РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **230 293** (13) **U1**

(51) МПК
G06F 21/55 (2013.01)

(12) ОПИСАНИЕ ПОЛЕЗНОЙ МОДЕЛИ К ПАТЕНТУ

Статус: действует (последнее изменение статуса: 27.11.2024)
Пошлина: учтена за 5 год с 03.07.2028 по 02.07.2029. Установленный срок для уплаты пошлины за 6 год: с 03.07.2028 по 02.07.2029. При уплате пошлины за 6 год в дополнительный 6-месячный срок с 03.07.2029 по 02.01.2030 размер пошлины увеличивается на 50%.

(52) СПК
G06F 21/552 *(2024.08)*

(21)(22) Заявка: **2024118424, 02.07.2024**

(24) Дата начала отсчета срока действия патента:
02.07.2024

Дата регистрации:
26.11.2024

Приоритет(ы):
(22) Дата подачи заявки: **02.07.2024**

(45) Опубликовано: **26.11.2024** Бюл. № **33**

(56) Список документов, цитированных в отчете о поиске: **RU 183015 U1, 07.09.2018. CN 102664772 B, 04.03.2015. CN 102111312 A, 29.06.2011. WO 2019161768 A1, 29.08.2019. US 9843488 B2, 12.12.2017. RU 2546236 C2, 10.04.2015.**

Адрес для переписки:
190000, Санкт-Петербург, ул. Большая Морская, 67, лит. А, ФГАОУ ВО ГУАП, ЦКНИ

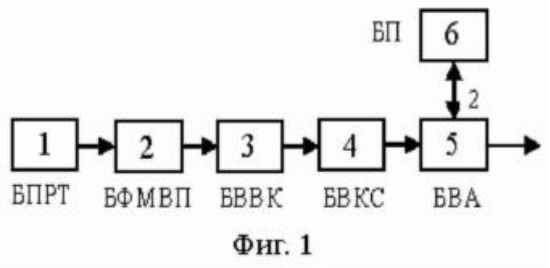
(72) Автор(ы):
Жданова Инна Михайловна (RU),
Дворников Сергей Сергеевич (RU),
Погорелов Андрей Анатольевич (RU),
Лапин Степан Павлович (RU),
Дворников Сергей Викторович (RU),
Лаута Олег Сергеевич (RU)

(73) Патентообладатель(и):
Федеральное государственное автономное образовательное учреждение высшего образования "Санкт-Петербургский государственный университет аэрокосмического приборостроения" (RU)

(54) Устройство обнаружения аномалий трафика

(57) Реферат:

Полезная модель относится к области информационных технологий, в частности к информационной безопасности, а именно к средствам обнаружения аномалий трафика для предотвращения несанкционированного доступа, контроля трафика и предотвращения сетевых атак. Техническим результатом полезной модели является повышение эффективности обработки сетевого трафика за счет идентификации структуры возникающих аномалий. Технический результат достигается за счет того, что устройство обнаружения аномалий трафика, включающее блок приема и разбора трафика, блок выявления аномалий, второй вход которого соединен с блоком памяти, дополнительно содержит последовательно соединенные блок формирования матрицы вейвлет-преобразования, блок выбора вейвлет-коэффициентов и блок вычисления коэффициентов сравнения, при этом вход блока формирования матрицы вейвлет-преобразования соединен с выходом блока приема и разбора трафика, а выход блока вычисления коэффициентов сравнения соединен с первым входом блока выявления аномалий, выход которого является выходом устройства.



Фиг. 1

Полезная модель относится к области информационных технологий, в частности к информационной безопасности, а именно к средствам обнаружения аномалий трафика для предотвращения несанкционированного доступа, контроля трафика и предотвращения сетевых атак.

Существующие подходы к обнаружению вторжений обычно делятся на две категории: обнаружение злоупотреблений и обнаружение аномалий.

Обнаружение злоупотреблений обычно основано на базе сигнатур, такой способ способен защитить только от известных угроз и не способен обеспечить защиту от неизвестных ранее атак.

