МЕТОДИКА ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ НА ОСНОВЕ ИНТЕГРАЦИИ МЕТОДОВ ВЕЙВЛЕТ-АНАЛИЗА И МАТЕМАТИЧЕСКОЙ СТАТИСТИКИ

Котенко И.В.[1], Саенко И.Б.[2], Бортникер П.В.[3]

Ключевые слова: *компьютерные атаки, обнаружение вторжений, белый шум, вейвлет-анализ, коэффициенты разложения, закон распределения, статистическая гипотеза.*

Аннотация

Цель работы: состоит в разработке методики обнаружения сетевых вторжений, основанной на применении методов вейвлет-анализа и математической статистики, позволяющей своевременно обнаруживать сетевые вторжения.

Методы исследования: системный анализ проблемы обнаружения сетевых вторжений, методы оценивания выборок данных по статистическим гипотезам, методы обнаружения сетевых вторжений на основе анализа энергетического спектра сигнала, восстановленного по коэффициентам вейвлет-разложения.

Результаты исследования: предложены модели статистической оценки вейвлетов, отобранных для обнаружения сетевых вторжений, в которых выбор наиболее предпочтительного вейвлета производится по результатам проверки статистических гипотез о равенстве средних значений, дисперсий и законов распределения в эталонной и зашумленной (подверженной вторжениям) выборках сетевого трафика; разработана методика обнаружения сетевых вторжений, основанная на анализе энергетического спектра сигнала, восстановленного по коэффициентам разложения, полученным с использованием наиболее предпочтительного вейвлета; произведена оценка чувствительности обнаружения сетевых вторжений методом спектрального вейвлет-анализа по отношению к частотному диапазону сигнала, восстановленного по коэффициентам вейвлет-разложения.

DOI: 10.24412/1994-1404-2024-4-23-31

Введение

Стремительное развитие вычислительной техники привело к тому, что компьютерные сети стали использоваться как полнофункциональные распределенные вычислительные устройства для обработки и передачи данных [1]. Многие специалисты в области компьютерной безопасности изучали вопрос важности анализа методов вторжения в компьютерные сети с целью определения наилучших методов борьбы с ним [4, 12]. В [9, 13] и ряде других работ были проанализированы различные методы вторжения в сети, и сделаны предположения, что метод вейвлет-преобразований является одним из наиболее полезных для построения методик обнаружения таких вторжений и определения состояния сложных объектов. Любое вторжение в компьютерные сети организации представляет серьезную угрозу ее безопасности и может нанести непоправимый ущерб; обнаружение и предотвращение вторже-

[1] ***Котенко Игорь Витальевич****, заслуженный деятель науки РФ, доктор технических наук, профессор, главный научный сотрудник и руководитель лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. ORCID: 0000-0001-6859-7120.*

E-mail: ivkote@comsec.spb.ru

[2] ***Саенко Игорь Борисович****, доктор технических наук, профессор, главный научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. ORCID: 0000-0002-9051-5272.*

E-mail: ibsaen@comsec.spb.ru

[3] ***Бортникер Пётр Владимирович****, аспирант, лаборатория проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра Российской академии наук (СПб ФИЦ РАН), г. Санкт-Петербург, Россия. ORCID: 0009-0008-1708-1480.*

E-mail: bort29@mail.ru

ний является одной из ключевых задач для обеспечения безопасности организации.

Данная проблема привлекает повышенное внимание отечественных и зарубежных исследователей в области информационной безопасности. Достаточно большая часть исследований связана с разработкой эффективных подходов к обнаружению аномалий сетевого трафика методами статистического анализа и вейвлет-анализа, развивая идеи динамического подхода [5].

Вейвлетами называется совокупность функций, которые имеют определенную форму, а также могут быть локализованы как по времени, так и по частоте. Стоит отметить, что все эти функции порождает одна основополагающая функция с помощью ее масштабирования по времени. Также необходимо отметить, что у всех подобных функций интегральное значение равно нулю [6]. Примеры некоторых вейвлетов приведены на рисунке 1.

