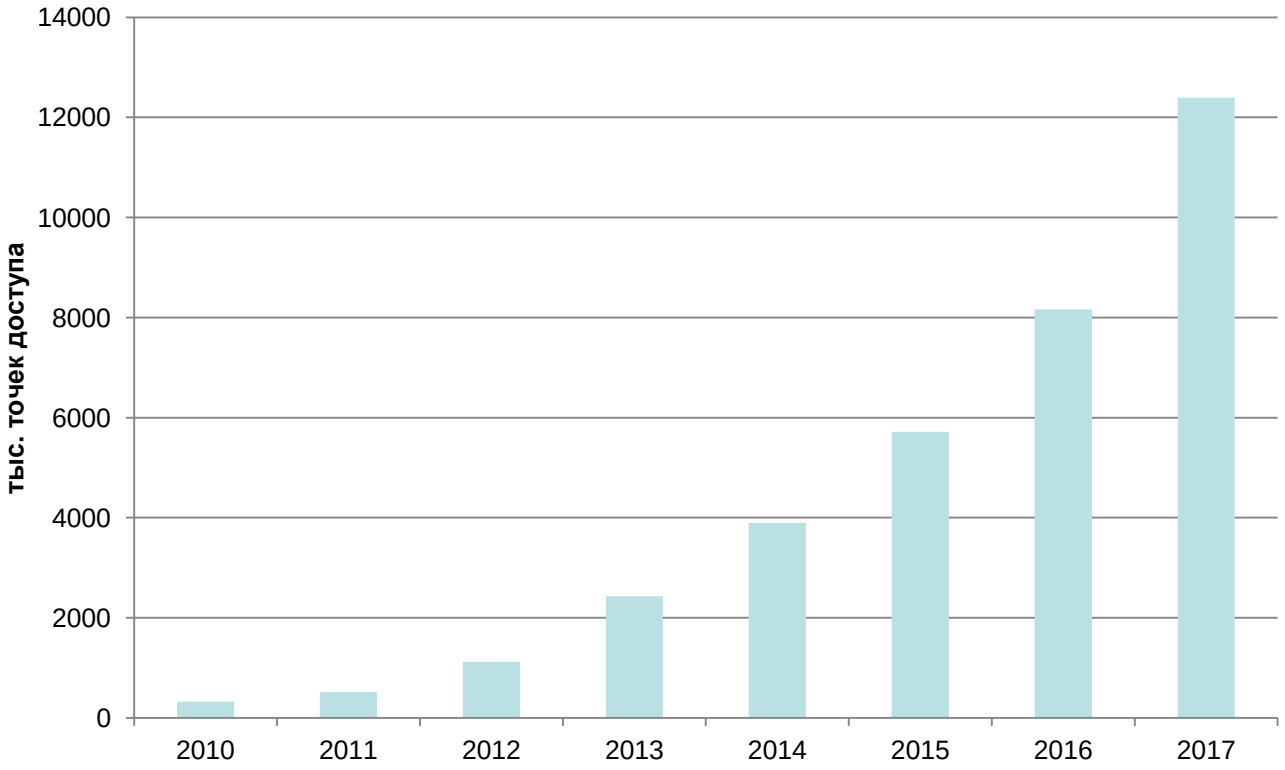
В.П.Кочин

Проектирование и обеспечение безопасности беспроводных компьютерных сетей

Проектирование беспроводных сетей



Прогноз MindCommerce по количеству точек доступа Wi-Fi в мире

Проектирование беспроводных сетей

Одной из проблем проектирования беспроводной сети является построение модели распространения радиоволн в помещениях.

При разработке модели распространения радиоволн необходимо учитывать следующие факторы:

- Радиосигнал ослабляется с расстоянием и при прохождении препятствий.
- Радиоволны отражаются от препятствий, в результате чего интерференция волн в точке приема может привести к замиранию сигнала.
- Сигнал искажается помехами от различных электрических устройств.
- Препятствия и приемник радиосигнала могут находиться как в ближней, так и в дальней зоне излучения.

Проектирование беспроводных сетей

Критерии оптимальности функционирования беспроводных сетей:

- Стоимость.
- Безопасность.
- Пропускная способность.
- Характеристики качества обслуживания.
- Величина зоны покрытия.
- Максимальное количество одновременно подключаемых пользователей.
- Размер зон бесшовного роуминга.

