Применение методов машинного обучения в SDN в задачах обнаружения вторжений

С. С. Волков, И. И. Курочкин

***Аннотация*—Резкое увеличение количества абонентов телекоммуникационных сетей существенно осложнило использование традиционных сетевых архитектур. Чтобы соответствовать растущим потребностям абонентов телекоммуникационных сетей, была предложена архитектура SDN (Software-Defined Network). Поскольку технология SDN обеспечивает возможности сетевой виртуализации, разделяет плоскости управления и переадресации, реализует логически централизованное управление и открывает возможности гибкого конфигурирования сети в соответствии с потребностями сервисов и приложений. Эта архитектура особенно подходит для реализации сетей ЦОД. Такая сеть будет отличаться функциональностью, и поддерживать централизованное управление. В данной статье представлен обзор технологии программно-конфигурируемых сетей. Описаны особенности архитектуры данных сетей, а также основные преимущества данной технологии перед архитектурой традиционных сетей. Рассмотрен вопрос обеспечения безопасности в SDN. На основании анализа статей был сделан вывод, что решать проблему безопасности программно-конфигурируемых сетей можно с помощью методов машинного обучения. Представлен обзор различных исследований и экспериментов по использованию этих методов для выявления и предотвращения потенциальных атак в SDN. Методы машинного обучения также могут применяться для анализа трафика с учетом QoS (Quality of Service «качество обслуживания»). Рассмотрены работы, посвященные обеспечению качества обслуживания программно-конфигурируемых сетей. В том числе с использованием методов машинного обучения.**

***Ключевые слова*—Программно-конфигурируемые сети, ПКС, информационная безопасность, машинное обучение, SDN.**

I. Введение

Резкое увеличение количества подключенных устройств к сети Интернет привело к ряду полезных решений в различных областях, таких как сельское хозяйство, здравоохранение, промышленность, коммерции. Такое огромное увеличение спроса на подключение бросило вызов традиционным сетевым архитектурам. Чтобы соответствовать спросу, была предложена архитектура – программно-конфигурируемая сеть (Software-Defined Network, SDN), в которой функционал управления (control plane) отделен (абстрагирован) от нижележащего уровня пересылки пакетов (data plane). SDN предлагает возможность программирования сети и позволяет динамически изменять политику потоков.

Следует отметить, что часто вместе с термином “SDN” соседствует еще одна аббревиатура - NFV (network-functions virtualization) - виртуализация сетевых функций. SDN и NFV во многом похожи, имеют много одинаковых компонентов и преследуют решение близких задач. Виртуализация сетевых функций NFV (Network Functions Virtualization) – технология виртуализации физических сетевых элементов телекоммуникационной сети, в которой сетевые функции исполняются программными модулями, работающими на стандартных серверах и виртуальных машинах в них. Эти программные модули могут взаимодействовать между собой для предоставления услуг связи, чем ранее занимались аппаратные платформы. SDN и NFV, в общем, не зависят друг от друга, хотя NFV может в значительной степени дополнять SDN.

Особое внимание хотелось бы уделить крупным центрам обработки данных (ЦОД). Рост, который продемонстрировали сети ЦОД превратил эти сети в ключевой элемент корпоративной информационно-вычислительной инфраструктуры. Чтобы сети ЦОД могли поспевать за ростом данных из новых источников, требуются новые возможности серверов, как для хранения, так и для обработки все более сложных сервисных взаимодействий. Однако архитектуры и технологии традиционных ЦОД перестают соответствовать возникающим требованиям к высокой эффективности, интеллектуальности и удобству работы. Это привело к необходимости использования SDN. Поскольку технология SDN обеспечивает возможности сетевой виртуализации, разделяет плоскости управления и переадресации, реализует логически централизованное управление и открывает возможности сети для приложений верхних уровней, она особенно подходит для реализации сетей ЦОД. Такая сеть будет отличаться функциональностью, поддерживающей централизованное управление.

Тем не менее, эта новая инновационная и улучшенная технология также вносит и новые проблемы безопасности в сетевую архитектуру. Теперь основной

Статья получена 06 июня 2019. Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №18-29-03264.