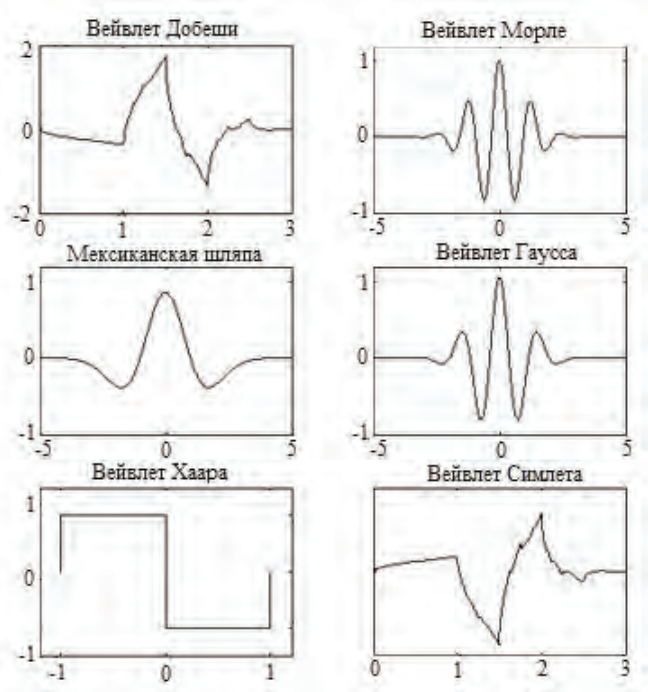


Рис. 1. Примеры вейвлетов

К наиболее распространенным методам применения вейвлет-анализа для обнаружения атак относятся:

определение момента распределенной атаки отказа в обслуживании (DDoS) путем сравнения вейвлет-коэффициентов на разных интервалах времени; недостатком данного метода является его высокая вычислительная сложность [3];

- определение DDoS-атак с помощью энергетического распределения, основанного на вейвлет-анализе; в данном алгоритме рассчитываются энергетические изменения различий в распределении трафика, вызванные порождением аномального выброса из-за влияния DDoS- атаки [6];
- вейвлет-декомпозиция сетевого трафика в совокупности с методами математической статистики; заключается в представлении его в виде набора вейвлет-коэффициентов, которые задают некоторую выборку; в процессе обработки выборки методами математической статистики происходит обнаружение аномальных выбросов [2];
- алгоритм Бродского-Дарховского, применяемого для контроля совпадения или различия текущего среднего значения в двух смещающихся «окнах» [11].

В связи с тем, что при решении задач информационной безопасности большую роль играет время, в исследованиях подобного типа часто возникают проблемы, связанные с определением наиболее приемлемого вейвлета, позволяющего за минимальное время и с высокой точностью установить наличие вторжения. Решению данной проблемы и посвящена настоящая работа.

Статистическая оценка и выбор вейвлетов для обнаружения вторжений

Для исследований были отобраны следующие три типа вейвлетов: Добеши, «Мексиканская шляпа» и Хаара. Они считаются наиболее популярными [7].

С помощью пакета компьютерной математики MATLAB была проведена генерация сигналов без помех (эталонный сигнал) и с помехами (сигнал, имитирующий сетевые вторжения). Эталонный сигнал содержал 4 гармоники. Второй сигнал был получен из эталонного путем добавления белого шума с уровнем 10% от среднеквадратичного значения сигнала. Оба сигнала показаны на рисунке 2.

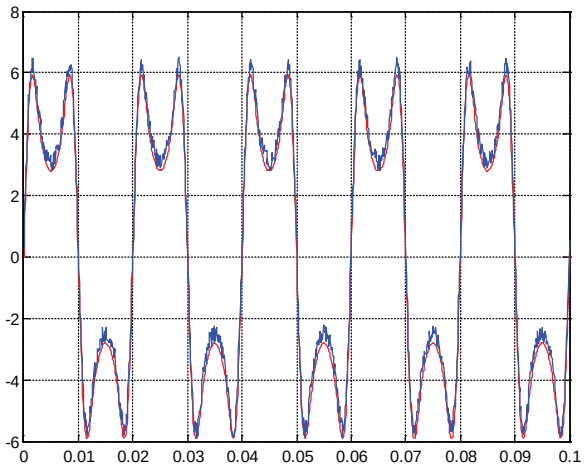


Рис. 2. Результаты генерации исследуемых сигналов (синий цвет – эталонный сигнал; красный – зашумленный)

Далее оба сигнала были подвержены вейвлет-разложению с применением отобранных типов вейвлетов. Коэффициенты разложения двух сигналов по трем типам вейвлетов показаны на рисунке 3.

Дальнейшее моделирование заключалось в обработке оцифрованных массивов вейвлет-коэффициентов методами математической статистики в части проверки статистических гипотез о равенстве средних

