(19) Евразийское патентное ведомство

(21) 202392415 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2024.07.31

(22) Дата подачи заявки
2023.09.25

(51) Int. Cl. ***H04L 41/14*** (2022.01)
H04L 41/08 (2022.01)
G06F 18/23 (2023.01)
G06F 16/906 (2019.01)

(54) СПОСОБ И СИСТЕМА ФОРМИРОВАНИЯ КЛАСТЕРОВ УЗЛОВ В КОМПЬЮТЕРНОЙ СЕТИ

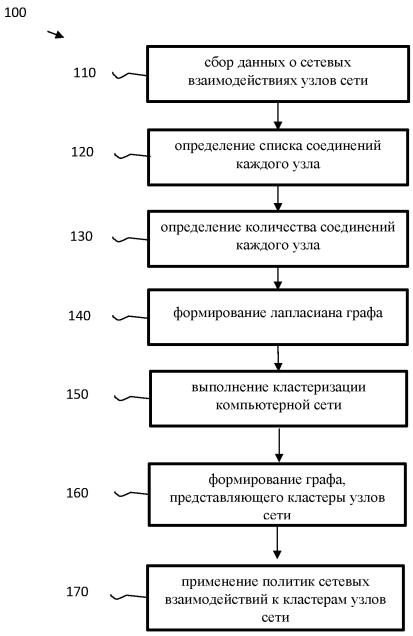
(31) **2023101335**
(32) **2023.01.23**
(33) **RU**

(71) Заявитель:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(72) Изобретатель:
Белый Алексей Владимирович, Жиров Дмитрий Викторович (RU)

(74) Представитель:
Герасин Б.В. (RU)

(57) Изобретение в общем относится к области сетей связи, а в частности к способу и системе кластеризации сети связи на основе данных сетевых взаимодействий. Техническим результатом является повышение безопасности сети за счет точности кластеризации узлов сети. Указанный технический результат достигается благодаря осуществлению способа формирования кластеров узлов в компьютерной сети, выполняющийся по меньшей мере одним вычислительным устройством, и содержащий этапы, на которых собирают данные о сетевых взаимодействиях всех узлов компьютерной сети за выбранный период времени, причем указанные данные содержат по меньшей мере локальные и удаленные IP-адреса и порты узлов; определяют список сетевых соединений каждого узла компьютерной сети; определяют на основе данных количество сетевых соединений каждого узла к сервисам путем построения матрицы смежности двудольного графа; формируют лапласиан графа на основе данных и определяют собственные значения и собственные вектора каждого узла; выполняют кластеризацию компьютерной сети на основе значений собственных векторов, причем процесс кластеризации продолжается до критерия останова; формируют граф, представляющий собой кластеры узлов компьютерной сети; применяют политики сетевых взаимодействий в соответствии с полученными кластерами узлов компьютерной сети.



202392415 A1

202392415 A1

МПК: H04L 41/00

СПОСОБ И СИСТЕМА ФОРМИРОВАНИЯ КЛАСТЕРОВ УЗЛОВ В КОМПЬЮТЕРНОЙ СЕТИ

ОБЛАСТЬ ТЕХНИКИ

[0001] Заявленное техническое решение в общем относится к области сетей связи, а в частности к способу и системе кластеризации сети связи на основе данных сетевых взаимодействий.

УРОВЕНЬ ТЕХНИКИ

[0002] В настоящее время в мире большое внимание уделяется области сетевой безопасности. Решения, направленные на обеспечение безопасности сетей, позволяют защитить как данные, в том числе критические, передающиеся внутри сети, так и обеспечить защиту от множества угроз и работоспособность сети в целом, что, соответственно, является неотъемлемой частью работоспособности любого современного предприятия или организации.

[0003] Одним из важных инструментов в управлении сетевыми взаимодействиями на предприятиях и организациях является установление политик сетевой безопасности. Политики сетевых взаимодействий позволяют выявлять как аномалии в поведении устройств сети, так и обеспечивать изоляцию определенных групп от других участников сети, например, для предотвращения утечки критических данных. Как правило, для формирования политик сетевых взаимодействий, требуется сформировать кластеры внутри сети, т.е. разбить все устройства сети на определенные группы, что является сложной и нетривиальной задачей. Точность и качество такого разбиения будет прямо влиять на безопасность сети.

[0004] Так, в известном уровне техники, для формирования кластеров в сети применяются подходы, основанные на кластеризации графа связей между хостами сети и интенсивности взаимодействий между хостами сети.

[0005] Недостатками такого подхода является низкая точность и эффективность кластеризации сети из-за невозможности определения кластеров в сети при заранее неизвестном количестве кластеров в этой сети. Кроме того, из-за построения кластеров только на основе взаимодействии хостов сети, сформированные группы могут включать узлы, фактически не относящиеся к указанной группе, что соответственно приводит к снижению безопасности сети.

[0006] Из уровня техники также известно решение, раскрытое в патенте США № US 7945668 B1 (NARUS INC), опубл. 17.05.2011. Указанное решение, в частности, раскрывает способ профилирования сетевой активности на основе кластеризации сети. Так, для профилирования сетевой активности, из собранных данных о сетевой активности формируется матрица ассоциаций и сокращенная матрица, на основе которой генерируются промежуточные кластеры, которые в последствии объединяются в совместные кластера в соответствии со степенью похожести объектов. По указанным кластерам выполняются сетевые операции.