Проектирование беспроводных сетей

Величина зоны покрытия

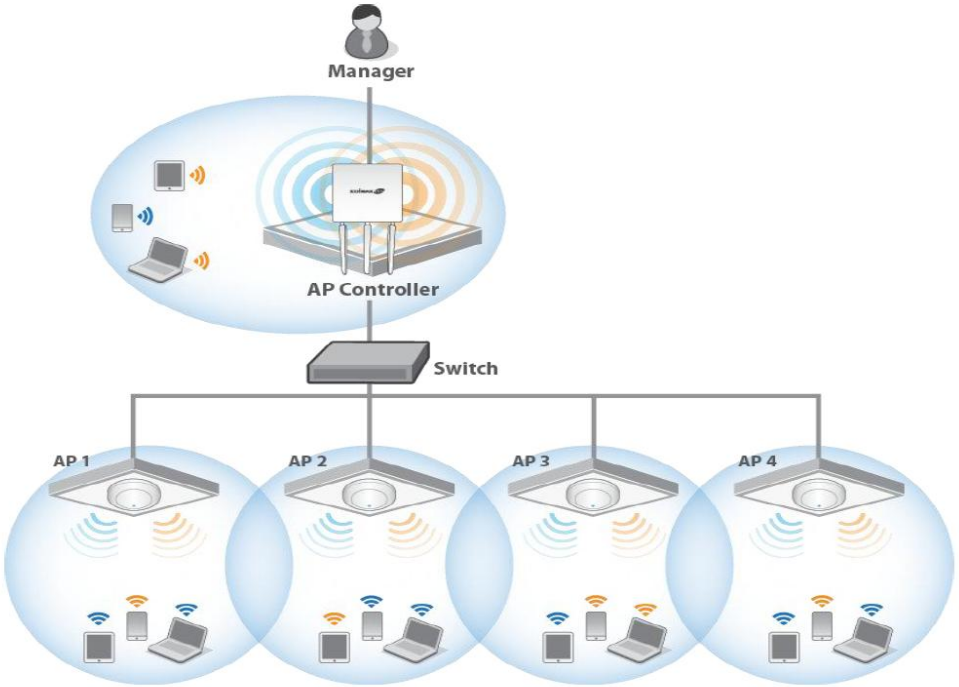
На зону покрытия внутри помещения оказывают влияние следующие параметры:

- количество и размещение точек доступа,
- излучаемая ими мощность,
- разрешенные и требуемые минимально допустимые скорости передачи данных,
- применяемый частотный диапазон,
- распределение и ширина полосы используемых каналов,
- тип антенн,
- структура стен.

Большинство из этих параметров являются априори заданными характеристиками беспроводных точек доступа или параметрами окружения и остаются постоянными в процессе расчета оптимизационной модели

Проектирование беспроводных сетей

Обеспечение **бесшовного роуминга** тесно связано с зоной покрытия. Одним из условий обеспечения бесшовного роуминга является обеспечение неразрывной зоны покрытия. В этом случае при наличии контроллеров управления беспроводными точками доступа появляется возможность обеспечения бесшовного роуминга.



Проектирование беспроводных сетей

Пропускная способность

Пропускная способность является одной из главных характеристик, наряду с уровнем сигнала, определяющей производительность беспроводной сети.

На пропускную способность оказывают влияние следующие параметры:

- уровень сигнала в точке приема,
- количество одновременно подключенных абонентов к точке доступа,
- используемый Wi-Fi стандарт,
- ширина используемых каналов.

Проектирование беспроводных сетей

Характеристики качества обслуживания QoS:

- пропускная способность,
- время задержки,
- джиттер,
- вероятность потери пакета.

Так как характеристики физического уровня (уровень сигнала, количество одновременно подключенных пользователей) являются непосредственно измеряемыми (оцениваемыми) в процессе оптимизации, то существует необходимость построения модели трансляции характеристик качества обслуживания.

Максимальное количество одновременно подключаемых пользователей.

В большинстве работ данный критерий не рассматривается вообще. Однако он является важным при организации беспроводного доступа в больших аудиториях.

Проектирование беспроводных сетей

Стоимость

Критерий стоимости является часто используемым при построении беспроводных сетей.