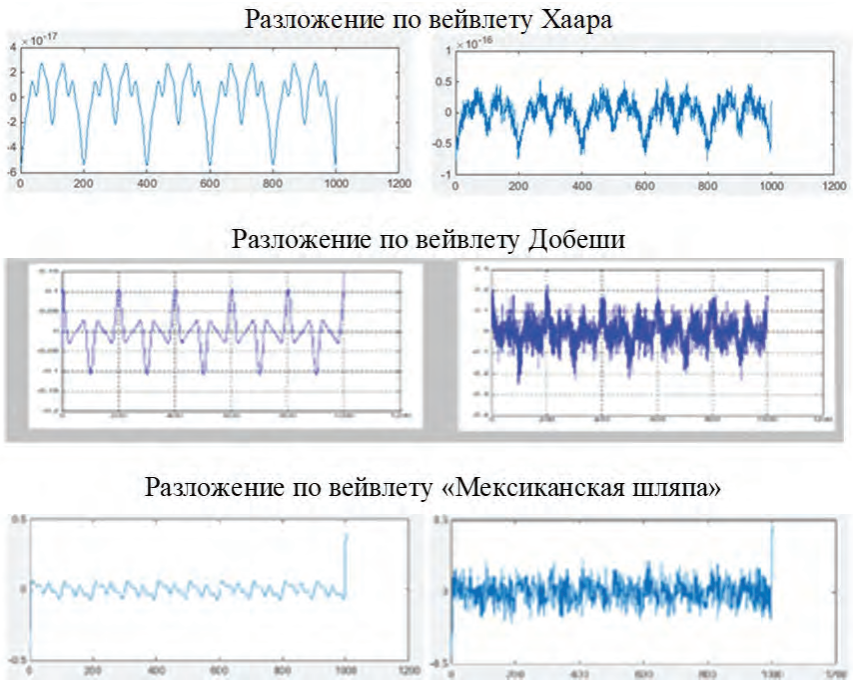


Рис. 3. Коэффициенты разложения эталонного и зашумленного сигналов

значений, дисперсий и видов закона распределения. В первую очередь были проверены гипотезы о равенстве средних и дисперсий для выборок С1 (коэффициенты эталонного сигнала) и затем С2 (коэффициенты сигнала с помехой). При этом были исключены экстремальные выбросы (грубые промахи). Затем были исследованы законы распределения массивов с помощью критериев согласия. В случае, если вид закона распределения выяснить не удавалось, проверялась гипотеза об однородности выборок по критерию Колмогорова-Смирнова [8]. Уровень значимости везде принимался равным 0,05. Вывод по принятию основной гипотезы делался на основе выборочного значения тестовой статистики *p*. Если значение тестовой статистики было меньше уровня значимости, то основная гипотеза не принималась.

В результате проведенных исследований были получены следующие результаты проверки статистических гипотез.

Для вейвлета Хаара гипотеза о соответствии выборок нормальному распределению отклоняется, так как *p*-значение тестовой статистики было равно 0,0. Следовательно, можно считать на уровне значимости 0,05, что массивы коэффициентов С1 и С2 для вейвлета Хаара не согласуются с нормальным распределением. При этом тест Колмогорова-Смирнова для этих двух совокупностей свидетельствует о том, что выборки имеют значительное различие в законах распределения. Проверка гипотез о равенстве средних и дисперсий показала, что в пределах уровня значимости средние двух выборок можно считать одинаковыми, но дисперсии считать равными нельзя.

Для вейвлета Добеши проверка статистической гипотезы о виде закона распределения показала, что на уровне значимости 0,05 массив коэффициентов С2 согласуется с нормальным распределением. При этом для массива С1 не представляется возможным подобрать подходящий вид распределения. Несмотря на то, что оно было больше всего похоже на нормальное, оно имело слишком большое скопление элементов вокруг своего среднего значения. Гипотеза о равенстве дисперсий при выбранном уровне значимости отвергается, а гипотеза о равенстве средних принимается.

Для вейвлета «Мексиканская шляпа» гипотеза о соответствии массивов коэффициентов С1 и С2 нормальному распределению отклоняется (*p*-значение тестовой статистики равно 0,0000, что меньше, чем 0,05). При этом тест Колмогорова-Смирнова показывает большое различие в распределении выборок. Средние значения двух выборок можно считать одинаковыми, а генеральные дисперсии двух выборок нельзя считать равными, так как они значимо отличаются.

Итоговые результаты сравнительной оценки статистической обработки массивов коэффициентов вейвлет-разложений для всех рассмотренных типов вейвлетов представлены в таблице 1.

Проведенный анализ позволяет сделать вывод, что из трех типов рассмотренных вейвлетов наиболее подходящим для последующего исследования является вейвлет «Мексиканская шляпа».

Методика обнаружения сетевых вторжений

Взаимосвязь этапов методики обнаружения сетевых вторжений показана на рисунке 4.

Для представления сетевого трафика в виде сигнала было использовано программное средство Wireshark.