[0007] Недостатком указанного решения является низкая точность непосредственно процесса кластеризации из-за разбиения промежуточных кластеров на основе метрики связности и дальнейшее объединение указанных кластеров в совместный по пороговому значению, что, соответственно, может привести к некорректному итоговому кластеру, и, как следствие не обеспечить требуемую безопасность сети.

[0008] Общими недостатками существующих решений является отсутствие эффективного способа кластеризации узлов сети, обеспечивающего точный процесс разбиения узлов на группы за счет дополнительных данных о сервисах, с которыми взаимодействуют хосты и интенсивности взаимодействия хостов и сервисов, что, соответственно, позволяет более эффективно формировать политики сетевой безопасности, выявлять аномалии в сетевых узлах и повышает защищенность сети и данных. Кроме того, такого рода решение, должно обеспечивать возможность определить заранее неизвестное количество кластеров в сети.

РАСКРЫТИЕ ИЗОБРЕТЕНИЯ

[0009] В заявленном техническом решении предлагается новый подход к формированию кластеров узлов в компьютерной сети. В данном решении используются данные о взаимодействии сервисов и хостов для формирования кластеров узлов, что соответственно повышает точность формирования таких кластеров и обеспечивает возможность применения сетевых операций к указанным кластерам.

[0010] Таким образом, решается техническая проблема обеспечения точности кластеризации узлов сети.

[0011] Техническим результатом, достигающимся при решении данной проблемы, является повышение безопасности сети за счет точности кластеризации узлов сети.

[0012] Указанный технический результат достигается благодаря осуществлению способа формирования кластеров узлов в компьютерной сети, выполняющийся по меньшей мере одним вычислительным устройством, и содержащий этапы, на которых:

a) собирают данные о сетевых взаимодействиях всех узлов компьютерной сети за выбранный период времени, причем указанные данные содержат по меньшей мере: локальные и удаленные IP-адреса и порты узлов;

b) определяют, на основе данных, полученных на этапе, a), список сетевых соединений каждого узла компьютерной сети;

c) определяют, на основе данных, полученных на этапе b), количество сетевых соединений каждого узла к сервисам путем построения матрицы смежности двудольного графа;

d) формируют лапласиан графа на основе данных, полученных на этапе c), и определяют собственные значения и собственные вектора каждого узла;

e) выполняют кластеризацию компьютерной сети на основе значений собственных векторов, полученных на этапе e), причем процесс кластеризации продолжается до критерия останова;

f) формируют граф, представляющий собой кластеры узлов компьютерной сети;

g) применяют политики сетевых взаимодействий в соответствии с полученными кластерами узлов компьютерной сети.

[0013] В одном из частных вариантов реализации сервисы представляют собой по меньшей мере одно из: приложение, база данных, программное средство, запущенное на узле.

[0014] В другом частном варианте реализации политики сетевых взаимодействий представляют собой, по меньшей мере, одно из следующего:

a) ограничение сетевых взаимодействий между кластерами узлов;

b) ограничение сетевых взаимодействий между определенными кластерами узлов;

c) обеспечение сетевого взаимодействия узлов сети внутри кластера;

d) ограничение аномальных сетевых взаимодействий определенных узлов сети.

[0015] Кроме того, заявленные технические результаты достигаются за счет системы формирования кластеров узлов, содержащей:

по меньшей мере один процессор;

по меньшей мере одну память, соединенную с процессором, которая содержит машиночитаемые инструкции, которые при их выполнении по меньшей мере одним процессором обеспечивают выполнение способа формирования кластеров узлов в компьютерной сети.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0016] Признаки и преимущества настоящего изобретения станут очевидными из приводимого ниже подробного описания изобретения и прилагаемых чертежей.

[0017] Фиг. 1 иллюстрирует блок-схему выполнения заявленного способа.

[0018] Фиг. 2 иллюстрирует интенсивность взаимодействия хостов и сервисов в компьютерной сети.

[0019] Фиг. 3 иллюстрирует результат кластеризации сети.

[0020] Фиг. 4 иллюстрирует пример общего вида вычислительной системы, которая обеспечивает реализацию заявленного решения.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

[0021] Заявленное техническое решение предлагает новый подход, обеспечивающий повышение точности кластеризации узлов сети, что, как следствие, обеспечивает более гибкое и эффективное управление политиками сетевой безопасности, а также повышает защищенность сети в целом. Кроме того, указанное техническое решение обеспечивает возможность выявления аномальных узлов на основе сформированных кластеров.

[0022] Техническое решение может быть реализовано в виде распределенной компьютерной системы.

[0023] В данном решении под системой подразумевается компьютерная система, ЭВМ (электронно-вычислительная машина), ЧПУ (числовое программное управление), ПЛК (программируемый логический контроллер), компьютеризированные системы управления и любые другие устройства, способные выполнять заданную, чётко определённую последовательность вычислительных операций (действий, инструкций).

[0024] Под устройством обработки команд подразумевается электронный блок либо интегральная схема (микропроцессор), исполняющая машинные инструкции (программы).

[0025] Устройство обработки команд считывает и выполняет машинные инструкции (программы) с одного или более устройства хранения данных, например таких устройств, как оперативно запоминающие устройства (ОЗУ) и/или постоянные запоминающие устройства (ПЗУ). В качестве ПЗУ могут выступать, но, не ограничиваясь, жесткие диски (HDD), флэш-память, твердотельные накопители (SSD), оптические носители данных (CD, DVD, BD, MD и т.п.) и др.