С. С. Волков, Российский Университет Дружбы Народов, г. Москва, Россия (e-mail: volkserg1@gmail.com).

И. И. Курочкин, Институт проблем передачи информации им. А.А. Харкевича Российской академии наук, г. Москва, Россия (e-mail: qurochkin@gmail.com)

целью атак является центральный контроллер. Контроллер уязвим для различных атак, например, для распределенных атак отказа в обслуживании (Distributed Denial of Service, DDoS), которые могут привести к исчерпанию ресурсов сети. В результате услуги, предоставляемые контроллером, могут стать недоступны. Для обеспечения защиты SDN необходима интеграция системы обнаружения вторжений (Intrusion Detection System, IDS). Обнаружение атак требует адаптивного и точного классификатора, который способен принимать решения на основе неопределенной информации. Очень важно обнаружить атаку в контроллере на ранней стадии. Важной особенностью SDN-сети является то, что наличие OpenFlow технологически позволяет использовать саму сеть как сенсор, поскольку информация о потоках может быть получена из всех критических и важных точек.

В статье рассмотрены основные преимущества SDN, возможные типы атак на сеть данного типа, а также существующие работы, связанные с обеспечением безопасности SDN с помощью методов, основанных на машинном обучении.

II. Описание технологии SDN

Программно-конфигурируемая сеть – метод администрирования компьютерных сетей, позволяющий управлять услугами сети, когда функционал управления (control plane) отделен (абстрагирован) от нижележащего уровня пересылки пакетов (data plane). Планирование сети и управление трафиком при этом происходит программным путем. Для приложений верхнего уровня предоставляются интерфейсы прикладного программирования (Application Programming Interface, API). Таким образом, ввод новых услуг на сети ускоряется и облегчается.

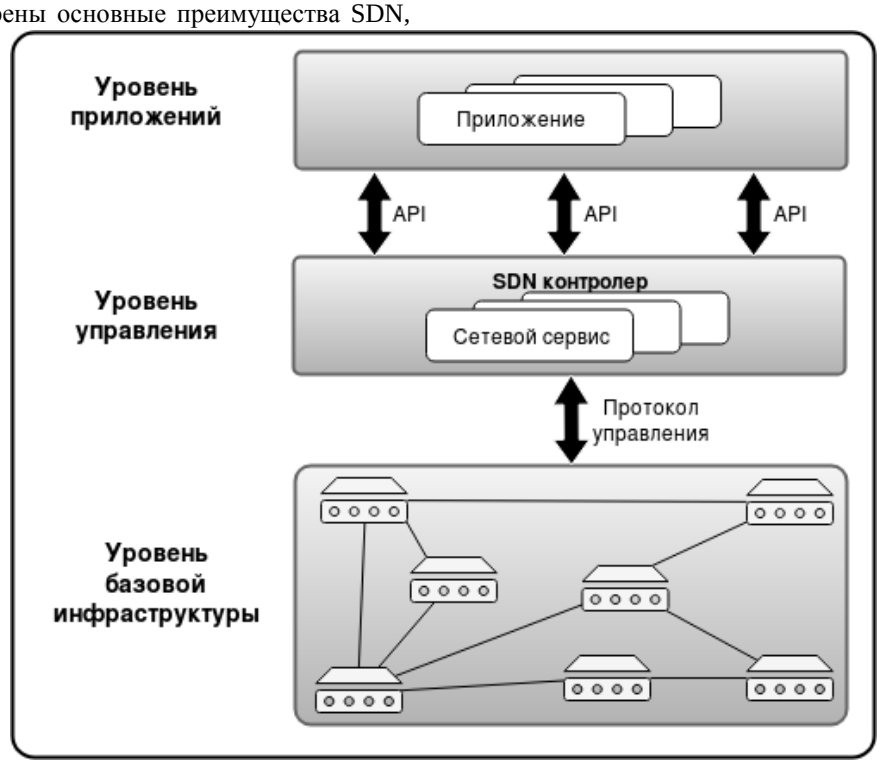

Рисунок 1. Архитектура SDN

В архитектуре SDN выделяют три уровня [19] (рисунок 1):

1. Инфраструктурный уровень, включающий в себя набор сетевых устройств.
2. Уровень управления, включающий операционную систему, которая обеспечивает приложениям сетевые сервисы и программный интерфейс для управления сетевыми устройствами и сетью.
3. Уровень сетевых приложений для управления сетью.