Таблица 1

Результаты сравнительной оценки статистической обработки массивов коэффициентов вейвлет-разложений

Тип вейвлета	Статистическая гипотеза о виде закона распределения	Статистическая гипотеза о равенстве средних	Статистическая гипотеза о равенстве дисперсий
Вейвлет Хаара	Гипотеза о нормальном распределении отвергается в обоих случаях	Гипотеза принимается	Гипотеза отвергается
Вейвлет Добеши	Гипотеза о нормальном распределении принимается для массива С2 и отвергается для массива С1	Гипотеза принимается	Гипотеза отвергается
Вейвлет «Мексиканская шляпа»»	Гипотеза о нормальном распределении принимается для массива С2 и отвергается для массива С1	Гипотеза отвергается	Гипотеза отвергается

Проводилось сканирование обычной деятельности пользователя в сети в течение 25 минут. Полагалось, что этого времени достаточно для обнаружения вторжения. Полученная зависимость интенсивности сигнала от времени была принята в качестве эталонного трафика и сохранена в формате CSV.

Для проведения вейвлет-анализа сетевого трафика использовался программный пакет MATLAB. Для вейвлет-разложения использовался вейвлет «Мексиканская шляпа», который был выбран в качестве наиболее предпочтительного по результатам проверки статистических гипотез. Было произведено считывание данного сигнала, после чего применено вейвлет-разложение до уровня $N = 3$, и получены детализирующие коэффициенты для третьего (DC3), второго (DC2) и первого (DC1) уровней разложения.

Для нахождения компонентов сигнала, которые соответствуют вейвлет-коэффициентам DC1, DC2 и DC3 было выполнено прямое восстановление сигнала по каждому набору детализирующих коэффициентов, то есть на высокой, средней и низкой частоте.

Графики сигнала, восстановленного по детализирующим коэффициентам, показаны на рисунке 5.

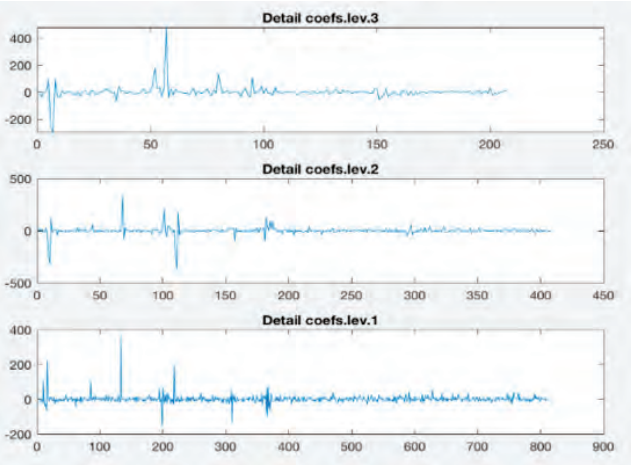
Для получения количественных характеристик был применен подход, который основан на получении энергетического спектра сигнала, восстановленного по вейвлет-коэффициентам, и который был предварительно исследован в [14]. Для энергетического спектра вычислялась кумулята энергии на высоких, средних и низких частотах.

Кумулятой энергии называется частотное накопление спектральной плотности энергии в пределах полосы частот $[f_1; f_2]$. Кумулята энергии μ вычисляется по следующей формуле:

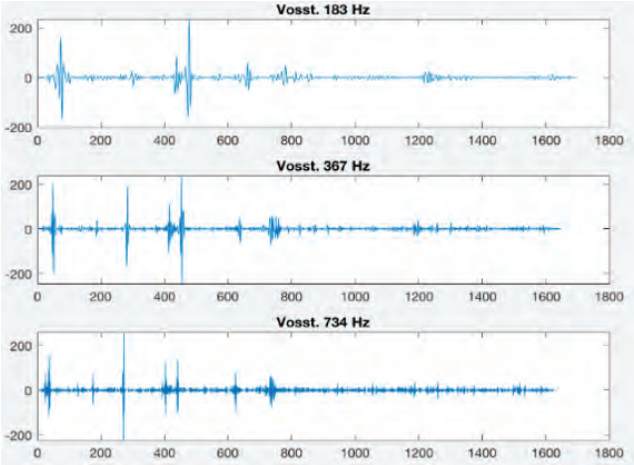
$$\varepsilon = \int_{f_1}^{f_2} E(f)\,df,$$

где $E(f)$ – спектральная плотность энергии; f – частота.

Рис. 4. Этапы методики обнаружения сетевых вторжений



Детализирующие коэффициенты



Восстановленные сигналы

Рис. 5. Детализирующие коэффициенты и восстановленные по ним сигналы

Для рассматриваемого эталонного сигнала определение кумуляты энергии привело к следующим результатам. Предельное значение кумуляты энергии эталонного сигнала на высокой частоте равно $\mu_1 = 4{,}7 \cdot 10^5$, на средней частоте – $\mu_2 = 7 \cdot 10^5$, а на низкой – $\mu_3 = 5 \cdot 10^5$. Если перейти к натуральным логарифмам для данных значений, то на высоких частотах это значение будет равно 13,06, на средних частотах – 13,46, на низких частотах – 13,12.

Вейвлет-анализ трафика сети, подверженной вторжению, заключался в следующем.

