MESH NETWORK: ЗАЩИЩЕННАЯ СЕТЬ ИЛИ "ДЫРА" В БЕЗОПАСНОСТИ?

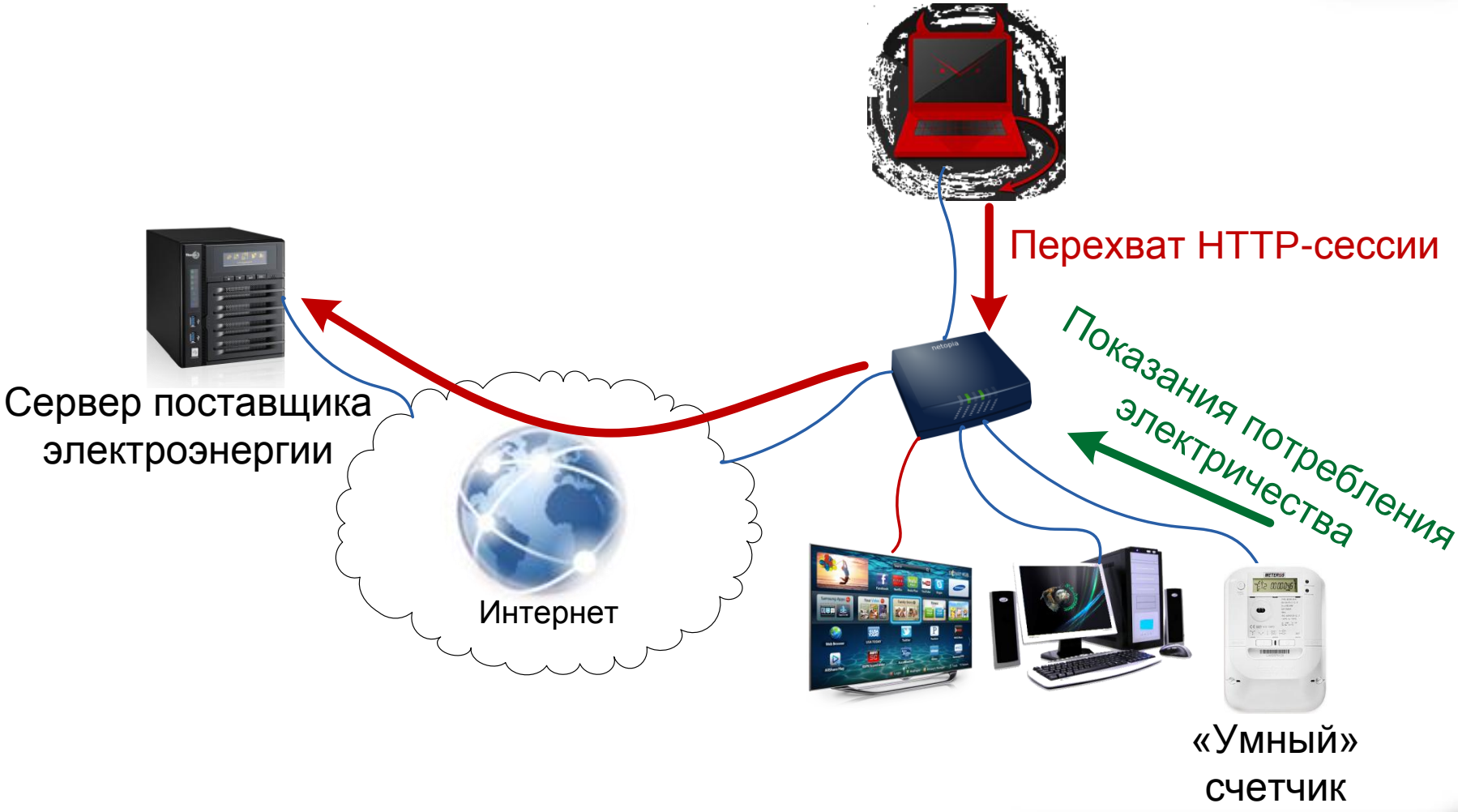
Москвин Д.А.