Безопасность

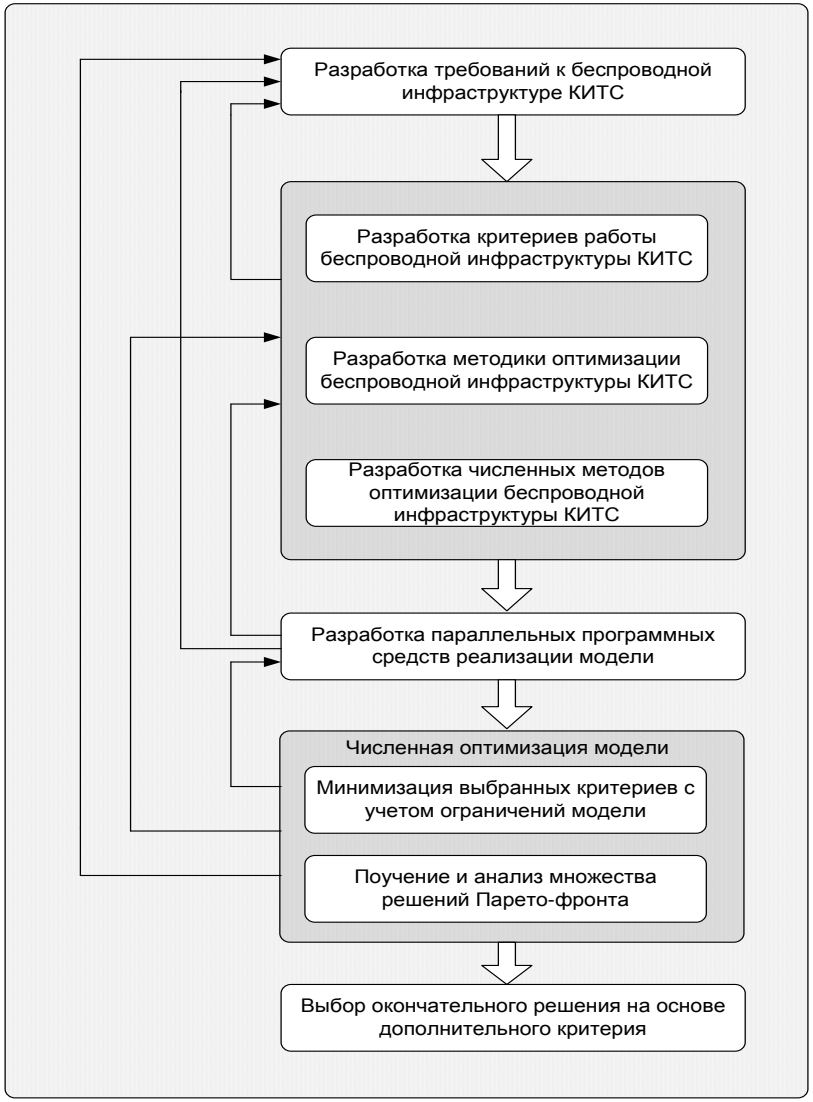
В беспроводных сетях к традиционным уязвимостям компьютерных сетей добавляются угрозы, связанные с открытой средой передачи данных. Получение количественных характеристик для такого критерия как безопасность затруднено из-за отсутствия четких общепринятых правил и сильно зависит от компетенции и квалификации экспертов, разрабатывающих количественные оценки безопасности беспроводных сетей.

Проектирование беспроводных сетей

Название метода	Способ оптимизации	Преимущества	Недостатки
главного критерия	Однокритериальный	Простота реализации и невысокая вычислительная сложность	Сложность в выборе главного критерия
линейной свертки	Однокритериальный	Простота реализации и возможность распараллеливания	Сложность в определении «весов» критериев
моделирования отжига	Многокритериальный	Простота реализации	Плохо распараллеливается Высокая вероятность «застревания» в локальном экстремуме
табуированного поиска	Многокритериальный		Возможность распараллеливания алгоритма сильно ограничена Сложность назначения срока действия табу
роящихся частиц	Многокритериальный		Плохо распараллеливается Высокая вычислительная сложность Сложность выбора оптимальных параметров
муравьиных колоний	Многокритериальный		Невозможность применения для оптимизации расположения точек доступа в помещениях
пчелиной колонии	Многокритериальный	Хорошо распараллеливается При многокритериальной оптимизации позволяет получать на выходе множества решений, оптимальных по Парето	Высокая вычислительная сложность Сложность выбора параметров алгоритма
генетические алгоритмы	Многокритериальный	Высокая степень распараллеливаемости на различных этапах работы алгоритма. Параметры генетических алгоритмов остаются постоянными на протяжении всего процесса эволюции	Высокая вычислительная сложность