Поскольку первыми действиями злоумышленника, который провел атаку и получил доступ к чужой сети, является похищение большого количества данных, первым признаком вторжения в сеть является скачивание файлов большого объема. Для проведения моделирования такой атаки были поставлены на скачивание несколько подобных файлов.

Во время скачивания файлов осуществлялось сканирование сетевого трафика с помощью средства Wireshark. Сканирование атакуемого трафика, так же, как и в случае эталонного трафика, проводилось 25 минут. В результате был получен сигнал в виде зависимости интенсивности от времени.

Далее проводилось считывание трафика в MATLAB с последующим вейвлет-анализом и определением кумуляты энергии данного трафика. Графики атакуемого сетевого трафика и его кумуляты энергии (на высокой, средней и низкой частоте) представлены на рисунке 6.

Предельное значение кумуляты энергии атакуемого трафика на высокой частоте равно $\mu_1 = 12 \cdot 10^7$, на средней частоте – $\mu_2 = 11{,}8 \cdot 10^7$, а на низкой частоте – $\mu_3 = 11{,}6 \cdot 10^7$. Натуральный логарифм для данных значений будет равен на высокой частоте – 18,6, на средней частоте – 18,59, на низкой частоте – 18,57.

Рассмотрим теперь непосредственно процесс обнаружения вторжения в сеть.

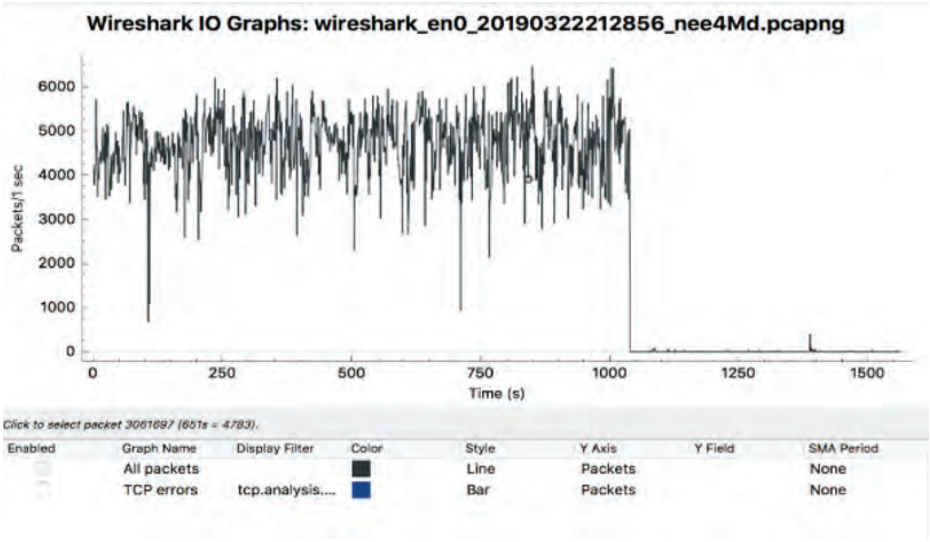
После проведения вейвлет-анализа нормального сетевого трафика, принятого за эталонный сигнал, и вейвлет-анализа сетевого трафика, полученного в момент моделирования атаки, были получены следующие результаты. Значение кумуляты энергии сетевого трафика, полученного в момент моделирования атаки, значительно превышает значение кумуляты энергии эталонного сигнала. И на высокой, и на средней, и на низкой частотах было получено различие в значениях кумулят на 2 порядка.

После этого было проведено повторное моделирование атаки и повторный вейвлет-анализ атакуемого сетевого трафика. На этот раз трафик сканировался на протяжении 40 минут. Результат получился аналогичным – на всех частотах значение кумуляты энергии сетевого трафика, полученного в момент моделирования атаки, превышало значение кумуляты энергии эталонного сигнала более чем в 200 раз.

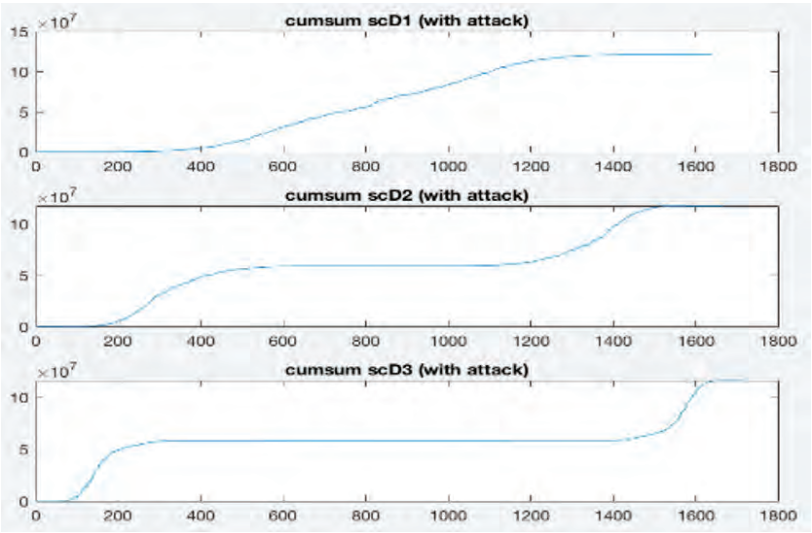
Таким образом, можно сделать вывод о том, что, если значение кумуляты энергии сетевого трафика значительно превышает значение кумуляты энергии эталонного сетевого трафика, это говорит о том, что сеть подвержена вторжению.