[0026] Программа — последовательность инструкций, предназначенных для исполнения устройством управления вычислительной машины или устройством обработки команд.

[0027] Термин «инструкции», используемый в этой заявке, может относиться, в общем, к программным инструкциям или программным командам, которые написаны на заданном языке программирования для осуществления конкретной функции, такой как, например, получение артефактов программно-аппаратного решения, формирование цифрового стандарта программно-аппаратного решения, формирование результатов проверки программно-аппаратного решения, анализ данных и т. п. Инструкции могут быть осуществлены множеством способов, включающих в себя, например, объектно-ориентированные методы. Например, инструкции могут быть реализованы, посредством языка программирования C++, Java, Python, различных библиотек (например, MFC; Microsoft Foundation Classes) и т. д. Инструкции, осуществляющие процессы, описанные в этом решении, могут передаваться как по проводным, так и по беспроводным каналам передачи данных, например Wi-Fi, Bluetooth, USB, WLAN, LAN и т. п.

[0028] На **Фиг. 1** представлена блок схема способа **100** формирования кластеров узлов в компьютерной сети, который раскрыт поэтапно более подробно ниже. Указанный способ **100** заключается в выполнении этапов, направленных на обработку различных цифровых данных. Обработка, как правило, выполняется с помощью системы, например, системы **400**, которая может представлять, например, сервер, компьютер, мобильное устройство, вычислительное устройство и т. д. Более подробно элементы системы **400** раскрыты на **Фиг. 4**

[0029] На этапе **110** собирают данные о сетевых взаимодействиях всех узлов компьютерной сети за выбранный период времени, причем указанные данные содержат по меньшей мере: локальные и удаленные IP-адреса и порты узлов.

[0030] На указанном этапе **110** выполняется сбор данных о сетевой активности каждого узла сети. Узел сети может представлять собой вычислительное устройство, подключенное к вычислительной сети предприятия. Вычислительным устройством может являться, например, сервер, персональный компьютер, планшет, периферийное устройство, подключенное к сети и т.д. Вычислительная сеть может являться локальной вычислительной сетью предприятия, корпоративной сетью и т.д. Под предприятием может пониматься, любая организация, компания, фирма и т.д., обладающая структурной сетью связи. Так, сетевую активность узлов могут получать с помощью анализаторов сетевого трафика. Анализаторы сетевого трафика представляют собой программно-аппаратные средства для перехвата и анализа сетевого трафика сети. Кроме того, в качестве агента, выполняющего сбор сетевой активности на предприятии может быть использовано непосредственно оборудование сети, например, маршрутизаторы сети. Также, могут применяться и другие средства получения сетевой активности, например, протокол Netflow

от компании Cisco, Hadoop и т.д. Собираемые данные о сетевой активности сохраняются в системе, такой как система **400**, в виде логов журнала, например, parquet-файлов кластера Hadoop. Так, в одном варианте осуществления, данные о сетевой активности хранятся в неструктурированном виде и извлекаются посредством регулярных выражений. Указанная активность может собираться в определенные периоды времени, например, раз в час и содержать в себе информацию о потоках сетевого взаимодействия, включая следующие поля: локальный IP-адрес устройства сети, локальный порт, удаленный IP-адрес, удаленный порт, состояние соединения, дата и время соединения, тип протокола, имя хоста и т.д. Под хостом в данном решении следует понимать любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах. Так хостом может являться сервер, компьютер, подключенный к сети связи и т.д.

[0031] На этапе **120** определяют, на основе данных, полученных на этапе **110**, список сетевых соединений каждого узла компьютерной сети. На основе данных о сетевых взаимодействиях, содержащих по меньшей мере локальные и удаленные IP-адреса и порты узлов сети, отфильтровываются записи, в которых локальный IP адрес и удаленный IP адрес равны 127.0.0.1 или 0.0.0.0, что означает взаимодействие хоста исключительно внутри своего домена. Указанная фильтрация необходима, в частотности, для исключения данных о сетевых взаимодействиях внутренних процессов хоста, т.е. данных, не относящихся к процессу кластеризации. Отфильтрованный набор данных разделяется на два поля, содержащие данные о взаимодействиях каждого хоста и данные о взаимодействиях с сервисами. В данном решении под сервисами следует понимать любое программное средство и/или приложение, запущенное на хосте, к которому осуществлялось обращение. Так, сервисом может являться база данных, приложение совместной работы, приложение видеоконференции и т.д.

[0032] На этапе **130** определяют, на основе данных, полученных на этапе **120**, количество сетевых соединений каждого узла к сервисам путем построения матрицы смежности двудольного графа.

[0033] На **фиг. 2** раскрыт пример двудольного графа. Указанный граф отображает все взаимодействия хостов (круги) с сервисами (квадраты) в компьютерной сети. Т.к. граф — это структура данных, которая представляет собой сеть со связями внутри, то для обеспечения возможности определения всех связей между узлами сети, на этапе **130** строится граф. Указанный граф может быть сформирован в системе управления безопасностью и отображен, посредством интерфейсов ввода/вывода. Для формирования указанного графа, характеризующего интенсивность взаимодействия узлов в сети, на

указанном этапе **130**, из двух полей данных о сетевых взаимодействиях, полученных на этапе **120,** формируют прямоугольную матрицу, в которой в строках идут все встречающиеся значения сервисов, а в столбцах все встречающиеся значения хостов. На основе указанной матрицы формируется матрица смежности двудольного графа. Она является квадратной, состоящей из четырёх блоков: два квадратных блока по главной диагонали и два прямоугольных блока – над главной диагональю, под диагональю. Размер матрицы равен количеству хостов и сервисов. В ячейках матрицы получается количество сетевых соединений от хоста к сервису за рассматриваемый период. В указанной матрице смежности, индексы строк и столбцов представляют узлы, а записи представляют отсутствие или наличие ребра между узлами. Веса на рёбрах могут представлять интенсивность взаимодействий, между соединёнными ими хостами.