Современные сетевые устройства

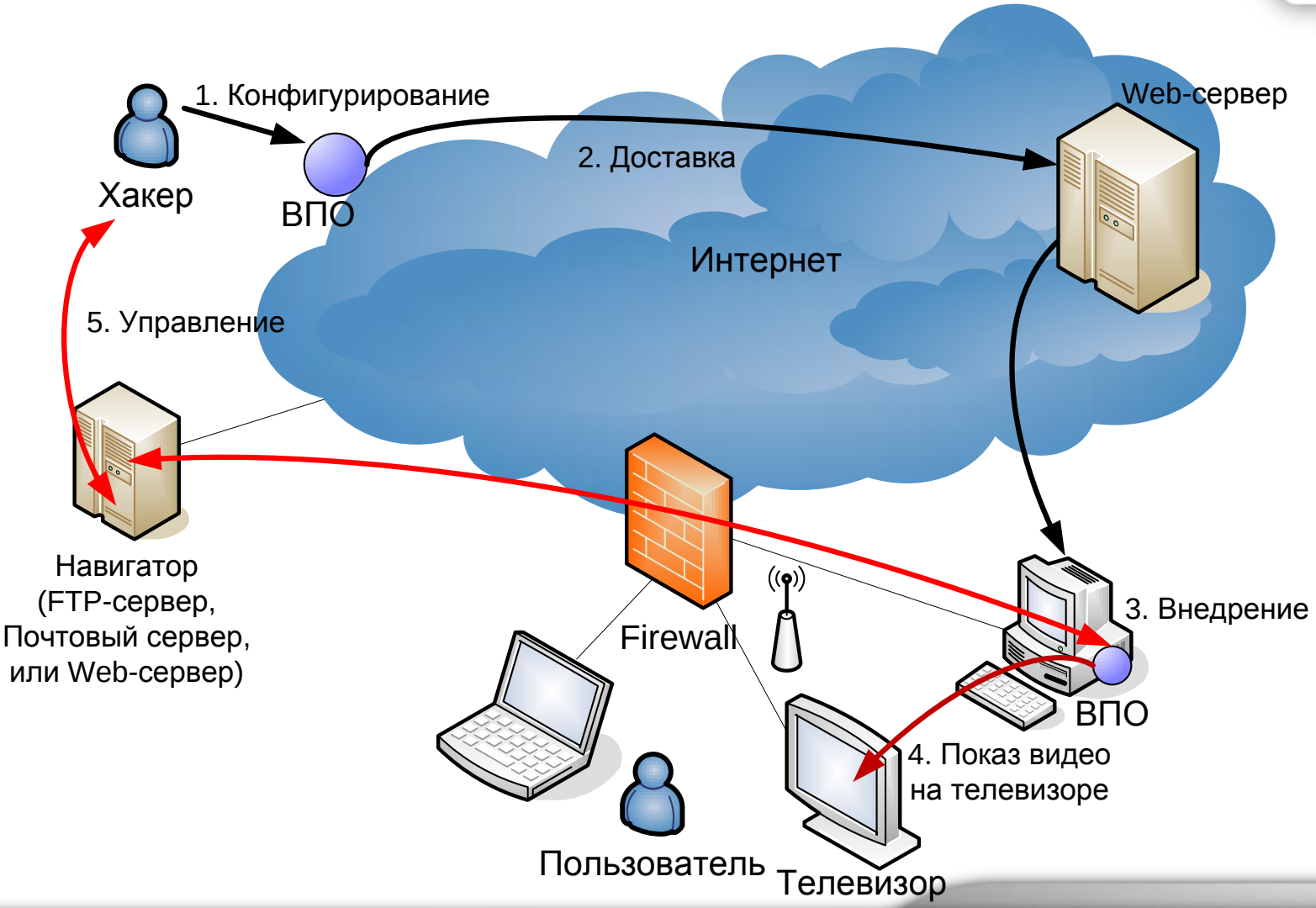
Первые инциденты

2007 год – Crazy Toaster

Схема атаки на «умный» счетчик



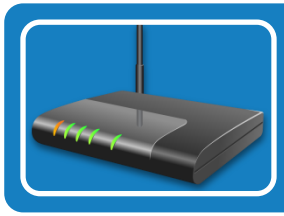
Сценарий атаки на телевизор



Mesh-сети

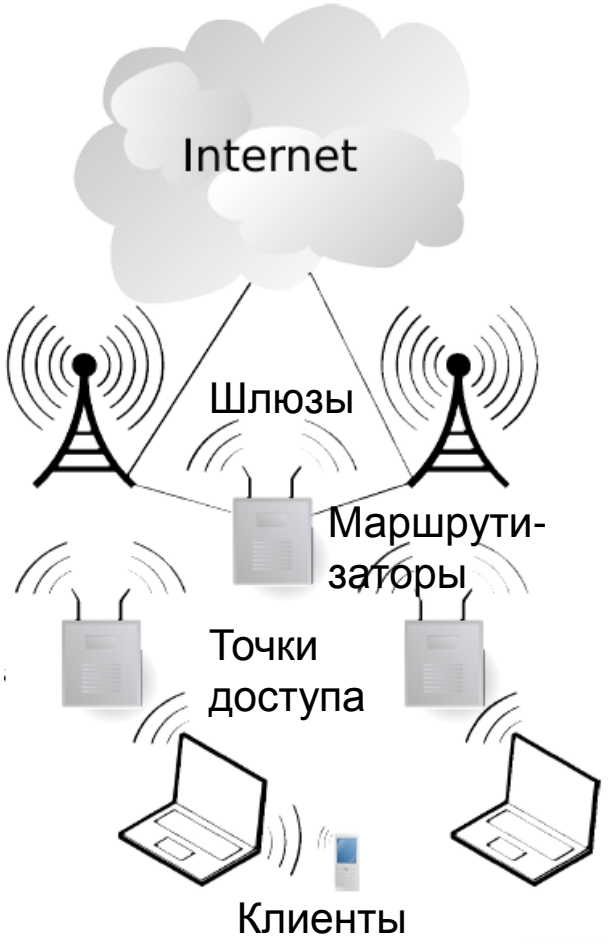
Сети ячеистой структуры

Состоят из стационарных роутеров, клиентов и шлюзов



Роутеры образуют беспроводную магистраль

Для подключения к Интернету используются шлюзы



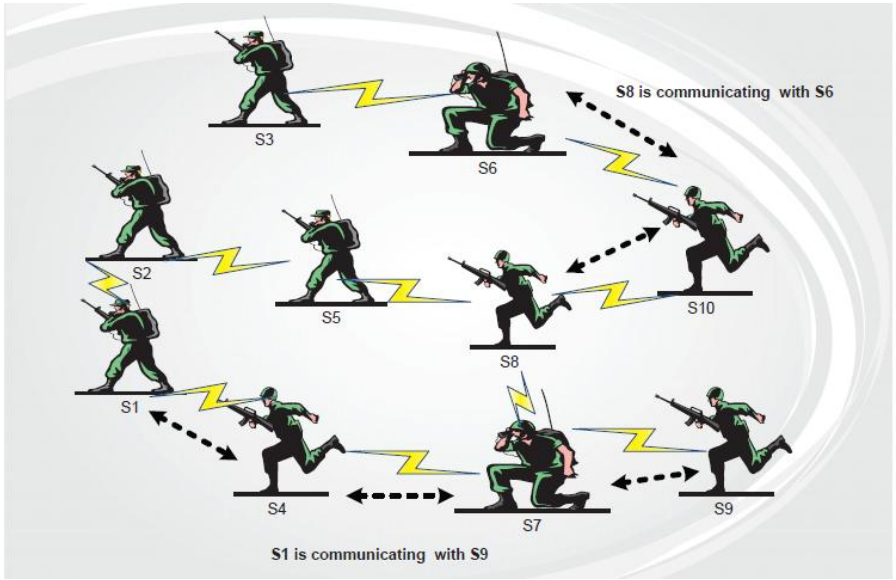
Терминология

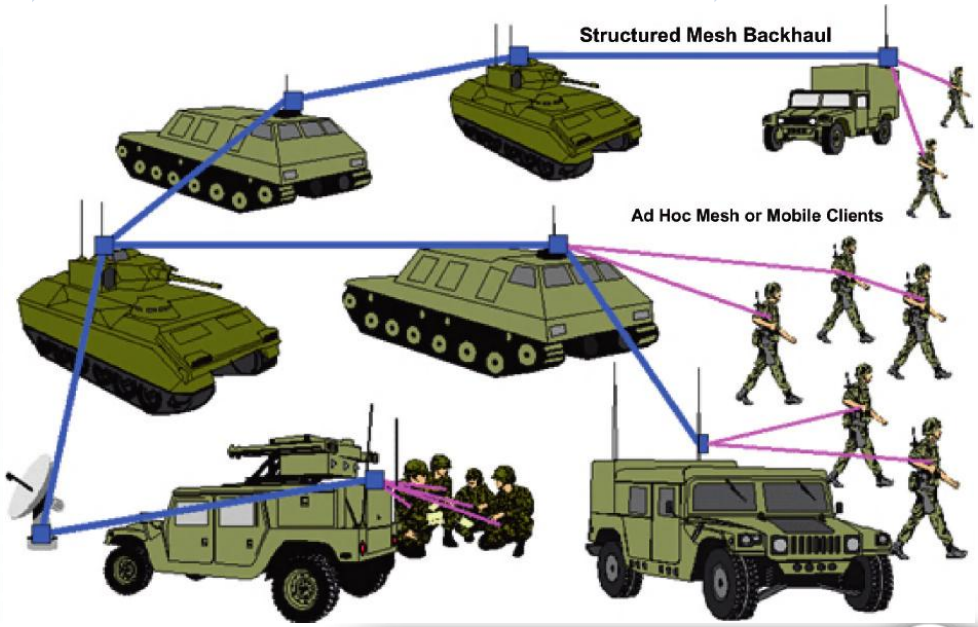
История развития самоорганизующихся сетей

1973 PRnet

1990 GloMo

2000е «Тактический интернет», M@TIS





Основные преимущества самоорганизующихся сетей

Быстрое развёртывание

Масштабируемость

Отказоустойчивость и самовосстанавливаемость

Применение самоорганизующихся сетей

Домашние и офисные сети

- охранные и противопожарные датчики и сигнализации
- «умные» дома

Управление дорожным движением

- контроль и управление безопасностью дорожного движения
- взаимодействие участников дорожного движения (автомобилей, светофоров, знаков, пешеходов)
- координация общественного транспорта

Военные сети и сети служб оперативного реагирования

- связь при спецоперациях и чрезвычайных ситуациях
- управление и координация беспилотных наземных и летательных аппаратов
- самовосстанавливающиеся минные поля

Мониторинг окружающей среды

- мониторинг климата и экологии: температуры, влажности, давления, загрязнённости воздуха
- приборы учета газа, воды, электроэнергии
- контроль целостности и безопасности водо- и газопроводов, природной активности, состояния несущих конструкций зданий и сооружений

Интернет без провайдеров

- общественные городские сети
- Интернет и локальные сети в отдаленных и труднодоступных областях

