(19) Евразийское патентное ведомство

(11) 036842 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2020.12.25

(21) Номер заявки
201790324

(22) Дата подачи заявки
2015.09.02

(51) Int. Cl. ***H04L 29/06*** (2006.01)
H04L 12/715 (2013.01)

(54) УСТРОЙСТВО И СПОСОБ ДЛЯ УПРАВЛЕНИЯ КОНФИГУРАЦИЕЙ СЕТИ СВЯЗИ

(31) **10 2014 217 944.0; 10 2015 107 073.1**
(32) **2014.09.08; 2015.05.06**
(33) **DE**
(43) **2017.08.31**
(86) **PCT/EP2015/070057**
(87) **WO 2016/037917 2016.03.17**

(71)(73) Заявитель и патентовладелец:
РАЙНМЕТАЛЛ ДЕФЕНС ЭЛЕКТРОНИКС ГМБХ (DE)

(72) Изобретатель:
Штемайер Хенрих (DE)

(74) Представитель:
Поликарпов А.В., Соколова М.В., Путинцев А.И., Черкас Д.А., Игнатьев А.В. (RU)

(56) ZHOU HAIFENG ET AL: "Evolving defense mechanism for future network security", IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER, PISCATAWAY, US, vol. 53, no. 4, 8 April 2015 (2015-04-08), pages 45-51, XP011577593, ISSN: 0163-6804, DOI: 10.1109/MCOM.2015.7081074 [retrieved on 2015-04-06] Seite 45, rechte Spalte, Abschnitt "INTRODUCTION", Seite 47, linke Spalte, zweiter Absatz, Seite 47, Abschnitt "NETWORK CONFIGURATION VARIATION"

KAMPANAKIS PANOS ET AL: "SDN-based solutions for Moving Target Defense network protection", PROCEEDING OF IEEE INTERNATIONAL SYMPOSIUM ON A WORLD OF WIRELESS, MOBILE AND MULTIMEDIA NETWORKS 2014, IEEE, 19 June 2014 (2014-06-19), pages 1-6, XP032656398, DOI: 10.1109/WOWMOM.2014.6918979 [retrieved on 2014-10-08] Seite 2, linke Spalte, zweiter Absatz, Seite 3, linke Spalte, Abschnitt "Potential attacker countermeasures", Seite 3, rechte Splate, Abschnitt "Service version and OS hiding, Seiten 4 und 5, Abschnitt "Random Host or Route mutation" figures 1, 2

(57) Предлагается устройство (10) и способ для управления сетью (100) связи, содержащей множество терминалов (21-28) для передачи данных, при этом устройство (10) содержит блок (11) управления, сконфигурированный для разделения плоскости (L1) данных и плоскости (L2) управления для передачи данных и модификации по меньшей мере одной характеристики сети (100) связи, видимой из объекта (200), расположенного вне сети (100) связи, во время сеанса связи с использованием отделенной плоскости (L2) управления.

036842 B1

036842 B1

Настоящее изобретение относится к устройству для управления сетью связи, содержащей множество терминалов, предназначенных для передачи данных. Настоящее изобретение также относится к маршрутизатору, содержащему такое устройство, коммутатору, содержащему такое устройство, межсетевому экрану, содержащему такое устройство, и к сети связи, содержащей такое устройство. Кроме того, настоящее изобретение относится к способу и компьютерному программному изделию для управления сетью связи.

Уровень техники настоящего изобретения относится к безопасности (IT-безопасность) сетей связи, таких как сети связи компаний, университетов, органов государственной власти и других организаций.

Сети связи компаний и подобные им сети в значительной степени подвержены атакам злоумышленников, в частности, с целью слежки за этими сетями. Сценарии угроз, касающиеся сетей связи, все в большей степени становятся специализированными, часто запланированы на длительный отрезок времени, и в них используются специальные технологии маскировки. Часто злоумышленники при атаке на сети связи специально ищут слабые места в стратегии безопасности компаний и т.п.

Известные решения по обеспечению безопасности, такие как межсетевые экраны, IPS и антивирусы, а также Интернет-шлюзы конфигурируются для обнаружения известных схем атак путем применения алгоритма, зависящего от принимаемых мер обеспечения безопасности. Однако новое поколение атак является динамичным и не ограничено известными схемами атак. Например, цели атак преследуются по нескольким векторам и фазам атаки, что значительно увеличивает потенциальную угрозу для сетей компаний.

В этом случае известные статичные конфигурации сетей имеют недостаток, заключающийся в том, что они являются легкой целью для слежки и атаки злоумышленниками, такими как несанкционированные лица.

В свете вышеизложенного цель настоящего изобретения заключается в предложении более безопасной сети связи.

В соответствии с первым аспектом предлагается устройство для управления сетью связи, содержащей множество терминалов, предназначенных для передачи данных. Устройство содержит блок управления, сконфигурированный для разделения плоскости данных и плоскости управления для передачи данных и модификации по меньшей мере одной характеристики сети связи, видимой извне сети связи, во время сеанса связи с использованием отделенной плоскости управления.

Поскольку блок управления модифицирует, более конкретно - динамически модифицирует, по меньшей мере одну характеристику сети связи, видимую извне сети связи, в процессе каждого отдельного сеанса связи, внешнему наблюдателю за сетью связи или злоумышленнику становится практически невозможно следить за сетью связи, поскольку конфигурация и, таким образом, вид сети связи неопределимы и непредсказуемы для внешнего наблюдателя. Дополнительно или в альтернативном варианте также возможно модифицировать видимые шаблоны данных сети связи. Это повышает безопасность сети связи.

Примерами по меньшей мере одной характеристики сети связи, модифицируемой блоком управления, являются изменение виртуального адреса терминалов сети связи, изменение конфигурации сети связи, изменение поведения маршрутизации сети связи и изменение приложений и/или распределения их портов.

Под сеансом связи или сеансом понимается связь между одним из терминалов сети связи и устройством, находящимся вне или в пределах сети связи. Сеанс связи также может быть основан на протоколах без сохранения состояния, таких как HTTP (Hypertext Transfer Protocol, протокол передачи гипертекста).

Блок управления может быть реализован в виде аппаратного и/или программного обеспечения. В случае аппаратной реализации блок управления может быть выполнен в виде устройства или части устройства, например в виде компьютера, или микропроцессора, или маршрутизатора, или коммутатора. В случае программной реализации блок управления может быть выполнен в виде компьютерного программного изделия, такого как функция, подпрограмма, часть программного кода или исполняемый объект.

