ЗАЩИТА ИНФОРМАЦИИ НА ОСНОВЕ КОДИРОВАНИЯ УРОВНЕЙ ГИПЕРПОВЕРХНОСТИ ДУАЛЬНОЙ РЕШЕТКИ

С.Б. Саломатин, Т.А. Андриянова

Решетка L определяется как дискретная, имеющая базис, абелева подгруппа действительных или комплексных n-мерных векторных пространств V и базисом v. Каждая решетка имеет свою дуальную решетку с инверсным по отношению к v базисом u.

Вычислительные задачи теории решеток связаны:

– с нахождением наиболее короткого ненулевого вектора s в L (ShortestVectorProblem (SVP));

– нахождением вектора в решетки, наиболее близко расположенным к точке вне решетки (ClosestVectorProblem (CVP));

– нахождением аппроксимирующих векторов задач apprSVP и apprCVP.

Вектор s позволяет формировать различные уровни дуальной решетки, образовывая, так называемые, скрытые гиперповерхности H. Например, определяя дуальную решетку как множество y, скрытая гиперповерхность k-го уровня формируется как множество векторов y, удовлетворяющих равенству ys = k.

Алгоритм кодирования. Логический ноль кодируется случайной точкой, располагающейся между уровнями гиперповерхностей. Логическая единица кодируется случайной точкой в узле уровня дуальной решетки.

Алгоритм декодирования. Принятый вектор декодируется как логический ноль, если его проекция достаточно далека от решетки гиперповерхности. Принятый вектор декодируется как логическая единица, если его проекция распложена вблизи от гиперповерхности.

При неизвестном случайном k задача раскрытия системы становится трудно выполнимой, что позволяет классифицировать предлагаемую схему как вариант криптографической системы с открытым ключом — структурой решетки. Закрытым ключом может служить величина уровня k.

ОЦЕНКА ВНУТРИСИСТЕМНОЙ ЭМС В СЕТЯХ СОТОВОЙ СВЯЗИ СТАНДАРТА GSM ВНУТРИ ЗДАНИЙ

А.С. Свистунов

В связи с постоянным ростом территориальной плотности базовых станций (БС) сотовой связи, а также использованием завышенных уровней электромагнитных излучений БС большой интерес представляет вопрос о состоянии внутрисистемной электромагнитной совместимости (ЭМС) сотовых радиосетей и о связи уровня внутрисистемных помех в этих сетях с их безопасностью для населения.

Оценки внутрисистемной ЭМС выполнены на основе имитационного моделирования фрагмента сети сотовой связи стандарта GSM с использованием модели городской застройки при размещении абонентских станций (АС) внутри зданий на разных этажах и многолучевой модели распространения радиоволн. Принято, что уровень внутрисистемной ЭМС определяется значением отношения «сигнал/(помеха+шум)» (*SNIR*) на входе приемника АС. Использованы сценарии, в которых реализована трехсекторная структура сайтов сети при различной размерности *N* кластера частотного планирования.

При частотно-территориальном планировании сотовой сети с размерностью кластера $N = 4$, и высотах подвеса антенн БС, соизмеримых с высотой городской застройки, относительное количество АС, для которых условия внутрисистемной ЭМС неудовлетворительны ($SNIR \le 9$ дБ), достигает 10…25%. При увеличении размерности кластера до $N = 7$ данное относительное количество АС снижается до 2…4%. Снижение эквивалентной изотропной излучаемой мощности БС с 53 дБм до 43 дБм не приводит к существенному росту данного относительного количества АС. Изменение высот подвеса антенн БС неоднозначно влияет на внутрисистемную ЭМС: увеличение высот подвеса антенн БС улучшает внутрисистемную ЭМС нижних этажах зданий, но сопровождается ее очевидным ухудшением на верхних этажах. Поэтому высоты подвеса антенн БС являются параметром, подлежащим оптимизации в конкретных условиях.

Таким образом, можно утверждать, что качество связи определяется только уровнем внутрисистемной ЭМС, фактически определяемым уровнем внутрисетевых помех и распределением значений *SNIR* на входе множества АС сети, а также за счет оптимизации сети, динамического перераспределения радиочастотного ресурса между БС в различное время суток и т.п. На территории городской застройки использование уровней ЭИИМ БС выше 43–45 дБм нецелесообразно, поскольку