Проектирование беспроводных сетей

Структура задачи оптимизации беспроводных КИТС



Безопасность беспроводных сетей

Угрозы безопасности беспроводных сетей

Подслушивание

Наиболее распространенная проблема в таких открытых и неуправляемых средах, как беспроводные сети, - возможность анонимных атак. Анонимные вредители могут перехватывать радиосигнал и расшифровывать передаваемые данные

Отказ в обслуживании (Denial of Service - DOS)

Полную парализацию сети может вызвать атака типа DOS. Во всей сети, включая базовые станции и клиентские терминалы, возникает такая сильная интерференция, что станции не могут связываться друг с другом.

Угрозы криптозащиты

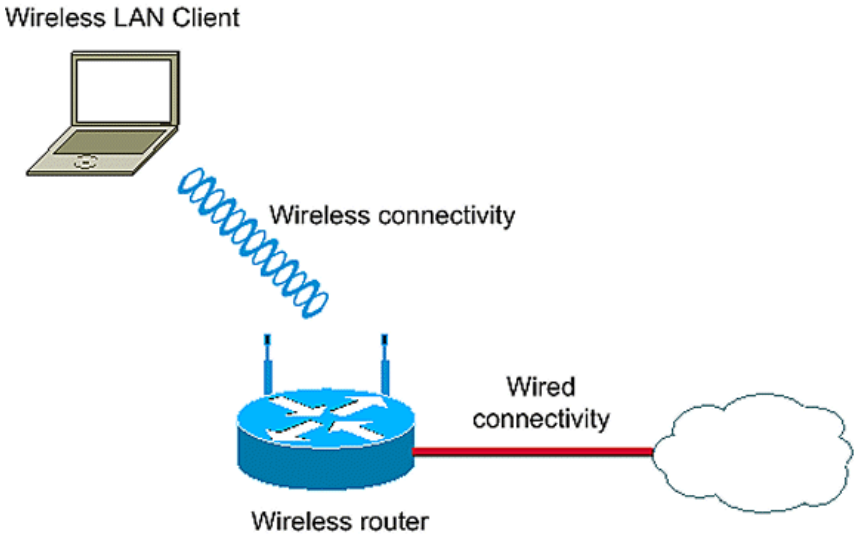
В беспроводных сетях применяются криптографические средства для обеспечения целостности и конфиденциальности информации.

Безопасность беспроводных сетей

Любое взаимодействие точки доступа (сети), и беспроводного клиента, построено на:

Аутентификации — как клиент и точка доступа представляются друг другу и подтверждают, что у них есть право общаться между собой;

Шифровании — какой алгоритм шифрования передаваемых данных применяется, как генерируется ключ шифрования, и когда он меняется.



Безопасность беспроводных сетей

Аутентификация

- **Open** — так называемая открытая сеть, в которой все подключаемые устройства авторизованы сразу
- **Shared** — подлинность подключаемого устройства должна быть проверена ключом/паролем
- Контроль за подключением к точке доступа на основе **MAC-адресов**
- Контроль за подключением к точке доступа на основе имени сети
- **EAP** — подлинность подключаемого устройства должна быть проверена по протоколу EAP внешним сервером

Безопасность беспроводных сетей

Шифрование

None — отсутствие шифрования, данные передаются в открытом виде

WEP — основанный на алгоритме RC4 шифр с разной длиной статического или динамического ключа (64 или 128 бит)

WPA — улучшенная замена WEP с дополнительными проверками и защитой

WPA2 — новый стандарт, основанный на AES256 с дополнительными проверками и защитой

Безопасность беспроводных сетей

WEP (Wired Equivalent Privacy)

Используется на беспроводных устройствах для шифрования всего трафика с целью предотвращения несанкционированного подключения к сети и доступа к передаваемой информации. Шифрование использует RC4 алгоритм. Протокол безопасности WEP предусматривает два способа аутентификации пользователей: Open System (открытая) и Shared Key (общая).

Безопасность беспроводных сетей

WPA (Wi-Fi Protected Access)

Основные достоинства WPA:

• Усовершенствованный механизм шифрования RC4, основанный на «временном протоколе целостности ключей» - Temporal Key Integrity Protocol. TKIP предусматривает замену одного статического ключа WEP ключами, которые автоматически генерируются и рассылаются сервером аутентификации.

