2. Голиков В.Ф., Черная И.И., Зельманский О.Б. Методологические основы информационной безопасности: учеб-метод. пособие. Минск, БГУИР, 2010. 67 с.
3. Михальцов М.В. // Тез. докл. 48-й научной конференции аспирантов, магистрантов и студентов БГУИР по направлению 8: Информационные системы и технологии / под ред. В.Л. Николаенко и Г.В. Сечко. Минск: ИИТ БГУИР, 2012. С. 34.

ЗАЩИТА ДАННЫХ ПРИ ПОСЛЕДОВАТЕЛЬНОЙ НОРМЕННОЙ ОБРАБОТКЕ ИНФОРМАЦИИ

ХОАНГ НГОК ЗЫОНГ

Для защиты информации от искажений, возникающих в канале связи, широко применяется помехоустойчивое кодирование. Известно, что с увеличением кратности ошибок возникает «проблема селектора». Для снижения влияния проблемы селектора в [1, 2] предложено норменное кодирование. Однако при увеличении кратности корректируемых ошибок, а также длинны кодов, вычислительная сложность реализации декодеров резко растет.

В данной работе рассматривается поход к сжатию множества норм табличным методом образующих норменных циклотомических классов, сущность которого заключается в использовании величины переходов из одного образующего циклотомического класса в другой. В результате этого, можно использовать только одну образующую норму для коррекции ошибок. Величина перехода из одного в другой циклотомический класс может быть представлена в виде таблицы. Рассматривает пример БЧХ-кода n=31, t=3, для которого существует 145 образующих векторов ошибок, с 29 образующими норменных циклотомических классов (в каждом классе 5 образующих векторов ошибок). Пусть $(N_1^{обр}, N_2^{обр}, N_3^{обр})$ образующие норменных классов. Чтобы перейти из одного $(N_{1,1}^{обр}, N_{1,2}^{обр}, N_{1,3}^{обр})$ в другой $(N_{2,1}^{обр}, N_{2,2}^{обр}, N_{2,3}^{обр})$ используются величину Δ_1, Δ_2, Δ_3, которые находятся из условий $N_{2,1}^{обр} = N_{1,1}^{обр} + \Delta_1; N_{2,2}^{обр} = N_{2,1}^{обр} + \Delta_2; N_{2,3}^{обр} = N_{1,3}^{обр} + \Delta_3$, для этого нужно 29 Δ_1, Δ_2, Δ_3.

Литература

1. Конопелько В.К., Липницкий В.А. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М., 2004.
2. Липницкий В.А., Конопелько В.К. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007.

ПАКЕТНАЯ ФИЛЬТРАЦИЯ ТРАФИКА В БЕСПРОВОДНЫХ ЯЧЕИСТЫХ СЕТЯХ НА ОСНОВЕ РАСПРЕДЕЛЕННОГО МЕЖСЕТЕВОГО ЭКРАНА

А.А. ЮРЕВИЧ, В.Ю. ЦВЕТКОВ, А.С. АЛЬ-АЛЕМ

В компьютерных сетях применяются системы защиты на основе межсетевых экранов. Системы защиты осуществляют блокировку атак, предотвращают «фоновый» трафик, ограничивают доступ в сеть извне, контролируют трафик внутри сети и регистрируют сетевую активность. Ключевыми узлами беспроводных ячеистых сетей являются беспроводные маршрутизаторы с невысокой вычислительной мощностью. Это затрудняет реализацию на их базе пакетных фильтров и сетевых экранов. Предлагается метод построения распределенного межсетевого экрана, узлами которого являются беспроводные ячеистые маршрутизаторы с операционной системой Linux/UNIX. Суть метода состоит

в применении прикладного TCP/IP сервера для управления набором правил пакетного фильтра (в GNU/Linux используется iptables) на маршрутизаторах. Для запуска приложения TCP/IP сервера при появлении трафика на детерминированных портах предлагается использовать суперсервер xinetd (extended Internet daemon). Метод позволяет централизованно и быстро вносить изменения в правила пакетных фильтров на все маршрутизаторы в сети. Использование распределенного межсетевого экрана обеспечивает низкую уязвимость к DoS-атакам, отсутствие единой точки отказа, высокую пропускную способность сети и делает возможным применение локальных и глобальных политик.

АНАЛИЗ БОРТОВЫХ СИСТЕМ ВИДЕОФИКСАЦИИ ДЛЯ ОХРАНЫ РАСПРЕДЕЛЕННЫХ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

А.А. ЖУРАВЛЕВ, В.Ю. ЦВЕТКОВ

Произведен анализ существующих систем видеофиксации, предназначенных для беспилотных летательных аппаратов (БПЛА) и обеспечивающих мониторинг территорий и распределенных объектов с целью выявления незаконной деятельности вблизи критически важных объектов. Выявлены основные параметры систем видеофиксации, определяющие выбор метода эффективного кодирования для сжатия видеоданных, фиксируемых на борту БПЛА. Установлено, что при выборе метода видеокодирования необходимо учитывать угол наклона камеры, аберрации оптической системы, а также разрешающую способность матрицы видеокамеры. Последний параметр особенно важен, так как определяет качество воспроизведения видеоданных после декодирования. Увеличение размера матрицы позволяет повысить качество воспроизведения видеоданных, но только при увеличении скорости передачи. Если полоса канала ограничена, увеличение размера матрицы ведет к необходимости повышения коэффициента сжатия видеоданных, что вызывает снижение качества их воспроизведения. С другой стороны, использование оптического увеличения для повышения детальности формируемых на борту БПЛА видеоданных приводит к уменьшению площади перекрытия соседних кадров и снижению эффективности методов сжатия, основанных на блочной компенсации движения.

АНАЛИЗ ЗАЩИЩЕННОСТИ СИСТЕМ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ

Ю.А. СЕЛИВАНОВА, В.Ю. ЦВЕТКОВ

Проведен анализ защищенности сервисов в коммуникационных системах Microsoft Lync Server 2010, Skype и ooVoo. Установлено, что данные системы используют следующие технологии информационной безопасности. В Microsoft Lync Server 2010 для аутентификации пользователей и серверов используются протоколы TLS и MTLS с криптографическими алгоритмами RSA-RC4-128-SHA. Пользователи локальной сети аутентифицируются средствами протокола Kerberos, а внешние — с использованием TLS-DSK или NTLMv2. SIP-каналы шифруются средствами TLS. Трафик аудио и видео защищается протоколом SRTP с применением AES-128. Трафик веб-конференций шифруется в HTTPS-канале. в Skype для аутентификации пользователей используется протокол TLS, для шифрования и защиты целостности