Средством, которое может использоваться для реализации блока управления, является SDN-контроллер OpenMUL с открытым исходным текстом (см. ссылочный материал [1]). OpenMUL-контроллер поддерживает основанную на стандарте SDN/OpenFlow платформу управления, которая реализована на C. В данном случае блок управления предпочтительно сконфигурирован для использования OpenFlow (см. ссылочный материал [2]), а также технологии защиты с использованием движущихся целей (MTD, Moving-Target-Defence, см. ссылочный материал [3]). Посредством использования MTD блок управления сконфигурирован для динамической модификации сети связи. OpenFlow представляет собой протокол связи, который обеспечивает доступ к аппаратным компонентам коммутатора или маршрутизатора, которые обрабатывают входящие сетевые пакеты (так называемая плоскость переадресации).

Непосредственно устройство может быть реализовано с помощью аппаратного и/или программного обеспечения. В случае аппаратной реализации устройство может быть выполнено в виде компьютера, части маршрутизатора, части коммутатора или части межсетевого экрана. В случае программной реали-

зации устройство может быть выполнено в виде компьютерного программного изделия, такого как функция, подпрограмма, часть программного кода или исполняемый объект.

Сеть связи также может называться сетью или компьютерной сетью и представлять собой, например, LAN (Local Area Network, локальная сеть) или WAN (Wide Area Network, глобальная сеть).

Разделение плоскости данных и плоскости управления для передачи данных обеспечивается, например, посредством программно-определяемой сети (Software-Defined-Networking, см. ссылочные материалы [4] и [5]).

Примеры терминалов сети связи включают калькуляторы, компьютеры, маршрутизаторы, коммутаторы, межсетевые экраны, встроенные системы и т.п.

В соответствии с вариантом осуществления блок управления сконфигурирован для упреждающей модификации по меньшей мере одной характеристики сети связи, видимой извне сети связи, во время сеанса связи с использованием отделенной плоскости управления.

Таким образом, блок управления сконфигурирован для упреждающей модификации по меньшей мере одной видимой характеристики. С этой целью по меньшей мере одна характеристика системы связи модифицируется еще до возникновения угрозы или повреждения сети связи. Следовательно, может обеспечиваться упреждающая безопасность сети связи в реальном времени.

В данном случае упреждающая модификация, в частности, понимается как модификация по меньшей мере одной видимой характеристики в конце каждого отдельного потока данных. Таким образом, в отличие от обычной ответной модификации настоящий блок управления сконфигурирован для упреждающей модификации или упреждающей и ответной модификации в случае идентифицированной угрозы или обнаруженного повреждения.

Более конкретно, блок управления сконфигурирован для упреждающей модификации сети связи таким образом, чтобы могли динамически устанавливаться различные зоны безопасности с различными уровнями безопасности и/или различными функциями безопасности. Например, блок управления может изменять установленную зону безопасности в зависимости от идентифицированных сценариев угрозы. Кроме того, блок управления предпочтительно сконфигурирован для установления дневного и ночного режима работы сети связи, характеризующихся различными уровнями безопасности.

В соответствии с другим вариантом осуществления блок управления сконфигурирован для изменения виртуального адреса по меньшей мере одного из множества терминалов во время сеанса связи с использованием отделенной плоскости управления. Виртуальный адрес представляет собой логический адрес, который может быть преобразован логическим или компьютерным блоком в физический адрес.

В соответствии с другим вариантом осуществления устройство содержит генератор случайных значений для вывода случайного значения. В данном случае блок управления сконфигурирован для изменения виртуального адреса в зависимости от случайного значения, выведенного генератором случайных значений.

В соответствии с другим вариантом осуществления блок управления сконфигурирован для модификации конфигурации сети связи во время сеанса связи с использованием отделенной плоскости управления. Изменение конфигурации сети связи предпочтительно включает изменение установленных уровней безопасности или зон безопасности сети связи. Следовательно, устройство по-разному может реагировать на различные сценарии атак путем изменения конфигурации сети связи.

В соответствии с другим вариантом осуществления блок управления сконфигурирован для модификации поведения маршрутизации во время сеанса связи с использованием отделенной плоскости управления. Вследствие предлагаемого изменения поведения маршрутизации сети связи злоумышленник не может прийти к какому-либо полезному решению на основе записи или регистрации поведения маршрутизации сети связи из-за отсутствия статической характеристики поведения маршрутизации.

В соответствии с другим вариантом осуществления блок управления сконфигурирован для модификации по меньшей мере одного приложения сети связи во время сеанса связи с использованием отделенной плоскости управления. Вследствие изменения приложения сети связи злоумышленник не сможет получить какую-либо полезную информацию о сети связи.

В соответствии с другим вариантом осуществления блок управления сконфигурирован для модификации по меньшей мере одного назначения порта по меньшей мере одного приложения во время сеанса связи с использованием отделенной плоскости управления. Вследствие изменения назначения порта приложения сети связи злоумышленник не сможет получить какую-либо полезную информацию о сети связи.

В соответствии с другим вариантом осуществления блок управления сконфигурирован для замены первого алгоритма шифрования, используемого сетью связи, на второй алгоритм шифрования во время сеанса связи.

В данном случае блок управления предпочтительно выбирает второй алгоритм шифрования из множества подготовленных алгоритмов шифрования.

Преимущество состоит в том, что злоумышленник не сможет получить полезную информацию о сети связи, поскольку используется не статический алгоритм шифрования, а осуществляется замена алгоритма шифрования.

Под алгоритмом шифрования понимается алгоритм расчета по меньшей мере одной криптографической величины, например, с использованием криптографической функции. Алгоритмы шифрования включают такие алгоритмы шифрования, как SSL (Secure Sockets Layers, протокол безопасных соединений), а также алгоритмы, использующие цифровые подписи. Криптографические величины могут включать криптографические ключи, такие как симметричные ключи и/или значения хеш-функции.

В соответствии с другим вариантом осуществления блок управления сконфигурирован для модификации шаблона данных сети связи, в частности, профиля полезной нагрузки по меньшей мере одного терминала.

Путем модификации шаблона данных или нескольких шаблонов данных сети связи блок управления активизируется для имитации трафика данных для злоумышленника. Имитированный трафик данных может также называться имитацией данных или имитацией связи. Кроме того, блок управления предпочтительно сконфигурирован для изменения терминала, связанного с сетью связи, то есть сетевых терминалов или участников сетевого взаимодействия, для того чтобы модифицировать шаблон данных сети связи. Путем модификации шаблона данных в значительной степени затрудняется успешное выполнение сравнения двоичных шаблонов злоумышленником.

В соответствии с другим вариантом осуществления сеанс связи включает множество транзакций данных (потоков данных). В данном случае блок управления сконфигурирован для модификации по меньшей мере одной характеристики сети связи, видимой извне сети связи, после подмножества, входящего в множество транзакций.

Подмножество транзакций, после которых блок управления модифицирует по меньшей мере одну видимую характеристику сети связи, может инициироваться или указываться генератором случайных значений.