• Аутентификация пользователей при помощи 802.1x и EAP

• Режим Pre-Shared Key (PSK), позволяющий вручную задавать ключи.

Безопасность беспроводных сетей

WPA2 (Wi-Fi Protected Access)

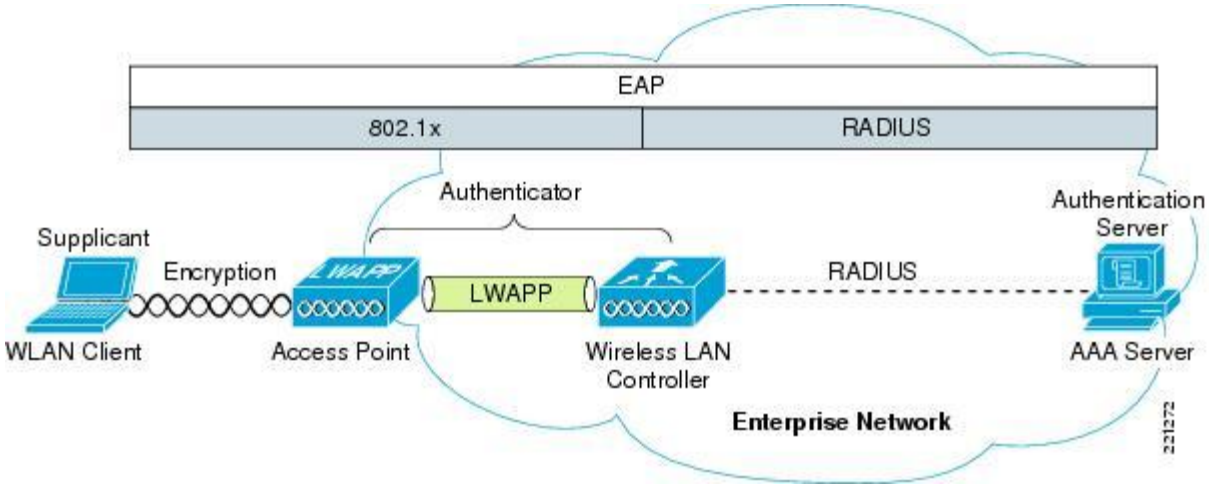
WPA2 определяется стандартом **IEEE 802.11i**, принятым в июне 2004 года, и призван заменить WPA.

В нём реализован алгоритм шифрования CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol – протокол блочного шифрования с кодом аутентичности сообщения и режимом сцепления блоков и счётчика), использующий алгоритм AES (Advanced Encryption Standard – симметричный алгоритм блочного шифрования), за счет чего WPA2 стал более защищенным, чем предыдущий тип безопасности.

В отличие от TKIP, управление ключами и целостностью сообщений осуществляется одним компонентом, построенным вокруг AES с использованием 128-битного ключа, 128-битного блока.

Безопасность беспроводных сетей

WPA2 Enterprise



Безопасность беспроводных сетей

EAP (*Extensible Authentication Protocol*) — фреймворк аутентификации, который часто используется в беспроводных сетях и соединениях точка-точка.
EAP используется для выбора метода аутентификации, передачи ключей и обработки этих ключей подключаемыми модулями называемыми методами EAP. Существует множество методов EAP, как определенных вместе с самим EAP, так и выпущенных отдельными производителями.

Безопасность беспроводных сетей

EAP

EAP-FAST — разработан фирмой Cisco; позволяет проводить авторизацию по логину-паролю, передаваемому внутри TLS туннеля между пользователем и RADIUS-сервером