[0034] Указанную матрицу сохраняют в память системы **200**. На основе указанной матрицы формируется двудольный граф. Таким образом, на указанном этапе **130** формируется количество сетевых взаимодействий каждого хоста с сервисами, т.е. обеспечивается возможность определения общего количества хостов и общего количества сервисов, а также интенсивность их взаимодействий.

[0035] Далее на основе полученных данных выполняется процесс кластеризации сети. В одном частном варианте осуществления кластеризация узлов сети выполняется с помощью алгоритма спектральной кластеризации. Более подробно алгоритм спектральной кластеризации раскрыт на этапах **140-160.**

[0036] Алгоритм спектральной кластеризации обеспечивает возможность выделения кластеров в компьютерных сетях на основе взаимодействий, происходящих в этих сетях.

[0037] На этапе **140** формируют лапласиан графа на основе данных, полученных на этапе **130**, и определяют собственные значения и собственные вектора каждого узла.

[0038] Важно понимать концепцию собственных значений и собственных векторов матриц. Для квадратной матрицы A, если существует ненулевой вектор x и некоторый скаляр λ, такие, что $Ax = \lambda x$, то x называется собственным вектором матрицы A с соответствующим собственным значением λ. Матрица A, по сути, является функцией, которая отображает векторы в новые векторы. Большинство векторов поменяются совершенно произвольным образом, когда к ним будет применен A, но собственные векторы меняются только по величине. Собственный вектор масштабируется в соответствии с собственным значением λ. Собственные векторы помогают описать динамику систем, представленных матрицами, а именно динамику сети связи. Указанные собственные вектора необходимы для реализации алгоритма спектральной кластеризации.

[0039] Так, на указанном этапе **140** находятся собственные значения и собственные вектора матрицы. Указанные собственные вектора отражают данные о принадлежности узла к кластеру. Так как матрица симметричная относительно главной диагонали и состоит из вещественных чисел, все собственные числа являются неотрицательными вещественными числами. А собственные вектора состоят из вещественных чисел. Далее рассматриваются собственные значения в порядке возрастания и соответствующие им собственные векторы. При этом первое собственное значение матрицы всегда равно 0 (по построению матрицы, степень каждой вершины равна сумме по строке и по столбцу матрицы смежности графа). В общем случае число нулевых собственных чисел равно количеству компонент связности графа. Так, нулевые собственные значения представляют компоненты связности, соответственно, собственные значения около нуля говорят нам, что существует разделение двух компонентов. Так, например, при наличии четырех собственных значений перед разрывом, будет означать, что существует четыре кластера. Векторы, связанные с первыми тремя положительными собственными значениями, должны дать нам информацию о том, какие три разреза необходимо сделать на графике, чтобы назначить каждый узел одному из четырех приближенных компонентов.

[0040] Таким образом, определение собственных значений обеспечивает возможность определения количества кластеров в сети. Следовательно, на указанном этапе 140 получают данные о количестве кластеров в сети.

[0041] На этапе **150** выполняют кластеризацию компьютерной сети на основе значений собственных векторов, полученных на этапе **140**, причем процесс кластеризации продолжается до критерия останова.

[0042] Для непосредственного определения количества кластеров в сети и принадлежности каждого узла к определенному кластеру, рассматриваются в цикле собственные вектора, начиная со второго. Смотрятся знаки чисел, входящих в собственный вектор. Если больше нуля, то соответствующая вершина графа относится к одному кластеру, если меньше нуля, к другому. Если значение близко к нулю, то такие вершины относятся или к первому, или ко второму кластеру или выделяются в отдельный кластер (плохо различимые вершины). Рассмотрение каждого последующего собственного вектора даст разбиение уже полученных кластеров на более мелкие части. Эмпирически подобранный критерий останова позволяет рассматривать собственные вектора, соответствующие собственным числам меньше 1. Обычно это 4-10 собственных векторов. Далее в спектре матрицы встречаются несколько десятков или сотен собственных чисел, равных 1. Если рассматривать разбиения, используя соответствующие собственные вектора, то получающиеся разбиения не затрагивают разбиения хостов на кластеры, но

делают всё более детальные разбиения сервисов. Благодаря указанной особенности обеспечивается возможность точного разбиения узлов на кластеры сети. При этом, стоит отметить, что также сокращается время и требуемые затрачиваемые вычислительные ресурсы, т.к. в известных из уровня техники алгоритмах рассматриваются все вектора, что приводит к неточному разбиению узлов на кластеры.

[0043] На этапе **160** формируют граф, представляющий собой кластеры узлов компьютерной сети;

[0044] На основе данных, полученных на этапе **150**, выполняется формирование графа, представляющего собой кластеры узлов. Так, указанный процесс может выполняться в системе **400.** Результат формирования графа может быть представлен администратору сети, например, в графическом интерфейсе.