В соответствии с другим вариантом осуществления сеанс связи включает множество транзакций данных, при этом блок управления сконфигурирован для модификации по меньшей мере одной характеристики сети связи, видимой извне сети связи, после каждой из множества транзакций.

Путем изменения характеристики или характеристик после транзакции уровень безопасности для сети связи может повышаться.

В соответствии с другим вариантом осуществления блок управления сконфигурирован для разделения плоскости управления и плоскости данных для передачи данных с использованием программно-определяемой сети. Программно-определяемая сеть представляет собой подход для построения устройств или терминалов для сети связи и программного обеспечения, которое отделяет друг от друга два существенных компонента, а именно: команды обработки данных и команды управления, и абстрагирует их (с этой целью см. ссылочные материалы [4] и [5]).

В соответствии с другим вариантом осуществления устройство содержит один генератор случайных значений, связанный с блоком управления. Генератор случайных значений сконфигурирован для случайного или квазислучайного запуска блока управления с целью модификации по меньшей мере одной характеристики сети связи, видимой извне сети связи, по меньшей мере один раз во время сеанса связи, а в более конкретном случае - несколько раз во время сеанса связи. Генератор случайных значений или генератор случайных чисел генерирует ряд случайных значений или случайных чисел. Генератор случайных значений может формироваться в виде детерминированного генератора случайных чисел или недетерминированного генератора случайных чисел.

В соответствии с другим вариантом осуществления устройство содержит первый блок защиты, предназначенный для обнаружения, изоляции и противодействия доступам из несанкционированных объектов к сети связи. В соответствии с этим вариантом осуществления первый блок защиты способен обнаружить атаку или доступ из одного объекта, несанкционированного для сети связи, с целью изоляции обнаруженной атаки в сети связи и принятия мер против этой атаки.

В соответствии с другим вариантом осуществления устройство содержит второй блок защиты, предназначенный для предупреждения и оповещения системы определения, связанной с устройством. Второй блок защиты предпочтительно сконфигурирован для предупреждения и оповещения системы определения, связанной с устройством и управляемой, например, государственной организацией.

В соответствии с другим вариантом осуществления устройство содержит третий блок защиты, предназначенный для восстановления по меньшей мере одной критической сетевой функции.

В данном случае третий блок защиты, в частности, может быть сконфигурирован для запуска по меньшей мере одного резервного блока с целью выполнения критической сетевой функции при обнаружении ее отказа, для того чтобы восстановить критическую сетевую функцию. Соответственно, преимущество настоящего устройства состоит в том, что оно способно автоматически восстанавливать критические сетевые функции.

В соответствии с другим вариантом осуществления устройство содержит блок анализа, предназначенный для выполнения анализа данных во время доступа несанкционированных объектов к сети связи.

В соответствии с другим вариантом осуществления устройство содержит блок определения данных, предназначенный для определения, с использованием предоставленных данных анализа, данных о состоянии, которые, в частности, могут указать на ситуацию безопасности сети связи.

В соответствии с другим вариантом осуществления устройство содержит блок интерфейса, предназначенный для передачи данных о состоянии в систему определения, связанную с устройством. В данном случае система определения может быть также связана с устройством, например, через Интернет. Блок интерфейса также сконфигурирован для установления криптографически защищенной передачи между системой определения и устройством. Например, блок интерфейса может также устанавливать защищенный туннель связи между устройством и системой определения.

В соответствии с другим вариантом осуществления сеть связи содержит инфраструктуру, включающую уровни, которые расположены один над другим в виде стека. В частности, в стеке инфраструктуры последовательно расположены следующие уровни: уровень 1, уровень 2, уровень 3, уровень 4, уровень 5, уровень 6, уровень 7. В данном случае блок управления реализован в виде виртуальной оверлейной сети, которая перекрывает уровень 2 и уровень 3.

В соответствии с другим вариантом осуществления виртуальная оверлейная сеть реализуется с использованием виртуальной расширяемой LAN. Например, оверлейная сеть реализуется посредством VXLAN (Virtual Extensible LAN, виртуальная расширяемая локальная сеть). VXLAN представляет собой протокол инкапсуляции, позволяющий оверлейной сети функционировать в существующей инфраструктуре уровня 3 (см. ссылочный материал [6]).

В соответствии с другим вариантом осуществления блок управления встраивается в межсетевой экран, в коммутатор или в маршрутизатор сети связи.

В соответствии с другим вариантом осуществления блок управления реализуется программно.

В соответствии с другим вариантом осуществления устройство поддерживает IPv4 (Интернет-протокол версии 4, см. ссылочный материал [7]) и IPv6 (Интернет-протокол версии 6, см. ссылочный материал [8]).

В соответствии с другим вариантом осуществления устройство использует комбинацию протокола обеспечения безопасности и протокола туннелирования. С помощью протокола туннелирования можно дополнительно повысить уровень безопасности при передаче данных.

Примером протокола обеспечения безопасности является IPsec (см. ссылочный материал [9]). Примером протокола туннелирования является L2TP (см. ссылочный материал [10]). Другим примером подходящего протокола туннелирования является открытая VPN (см. ссылочный материал [11]).

Соответствующий блок, такой как блок анализа или блок защиты, может быть реализован в виде аппаратного и/или программного обеспечения. В случае аппаратной реализации блок может быть выполнен в виде устройства или части устройства, например в виде компьютера, или микропроцессора, или коммутатора. В случае программной реализации блок может быть выполнен в виде компьютерного программного изделия, такого как функция, подпрограмма, часть программного кода или исполняемый объект.

Согласно второму аспекту предлагается маршрутизатор для сети связи, в который встроено устройство, соответствующее первому аспекту или одному из вариантов его осуществления. В частности, под маршрутизатором понимается сетевое устройство, которое может пересылать сетевые пакеты между несколькими сетями связи. Маршрутизатор может применяться для подключения к Интернету, для безопасной связи нескольких местоположений компании или, при необходимости, для непосредственной связи нескольких локальных сетевых сегментов с использованием адаптации к различным Интернет-протоколам.

Согласно третьему аспекту предлагается коммутатор для сети связи, в который встроено устройство, соответствующее первому аспекту или одному из вариантов его осуществления. Под коммутатором понимается элемент связи, который соединяет друг с другом два сетевых сегмента. В пределах сетевого сегмента требуется принимать меры для того, чтобы пакеты данных достигали своего пункта назначения. Коммутатор может также называться сетевым коммутатором или распределителем.

Согласно четвертому аспекту предлагается межсетевой экран для сети связи, в который встроено устройство, соответствующее первому аспекту или одному из вариантов его осуществления. Под межсетевым экраном понимается сетевой элемент, который защищает от нежелательных сетевых доступов сеть связи, часть сети связи или отдельный компьютер сети связи. Межсетевой экран может представлять систему безопасности или может входить в состав системы безопасности.