Для тестирования разработанной методики было проведено сканирование большого числа различных сигналов, соответствующих обычной деятельности пользователя в сети и соответствующих сетевому трафику, подверженному атаке.

Из того, что значение кумуляты энергии возрастает при увеличении времени прохождения сигнала, следует, что значение кумуляты энергии сигнала, сканированного в течение длительного процесса атаки, заметно превышает значение кумуляты энергии сигнала, сканированного в течение нескольких минут. Это позволяет обнаружить вторжение на раннем этапе и принять соответствующие меры по его предотвращению. Кроме того, это позволяет понять, на какой стадии



Атакуемый сетевой трафик в Wireshark



Кумулята энергии атакуемого трафика

Рис. 6. Графики атакуемого сетевого трафика и его кумуляты энергии

находится атака, если ее не получилось обнаружить в начале ее реализации.

Для оценки чувствительности методики была найдена степень уязвимости атакуемого трафика, который был обработан с помощью вейвлет-анализа. Для вычисления степени уязвимости трафика предложена следующая формула:

$$N_{\text{у}} = \frac{ln\,\varepsilon_{\text{э}}}{ln\,\varepsilon_{\text{а}}},$$

где $\varepsilon_{\text{э}}$ – кумулята энергии эталонного трафика; $\varepsilon_{\text{а}}$ – кумулята энергии атакуемого трафика.

На высокой частоте степень уязвимости равна $N_{\text{у}}$ = 18,6 / 13,06 = 1,424, на средней частоте – $N_{\text{у}}$ = 18,59 / 13,46 = 1,38, на низкой частоте – $N_{\text{у}}$ = 18,57 / 13,12 = 1,415. Данные результаты позволяют сделать вывод о том, что наиболее уязвимым является сетевой трафик, проходящий на высоких частотах.

При вычислении степени уязвимости для других сигналов, подверженных вторжению при моделировании соответствующей атаки, получились аналогичные результаты – на высокой частоте степень уязвимости была наибольшей.

Заключение

В настоящей работе предложен новый подход к обнаружению вторжений в компьютерные сети, основанный на применении методов вейвлет-анализа и математической статистики. Математическая статистика используется для оценки и выбора наиболее приемлемого вейвлета посредством проверки статистических гипотез о равенстве средних значений, дисперсий и видов распределения выборок, полученных на эталонном и зашумленном сигнале. Вейвлет-анализ используется для получения графиков кумуляты энергии

эталонного и реального сетевых сигналов, сравнение которых позволяет сделать вывод о наличии или отсутствии сетевых вторжений. Если на всех частотах значение кумуляты энергии атакуемого трафика превышает значение кумуляты энергии эталонного сигнала более чем на 2 порядка, то это свидетельствует о наличии сетевого вторжения.

Проведенный сравнительный анализ вейвлетов Хаара, Добеши и «Мексиканская шляпа» показал предпочтительность для обнаружения сетевых вторжений последнего, поскольку именно данный вейвлет лучше всего выявляет статистически значимые различия коэффициентов разложения сигнала по его базису.

Дальнейшее направление исследований связывается с исследованием возможности совместного использования методов вейвлет-анализа и математической статистики для обнаружения и классификации компьютерных атак различных типов.

*Рецензент: **Лаута Олег Сергеевич**, доктор технических наук, профессор кафедры комплексного обеспечения информационной безопасности Государственного университета морского и речного флота имени адмирала С.О. Макарова, г. Санкт-Петербург, Россия.*