Программно-конфигурируемые сети часто используются для построения инфраструктурных облачных сервисов, в условиях, когда по запросу потребителей услуг необходимо автоматически и в кратчайшие сроки создавать виртуальные узлы и выделять виртуальные сетевые ресурсы. Также использование программно-конфигурируемых сетей целесообразно в крупных центрах обработки данных, позволяя сократить расходы на сопровождение сети за счет централизации управления на программном контроллере и повысить процент использования ресурсов сети благодаря динамичному управлению [20].

Наиболее перспективным и активно развивающимся протоколом для SDN является OpenFlow, но есть и другие: ForCES, Open vSwitch Database (OVSDB), POF OpFlex, OpenState, revised open-flow library (ROFL), hardware abstraction layer (HAL), programmable abstraction of data path [19]. OpenFlow — протокол управления процессом обработки данных, передающихся по сети передачи данных маршрутизаторами и коммутаторами, реализующий технологию программно-конфигурируемой сети. Первая версия OpenFlow (v1.1) была реализована 28 февраля 2011 года. Разработкой стандарта занималась Open Networking Foundation (ONF). Протокол используется для управления сетевыми коммутаторами и маршрутизаторами с центрального устройства — контроллера сети. Контроллером в сети может

выступать отдельный сервер или даже обычный компьютер администратора, на котором установлена сетевая операционная система, обеспечивающая интерфейсы управления между сетевыми приложениями и коммутаторами сети. Контроллер используется для управления таблицами потоков коммутаторов, на основании которых принимается решение о передаче принятого пакета на конкретный порт коммутатора. Таким образом, в сети формируются прямые сетевые соединения с минимальными задержками передачи данных и необходимыми параметрами.

III. Преимущества SDN

В результате стремительного развития информационных технологий можно наблюдать следующие тенденции развития корпоративных сетей и сетей центров обработки данных:

- Стремительный рост объемов трафика и изменение его структуры в сторону передачи видео и унифицированных коммуникаций.
- Необходимость обработки больших данных (Big Data) привела к появлению высокопроизводительных вычислительных центров.
- Рост популярности облачных технологий. Как следствие, развитие технологий виртуализации для предоставления облачных сервисов (Cloud Bursting).

Проблема традиционных сетей больших масштабов заключается в распределенном управлении сетевыми устройствами. Изменение конфигурации такой сети является сложной задачей и может занимать много времени.

SDN могут предоставить новые возможности, позволяя решать задачи повышения пропускной способности каналов, упрощения управления сетью, перераспределения нагрузки и повышения масштабируемости сети. К основным преимуществам архитектуры SDN относительно традиционных современных сетей можно отнести [21]:

1. *Глубокая интеграция*. Каждый веб-сервис может направить требования к пропускной способности к контроллеру, который отвечает за удовлетворение запроса.
2. *Уменьшение стоимости развертывания сетей*. Вместо физического обновления компонентов под решение конкретных задач, достаточно обновить программное обеспечение контролера.
3. *Переход от распределенного к централизованному управлению*. Процесс внедрения новых алгоритмов маршрутизации трафика или их изменение становится проще.
4. *Возможность разработки и развития сетевых программных модулей*. SDN-контроллер имеет интерфейсы API, которые могут использоваться приложениями.
5. *Глобальное представление и планирование*. Контроллер ссылается на глобальное представление о сети, тем самым, использование сетевых ресурсов может стать более рациональным, а также масштабирование сети становится проще.
6. *Открытость ПО и инструментов*, позволяющая не зависеть от производителей сетевых устройств.
7. *Удобство администрирования и отладки*. Все управление сетью сосредоточено (логически) в одном месте, в контроллере SDN. Администратор может быстро изменять правила работы сети для адаптации к изменившимся требованиям.

IV. Безопасность в SDN

Поскольку архитектура SDN предполагает совершенно иной подход к реализации сетевой инфраструктуры, она также приносит новые проблемы безопасности в сети. Теперь основной целью атак является центральный контроллер, так как он является ключевым компонентом в управлении всей инфраструктурой SDN.