Согласно пятому аспекту предлагается сеть связи, которая включает в свой состав множество терминалов передачи данных и устройство, соответствующее первому аспекту или одному из вариантов его осуществления.

В соответствии с шестым аспектом предлагается способ для управления сетью связи, содержащей множество терминалов, предназначенных для передачи данных. Способ включает разделение плоскости управления и плоскости данных для передачи данных и модификацию по меньшей мере одной характеристики сети связи, видимой извне сети связи, во время сеанса связи с использованием отделенной плоскости управления.

Согласно седьмому аспекту предлагается компьютерное программное изделие, инициирующее в программно-управляемом блоке выполнение способа, соответствующего шестому аспекту.

Компьютерное программное изделие, такое как компьютерные программные средства, может пре-

доставляться или поставляться в виде носителя информации, такого как USB-карта, CD-ROM, DVD, или в виде файла, который может загружаться из сервера, подключенного к сети. Загрузку можно выполнить, например, в сети беспроводной связи путем передачи соответствующего файла, содержащего компьютерное программное изделие или компьютерные программные средства.

Варианты осуществления и признаки, описанные для предлагаемого устройства, соответственно применимы к предлагаемому способу.

Возможные дополнительные варианты осуществления настоящего изобретения включают также неявно указанную комбинацию приведенных выше или ниже признаков или вариантов осуществления, описываемых на примерах реализации. В данном случае специалист в этой области техники также может добавить отдельные аспекты в качестве улучшений или расширений соответствующей фундаментальной формы изобретения.

Далее настоящее изобретение объясняется более подробно на основе предпочтительных вариантов осуществления со ссылкой на прилагаемые чертежи.

На фиг. 1 показана схематическая блок-схема первого варианта осуществления устройства для управления сетью связи;

на фиг. 2 показана схематическая блок-схема второго варианта осуществления устройства для управления сетью связи;

на фиг. 3 показана схематическая блок-схема третьего варианта осуществления устройства для управления сетью связи;

на фиг. 4 показана схематическая блок-схема сети связи, содержащей устройство, соответствующее одной из блок-схем, изображенных на фиг. 1-3;

на фиг. 5 показана схематическая блок-схема архитектуры SDN с раздельными плоскостями данных и управления для реализации блока управления;

на фиг. 6 показана схематическая блок-схема варианта осуществления маршрутизатора с устройством для управления сетью связи, соответствующим одной из блок-схем, показанных на фиг. 1-3;

на фиг. 7 показана схематическая блок-схема варианта осуществления коммутатора с устройством для управления сетью связи, соответствующим одной из блок-схем, показанных на фиг. 1-3;

на фиг. 8 показана схематическая блок-схема варианта осуществления межсетевого экрана с устройством для управления сетью связи, соответствующим одной из блок-схем, показанных на фиг. 1-3; и

на фиг. 9 показан алгоритм, реализующий способ для управления сетью связи.

Одинаковые элементы или элементы, выполняющие одинаковые функции, на чертежах обозначаются одинаковыми ссылочными номерами, если не указано иное.

На фиг. 1 показана схематическая блок-схема первого варианта осуществления устройства 10 для управления сетью 100 связи. Сеть 100 связи содержит множество терминалов 21-26, служащих для передачи данных. Множество терминалов 21-26 может включать в свой состав маршрутизатор, коммутаторы, межсетевые экраны, компьютеры, персональные компьютеры, встроенные системы, оборудование управления и т.п. Сеть 100 связи представляет собой, например, LAN (Local Area Network, локальная сеть) или WAN (Wide Area Network, глобальная сеть). Устройство 10 для управления сетью 100 связи также может называться устройством 10 управления.

Согласно варианту осуществления, показанному на фиг. 1, устройство 10 содержит блок 11 управления, блок 12 анализа, блок 13 DNS (Domain Name Server, сервер доменных имен) и блок 18 защиты. Блок 11 управления, блок 12 анализа, блок 13 DNS и блок 18 защиты могут быть логически либо физически связаны или соединены друг с другом. Например, устройство 10 может быть выполнено в виде компьютера, в который встроены блок 11 управления, блок 12 анализа, блок 13 DNS и блок 18 защиты.

Блок 11 управления устройства сконфигурирован для разделения плоскости L1 данных (см. фиг. 5) и плоскости L2 управления (см. фиг. 5) для передачи данных. Плоскость L1 данных также может называться слоем или уровнем данных. Плоскость L2 управления также может называться слоем или уровнем управления.

Кроме того, блок 11 управления сконфигурирован для модификации по меньшей мере одной характеристики сети 100 связи, видимой из объекта 200, расположенного вне сети связи (см. фиг. 4), с использованием отделенной плоскости L2 управления. Например, вне сети 100 связи может находиться такой объект, как компьютер, который расположен в Интернете 200 (см. фиг. 4) и который не санкционирован и/или не аутентифицирован относительно сети 100 связи.

Примерами по меньшей мере одной характеристики сети 100 связи, которые модифицируются блоком 11 управления, являются: изменение виртуальных адресов терминалов 21-26 сети 100 связи, изменение конфигурации сети 100 связи, изменение поведения маршрутизации сети 100 связи и/или изменение приложений и/или распределения портов приложений в сети 100 связи.

В частности, блок 11 управления сконфигурирован для упреждающей модификации сети 100 связи. В данном случае блок 11 управления особым образом сконфигурирован для упреждающей модификации сети 100 связи таким образом, чтобы устанавливались различные зоны безопасности с различными уровнями безопасности в сети 100 связи и/или с различными функциями безопасности в сети 100 связи. Более конкретно, блок 11 управления в зависимости от сценария идентифицированной угрозы может изменять

установленные зоны безопасности и вместе с тем конфигурацию сети 100 связи.

Кроме того, блок 11 управления сконфигурирован для замены первого алгоритма шифрования, используемого сетью 100 связи, на второй алгоритм шифрования во время работы сети 100 связи.

Дополнительно или в альтернативном варианте блок 11 управления сконфигурирован для модификации шаблона данных сети 100 связи. Примером такого шаблона данных сети 100 связи является профиль полезной нагрузки по меньшей мере одного из терминалов 21-26.

Сеанс связи, описанный выше, может включать множество транзакций данных (потоков данных). В данном случае блок 11 управления сконфигурирован для модификации по меньшей мере одной характеристики сети 100 связи, видимой из объекта 200, расположенного вне сети 100 связи, после подмножества, входящего в множество транзакций. Подмножество, входящее в множество транзакций, также может состоять из одного элемента, и, таким образом, блок 11 управления модифицирует по меньшей мере одну видимую характеристику сети 100 связи после каждой отдельной транзакции.