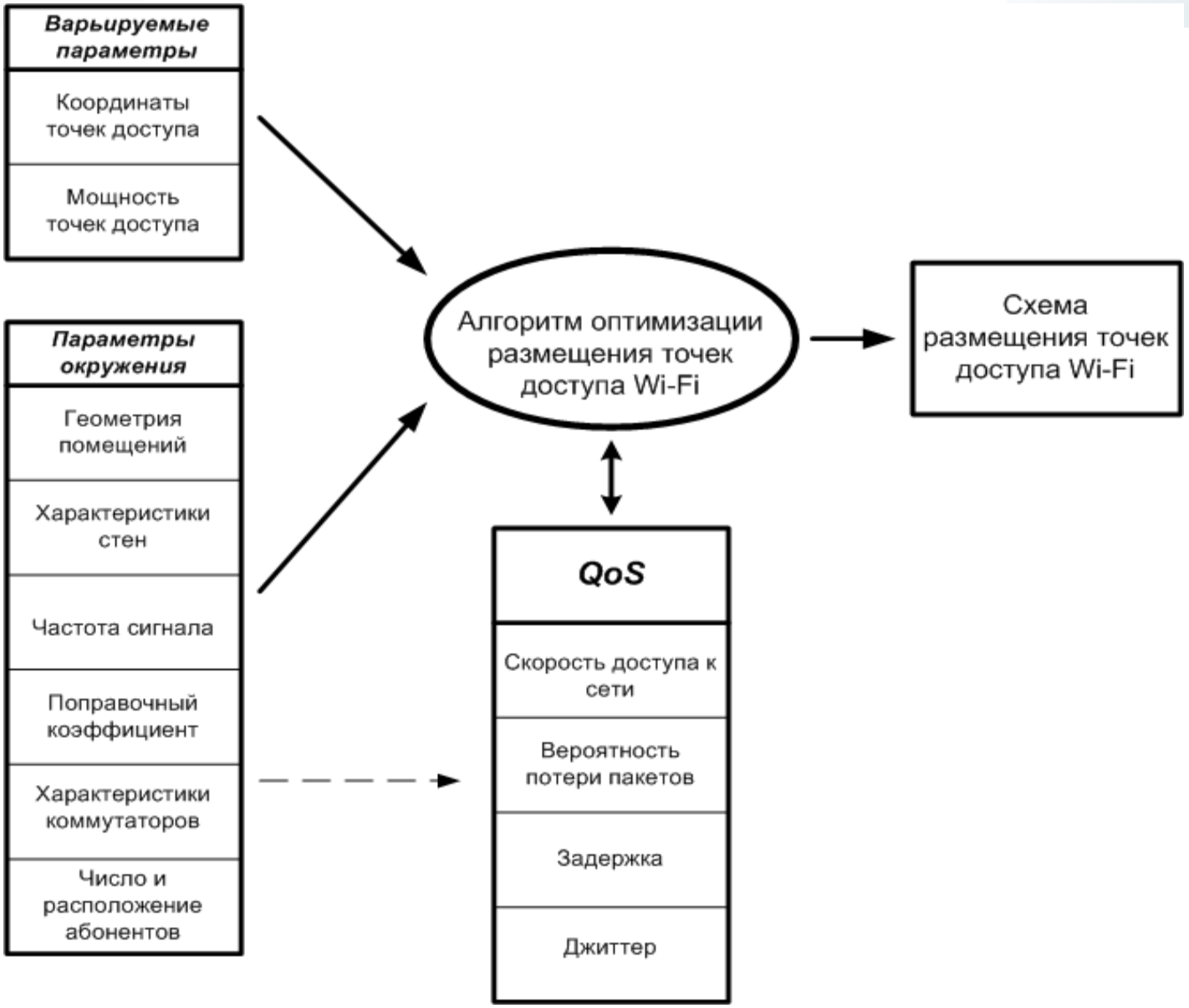
EAP-TLS . Использует инфраструктуру открытых ключей (PKI) для авторизации клиента и сервера через сертификаты, выписанные доверенным удостоверяющим центром (CA).

EAP-TTLS аналогичен EAP-TLS, но при создании туннеля не требуется клиентский сертификат. В таком туннеле, аналогичном SSL-соединению браузера, производится дополнительная авторизация (по паролю или как-то ещё).

PEAP-MSCHAPv2 — схож с EAP-TTLS в плане изначального установления шифрованного TLS туннеля между клиентом и сервером, требующего серверного сертификата. В дальнейшем в таком туннеле происходит авторизация по известному протоколу MSCHAPv2

PEAP-GTC (Generic Token Card) — аналогично предыдущему, но требует карт одноразовых паролей

