ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

конференция РусКрипто

НЕОБИТ

# Применение адаптивного управления для противодействия атакам внутренних нарушителей в WSN-сетях

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №19-37-90027\19

Докладчик: Овасапян Т.Д.

# Цель и задачи исследования

Цель исследования: оценка эффективности применения адаптивной системы управления для противодействия атакам внутренних нарушителей в беспроводных сенсорных сетях.

Задачи:

1. Анализ принципов функционирования и особенностей WSN-сетей.
2. Анализ существующих методов обеспечения безопасности WSN-сетей и их недостатков.
3. Разработка адаптивного метода защиты WSN-сети от актуальных атак.
4. Экспериментальная оценка эффективности разработанного метода.

# Актуальность исследования

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Области применения WSN-сетей


Военные действия


Контроль экологических параметров


Метеорология


Сельское хозяйство


Мониторинг и прогнозирование чрезвычайных ситуаций

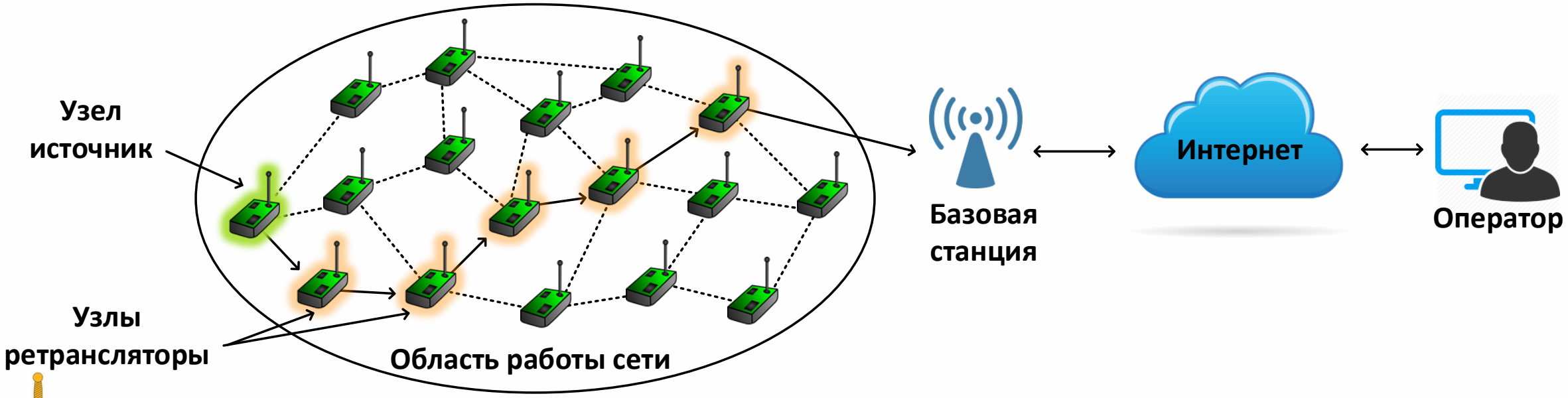

Контроль производственных процессов

# Технология WSN

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

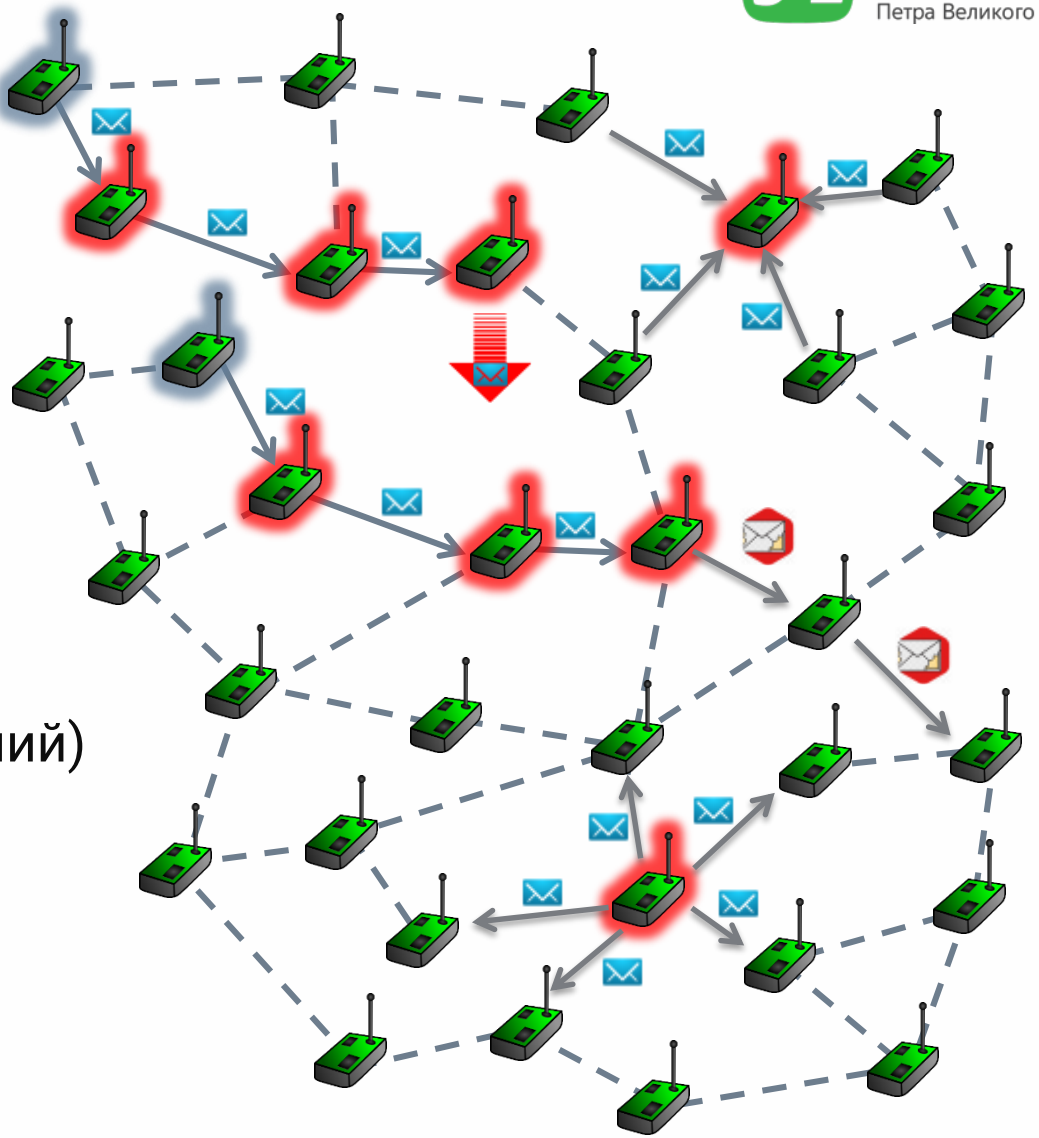