Выделяют следующие виды атак: атаки электронной почты (mailbombing), переполнение буфера, использование специализированных программ (вирусов, снифферов, троянских коней, почтовых червей, rootkit-ов и т.д.), сетевая разведка, использование чужого IP-адреса (IP-спуфинг), атака посредника (man-in-the-middle), инъекция (SQL-инъекция, PHP-инъекция, межсайтовый скриптинг или XSS-атака, XPath-инъекция), отказ в обслуживании (DoS- и DDoS- атаки), phishing-атаки и так далее [22]. Не все из них возможно применить непосредственно на программно-конфигурируемые сети.

Существует классификация атак, специфичных для SDN. Все возможные атаки можно разделить следующим образом [41]:

- Атаки на функционал управления (control plane):
    - Packet-In Flooding - одна из разновидностей DoS атак
    - Service Chain Interference (нарушение последовательного выполнения приложений) – данная атака может привести к двум последствиям: 1) вредоносное приложение может участвовать в цепочке и удалить управляющее сообщение до того, как другие приложения получат необходимую информацию. 2) вредоносное приложение может попасть в бесконечный цикл, чтобы остановить цепное выполнение приложений
    - Internal Storage Abuse (использование внутренней памяти контролера)
    - Control Message Manipulation (манипуляции управляющими сообщениями)
    - Control Message Abuse (подмена управляющего сообщения)
    - Northbound API Abuse - Приложение SDN может манипулировать поведением других приложений, используя плохо спроектированный Northbound API.
    - Resource Exhaustion (исчерпание ресурсов)
    - System Variable Manipulation (манипуляция системными переменными)
    - System Command Execution (выполнение системных команд)
    - Network Topology Poisoning (изменение

топологии сети)

- Атаки на канал управления (control channel):
  - Man-In-The-Middle (атака посредника)
  - Eavesdrop - злоумышленник может прослушать канал управления, чтобы украсть конфиденциальную информацию
- Атаки на уровень управления данными (data plane):
  - Flow Rule Flooding (генерация большого потока правил)
  - Switch Firmware Abuse (изменение свойств коммутатора)
  - Control Message Manipulation (манипуляции управляющими сообщениями)

В работе [23] представлено описание основных уязвимостей технологии SDN, а также протокола OpenFlow. Приведено несколько примеров использования уязвимостей с целью нарушения работоспособности системы. В качестве противодействия угрозам информационной безопасности в сетях SDN рассмотрены следующие методы:

- Предварительное выявление несоответствий в конфигурации сети (может быть достигнуто применением модулей верификации).
- Усовершенствование подходов к контролю потоков трафика (достигается благодаря использованию особенностей архитектуры SDN).
- Использование механизмов аутентификации и авторизации на уровне приложений. Предлагаются механизмы, адаптированные для разграничения доступа различных служб и сетевых сервисов.

Из-за централизации управления SDN сетей наиболее серьезной угрозой для них являются атаки типа «отказ в обслуживании», которые могут привести к исчерпанию ресурсов сети. Успешная реализация такой атаки может привести к следующим последствиям:

- Исчерпание ресурсов коммутатора. Легитимные пакеты либо вообще не будут обработаны данным сетевым узлом, либо их обработка будет сопровождаться задержками.
- Канал связи между контроллером и коммутатором не обеспечит доставки управляющих сообщений, будучи загруженным потоками данных.
- Контроллер будет перегружен приходящими запросами и не сможет обрабатывать управляющие сообщения, вызванные легитимным трафиком.

Существует несколько программных инструментов с открытым исходным кодом, которые отслеживают и ограничивают количество попыток входа в систему с определенного IP-адреса источника. Однако эти решения не могут эффективно противостоять злоумышленникам, проводящим цепочки атак, включающие множество IP-адресов. Для решения данной задачи требуется более детальный анализ всего трафика, а не отдельного соединения.

Для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность системы, используется система обнаружения вторжений (Intrusion Detection System, IDS).

Обычно архитектура IDS включает:

- Подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы.
- Подсистему анализа, предназначенную для выявления атак и подозрительных действий на основе имеющихся данных.
- Хранилище, обеспечивающее накопление результатов анализа.
- Консоль управления, позволяющая конфигурировать IDS.