Методика проектирования беспроводной структуры КИТС



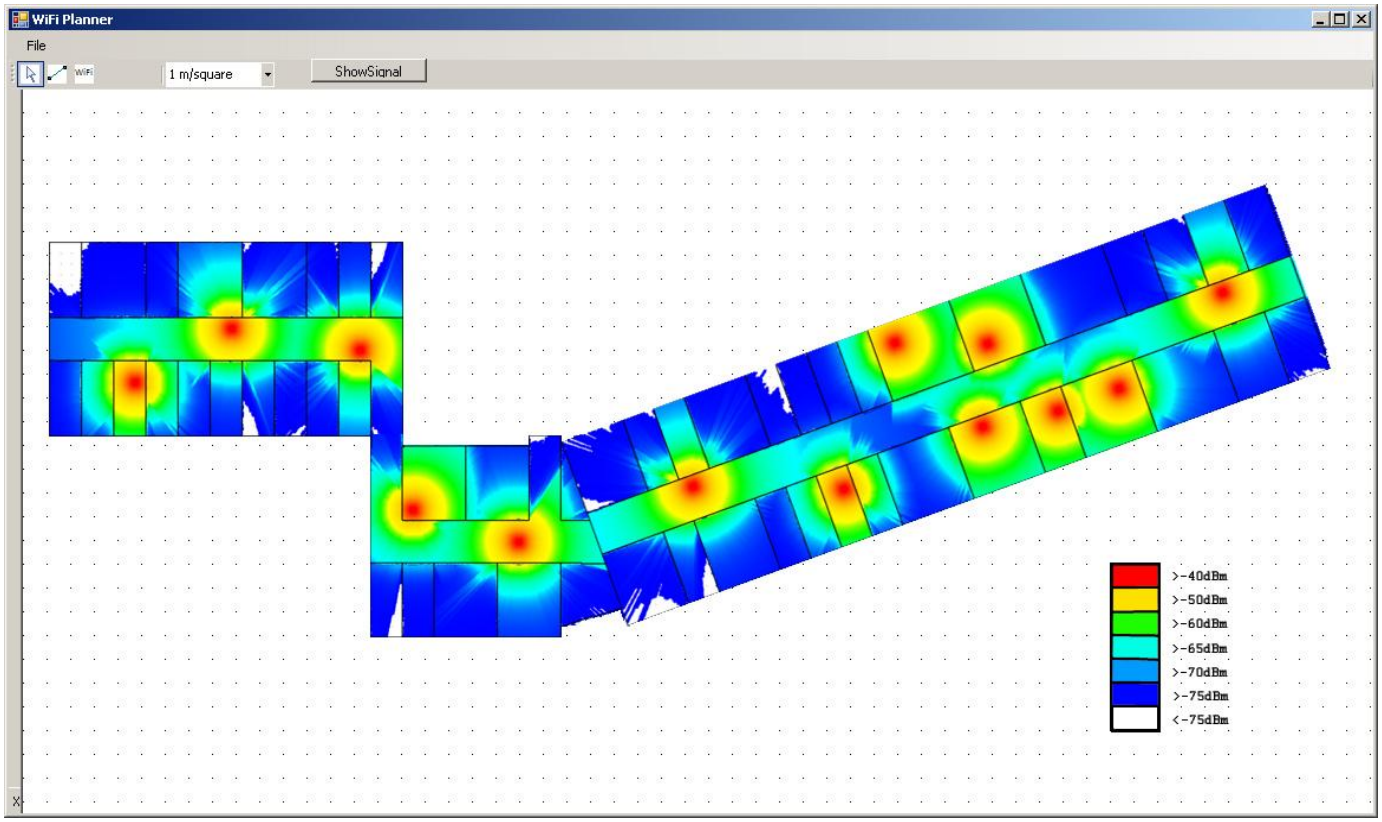
Построение модели оптимизации беспроводной сети

$$\begin{cases} \vec{X} = (X_1, \dots, X_N) \\ \alpha \le 0{,}1; T_{int} \le 40 \text{ мс}; B \ge 2 \text{ Мбит/с} \\ f_j(\vec{X}) \to max, j = \overline{1,3}, X \in D \end{cases}$$

N – количество точек доступа,
$X_i = \{x_i^x, x_i^y, P_i\}$, $i=1,..,N$ – координаты и излучаемая мощность i-й точки доступа,
α, – вероятность потери пакетов,
T_{int} – задержка пакетов в беспроводной сети,
B – скорость доступа к опорной сети,
f_j – множество критериев оптимальности (f_1 – пропускная способность, f_2 – величина зоны покрытия, f_3 – количество одновременно подключенных пользователей),
D – множество допустимых координат установки точек доступа и их мощностей.

Оптимизация расположения беспроводных точек доступа

Решение оптимизационной задачи (БГУ)



Спасибо за внимание!