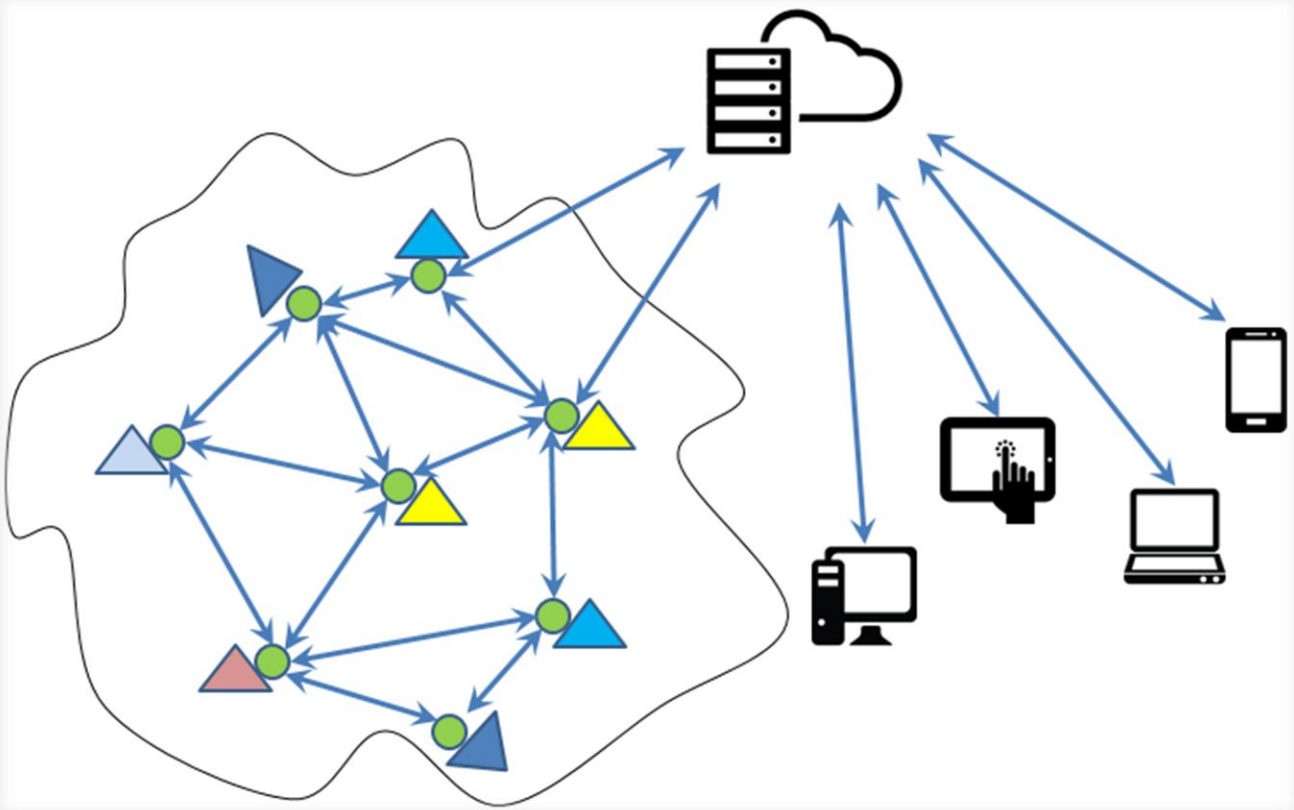
1. Разработка алгоритмов шифрования, ориентированных на использование в узлах с ограниченными вычислительными возможностями
2. Разработка алгоритмов шифрования с переменной длиной блока, а также с учетом энергопотребления узла
3. Разработка алгоритмов обмена и распределения ключами для узлов с ограниченными вычислительными возможностями

Аутентификация узлов и трафика

Направления исследования:

1. Разработка алгоритмов аутентификации узлов сети с учетом их ограниченных вычислительных возможностей
2. Разработка алгоритмов аутентификации трафика (обеспечение целостности данных)

Система сбора и передачи информации



Защита информации в беспроводных сенсорных сетях

Белорусский государственный университет

Мулярчик Константин Сергеевич, к.т.н.,
доцент кафедры телекоммуникаций и информационных технологий
k.mulyarchik@gmail.com
+375 (29) 556-65-78