Используемая среда

Wi-Fi

ZigBee

Z-Wave

Bluetooth

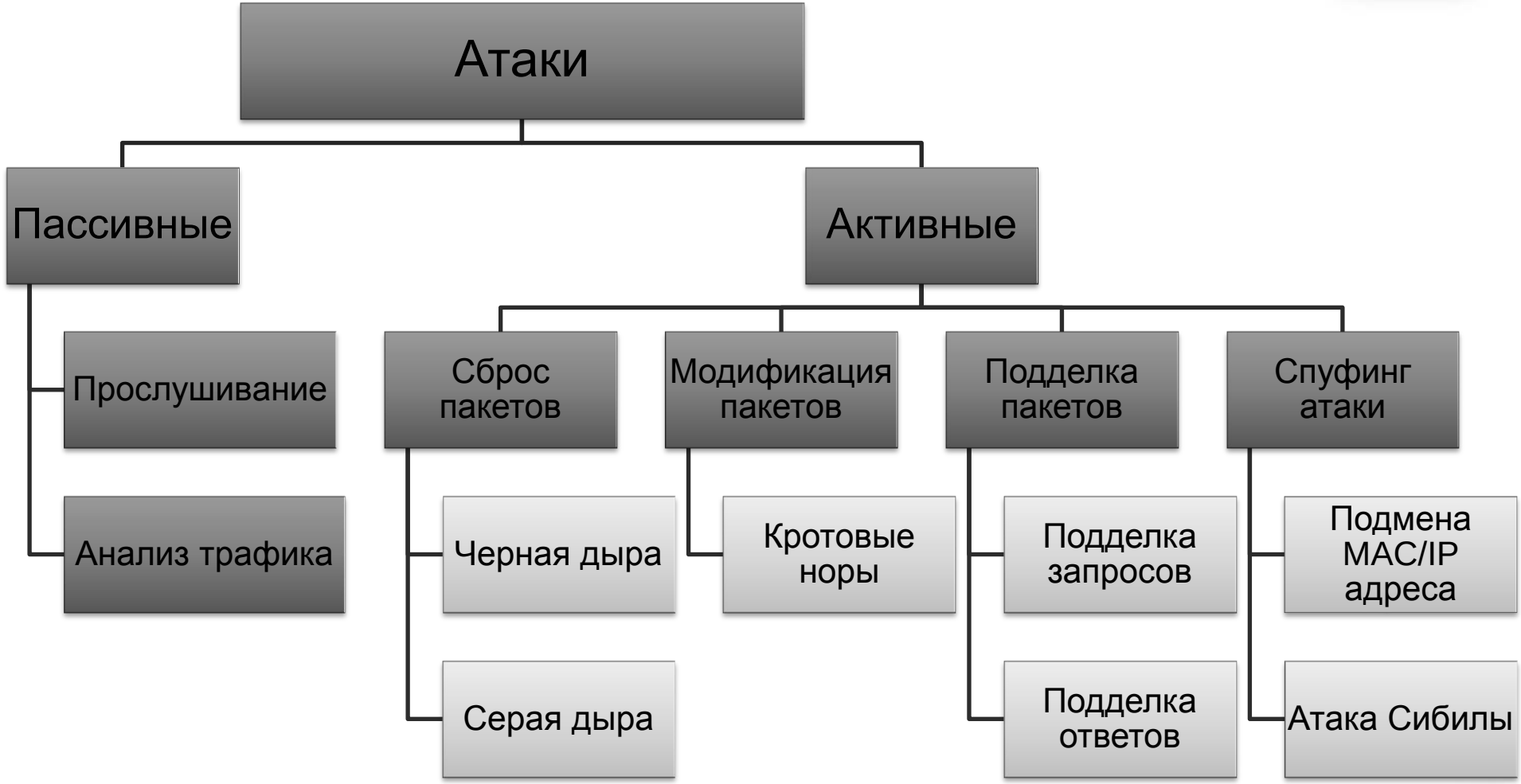
Internet

Существующие реализации

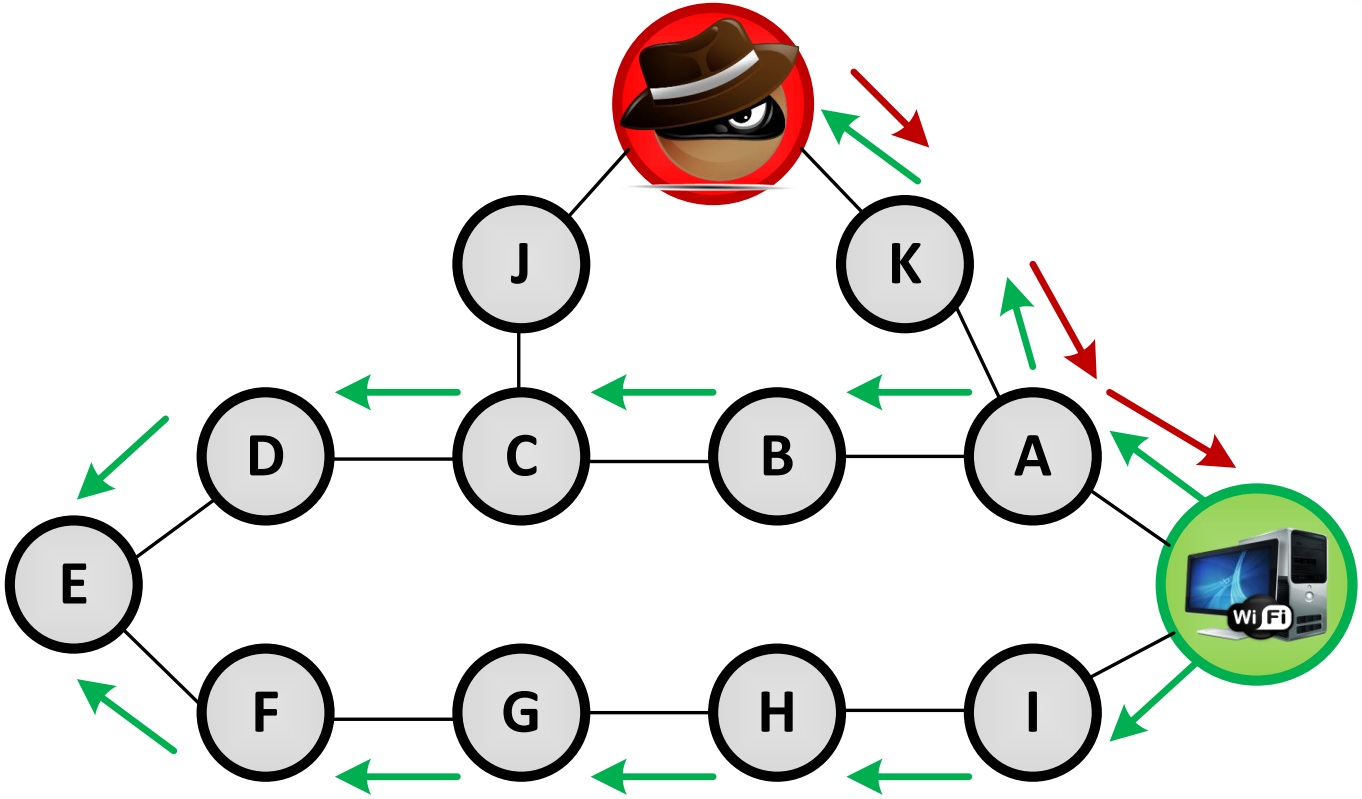
- Hyperboria
- Motorola Mesh
- M@TIS (США)
- Guifi (Испания)
- Athens Wireless Metropolitan Network
- Wasabinet (США)
- One node per child (Аффрика)

