изображения, эффективной пространственной обработки маркированного изображения, декодировании сообщения с использованием параметров внедренных решеток, расшифровке сообщения и коррекции ошибок, возникающих в процессе оптического считывания. Данный алгоритм позволяет формировать устойчивые кодовые образы, несущие как визуальную, так и скрытую информацию, воспринимаемую мобильными телефонами с экрана монитора и печатной продукции.

Результаты моделирования показывают, что данный алгоритм обеспечивает высокое субъективное и объективное качество маркированного изображения (PSPNR и WPSNR>29 дБ), высокую точность декодирования решеток и значительное увеличение емкости внедрения по сравнению с QR-кодами.

АЛГОРИТМ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ НА ОСНОВЕ ВЕЙВЛЕТ-АНАЛИЗА

Л.А. РУИС, М.А. МЛАГИ, А.А. БОРИСКЕВИЧ

В качестве альтернативы традиционному подходу обнаружения аномалий сетевого поведения использование современных методов обработки сигналов позволит эффективно проводить анализ сетевого трафика с целью выявления новых или неизвестных вторжений. Технологии обнаружения вторжений делятся на две категории: обнаружение злоупотреблений и обнаружения аномалий. Подходы обнаружения злоупотреблений ограничиваются известными атаками, поэтому выявления новых атак или вариантов известных атак является одной из трудных проблем, с которыми сталкиваются методы обнаружения злоупотреблений.

В связи с этим целью работы является разработка эффективного алгоритма обнаружения сетевых аномалий, основанный на использовании современной технологии вейвлет-анализа, аппроксимационной авторегрессионной модели и технологии обнаружения выбросов.

Моделирование нормального сетевого трафика состоит из следующих двух этапов: вейвлет-декомпозиции и генерации авторегрессионной модели. Исходный сигнал сетевого трафика преобразуется в множество аппроксимационных вейвлет-коэффициентов, которые используются для построения модели предсказания нормального трафика сети. Данная модель используется для формирования сигнала состояния сетевого поведения, идентификации пиков которого осуществляется с помощью алгоритма обнаружения выбросов, и принятия решения о типе вторжений. Для реализации вейвлет-анализа сетевого трафика были использованы следующие базисные вейвлет-функции: Haar, Bior5.3, Bior9.7, Coiflet и Symlet. Установлено что, вейвлет-функция Haar является наилучшей по критерию быстродействия и точности обнаружения различных сетевых атак при использовании базы пакетов сетевых трафиков 1999 DARPA.

АЛГОРИТМ ОБНАРУЖЕНИЯ СЕТЕВЫХ АНОМАЛИЙ НА ОСНОВЕ ГЛАВНЫХ КОМПОНЕНТ И ОПОРНЫХ ВЕКТОРОВ

К.В. ГОНСАЛЕС, Л.А. РУИС, А.А. БОРИСКЕВИЧ

Информационные технологии обрабатывают огромный объем трафика информации, что требует ускорение процессов обработки для оперативности и управления доступа к информации и услугам. В этом случае ускорение управления доступа состоит в уменьшении объема обрабатываемого трафика на основе определения главных компонент множества пакетов данных, что позволит применить эффективный метод идентификации с использованием классификаторов, основанных на опорных векторах пониженной размерности.

В связи с этим целью работы является разработка эффективного алгоритма обнаружения сетевых аномалий, основанного на использовании анализа главных компонент и технологии опорных векторов.

Предложенный алгоритм основан на анализе главных компонентов тестовых пакетов данных трафика TCP/IP, выборе оптимального числа значимых главных компонент на каждую категорию сетевого поведения по энергетическому критерию, формировании матриц PCA преобразования трафика, вычислении векторов признаков для каждой категории и эталонных векторов признаков и их сравнении с использованием метрики евклидового расстояния, принятия предварительного решения о типе категории с использованием порогового сравнения и классификация типов вторжений на основе ансамбля классификаторов SVM (10 классификаторов). Использование метода анализа главных компонент уменьшает пространство с 41-го до 6-ти признаков. Установлено, что предложенный алгоритм обеспечивает приблизительно 98% точность классификации или обнаружения атак с использованием базы пакетов сетевых трафиков 1999 DARPA, разделенной на 5 категорий: Normal, DoS, R2L, U2R и Probe.

ИТЕРАТИВНЫЙ АЛГОРИТМ ОБНАРУЖЕНИЯ НИЗКОКОНТРАСТНЫХ ОБЪЕКТОВ НА ОСНОВЕ ИЗБЫТОЧНОГО ДИСКРЕТНОГО ЛИФТИНГ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ В УСЛОВИЯХ НЕСТАБИЛЬНОСТИ ВИДЕОСЪЕМКИ

И.А. БОРИСКЕВИЧ

Традиционные подходы к обнаружению низкоконтрастных объектов на видеопоследовательности в условиях нестабильности видеосъемки требует значительных вычислительно-временных затрат на предварительную стабилизацию соседних видеокадров. Известные алгоритмы не позволяют осуществлять эффективное обнаружение целей в реальном масштабе времени. В связи с этим предложен итеративный алгоритм обнаружения объектов в видеопоследовательности, основанный на вычислении избыточного дискретного лифтинг вейвлет-преобразования, гистограммных метрик сходства окна поиска и эталонного целевого изображения и модифицированной процедуры оптимизации множества частиц. Он позволяет обнаружить низкоконтрастные динамические объекты за счет использования свойств избыточного дискретного вейвлет-преобразования и выбранного правила объединения вейвлет-матриц. Избыточное дискретное вейвлет-преобразование производит локализацию компонент исходного изображения в пространственно-частотной области с сохранением его энергии, что гарантирует отсутствие искажения значимых деталей и обеспечивает адаптацию к изменению контрастности. Гистограммные метрики обладают свойством инвариантности к масштабу и положению объектов поиска на изображении.

Моделирование проведено в среде MATLAB для первого уровня разложения вейвлет-функции Хаара. Последовательность тестовых кадров аэросъемки содержит низкоконтрастные объекты размером 200–300 пикселов. Определено оптимальное количество частиц и характер их распределения. Установлено, что наилучшими характеристиками по критериям эффективности обнаружения и времени выполнения алгоритма обладает расстояние Бхаттачария для объединенных аппроксимирующей и диагональной детализирующей вейвлет-матриц.

СПОСОБЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С ПАРОЛЯМИ В СЕТИ ИНТЕРНЕТ

А.А. БОРКУН

Информационная безопасность в сети Интернет постоянно снижается, что является одной из основных проблем, с которой столкнулось современное общество. Даже такое