Блок 12 анализа устройства 10 предпочтительно сконфигурирован для выполнения анализа данных во время доступа несанкционированных объектов к сети 100 связи. На фиг. 3 показана подробная схема такой поставки данных анализа в систему 300 определения, связанную с устройством 10. Эта система разъясняется ниже.

На фиг. 2 показана схематическая блок-схема второго варианта осуществления устройства 10 для управления сетью связи. Второй вариант осуществления, показанный на фиг. 2, включает все признаки первого варианта осуществления, показанного на фиг. 1. Кроме того, устройство 10, показанное на фиг. 2, содержит блок 14 анализа данных и генератор 19 случайных значений (ZW). Кроме того, на фиг. 2 показано, что блок 18 защиты содержит первый блок 15 защиты, второй блок 16 защиты и третий блок 17 защиты.

Блок 14 анализа данных сконфигурирован для определения данных о состоянии с использованием данных анализа, предоставленных блоком 12 анализа. В частности, данные о состоянии указывают на ситуацию безопасности сети 100 связи.

Как описано выше, генератор 19 случайных значений выводит случайное значение ZW. В данном случае блок 11 управления сконфигурирован для изменения, например, виртуального адреса одного из терминалов 21-26 в зависимости от случайного значения ZW, выведенного генератором 19 случайных значений. Кроме того, генератор 19 случайных значений может быть сконфигурирован для случайного или квазислучайного запуска блока 11 управления с целью модификации по меньшей мере одной характеристики, видимой из объекта 200, расположенного вне сети 100 связи, по меньшей мере один раз во время сеанса связи или же несколько раз во время сеанса связи.

Как было описано выше, блок 18 защиты, показанный на фиг. 2, содержит первый блок 15 защиты, второй блок 16 защиты и третий блок 17 защиты. Первый блок 15 защиты сконфигурирован для обнаружения, изоляции и противодействия доступам из несанкционированных объектов к сети 100 связи. Второй блок 16 защиты сконфигурирован для предупреждения и оповещения системы 300 определения, которая может быть связана с устройством 10. Третий блок 17 защиты сконфигурирован для восстановления по меньшей мере одной критической сетевой функции сети 100 связи.

В этом отношении на фиг. 3 показан третий вариант осуществления устройства 10 для управления сетью 100 связи. Третий вариант осуществления, показанный на фиг. 3, включает все признаки второго варианта осуществления, показанного на фиг. 2. Кроме того, устройство 10, показанное на фиг. 3, содержит блок 20 интерфейса, сконфигурированный для связи устройства 10 с системой 300 определения. Например, блок 20 интерфейса связан с блоком 12 анализа, блоком 13 DNS и блоком 14 анализа данных. Блок 20 интерфейса также может быть связан с другими блоками устройства 10, таким как блок 11 управления или генератор 19 случайных значений (не показанный на чертеже). Например, генератор 19 случайных значений может инициироваться через блок 20 интерфейса.

На фиг. 4 показана схематичная блок-схема сети 100 связи. Сеть 100 связи содержит устройство 10, реализованное в соответствии с одним из вариантов осуществления, показанных на фиг. 1-3.

Кроме того, в состав сети 100 связи, показанной на фиг. 4, входит ряд терминалов 21-23. Без нарушения общности в варианте осуществления, показанном на фиг. 4, изображено три терминала 21-23.

Кроме того, сеть 100 связи, показанная на фиг. 4, содержит маршрутизатор 30, коммутатор 40, первый межсетевой экран 51, второй межсетевой экран 52, демилитаризованную LAN 61, размещенную между первым межсетевым экраном 51 и вторым межсетевым экраном 52, и внутреннюю LAN 62, соединяющую множество терминалов 21-23 со вторым межсетевым экраном 52 (внутренним межсетевым экраном), а также с маршрутизатором 30, коммутатором 40 и устройством 10. Кроме того, на фиг. 4 показано, что сеть 100 связи может соединяться с Интернетом 200. Указанные выше несанкционированные объекты, которые потенциально могут атаковать сеть 100 связи, частично размещены в Интернете 200 или подключены к этой сети.

На фиг. 5 показана схематическая блок-схема архитектуры SDN с раздельными плоскостями L1 данных и плоскостями L2 управления для реализации блока 11 управления.

На фиг. 5 показано, что в данной архитектуре плоскость L1 данных, плоскость L2 управления и плоскость L3 приложений отделены друг от друга. Плоскости или уровни L1, L2, L3 соединены друг с

другом для взаимной связи через API 101-104 (Application Programming Interface, прикладной программный интерфейс).

API 101 также может называться нисходящим API (Southbound-API). Например, нисходящий API реализуется с использованием OpenFlow. API 102-104 также могут называться восходящими API (Northbound-API).

Физические сетевые устройства 21-25 и виртуальные сетевые устройства 26-28 размещаются в плоскости L1 данных. Количество и распределение физических сетевых устройств 21-25 и виртуальных сетевых устройств 26-28 в плоскости L1 данных приведено просто в качестве примера.

Плоскость L2 управления содержит управляющее программное обеспечение 70 SDN, в состав которого входят различные сетевые службы 81-83 для реализации блока 11 управления.

Плоскость L3 приложений содержит несколько приложений 91-93. Приложения 91-93 также могут называться коммерческими приложениями.

Как было описано выше, нижней плоскостью или уровнем архитектуры SDN является плоскость L1 данных, которая содержит множество сетевых устройств 21-28. В плоскости L2 управления различия между физическими и виртуальными сетевыми устройствами 21-28 или коммутаторами не устанавливаются. Таким образом, виртуальные сетевые устройства 26-28 также рассматриваются как устройства уровня L1 данных. Связь между плоскостью L1 данных и плоскостью L2 управления представлена нисходящим протоколом с помощью нисходящего интерфейса 101. В данном случае предварительное условие заключается в том, чтобы задействованные устройства 21-28 обрабатывали команду на уровне используемого нисходящего протокола. В частности, сетевым устройствам 21-28 требуется только поддерживать минимальный набор команд нисходящего протокола. Для реализации этого режима может использоваться Open Flow. Задача нисходящего протокола состоит в реализации базового набора команд для управления таблицами потоков в коммутаторах с целью обеспечения в плоскости L1 данных прозрачности в отношении степени сложности и гетерогенности.

Управляющее программное обеспечение 70 SDN размещается в плоскости L2 управления. Оно также может рассматриваться как промежуточное программное обеспечение, которое абстрагирует сетевые устройства 21-28 плоскости L1 данных для приложения SDN.