Протоколы маршрутизации Mesh-сетей

Классификация атак на протоколы маршрутизации



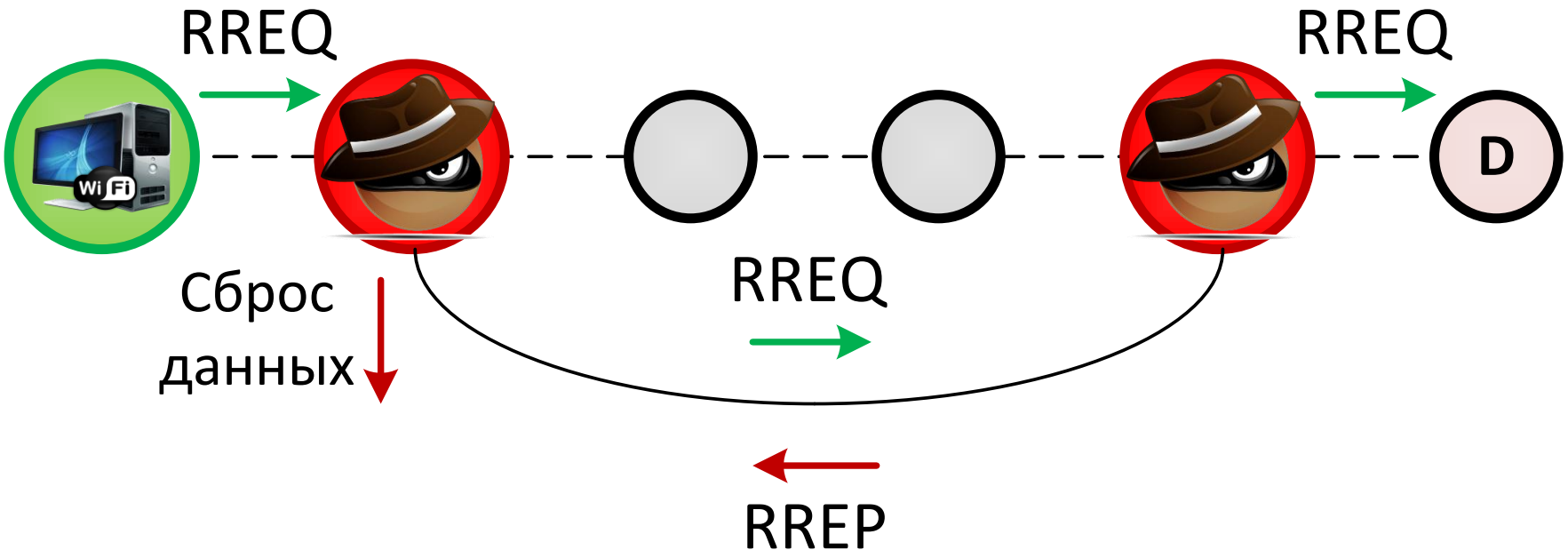
Атака «Черная дыра»



- Запрос (RREQ)

- Поддельный ответ (RREP)

Атака «Кротовая нора»



Известные инциденты

BlackHat 2013 - уязвимость в криптографической защите протокола Z-Wave

- Z-Wave используется в более чем 80% «умных» домов. С помощью обычного радиопередатчика можно перехватить пакеты внутри сети и передать свои.

Ноябрь 2013г. - компанией Symantec обнаружен червь Linux.Darlloz

- Червь работает на ARM, MIPS, PowerPC, заражает роутеры, ТВ-ресиверы, принтеры. Заражено ≈32000 устройств, 38% –техника «умного дома». Назначение - майнинг Mincoins и Dogecoins

Декабрь 2013г. - компанией Proofpoint обнаружена ботнет-сеть

- Ботнет-сеть, состоящая как из обычных компьютеров, так и из техники «умного дома» (роутеры, телевизоры, мультимедийные центры и холодильники). С 23.12.13 по 6.01.14 разослано 750000 спам-писем.

Методы защиты

использование наиболее защищенных протоколов маршрутизации (выбор зависит от назначения mesh-сети)

включение в состав mesh-сети специальных операторов, координирующих работу сети и деятельность узлов

использование специального ПО для обнаружения специфичных для mesh-сетей DoS-атак;

анализ паттернов — введение правил, разрешающих или запрещающих связи между определенными узалами mesh-сети и задающих уровни защиты этих связей

Выводы

В будущем за Mesh-сетями – 15% рынка доступа в Интернет, все сенсорные сети и «умные» дома, управление дорожным движением

«Неустойчивая» терминология

Защищенность от внешнего нарушителя, незащищенность от внутреннего


НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
НЕОБИТ