**Особенности:**

- Появление новых узлов
- Работа в общедоступных местах
- Потеря данных
- Отсутствие технического обслуживания
- Влияние на безопасность общества
- Ограниченность узлов в ресурсах



# Атаки на WSN-сети

1. Вывод узлов из строя
2. Эгоистичность
3. Выброс пакетов
4. Пассивная атака
5. Отправка по выделенному каналу (червоточина)
6. Фальсификация (отправка ложных сообщений)
7. Зашумление беспроводной среды
8. Модификация пакетов
9. Атака сбора пакетов (sink hole attack)



# Существующие методы обеспечения безопасности

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

| | |
|---|---|
| **Защищенное управление группой** | |
| Возможность анализа всех передаваемых сообщений в кластере | Проблема с мобильными узлами<br>Компрометация главного узла в кластере |
| **Безопасное агрегирование данных** | |
| Экономия трафика | Повышенное требование к ресурсам |
| **Использование криптографических методов** | |
| Защита от внедрения вредоносных узлов | Сложность поддержки<br>Дороговизна |
| **Системы обнаружения вторжений** | |
| Мгновенное реагирование на атаки | Требования к архитектуре сети |
| **Распределенный контроль поведения** | |
| Возможность защиты от актуальных атак | Зависимость от протоколов |