Обнаружение аномалий основано на предварительном обучении и статистическом анализе для формирования образа нормального функционирования информационной системы. Его изменение считается проявлением аномального функционирования системы.

Указанные методы до сих пор остаются одними из самых эффективных для предотвращения вторжений. Однако метод, основанный на сигнатурах, способен определить угрозу только на основе известной уязвимости, но не могут обеспечить защиты от неизвестных атак. Метод, основанный на статистике, способен обнаружить ранее неизвестную атаку (атаку нулевого дня), но при этом высока вероятность неправильного принятого решения, особенно в период обучения.

Из уровня техники известно решение по патенту US 9253201 B2, опубл. 02.02.2016, где раскрыта система и способ для определения сетевых аномалий.

Согласно известному решению, система содержит процессор, который получает обучающий набор протокола передачи данных, имеющий ряд параметров, определение контента и структуры, связанных с каждым из ряда параметров, обучение вероятностной модели посредством использования определенных контента и структуры каждого ряда параметров, в которых величина и размер заданы для вероятностной модели, получение протокола передачи данных, имеющего ряд параметров, которые передаются от первого процессора ко второму процессору через компьютерную сеть, сравнение полученного протокола передачи данных с вероятностной моделью и определение, является ли сообщение протокола передачи данных аномальным.

Недостатком такой системы является отсутствие возможности идентификации аномалии в структуре трафика в виде последовательности повторяющихся битов.

Из уровня техники известно решение по патенту US 9525696 B2, опубл. 20.12.2016, в котором раскрыта система и способ для определения сетевых аномалий.

Согласно известному решению, средство обработки сетевого пакета для реализации политики безопасности содержит множество аппаратных модулей для обработки сетевого трафика для выявления различных угроз. При этом в качестве модулей обработки трафика используются такие модули как: модуль сигнатур, модуль выявления аномалий и модуль выявлениях сетевых атак. Каждый из модулей выполнен с возможностью пропуска идентифицированного пакета, соответствующего политике безопасности компании.

Недостатком такой системы является отсутствие возможности идентификации аномалии в структуре трафика в виде последовательности повторяющихся битов.

В качестве прототипа выбрано техническое решение, представленное в патенте на полезную модель «Средство обнаружения вторжений» (Патент РФ №183015, G06F 21/00 (2013.01), 07.09.2018, Бюл. №25.

Согласно прототипу, средство обнаружения вторжений для обработки сетевого трафика, содержит блок приема и разбора трафика (БПРТ), блок памяти (БП) и соединенные с ним блок выявления новых устройств, блок анализа зашифрованного трафика, блок сигнатур, блок выявления аномалий (БВА), блок защиты от сетевых атак, при этом блок приема и разбора трафика соединен с блоком выявления новых устройств, который в свою очередь соединен с блоком анализа зашифрованного трафика, а блок анализа зашифрованного трафика выполнен с возможностью идентифицирования протокола шифрования и основного протокола.

Недостатком прототипа является отсутствие возможности идентификации аномалии в структуре трафика в виде последовательности повторяющихся битов.

Задача полезной модели заключается в создании устройства обнаружения аномалий трафика, способного не только обнаруживать аномалии трафика в виде последовательности повторяющихся битов, но и идентифицировать ее структуру.

Техническим результатом полезной модели является повышение эффективности обработки сетевого трафика за счет идентификации структуры возникающих аномалий.

Технический результат достигается за счет того, что устройство обнаружения аномалий трафика, включающее блок приема и разбора трафика, блок выявления аномалий, второй вход которого соединен с блоком памяти, дополнительно содержит последовательно соединенные блок формирования матрицы вейвлет-преобразования, блок выбора вейвлет-коэффициентов и блок вычисления коэффициентов сравнения, при этом вход блока формирования матрицы вейвлет-преобразования соединен с выходом блок приема и разбора трафика, а выход блок вычисления коэффициентов сравнения соединен с первым входом блок выявления аномалий, выход которого является выходом устройства.

