Содержание

Обзор алгоритмов выявления сетевых атак

Авторы
МИКОВА С.Ю.
ОЛАДЬКО В.С.
Журнал
Актуальные проблемы гуманитарных и естественных наук
Выпуск № 9-1 / 2015
***Ключевые слова**: сетевой трафик, обнаружение атак, алгоритм дискретного вейвлет-преобразования, алгоритм Бродского-Дарховского, алгоритм на основе сумме квадратов вейвлет-коэффициентов, алгоритм на основе максимума квадратов вейвлет-коэффициентов.*

В статье приведены алгоритмы выявления сетевых атак. Рассмотрен термин сетевой атаки. Проведен анализ четырех наиболее распространенных алгоритма выявления сетевых атак. Выделены основные характеристики, достоинства и недостатки.

Сетевая атака - действия с применением программных и (или) технических средств и с использованием сетевого протокола, направленные на реализацию угроз несанкционированного доступа к информации, воздействия на нее или на ресурсы автоматизированной информационной системы. [1]

В процессе реализации атаки могут возникать аномалии сетевого трафика, приводящие к отказу в обслуживании сетевых сервисов, утечке и нарушению целостности данных. Поэтому для предотвращения сетевых атак необходимо контролировать состояние элементов корпоративных сетей и своевременно выявлять аномалии сетевого трафика.

Анализ литературных источников показывает [2-5], что существует множество алгоритмов для выявления атак в сети. В настоящее время основными алгоритмами выявления сетевых атак являются:

1. алгоритм на основе дискретного вейвлет-преобразования;
2. алгоритм Бродского-Дарховского;
3. алгоритм на основе сумме квадратов вейвлет-коэффициентов;
4. алгоритм на основе максимума квадратов вейвлет-коэффициентов.

Обзор алгоритмов выявления сетевых атак приведён в таблице 1.

Обзор алгоритмов выявления сетевых атак
Таблица 1

Название алгоритма	Режимы алгоритма	Характеристика алгоритма
1. Алгоритм на основе дискретного вейвлетпреобразования с применением статистических критериев	1) Критерий Фишера 2) Критерий Кохрана	В данном алгоритме используется техника скользящих окон W1 и W2, позволяющая увеличить надёжность обнаружения незначительных аномалий, свидетельствующих о наличии сетевой атаки. Достоинства данного алгоритма: атака хорошо обнаруживается на каждом уровне БВП декомпозиции (критерий Фишера обнаруживает атаку наиболее явно). Недостатки данного алгоритма: при начальном уровне разложения обнаруживает наибольшее количество атак, но некоторые аномалии могут быть пропущены, если начать разложение с более старших уровней. На старших уровнях повышается количество возникновения ложных тревог.
2. Алгоритм обнаружения аномалий Бродского-Дарховского.	1. Стандартный режим 2. Режим скользящих окон	При выборе стандартного режима особое влияние проявляют шумы. При выборе алгоритма в режиме скользящего окна совокупное действие помех уменьшается, и выбросы, характеризующие начало и конец воздействия, представляются в более явном виде. Для практической реализации лучше использовать алгоритм в режиме скользящего окна.
3 .Алгоритм, основанный на сумме квадратов вейвлеткоэффициентов	1. Выявление аномалий с использованием вейвлета Хаара 2. Выявление аномалий с использованием вейвлета Добеши	Алгоритм обладает большой эффективностью. Наибольший эффект обнаруживается при использовании коэффициентов аппроксимации для вейвлетов Хаара на верхних уровнях разложения. Но увеличение размера окна анализа может привести к возрастанию вероятности правильного обнаружения аномалии, но при этом возрастает вероятность ложного обнаружения.
4. Алгоритм, основанный на максимуме квадратов вейвлет-коэффициентов	1. Алгоритм с использованием вейвлета Хаара 2. Алгоритм с использованием вейвлета Добеши	Алгоритм обладает меньшей эффективностью, чем алгоритм, основанный на сумме квадратов вейвлет-коэффициентов. Наиболее информативно отражают атаку в этом алгоритме коэффициенты аппроксимации с использование вейвлета Хаара.

Приведённые выше алгоритмы анализируют следующие параметры: ошибки первого рода, ошибки второго рода, количество правильно обнаруженных аномалий. Таким образом, по результатам проведенного анализа можно сделать вывод о том, что наиболее простыми в реализации являются алгоритм Бродского-Дарховского и алгоритм на основе дискретного вейвлет-преобразования с применением статистических критериев. Наиболее точным в обнаружении аномалий является алгоритм Бродского-Дарховского. При его использовании обнаруживается меньше ошибок 1-ого и 2-ого рода, чем при использовании алгоритма на основе дискретного вейвлет-преобразования с применением статистических критериев. Алгоритм Бродского-Дарховского имеет наибольшее количество правильно обнаруженных

аномалий, но при этом имеет большие требования к ресурсам.

Литература

1. ГОСТ Р 53114-2008. Государственный стандарт Российской Федерации: “Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения” пункт 3.3.7— М.: ИПК Издательство стандартов, 2008
2. О. И. Шелухин, Д.Ж. Сакалема, А.С. Филинова. Обнаружение вторжений и компьютерные сети. / О.И. Шелухин — М.: Горячая линия-Телеком, 2013. — 220 с
3. Шелухин О. И., Иванов Ю.А. Ригов В.Ю. Обнаружение DOS и DDOS- атак методом дискретного вейвлет-анализа / Т-Сотт-Телекоммуникации и Транспорт. - 2011. - №1. - С. 4446
4. Шелухин О.И., Филинова А.С. Обнаружение сетевых аномальных выбросов трафика методом разладки Бродского-Дарховского / T-Comm - Телекоммуникации и Транспорт. -2013.-№10 - том 7- С. 116-118.
5. Шелухин О.И., Панкрушин А.П. Оценка достоверности обнаружения аномалий сетевого трафика методами дискретного вейвлет-преобразования / T-Comm - Телекоммуникации и Транспорт.-2013. - №10/ - том 7 - С. 110-113.