# Существующие исследования

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

Е.С. Абрамов, Е.С. Басан РАЗРАБОТКА МОДЕЛИ ЗАЩИЩЕННОЙ КЛАСТЕРНОЙ БЕСПРОВОДНОЙ СЕНСОРНОЙ СЕТИ

Особенности:

- Иерархическая топология сети
- Модель доверия используется для определение главного узла в кластере

H. C. Leligou, P. Trakadas, S. Maniatis, P. Karkazis and T. Zahariadis, "Combining trust with location information for routing in wireless sensor networks“

Особенности:

- Использование протокола маршрутизации основанного на информации о местоположении узлов

# Защита на основе показателей поведения

- Каждый узел высчитывает показатель доверия $DT^{i,j}$ к соседнему узлу используя показатели поведения
- Узел считается вредоносным если показатель $DT$ меньше порогового значения

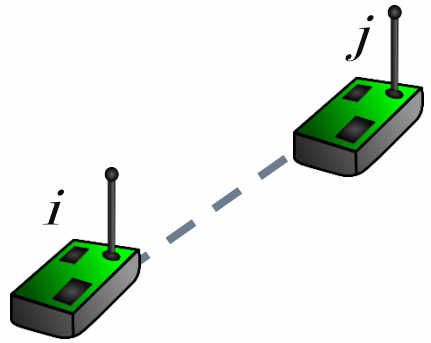



Таблица с показателями поведения

| № | Название метрики | Значение | Вес показателя |
|---|---|---|---|
| 1 | Факт ретрансляции узлом *j* пакета | $T_1^{i,j}$ | $W_1$ |
| 2 | Целостность пакета | $T_2^{i,j}$ | $W_2$ |
| 3 | Интенсивность генерирования данных | $T_3^{i,j}$ | $W_3$ |
| … | | | |

$$T_m^{i,j} = \frac{S_m^{i,j}}{S_m^{i,j} + F_m^{i,j}}$$

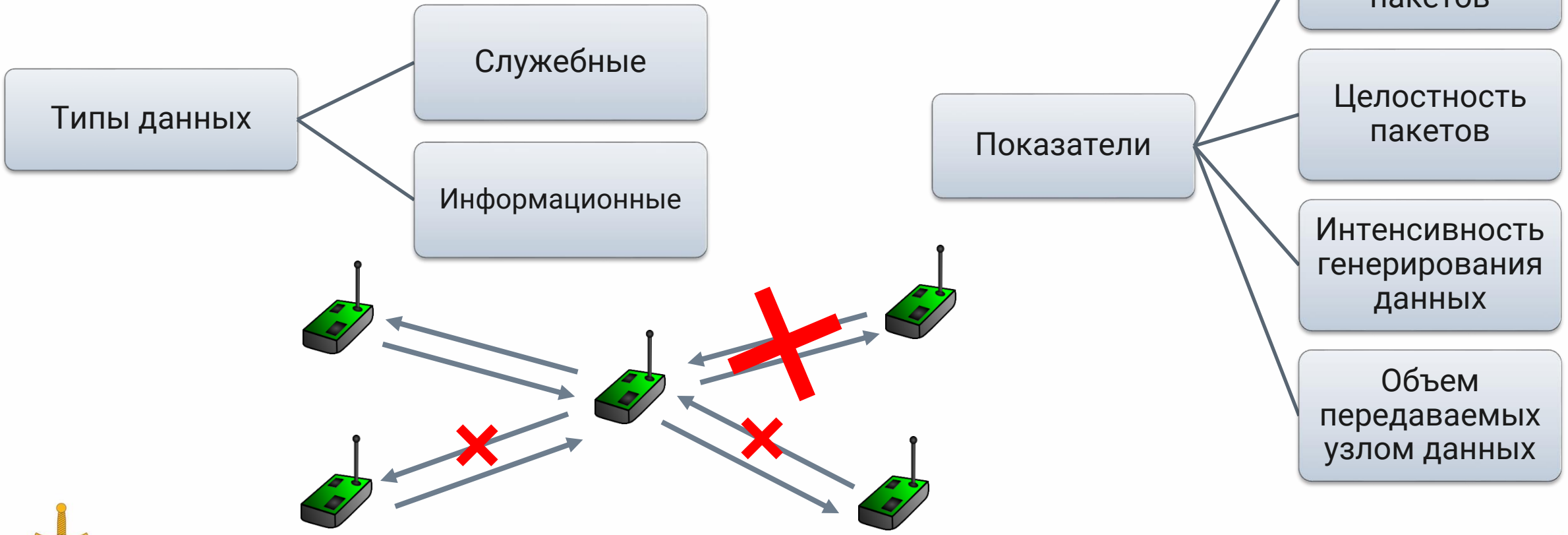
$S_m^{i,j}$ – число удачных событий между узлами *i* и *j*