На фиг. 6 показана схематическая блок-схема варианта осуществления маршрутизатора 30, в который встроено устройство 10 для управления сетью 100 связи. Устройство 10 реализовано в соответствии с одним из вариантов осуществления, показанных, например, на фиг. 1-3.

На фиг. 7 показана схематическая блок-схема варианта осуществления коммутатора 40, в который встроено устройство 10 для управления сетью 100 связи. Устройство 10 реализовано в соответствии с одним из вариантов осуществления, показанных, например, на фиг. 1-3.

На фиг. 8 показана схематическая блок-схема варианта осуществления межсетевого экрана 50, в который встроено устройство 10 для управления сетью 100 связи. Устройство 10 реализовано в соответствии с одним из вариантов осуществления, показанных, например, на фиг. 1-3.

На фиг. 9 показан алгоритм, реализующий способ для управления сетью 100 связи. Способ, показанный на фиг. 9, включает шаги 901 и 902.

На шаге 901 плоскость L1 данных и плоскость L2 управления для передачи данных разделяются друг от друга. В результате выполнения шага 901 образуется плоскость L2 управления, отделенная от плоскости L1 данных, и плоскость L1 данных, отделенная от плоскости L2 управления.

На шаге 902 характеристика сети 100 связи, видимая извне сети 100 связи, модифицируется с использованием отделенной плоскости L2 управления.

Хотя настоящее изобретение описано на основе вариантов его осуществления, оно может модифицироваться различными способами. Например, можно разместить устройство для управления сетью связи также в другом объекте сети связи, показанном на чертежах (например, в маршрутизаторе или коммутаторе). Кроме того, также можно разместить устройство для управления сетью связи вне сети связи. Кроме того, средство OpenMUL для реализации блока управления устройства для управления сетью связи приведено просто в качестве примера. С этой целью могут использоваться альтернативные средства.

Список ссылочных номеров

10 - устройство
11 - блок управления
12 - блок анализа
13 - блок DNS
14 - блок анализа данных
15 - первый блок защиты
16 - второй блок защиты
17 - третий блок защиты
18 - блок защиты
19 - генератор случайных значений
20 - блок интерфейса
21 - терминал

22 - терминал
23 - терминал
24 - терминал
25 - терминал
26 - терминал
27 - терминал
28 - терминал
30 - маршрутизатор
40 - коммутатор
50 - межсетевой экран
51 - межсетевой экран
52 - межсетевой экран
61 - LAN
62 - LAN
70 - управляющее программное обеспечение SDN
81-83 - сетевая служба
91-93 - приложение
100 - сеть связи
101 - API
102 - API
103 - API
104 - API
200 - Интернет
300 - система определения
L1 - плоскость данных
L2 - плоскость управления
L3 - плоскость приложений
ZW - случайное значение

Ссылочные материалы

[1] http://www.openmul.org/openmul-controller.html (ссылка, загруженная на дату приоритета)

[2] Nick McKeown и др.: OpenFlow: Enabling innovation in campus networks (реализация инноваций в университетских сетях), ACM Communications Review, апрель 2008

[3] http://www.dhs.gov/science-and-technology/csd-mtd (ссылка, загруженная на дату приоритета)

[4] Software-Defined Networking (программно определяемые сети): The New Norm for Networks, White Paper (новый стандарт сетей, техническое описание), Open Networking Foundation, 13 апреля 2012

[5] Sean Michael Kerner: OpenFlow Inventor Martin Casado on SDN, VMware, and Software Defined Networking Hype (создатель протокола OpenFlow Martin Casado об SDN, VMware и рекламе программно определяемых сетей), Enterprise Networking Planet, 29 апреля 2013

[6] RFC7348: Virtual extensible Local Area Network (VXLAN, виртуальная расширяемая локальная сеть): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks (структура для перекрытия виртуализованными сетями уровня 2 виртуализованных сетей уровня 3)

[7] RFC791 - Internet Protocol; Ipv4 (Интернет-протокол версии Ipv4)

[8] RFC3513 - Internet Protocol; Ipv6 (Интернет-протокол версии Ipv6)

[9] RFC4301-IPsec

[10] RFC2661-L2TP

[11] Open-VPN: https://openvpn.net/

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Устройство (10) для управления конфигурацией сети (100) связи, содержащей множество терминалов (21-28) для передачи данных, в которой разделены плоскость (L1) данных и плоскость (L2) управления, содержащее

блок (11) управления, выполненный с возможностью модификации по меньшей мере одной характеристики сети (100) связи, видимой для терминала (200), расположенного вне сети (100) связи, во время сеанса связи с использованием отделенной плоскости (L2) управления, при этом

упомянутая модификация включает изменение виртуального адреса по меньшей мере одного из множества терминалов (21-28) во время сеанса связи с использованием отделенной плоскости (L2) управления;

и генератор (19) случайных значений для вывода случайного значения (ZW), при этом блок (11) управления выполнен с возможностью изменения виртуального адреса в зависимости от случайного значения (ZW), выведенного генератором (19) случайных значений.

2. Устройство по п.1, отличающееся тем, что блок (11) управления выполнен с возможностью модификации сети (100) связи так, чтобы иметь возможность динамически устанавливать различные зоны безопасности с различными уровнями безопасности и/или различными функциями безопасности.

3. Устройство по любому из пп.1, 2, отличающееся тем, что упомянутая модификация также включает модификацию поведения маршрутизации сети (100) связи во время сеанса связи с использованием отделенной плоскости (L2) управления.

4. Устройство по любому из пп.1-3, отличающееся тем, что блок (11) управления выполнен с возможностью модификации по меньшей мере одного приложения сети (100) связи и/или преобразования портов по меньшей мере одного приложения во время сеанса связи с использованием отделенной плоскости (L2) управления.

5. Устройство по любому из пп.1-4, отличающееся тем, что блок (11) управления выполнен с возможностью замены первого алгоритма шифрования, используемого сетью (100) связи, на второй алгоритм шифрования во время сеанса связи.

6. Устройство по любому из пп.1-5, отличающееся тем, что блок (11) управления выполнен с возможностью модификации шаблона данных сети (100) связи, в частности профиля полезной нагрузки по меньшей мере одного из терминалов (21-28).

7. Устройство по любому из пп.1-6, отличающееся тем, что блок (11) управления выполнен с возможностью модификации по меньшей мере одной характеристики сети (100) связи, видимой для терминала (200), расположенного вне сети (100) связи, после выполнения подмножества транзакций, входящего в множество транзакций данных сеанса связи.

8. Устройство по любому из пп.1-7, отличающееся тем, что блок (11) управления выполнен с возможностью модификации по меньшей мере одной характеристики сети (100) связи, видимой для терминала (200), расположенного вне сети (100) связи, после каждой из множества транзакций данных сеанса связи.