[0045] Так, **фиг. 3** раскрывает результат кластеризации узлов сети предприятия, полученный в ходе создания указанного технического решения. Квадратами отмечены сервисы, а кругами – хосты. Указанный граф отражает фактическую структуру предприятия. Для формирования графа производилась симуляция физического взаимодействия вершин графа (вершины, принадлежащие к одному кластеру, притягиваются до определенного расстояния, вершины, принадлежащие различным кластерам, отталкиваются, вдоль рёбер действуют силы притяжения подобно растянутым резинкам).

[0046] На этапе **170** применяют политики сетевых взаимодействий в соответствии с полученными кластерами узлов компьютерной сети.

[0047] На указанном этапе **170**, к кластеризованной сети предприятия применяются политики сетевой безопасности в соответствии с установленными требованиями.

[0048] Так, политики сетевых взаимодействий представляют собой, по меньшей мере, одно из следующего: ограничение сетевых взаимодействий между кластерами узлов; ограничение сетевых взаимодействий между определенными кластерами узлов; обеспечение сетевого взаимодействия узлов сети внутри кластера; ограничение аномальных сетевых взаимодействий определенных узлов сети.

[0049] Так как сеть предприятия может обладать большим количеством хостов и сервисов, индивидуальное применение политики безопасности к каждому узлу является невыполнимой задачей. Указанный способ **100** благодаря реализации алгоритма кластеризации обеспечивает возможность эффективного управления безопасностью сети, а за счет точности алгоритма, достигнутой в указанном решении, также повышается защита сети в целом, т.к. политика сетевой безопасности устанавливается на релевантном кластере.

[0050] Так, продолжая рассмотрение этапа **170**, данные о кластеризации сети, полученные на этапе **160**, могут сравниваться с данными о кластерах, содержащимися в учётной системе, например, системе безопасности предприятия. Так, в указанной системе безопасности может содержаться, например, в базе данных, сведения о принадлежности узлов к определенному кластеру. Как упоминалось выше, кластером может являться группа узлов компьютерной сети, например, департамент, отдел и т.д. По результатам сравнения фактической и заданной структуры обнаруживаются аномалии, когда фактические и учётные кластера совпадают, допустим, на 80-90 процентов, а 10-20 процентов хостов попадают в другие кластера (собственно составляют аномалии). Такие случаи характеризуют нетипичное поведение узла в сети, например, обращение в базы данных, не использующихся в его кластере, что соответственно может указывать на аномальное поведение. К выявленным аномальным узлам далее могут быть применены меры безопасности, например, автоматическая временная блокировка, ограничение сетевых взаимодействий и т.д.

[0051] Кроме того, в еще одном частном варианте осуществления, по результатам определенных кластеров сети (этап **160**), система безопасности может автоматически применять сетевые политики, например, разрешающие сетевые взаимодействия внутри кластеров, и ограничивающие сетевые взаимодействия между кластерами. Для специалиста в данной области техники очевидно, что ограничения могут зависеть от степени критичности данных, обмениваемых каждым кластером. Так, например, кластеру, относящемуся к отделу, имеющему доступ к банковским тайнам, может быть ограничен обмен данными только внутри сети предприятия. В еще одном примере, отделу по связям с общественностью может быть применена политика, разрешающая использование сети Интернет, однако запрещающая скачивание файлов.

[0052] Таким образом, в приведенных материалах заявленного технического решения раскрывается эффективный и точный способ кластеризации сети связи предприятия для установления политик сетевой безопасности, обеспечивающий повышение безопасности сети за счет возможности установления групповых политик и выявления аномалий на основе точной кластеризации сети. Кроме того, как следует из приведенных материалов заявки, указанный способ кластеризации сети связи может являться частью способа ограничения сетевых взаимодействий на предприятии, т.е. защиты сети связи с помощью установления политик сетевой безопасности и/или выявления аномальных узлов в указанной сети связи.

[0053] На **Фиг. 4** представлен пример общего вида вычислительной системы **400**, которая обеспечивает реализацию заявленного способа или является частью компьютерной

системы, например, сервером, персональным компьютером, частью вычислительного кластера, обрабатывающим необходимые данные для осуществления заявленного технического решения.

[0054] В общем случае система **400** содержит такие компоненты, как: один или более процессоров **401**, по меньшей мере одну память **402**, средство хранения данных **403**, интерфейсы ввода/вывода **404**, средство В/В **405**, средство сетевого взаимодействия **406**, которые объединяются посредством универсальной шины.

[0055] Процессор **401** выполняет основные вычислительные операции, необходимые для обработки данных при выполнении способа **100**. Процессор **401** исполняет необходимые машиночитаемые команды, содержащиеся в оперативной памяти **402**.

[0056] Память **402**, как правило, выполнена в виде ОЗУ и содержит необходимую программную логику, обеспечивающую требуемый функционал.

[0057] Средство хранения данных **403** может выполняться в виде HDD, SSD дисков, рейд массива, флэш-памяти, оптических накопителей информации (CD, DVD, MD, Blue-Ray дисков) и т. п. Средства **403** позволяют выполнять долгосрочное хранение различного вида информации, например, данные о сетевой активности узлов и т. п.

[0058] Для организации работы компонентов системы **400** и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В **404**. Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь: PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т. п.

[0059] Выбор интерфейсов **404** зависит от конкретного исполнения системы **400**, которая может быть реализована на базе широко класса устройств, например, персональный компьютер, мейнфрейм, ноутбук, серверный кластер, тонкий клиент, смартфон, сервер и т. п.