$F_m^{i,j}$ – число неудачных событий

**Недостаток в контексте использования WSN – полное исключение узла с низким показателем доверия**

# Адаптивное поведение

Изменение принципов взаимодействия с соседним узлом в зависимости от его показателей поведения



# Набор правил

Если объем данных, который необходимо отправить узлу средний (*M*), показатель целостности высокий (*H*) и показатель ретрансляции средний (*M*), то отправить данному узлу пакет;

Показатель *I* – Целостность
Показатель *R* – Ретрансляция

*L* – Низкий
*M* – Средний
*H* – Высокий

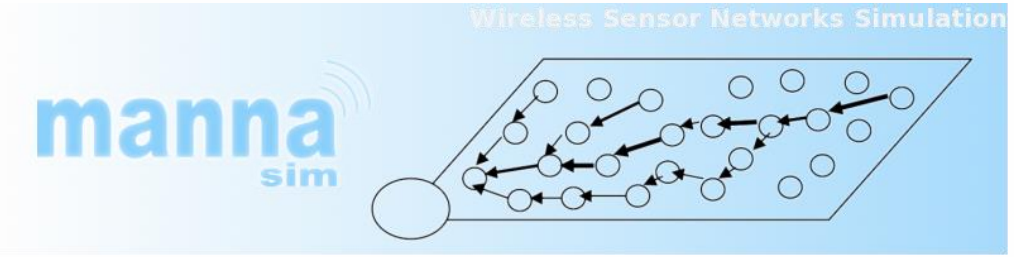
| Объем передаваемых узлом данных – Low | | | |
|---|---|---|---|
| Показатель I<br>Показатель R | L | M | H |
| L | NP | NP | P |
| M | NP | P | P |
| H | P | P | P |
| **Объем передаваемых узлом данных – Medium** | | | |
| Показатель I<br>Показатель R | L | M | H |
| L | NP | NP | NP |
| M | NP | P | P |
| H | NP | P | P |
| **Объем передаваемых узлом данных – High** | | | |
| Показатель I<br>Показатель R | L | M | H |
| L | NP | NP | NP |
| M | NP | NP | P |
| H | NP | P | P |