9. Устройство по любому из пп.1-8, отличающееся тем, что плоскость (L1) управления и плоскость (L2) данных для передачи данных разделены с использованием программно-определяемой сети.

10. Устройство по любому из пп.1-9, содержащее генератор (19) случайных значений, выполненный с возможностью случайного запуска блока (11) управления для модификации по меньшей мере одной характеристики, видимой для терминала (200), расположенного вне сети (100) связи, по меньшей мере один раз во время сеанса связи или несколько раз во время сеанса связи.

11. Устройство по любому из пп.1-10, содержащее первый блок (15) защиты для обнаружения, изоляции и противодействия доступам из несанкционированных объектов к сети (100) связи.

12. Устройство по п.11, содержащее второй блок (16) защиты для предупреждения и оповещения системы (300) определения, которая связана с устройством (10).

13. Устройство по п.11 или 12, содержащее третий блок (17) защиты для восстановления по меньшей мере одной критической сетевой функции.

14. Устройство по любому из пп.1-13, содержащее блок (12) анализа для выполнения анализа данных во время попыток доступа несанкционированных объектов к сети (100) связи.

15. Устройство по п.14, содержащее блок (14) определения данных для определения данных о состоянии с использованием предоставленных данных анализа, при этом данные о состоянии, в частности, применимы для указания на ситуацию безопасности сети (100) связи.

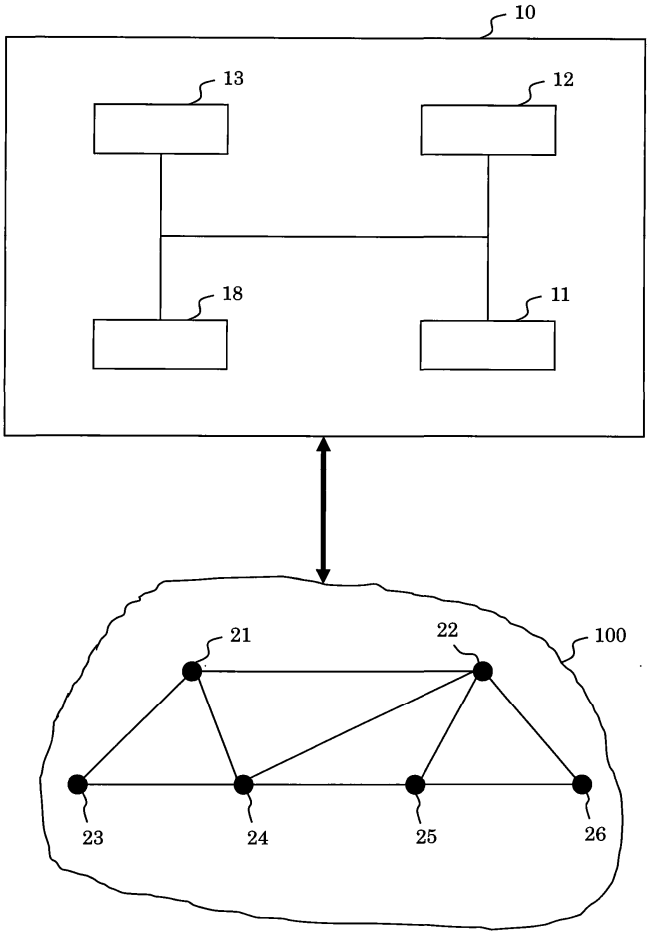
16. Устройство по любому из п.п.1-15, отличающееся тем, что блок (11) управления реализован в виде виртуальной оверлейной сети, перекрывающей уровень 2 и уровень 3 инфраструктуры уровней сети (100) связи, которые расположены один над другим в виде стека.

17. Способ управления, с помощью устройства по п.1, конфигурацией сети (100) связи, содержащей множество терминалов (21-28) для передачи данных, в которой разделены плоскость (L1) данных и плоскость (L2) управления, включающий следующие шаги:

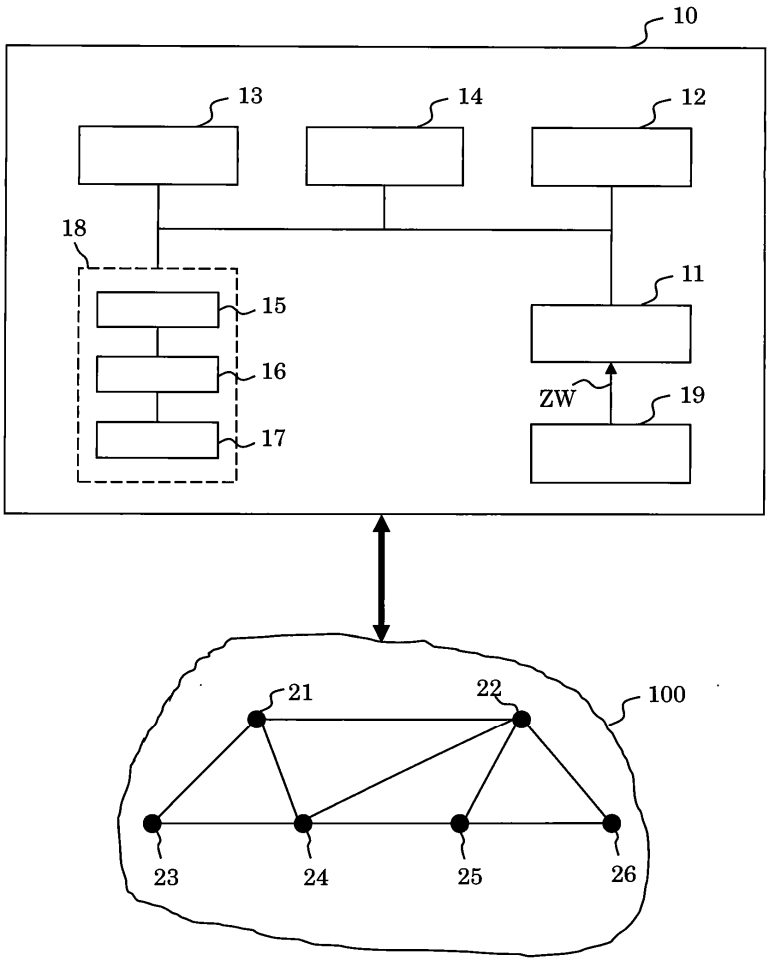
модификация (902) по меньшей мере одной характеристики сети (100) связи, видимой для терминала (200), расположенного вне сети (100) связи, во время сеанса связи с использованием отделенной плоскости (L2) управления, при этом

упомянутая модификация включает изменение виртуального адреса по меньшей мере одного из множества терминалов (21-28) во время сеанса связи с использованием отделенной плоскости (L2) управления; и