Выделяют два типа систем предотвращения вторжений: пассивные и активные. В пассивной IDS при обнаружении нарушения безопасности информация о нарушении записывается в журнал приложения, а информация об инциденте отправляется на консоль и/или администратору системы по определенному каналу связи. В активной IDS предусмотрены активные действия в ответ на нарушения. Это может быть сброс соединения или, например, перенастройка сетевого экрана для блокирования трафика от злоумышленника.

Активную IDS также называют системой предотвращения вторжений (Intrusion Prevention System, IPS). IPS-системы делятся на сетевые IPS (Network IPS), которые позволяют обнаруживать несанкционированные действия в сети, анализируя сетевой трафик, и IPS для рабочих станций и серверов (Host IPS), которые позволяют обнаруживать несанкционированные действия на отдельном сервере или рабочей станции. Отдельно необходимо выделить сетевые IPS-системы, основанные на поведенческом анализе и выявлении аномалий в сети. Именно такие системы используются для обнаружения и противодействия атак отказа в обслуживании (Denial of Service, DoS). Ядром IPS-системы является подсистема анализа, именно она отвечает за качество обнаружения несанкционированных действий. Предлагается рассматривать возможность функционирования данной подсистемы на основе алгоритмов машинного обучения. Обучив алгоритмы на данных работы сети, которые включают в себя случаи вторжения, можно создать классификатор, который будет анализировать поток трафика и реагировать на аномальное поведение потока как на потенциальную атаку системы.

В статье [18] говорится о тенденциях и характеристиках DDoS-атак в облачных вычислениях, а также представлен всесторонний обзор механизмов защиты от DDoS-атак с использованием SDN. Кроме того, исследованы различные варианты запуска DDoS-атак на SDN, а также методы противодействия DDoS-атакам. Эта работа позволяет понять, как в полной мере использовать преимущества SDN для защиты от DDoS-атак в облачных вычислительных средах.

Стоит также отметить исследования, уделяющие особое внимание информационной безопасности в SDN. Группа исследователей из техасского университета A&M в своих многочисленных работах рассматривает варианты предотвращения разного рода атак, а также предлагают решения по защите SDN. В работе [37] рассматривается атака переполнения плоскости данных,

которая может перегрузить инфраструктуру сетей SDN. А также представлена независимая от протокола инфраструктура защиты для программно-конфигурируемых сетей. В работе [38] авторы представили обзор безопасности программно-конфигурируемых сетей, а также возможности новых функций SDN в обеспечении защиты информации. В [39] авторы описывают методы защиты от атак, направленных на изменение топологии сети. Работа [40] посвящена автоматизации и стандартизации процесса идентификации уязвимостей в SDN. Авторы разработали инфраструктуру оценки безопасности, DELTA, которая может воспроизвести опубликованные атаки на сети SDN в различных средах тестирования.

V. Машинное обучение в SDN

При решении задачи обеспечения защиты SDN становится актуальным вопрос автоматизации процесса выявления потенциальных атак и принятия дальнейших решений. Даже если сетевой администратор способен идентифицировать потенциальную атаку и злоумышленника, может оказаться невозможным эффективно учитывать большое количество одновременных атак в режиме реального времени. Поэтому появляется необходимость в определенных правилах безопасности, которые обычно реализуются на контроллере SDN, аналогично правилам брандмауэра. Однако определение этих правил может быть сложной задачей, поскольку целью таких правил является ограничение доступа для вредоносных узлов или злоумышленников при одновременном предоставлении беспрепятственного доступа обычным пользователям. Для выявления злоумышленников среди потока пользователей могут быть использованы различные методы, включая машинное обучение. Но именно подходы, основанные на машинном обучении, показывают значительный потенциал в решении данной задачи [3]. Далее рассмотрены работы, посвященные вопросам обеспечения безопасности программно-конфигурируемых сетей с помощью методов машинного обучения.