# Сравнительный анализ систем симуляции

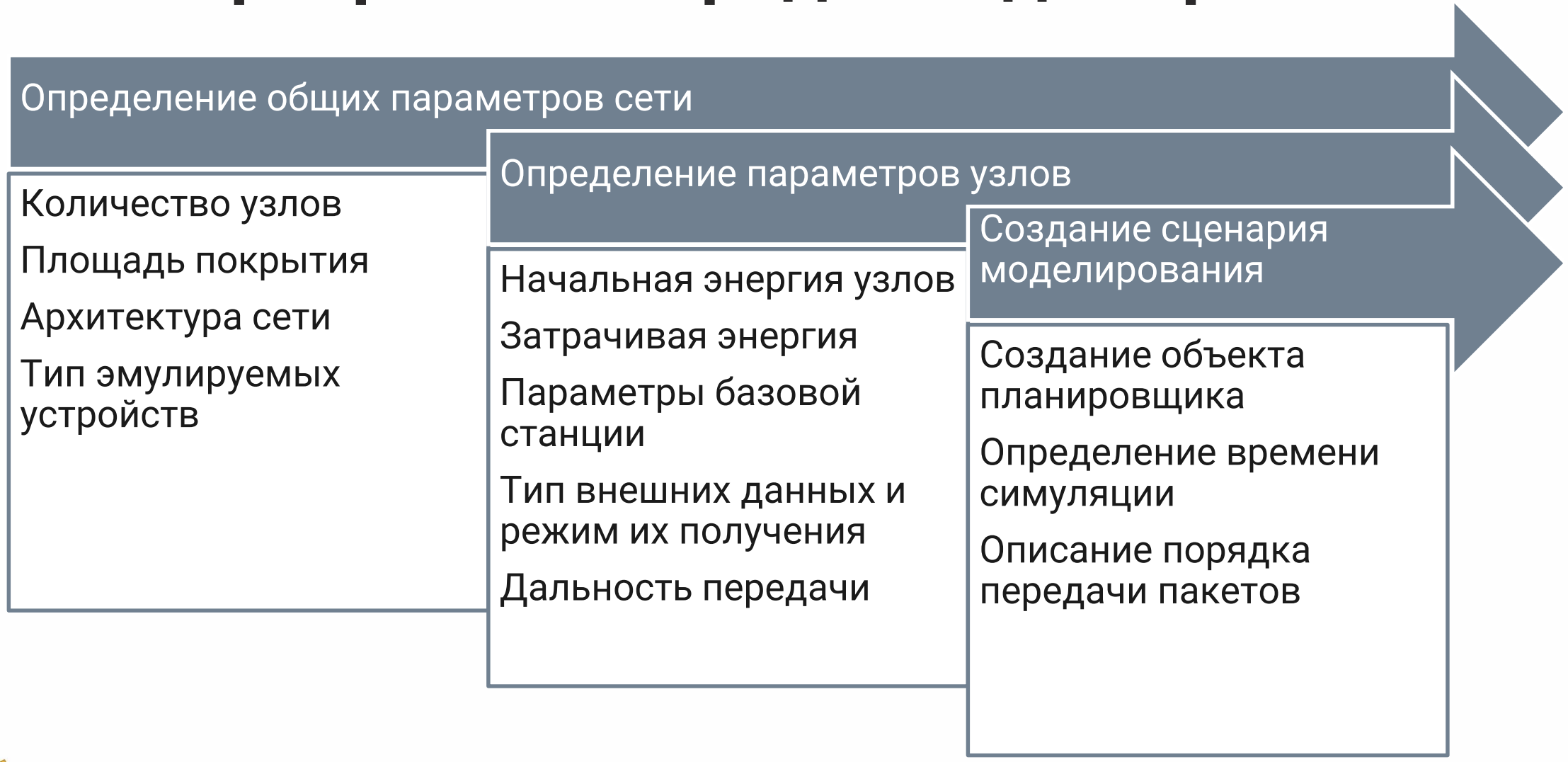
| Фреймворк | Платформа | Гибкость | Поддержка | Примечание |
|---|---|---|---|---|
| **SensorSim** | NS-2 | +/- | - | Разработка прекращена |
| **Avrora** | standalone | + | + | Предназначен для исследования поведения одного узла, а не сети в целом |
| **TRMSim** | standalone | +/- | - | Реализована на Java. Сложность в добавлении собственных модулей |
| **NetTopo** | standalone | - | + | Основная задача – визуализация сети |
| **MannaSim** | NS-2 | +/- | + | Моделирование процесса передачи данных ограничено возможностями NS-2 |
| **Castalia** | OMNeT++ | - | + | Предназначен для моделирования распространения радиосигнала. Отсутствие контроля затрат энергии. |
| **TinyOS** | standalone | - | + | Для полноценного использования необходимо наличие физического устройства |