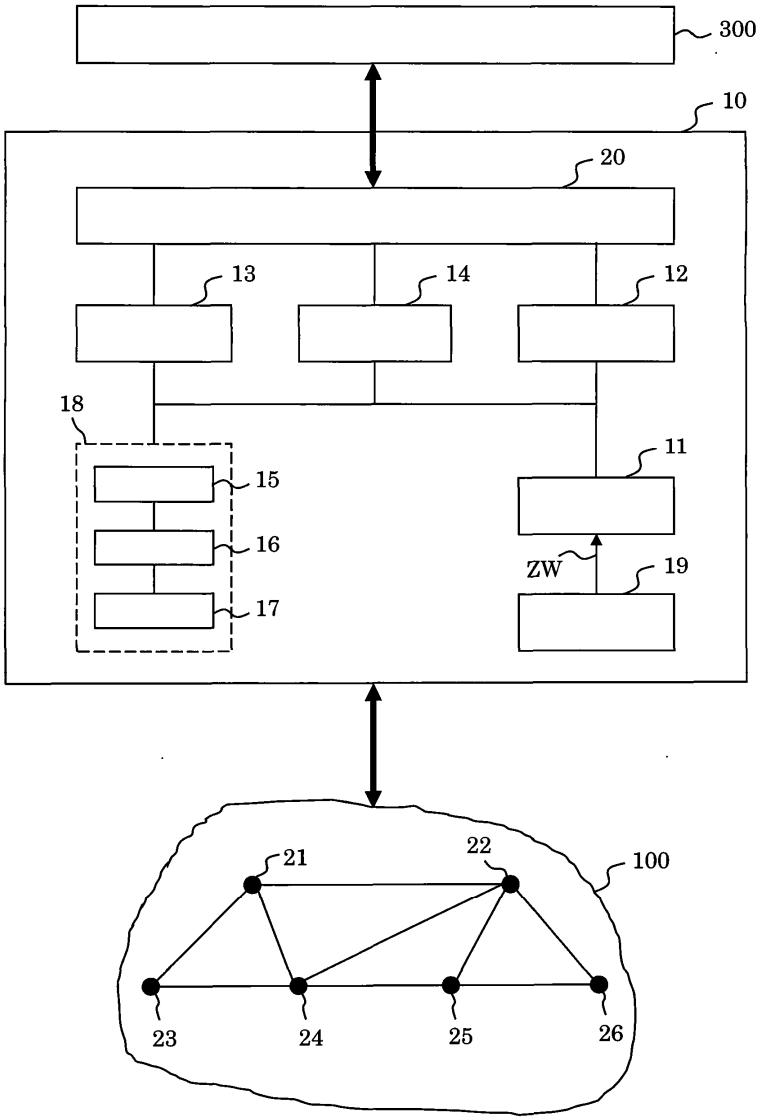
вывод генератором (19) случайных значений случайного значения (ZW), при этом упомянутое изменение виртуального адреса зависит от случайного значения (ZW), выведенного генератором (19) случайных значений.



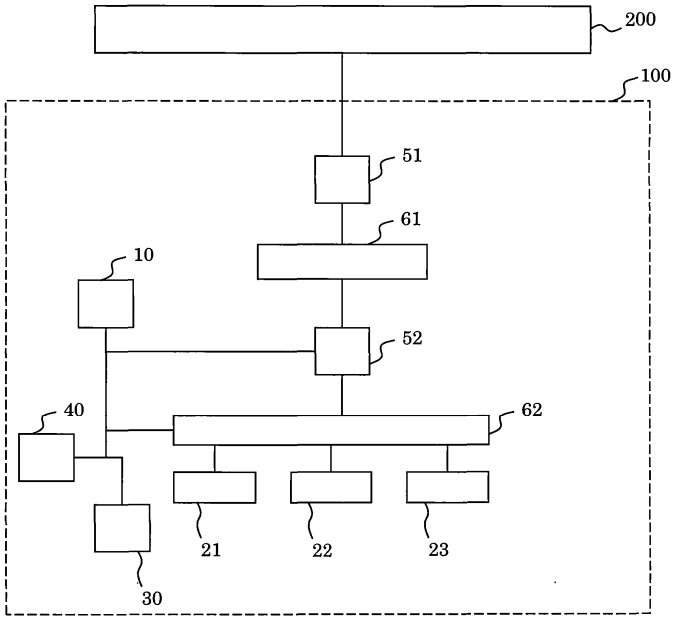
Фиг. 1



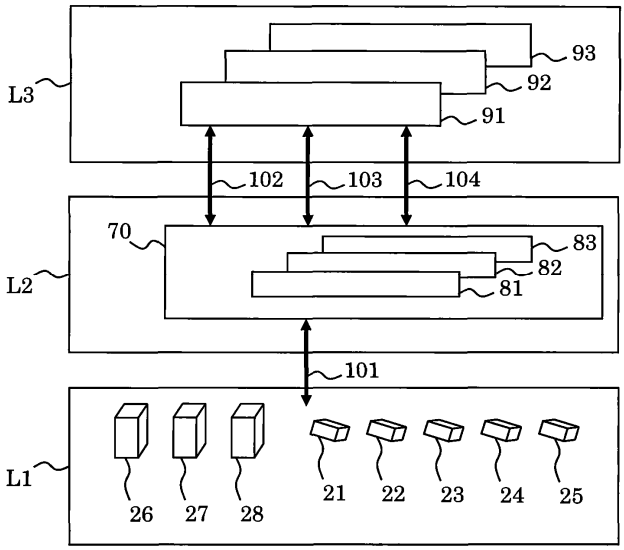
Фиг. 2


300
10
20
13
14
12
18
11
15
16
ZW
19
17
21
22
100
23
24
25
26

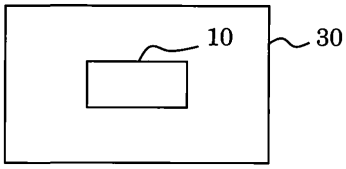
Фиг. 3


200
100
51
61
10
52
40
62
21
22
23
30

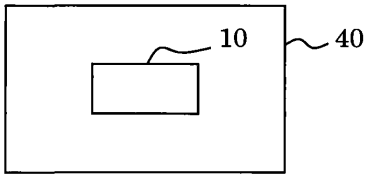
Фиг. 4



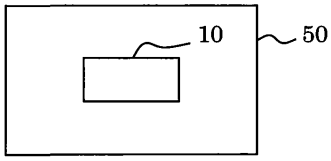
Фиг. 5



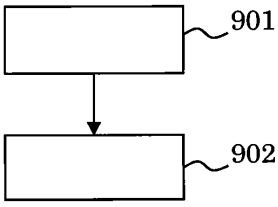
Фиг. 6



Фиг. 7



Фиг. 8



Фиг. 9

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2