E-mail: laos-82@yandex.ru

Литература

1. Шелухин О.И., Рыбаков С.Ю., Раковский Д.И. Классификация компьютерных атак с использованием мультифрактального спектра фрактальной размерности // Вопросы кибербезопасности. 2024. № 2 (60). С. 107–119. DOI: 10.21681/2311-3456-2024-2-107-119.
2. Видищева Е.В., Копырин А.С., Василенко М.С. Анализ и уточнение классификации аномалий и выбросов на экономических данных // Вестник Алтайской академии экономики и права. 2019. № 6–1. С. 41–46.
3. Золотарев А.И., Сидоркина И.Г., Смирнов В.И. Анализ гибридных алгоритмов обнаружения вторжений // Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и инфокоммуникационные системы. 2021. № 2 (50). С. 45–53. DOI: 10.25686/2306-2819.2021.2.45.
4. Котенко И.В., Саенко И.Б., Захарченко Р.И., Величко Д.В. Подсистема предупреждения компьютерных атак на объекты критической информационной инфраструктуры: анализ функционирования и реализации // Вопросы кибербезопасности. 2023. № 1(53). С. 2–17. DOI: 10.21681/2311-3456-2023-1-13-27.
5. Котенко И.В., Саенко И.Б., Захарченко Р.И., Величко Д.В. Динамическая модель контроля функционирования для предупреждения компьютерных атак // Правовая информатика. 2024. № 2. С. 35–43. DOI: 10.21681/1994-1404-2024-2-35-43.
6. Павлычев А.В., Стародубов М.И., Галимов А.Д. Использование алгоритма машинного обучения Random Forest для выявления сложных компьютерных инцидентов // Вопросы кибербезопасности. 2022. № 5 (51). С. 74–81. DOI: 10.21681/2311-3456-2022-5-74-81.
7. Guo T., Zhang T., Lim E., López-Benítez M., Ma F., Yu L. A Review of Wavelet Analysis and Its Applications: Challenges and Opportunities // IEEE Access, 2022, Vol. 10, pp. 58869-58903. DOI: 10.1109/ACCESS.2022.3179517.
8. Попов А.М., Сотников В.Н. Теория вероятностей и математическая статистика. М. : Издательство Юрайт, 2024. 425 с.
9. Шелухин О.И., Раковский Д.И. Разработка программно-аппаратного комплекса моделирования многозначных компьютерных атак // Вопросы кибербезопасности. 2024. № 4 (62). С. 116–130. DOI: 10.21681/2311-3456-2024-4-116-130.
10. Wang L., Zhang X. Anomaly detection for automated vehicles integrating continuous wavelet transform and convolutional neural network // Applied Sciences, 2023, Vol. 13, 5525. DOI: 10.3390/app1309552.
11. Bouzebda S., Ferfache A.A. Asymptotic properties of semiparametric M-estimators with multiple change points // Physica A: Statistical Mechanics and its Applications, 2023, Vol. 609, 128363. DOI: 10.1016/j.physa.2022.128363.
12. Красов А.В., Гельфанд А.М., Коржик В.И., Котенко И.В., Петрив Р.Б., Сахаров Д.В., Ушаков И.А., Шариков П.И., Юркин Д.В. Построение доверенной вычислительной среды. СПб. : ИП Петрив Роман Богданович, 2019. 108 с.
13. Kotenko I., Saenko I., Budko P., Vinogradenko A. Intelligent state assessment of complex autonomous objects based on wavelet analysis // Engineering Applications of Artificial Intelligence, 2023, Vol. 126, Part A, November 2023, 106869. P.1-20. DOI: 10.1016/j.engappai.2023.106869.
14. Saenko I., Bortniker P., Lauta O., Zhdanova I., Vasiliev N. An approach to early computer network intrusion detection based on the wavelet transform energy spectra analysis // Proceedings of the Seventh International Scientific Conference “Intelligent Information Technologies for Industry” (IITI’23). IITI 2023. Lecture Notes in Networks and Systems. Vol. 777. Springer, Cham. 2023. P. 71–80. DOI: 10.1007/978-3-031-43792-2_7.

TECHNIQUE FOR DETECTING NETWORK INTRUSIONS BASED ON THE INTEGRATION OF WAVELET ANALYSIS AND MATHEMATICAL STATISTICS METHODS

***Igor V. Kotenko**, Honored Scientist of the Russian Federation, Doctor of Technical Sciences, Professor, Chief Researcher and Head of the Laboratory of Computer Security Problems of the St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg, Russia. ORCID: 0000-0001-6859-7120.*
E-mail: ivkote@comsec.spb.ru

***Igor B. Saenko**, Dr. Sc. (Eng), Professor, Chief Researcher, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. ORCID: 0000-0002-9051-5272.*
E-mail: ibsaen@comsec.spb.ru

***Petr V. Bortniker**, Postgraduate Student, Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. ORCID: 0009-0008-1708-1480.*
E-mail: bort29@mail.ru

***Keywords:** computer attacks, intrusion detection, white noise, wavelet analysis, decomposition coefficients, distribution law, statistical hypothesis.*

Abstract

Purpose of work: consists in developing a method for detecting network intrusions based on the application of wavelet analysis methods and mathematical statistics, which allows for the timely detection of network intrusions.