# Экспериментальная система на основе MannaSim

| | |
|---|---|
| Является надстройкой над NS-2 | Имеет открытый исходный код |
| | Состав:  The Framework и Script Generator Tool (SGT) |
| Расширение класса мобильных узлов в NS-2 | Дополнительные режимы работы: "спящий режим" и "пробуждение". Управление компонентами устройств: датчики и процессор. |
| Отдельный подкласс энергетической модели | Учет потребления энергии при восприятии и обработке данных |
| Поддержка архитектур | Иерархическая, с наличием точек доступа, полностью распределенная |
| Протоколы маршрутизации | DSR, TORA, LEACH, Directed Diffusion, DSDV, AODV |



# Этапы разработки среды моделирования



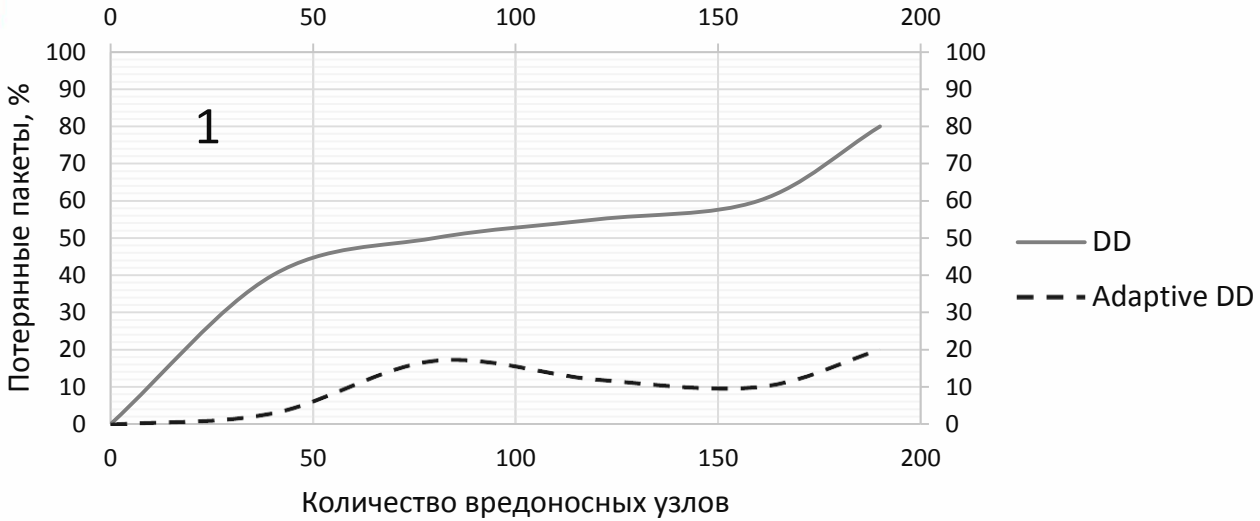
# Характеристики смоделированной сети

| Характеристики сети | |
|---|---|
| Количество узлов | 700 |
| Тип узлов | MicaZ |
| Стандарт связи | IEEE 802.11 |
| Протокол маршрутизации | Directed Diffusion |
| Тип восприятия данных | По расписанию (5 сек) |
| Площадь | 500 x 500 метров |
| Время симуляции | 600 секунд |
| Тип данных | Температура |
| Атаки | черная/серая дыра, истощение энергии |
| Начальная энергия | 10 Джоулей |

| Характеристики узлов | |
|---|---|
| Микропроцессор | ATmega128L |
| Частота | 7.3728 Мгц |
| Флэш-память | 128 Кб |
| RAM | 4 Кб |
| Радио | ChipCon CC2420 |
| Питание | 2 батареи AA |
| Размеры, мм | 225x125x25 |