Полезная модель поясняется фигурами, на которых представлены:

фиг. 1 - блок-схема устройства обнаружения аномалий трафика;

фиг. 2 - матрица вейвлет-коэффициентов контрольного трафика;

фиг. 3 - матрица вейвлет-коэффициентов первого аномального трафика;

фиг. 4 - матрица вейвлет-коэффициентов второго аномального трафика;

фиг. 5 - вейвлет-коэффициенты третьего ряда матрицы контрольного трафика;

фиг. 6 - вейвлет-коэффициенты третьего ряда матрицы первого аномального трафика;

фиг. 7 - вейвлет-коэффициенты третьего ряда матрицы второго аномального трафика.

При этом на фиг. 1 введены следующие обозначения:

1 - блок приема и разбора трафика;

2 - блок формирования матрицы вейвлет-преобразования;

3 - блок выбора вейвлет-коэффициентов;

4 - блок вычисления коэффициентов сравнения;

5 - блок выявления аномалий;

6 - блок памяти.

Устройство обнаружения аномалий трафика содержит последовательно соединенные блок приема и разбора трафика 1, блок формирования матрицы вейвлет-преобразования 2, блок выбора вейвлет-коэффициентов 3, блок вычисления коэффициентов сравнения 4 и блок выявления аномалий 5, а также блок памяти 6, выход которого соединен со вторым входом блок выявления аномалий 5, выход которого является выходом устройства.

Блок 1 приема и разбора трафика предназначен для сбора сетевого трафика на канальном уровне, поступающего или из глобальной сети Интернет, или из локальной сети.

Реализация блока приема и разбора трафика 1 известна, см. «Средство обнаружения вторжений», Патент РФ на полезную модель №183015, G06F 21/00 (2013.01), 07.09.2018, Бюл. №25.

Блок 2 формирования матрицы вейвлет-преобразования предназначен для формирования из входного битового потока трехмерную матрицу его вейвлет-преобразования.

Реализация блока формирования матрицы вейвлет-преобразования 2 известна, см. «СПОСОБ РАСПОЗНАВАНИЯ РАДИОСИГНАЛОВ», Патент РФ №2423735, G06K 9/00 (2006.01), опубл. 10.07.2011, Бюл. №19.

Блок 3 выбора вейвлет-коэффициентов предназначен для выделения из матрицы вейвлет-преобразования вейвлет-коэффициентов путем их фильтрации вдоль оси масштабирования (на фиг. 2, 3 и 4 обозначены переменной m).

Реализация блок выбора вейвлет-коэффициентов 4 известна, см. «СПОСОБ РАСПОЗНАВАНИЯ РАДИОСИГНАЛОВ», Патент РФ №2423735, G06K 9/00 (2006.01), опубл. 10.07.2011, Бюл. №19.

Блок 4 вычисления коэффициентов сравнения предназначен для усреднения вейвлет-коэффициентов, выделенных посредством БВВК.

Возможность выполнения технических операций с вейвлет-коэффициентами известна, см. «СПОСОБ РАСПОЗНАВАНИЯ РАДИОСИГНАЛОВ», Патент РФ №2261476 C1, G06K 9/00, опубл. 27.09.2005.

Блок 5 блок выявления аномалий предназначен для выявления аномалий путем сравнения вычисленных значений усредненных вейвлет-коэффициентов, с предварительно рассчитанными значениями.

Реализация блока выявления аномалий 5 известна, см. «Средство обнаружения вторжений», Патент РФ на полезную модель №183015, G06F 21/00 (2013.01), 07.09.2018, Бюл. №25.

Блок 6 блок памяти предназначен для хранения предварительно рассчитанными значениями усредненных вейвлет-коэффициентов, соответствующих различным структурам возникающих аномалий в обрабатываемом трафике.

Реализация блок памяти 6 известна, см. «Средство обнаружения вторжений», Патент РФ на полезную модель №183015, G06F 21/00 (2013.01), 07.09.2018, Бюл. №25.

Устройство работает следующим образом.