Research methods: system analysis of the problem of detecting network intrusions, methods for evaluating data samples using statistical hypotheses, methods for detecting network intrusions based on the analysis of the energy spectrum of a signal reconstructed using wavelet decomposition coefficients.

Results of the study: models of statistical evaluation of wavelets selected for detection of network intrusions are proposed, in which the most preferable wavelet is selected based on the results of testing statistical hypotheses about the equality of average values, variances and distribution laws in the reference and noisy (subject to intrusions) samples of network traffic; the technique for detecting network intrusions based on the analysis of the energy spectrum of the signal reconstructed by the decomposition coefficients obtained using the most preferable wavelet is developed; an assessment of the sensitivity of detecting network intrusions by the method of spectral wavelet analysis in relation to the frequency range of the signal reconstructed by the wavelet decomposition coefficients is made.

References

1. Sheloukhin O.I., Rybakov S.Yu., Rakovsky D.I. Classification of computer attacks using a multifractal spectrum of fractal dimension. Cybersecurity Issues, 2024. No. 2 (60), pp. 107-119. DOI: 10.21681/2311-3456-2024-2-107-119.
2. Vidishcheva E.V., Kopyrin A.S., Vasilenko M.S. Analysis and refinement of the classification of anomalies and outliers in economic data. Bulletin of the Altai Academy of Economics and Law, 2019. No. 6-1, pp. 41-46.
3. Zolotarev A.I., Sidorkina I.G., Smirnov V.I. Analysis of hybrid intrusion detection algorithms. Bulletin of the Volga State Technological University. Series: Radio engineering and infocommunication systems, 2021. No. 2 (50), pp. 45-53. DOI: 10.25686/2306-2819.2021.2.45.
4. Kotenko I.V., Saenko I.B., Zakharchenko R.I., Velichko D.V. Subsystem for preventing computer attacks on critical information infrastructure objects: analysis of functioning and implementation. Issues of cybersecurity, 2023. No. 1(53), pp. 2–17. DOI: 10.21681/2311-3456-2023-1-13-27.
5. Kotenko I.V., Saenko I.B., Zakharchenko R.I., Velichko D.V. Dinamicheskaya model' kontrolya funkcionirovaniya dlya preduprezhdeniya komp'yuternyh atak. Pravovaya informatika, 2024. No. 2, pp. 35-43. DOI: 10.21681/1994-1404-2024-2-35-43.
6. Pavlychev A.V., Starodubov M.I., Galimov A.D. Using the Random Forest machine learning algorithm to detect complex computer incidents. Cybersecurity Issues, 2022. No. 5 (51), pp. 74-81. DOI: 10.21681/2311-3456-2022-5-74-81.
7. Guo T., Zhang T., Lim E., López-Benítez M., Ma F., Yu L. A Review of Wavelet Analysis and Its Applications: Challenges and Opportunities, IEEE Access, 2022, Vol. 10, pp. 58869-58903. DOI: 10.1109/ACCESS.2022.3179517.

8. Popov A.M., Sotnikov V.N. Probability Theory and Mathematical Statistics. Moscow: Yurait Publishing House, 2024, 425 p.
9. Sheloukhin O.I., Rakovsky D.I. Development of a hardware and software complex for modeling multi-valued computer attacks Cybersecurity Issues, 2024. No. 4 (62), pp. 116-130. DOI: 10.21681/2311-3456-2024-4-116-130.
10. Wang L., Zhang X. Anomaly detection for automated vehicles integrating continuous wavelet transform and convolutional neural network. Applied Sciences, 2023, Vol. 13, 5525. DOI: 10.3390/app1309552.
11. Bouzebda S., Ferfache A.A. Asymptotic properties of semiparametric M-estimators with multiple change points. Physica A: Statistical Mechanics and its Applications, 2023, Vol. 609, 128363. DOI: 10.1016/j.physa.2022.128363.
12. Krasov A.V., Gelfand A.M., Korzhik V.I., Kotenko I.V., Petriv R.B., Sakharov D.V., Ushakov I.A., Sharikov P.I., Yurkin D.V. Postroyeniye doverennoy vychislitelnoy sredy. Sankt-Peterburg: IP Petriv Roman Bogdanovich, 2019.
13. Kotenko I., Saenko I., Budko P., Vinogradenko A. Intelligent state assessment of complex autonomous objects based on wavelet analysis. Engineering Applications of Artificial Intelligence, 2023, Vol. 126, Art. 106869, pp.1-20. DOI: 10.1016/j.engappai.2023.106869.
14. Saenko I., Bortniker P., Lauta O., Zhdanova I., Vasiliev N. An approach to early computer network intrusion detection based on the wavelet transform energy spectra analysis. In International Conference on Intelligent Information Technologies for Industry. Cham: Springer Nature Switzerland, 2023, pp. 71–80. DOI: 10.1007/978-3-031-43792-2_7.