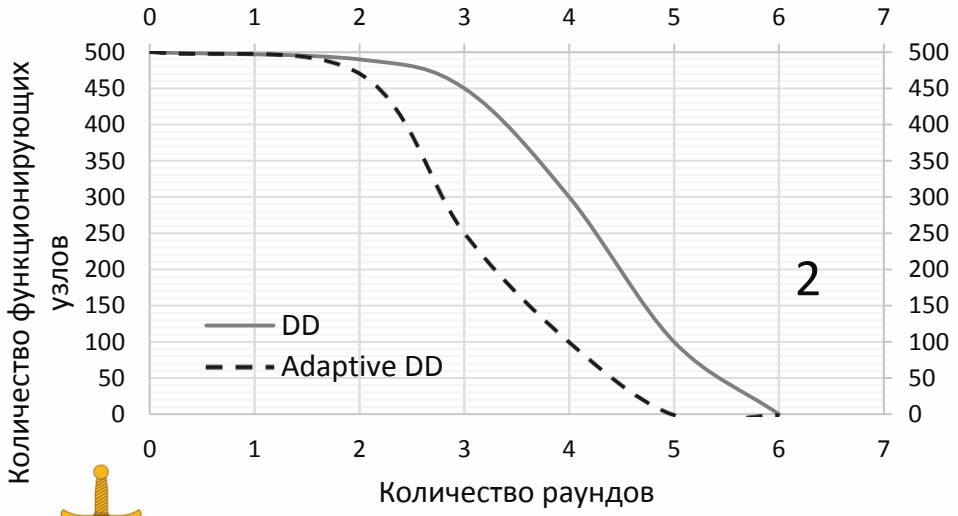
MicaZ

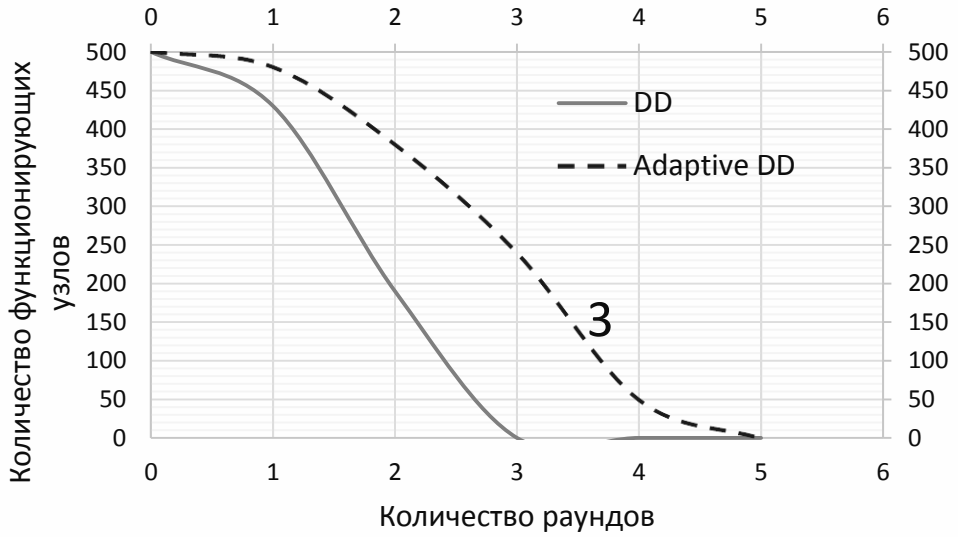
# Экспериментальная оценка




1 – Зависимость потерянных пакетов от количества атакующих узлов

2, 3 – Зависимость количества функционирующих узлов от времени



# Результаты исследования

1. Проанализированы принципы функционирования и особенности WSN-сетей.
2. Выявлены актуальные атаки на WSN-сети.
3. Проанализированы существующие методы обеспечения безопасности WSN-сетей и их недостатки.
4. Предложен метод защиты, основанный на адаптивном поведении узлов, в зависимости от показателя доверия.
5. Разработана среда моделирования на основе симулятора NS-2 и фреймворка MannaSim
6. Проведена экспериментальная оценка эффективности разработанного метода.