[0060] В качестве средств В/В данных **405** может использоваться: клавиатура, джойстик, дисплей (сенсорный дисплей), монитор, сенсорный дисплей, тачпад, манипулятор мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т. п.

[0061] Средства сетевого взаимодействия **406** выбираются из устройств, обеспечивающий сетевой прием и передачу данных, например, Ethernet карту, WLAN/Wi-Fi модуль, Bluetooth модуль, BLE модуль, NFC модуль, IrDa, RFID модуль, GSM модем и

т. п. С помощью средств **405** обеспечивается организация обмена данными между, например, системой **400**, представленной в виде сервера и вычислительным устройством пользователя, на котором могут отображаться полученные данные (кластеризация узлов сети) по проводному или беспроводному каналу передачи данных, например, WAN, PAN, ЛВС (LAN), Интранет, Интернет, WLAN, WMAN или GSM.

[0062] Конкретный выбор элементов устройства **400** для реализации различных программно-аппаратных архитектурных решений может варьироваться с сохранением обеспечиваемого требуемого функционала.

[0063] Представленные материалы заявки раскрывают предпочтительные примеры реализации технического решения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области техники. Таким образом, объем настоящего технического решения ограничен только объемом прилагаемой формулы.

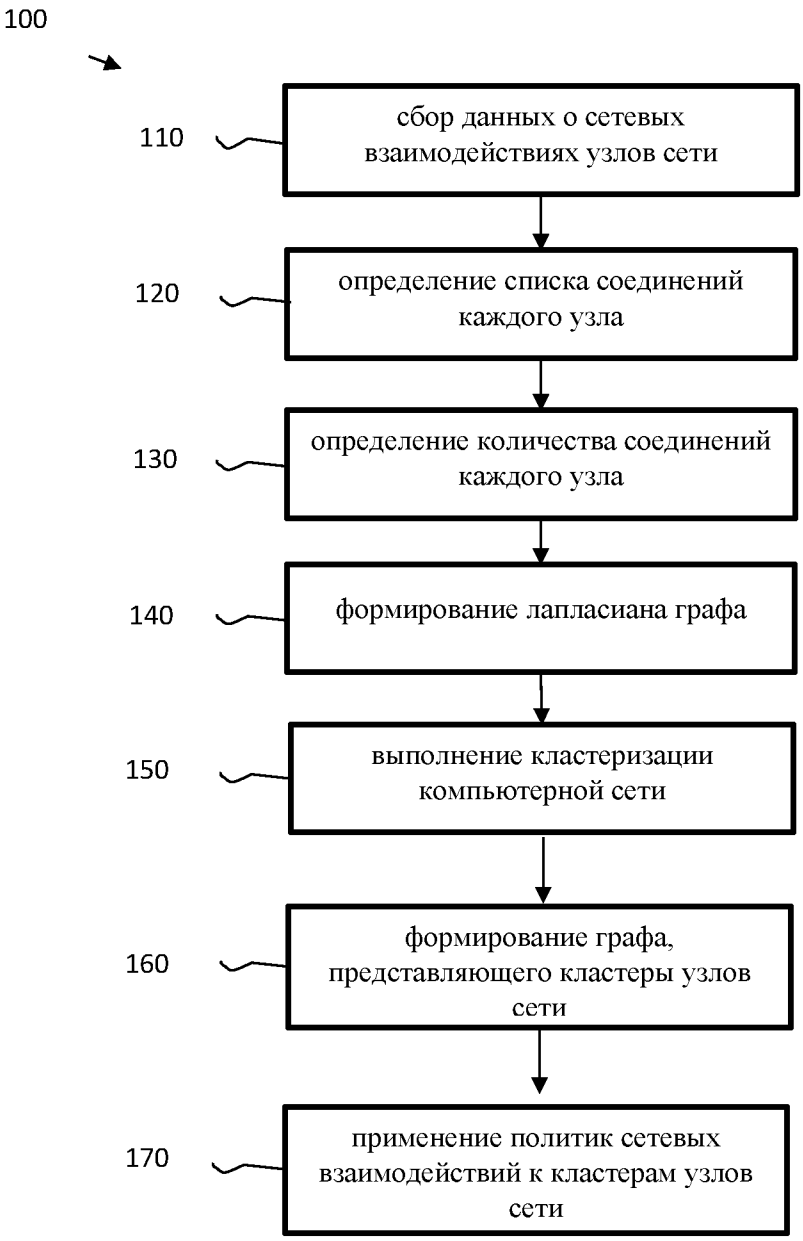
ФОРМУЛА

1. Способ формирования кластеров узлов в компьютерной сети, выполняющийся по меньшей мере одним вычислительным устройством, и содержащий этапы, на которых:
    a) собирают данные о сетевых взаимодействиях всех узлов компьютерной сети за выбранный период времени, причем указанные данные содержат по меньшей мере: локальные и удаленные IP-адреса и порты узлов;
    b) определяют, на основе данных, полученных на этапе, a), список сетевых соединений каждого узла компьютерной сети;
    c) определяют, на основе данных, полученных на этапе b), количество сетевых соединений каждого узла к сервисам путем построения матрицы смежности двудольного графа;
    d) формируют лапласиан графа на основе данных, полученных на этапе c), и определяют собственные значения и собственные вектора каждого узла;
    e) выполняют кластеризацию компьютерной сети на основе значений собственных векторов, полученных на этапе e), причем процесс кластеризации продолжается до критерия останова;
    f) формируют граф, представляющий собой кластеры узлов компьютерной сети;
    g) применяют политики сетевых взаимодействий в соответствии с полученными кластерами узлов компьютерной сети.
2. Способ по п. 1, характеризующийся тем, что сервисы представляют собой по меньшей мере одно из: приложение, база данных, программное средство, запущенное на узле.
3. Способ по п. 1, характеризующийся тем, что политики сетевых взаимодействий представляют собой, по меньшей мере, одно из следующего:
    a) ограничение сетевых взаимодействий между кластерами узлов;
    b) ограничение сетевых взаимодействий между определенными кластерами узлов;
    c) обеспечение сетевого взаимодействия узлов сети внутри кластера;
    d) ограничение аномальных сетевых взаимодействий определенных узлов сети.
4. Система формирования кластеров узлов в компьютерной сети, содержащая:

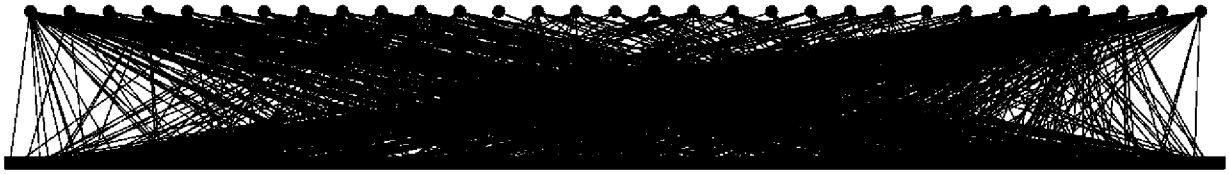
    по меньшей мере один процессор;

    по меньшей мере одну память, соединенную с процессором, которая содержит машиночитаемые инструкции, которые при их выполнении по меньшей мере одним процессором обеспечивают выполнение способа по любому из пп. 1-3.

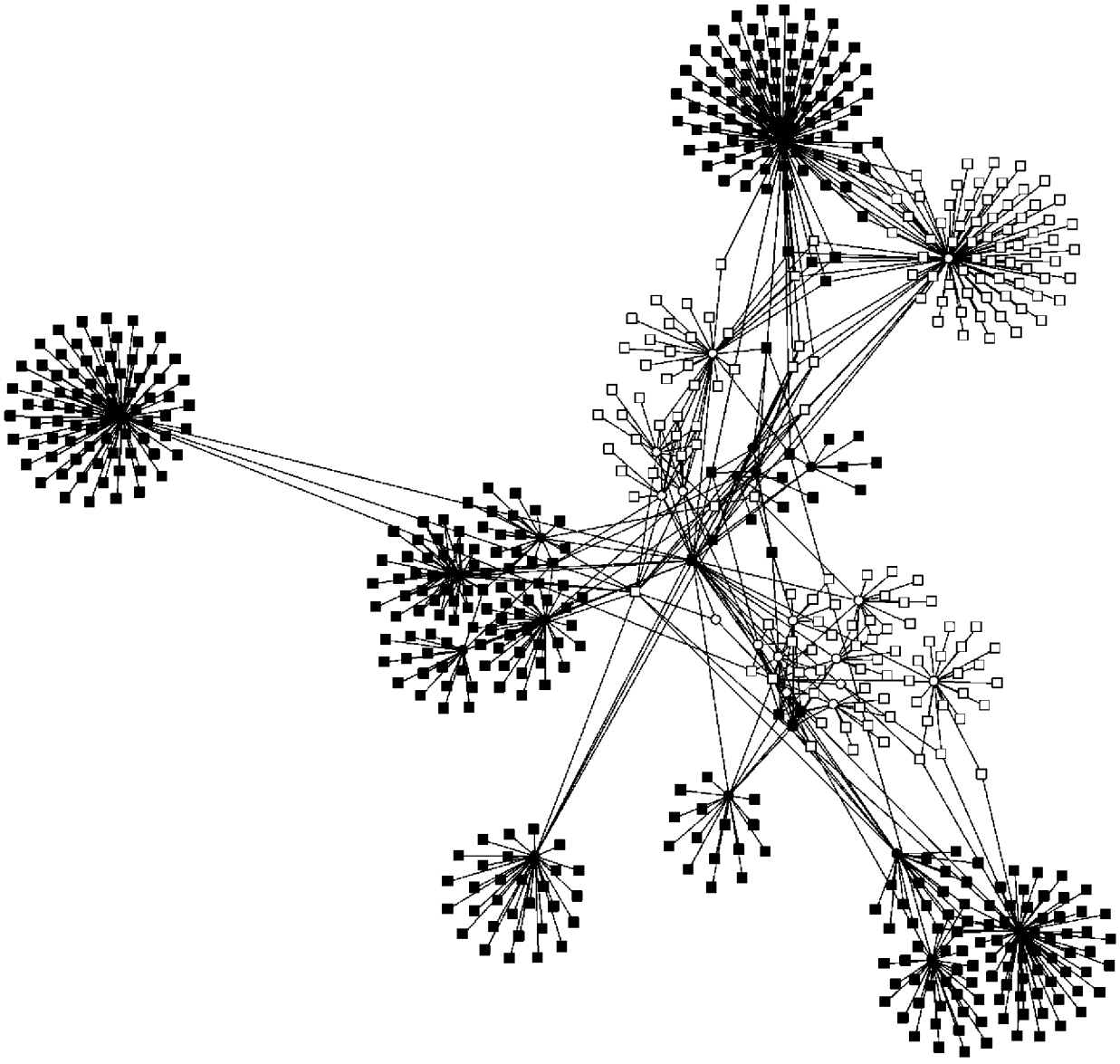
ЧЕРТЕЖИ К ОПИСАНИЮ



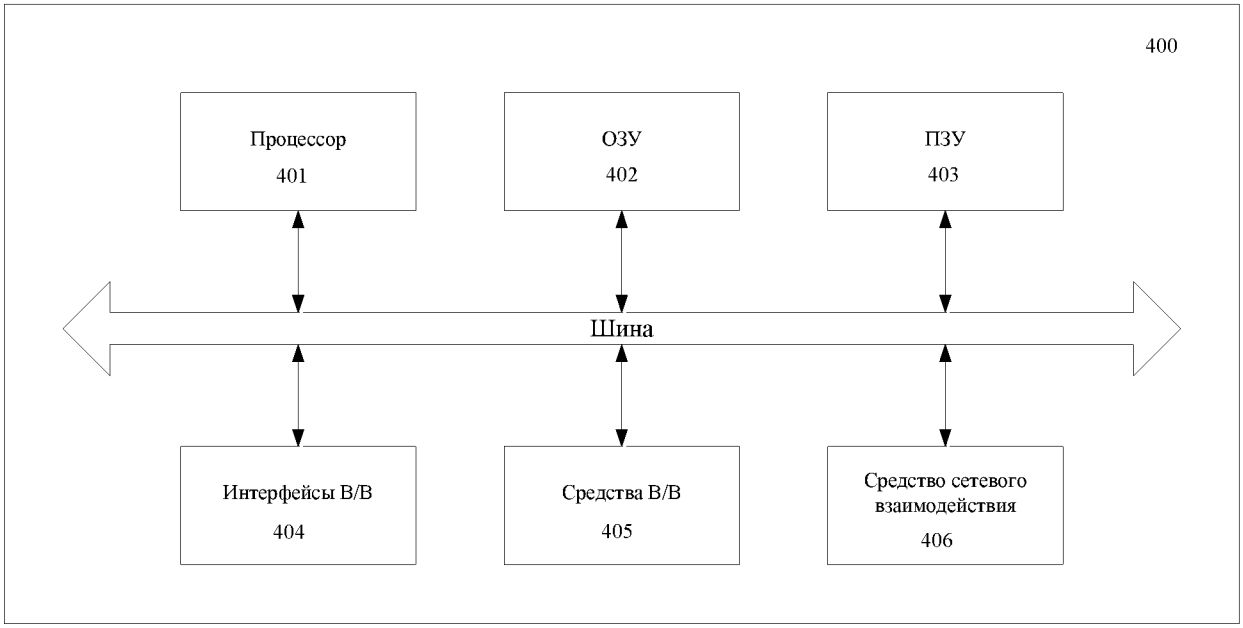
Фиг. 1



Фиг. 2



Фиг. 3


400
Процессор
401
ОЗУ
402
ПЗУ
403
Шина
Интерфейсы В/В
404
Средства В/В
405
Средство сетевого взаимодействия
406

Фиг. 4

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ

(статья 15(3) ЕАПК и правило 42 Патентной инструкции к ЕАПК)

Номер евразийской заявки:

202392415

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:

См. дополнительный лист

Б. ОБЛАСТЬ ПОИСКА:

Электронная база данных, использовавшаяся при поиске (название базы и, если возможно, используемые поисковые термины)

Espacenet, EAPATIS, Google

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
X	US 11178011 B1 (MICRO FOCUS LLC) 2021-11-16 Реферат, фиг.1-4, столбец 4, строки 44 - 55, столбец 3, строка 65 – столбец 4, строка 23, столбец 5, строки 8 - 18, столбец 7, строка 53 - столбец 8, строка 54	1-4
A	US 10833942 B2 (SPLUNK INC.) 2020-11-10 Реферат, формула, фиг. 13-16	1-4
A	US 11451971 B2 (HUAWEI TECHNOLOGIES CO., LTD.) 2022-09-20 Реферат, формула, столбец 17, строки 9-21, столбец 3, строка 55 - столбец 4, строка 60	1-4
A	US 10938654 B2 (VERIZON PATENT AND LICENSING INC.) 2021-03-02 Весь документ	1-4

☐ последующие документы указаны в продолжении графы

* Особые категории ссылочных документов:
«A» - документ, определяющий общий уровень техники
«D» - документ, приведенный в евразийской заявке
«E» - более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее
«O» - документ, относящийся к устному раскрытию, экспонированию и т.д.
"P" - документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета"

«T» - более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения
«X» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности
«Y» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории
«&» - документ, являющийся патентом-аналогом
«L» - документ, приведенный в других целях

Дата проведения патентного поиска: 11 июня 2024 (11.06.2024)

Документ подписан электронной подписью
Сертификат: 1711998581100
Владелец: CN=Аверкиев С.
Действителен: 01.04.2024-01.04.2025

Уполномоченное лицо:
Начальник Управления экспертизы С.Е. Аверкиев

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ
(дополнительный лист)

Номер евразийской заявки:

202392415

КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ (продолжение графы А)

МПК:

H04L41/14	(2022.01)
H04L41/08	(2022.01)
G06F18/23	(2023.01)
G06F 16/906	(2019.01)

СПК:

H04L 41/14
H04L 41/08
G06F 18/23
G06F16/9024
G06F 16/906