Из блока приема и разбора трафика 1 поступает битовый поток, который подают в блок формирования матрицы вейвлет-преобразования 2, где формируется его матрица вейвлет преобразования. Далее, посредством блока выбора вейвлет-коэффициентов 3 выделяют вейвлет-коэффициенты путем их фильтрации вдоль оси масштабирования. Выбор конкретного значения m, для которого осуществляют фильтрацию вейвлет-коэффициентов, производят на предварительном этапе по результатам предварительного анализа трафика. Для этого осуществляют вейвлет-преобразование трафика со всеми возможными аномалиями. И затем выбирают те значения m, для которого вейвлет-коэффициенты для всех возможных аномалий обеспечивают наибольшие различия.

Затем выделенные вейвлет-коэффициенты усредняют в блок вычисления коэффициентов сравнения 4 и подают в блок выявления аномалий 5, где они сравниваются с предварительно рассчитанными значениями усредненных вейвлет-

коэффициентов, соответствующих различным структурам возникающих аномалий в обрабатываемом трафике, которые хранятся в блок памяти 6.

Идентификацию структуры возникающих аномалий осуществляют по результатам сравнения. Инцидентным считается выбор той структуры аномалии, для которой различия соответствующей ей предварительно рассчитанного значения и усредненного значения вейвлет-коэффициентов анализируемого трафика будет минимальными.

В качестве примера на фиг. 2 показана матрица, соответствующая контрольному трафику битов 1010101010101010. На фиг. 3 - аналогичная матрица первого аномального трафика 1011111010101010. На фиг. 4 - аналогичная матрица второго аномального трафика 1010101010111110. На фиг. 5, 6 и 7 показаны вейвлет-коэффициенты, полученные в БВВК. Очевидны их визуальные различия, которые подтверждаются значениями, рассчитанными в блоке вычисления коэффициентов сравнения 4. Для контрольного трафика значение усредненных вейвлет-коэффициентов равно 3. Для первого аномального трафика - 6, для второго аномального трафика - 2,5.

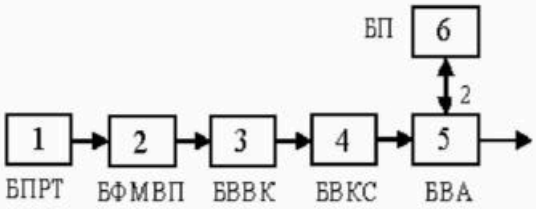
То есть различия усредненных значений вейвлет-коэффициентов позволяют однозначно идентифицировать первый и второй аномальные трафики.

При этом статистическая обработка первого и второго аномальных трафиков в виде расчета коэффициента корреляции дает одинаковые значения 0,775.

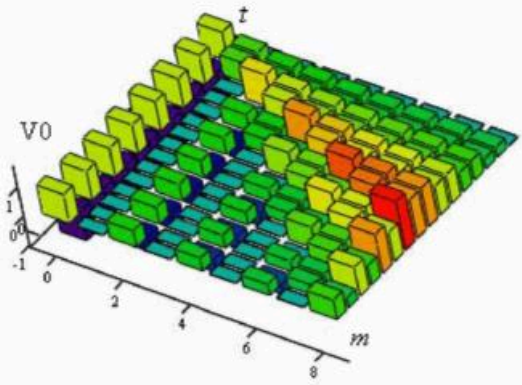
Результаты идентификации подтверждены на примере 200 различных структур аномалий, что указывает на достижение заявляемого технического результата полезной модели, а именно, повышение эффективности обработки сетевого трафика за счет идентификации структуры возникающих аномалий.

Формула полезной модели

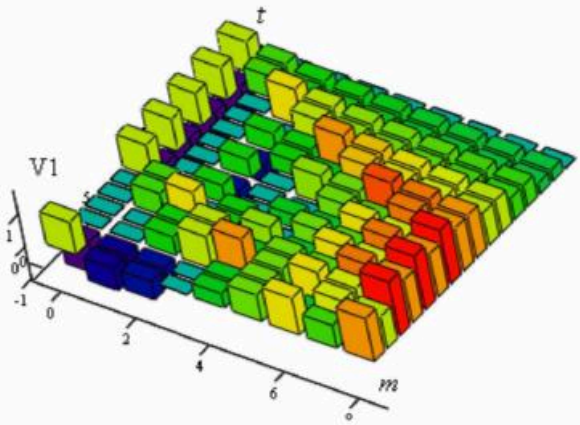
Устройство обнаружения аномалий трафика, включающее блок приема и разбора трафика, блок выявления аномалий, второй вход которого соединен с блоком памяти, отличающееся тем, что устройство дополнительно содержит последовательно соединенные блок формирования матрицы вейвлет-преобразования, блок выбора вейвлет-коэффициентов и блок вычисления коэффициентов сравнения, при этом вход блока формирования матрицы вейвлет-преобразования соединен с выходом блока приема и разбора трафика, а выход блока вычисления коэффициентов сравнения соединен с первым входом блока выявления аномалий, выход которого является выходом устройства.



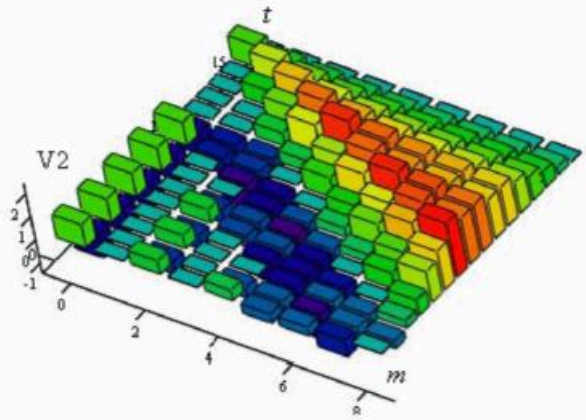
Фиг. 1



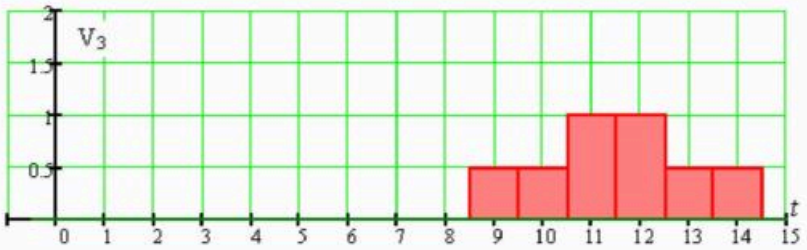
Фиг. 2



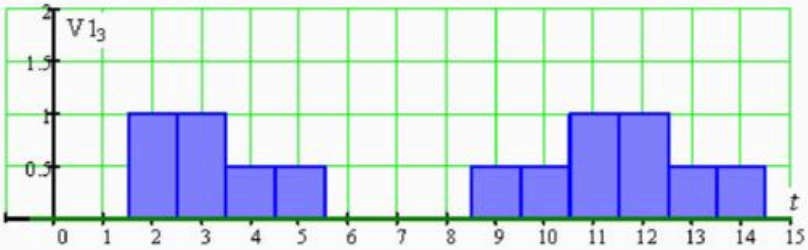
Фиг. 3



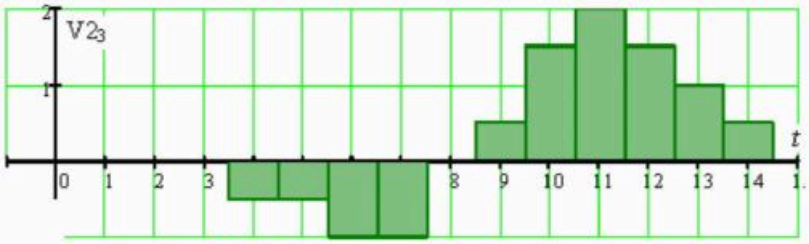
Фиг. 4



Фиг. 5



Фиг. 6



Фиг. 7