В [6] предложена основанная на глубоком обучении многовекторная система обнаружения DDoS-атак в программно-конфигурируемой сети. Авторы внедрили систему как сетевое приложение поверх SDN-контроллера. Используется глубокое обучение для сокращения числа признаков из большого набора, полученного из заголовков сетевого трафика. Оценка системы производится на основе различных показателей (accuracy, precision, recall, f-measure, ROC).

В работе [2] авторы рассматривают четыре широко известных алгоритма машинного обучения: деревья решений (C4.5), Байесовская сеть (Bayesian network), Таблица принятия решений (Decision Table) и Наивный байесовский классификатор (Naive-Bayes). Алгоритмы, полагаясь на собранные “исторические” данные и на текущее поведение трафика сети, должны предсказать возможную атаку на определенный узел. По результатам экспериментов наилучшую точность предсказания показал алгоритм, использующий Байесовскую сеть.

Байесовская сеть является графовой вероятностной моделью. Формально, байесовская сеть — это направленный ациклический граф, каждой вершине которого соответствует случайная переменная, а дуги графа кодируют отношения условной независимости между этими переменными. Вершины могут представлять переменные любых типов, быть взвешенными параметрами, скрытыми переменными или гипотезами. Байесовская сеть может быть использована в качестве классификатора и при правильном обучении может показать очень точные результаты классификации.

Еще одним широко используемым классификатором является SVM (Support Vector Machine - метод опорных векторов). Данный метод также показывает достаточно высокую точность и малое количество ложных срабатываний. В работе [4] представлен анализ классификатора SVM и сравнение его эффективности с другими классификаторами (RBF, Naive Bayes, J48, Random Forest). По результатам экспериментов SVM показал лучшую точность и наименьшее число ложных срабатываний.

Для обнаружения вторжений в SDN также возможно использование глубоких нейронных сетей. В работе [42] авторы используют GRU-RNN (Gated Recurrent Unit Recurrent Neural Network). Предложенный подход протестирован с использованием набора данных NSL-KDD. Результаты эксперимента показывают высокую точность обнаружения – 89%. Авторы пришли к заключению, что предлагаемая GRU-RNN действует эффективно и при этом не ухудшает производительность сети.

Для решения данной задачи можно использовать и многослойный персептрон. Так, например, в [5] авторы использовали модель, основанную на нейронной сети, которая была обучена на наборе данных NSL-KDD. Нейронная сеть состоит из 6 входных нейронов, которые соответствуют 6 выбранным признакам, характерным для потока:

- duration - время (количество секунд) соединения.
- protocol_type - тип протокола (tcp, udp и т. д.).
- src_bytes - количество байтов, переданных от источника к получателю.
- dst_bytes - количество байтов, переданных от получателя к источнику.
- count - количество подключений к хосту (за прошедшие 2 секунды), используемому текущим соединением.
- srv_count - количество подключений к сервису (за прошедшие 2 секунды), используемому текущим соединением.

Следом расположены три скрытых слоя (12, 6 и 3 нейронов). На выходе сеть имеет 2 нейрона. Данный метод продемонстрировал хороший потенциал и даже на 6 признаках показал точность (~76%), сравнимую с известными алгоритмами машинного обучения (J48, Naive Bayes (NB), NB Tree, Random Forest, Random Tree, SVM). Отсюда следует, что нейронные сети могут быть использованы для выявления аномального поведения

трафика в SDN.

Даже простые нейронные сети (например, однослойный персептрон) способны решать задачу обнаружения вторжений в программно-конфигурируемых сетях [9]. Модель обучали на том же наборе данных NSL-KDD. Для обучения сети используется метод обратного распространения ошибки (backpropagation). Анализ трафика проводился по семи выбранным признакам:

- duration - время (количество секунд) соединения.
- protocol_type - тип протокола (tcp, udp и т. д.).
- service (HTTP, telnet, ssh и т.д.).
- src_bytes - количество байтов, переданных от источника к получателю.
- dst_bytes - количество байтов, переданных от получателя к источнику.
- count - количество подключений к хосту (за прошедшие 2 секунды), используемому текущим соединением.
- srv_count - количество подключений к сервису (за прошедшие 2 секунды), используемому текущим соединением.

Данная модель смогла показать высокую точность на тестовой выборке. Это подтверждает возможность и актуальность применения нейронных сетей для решения задачи обнаружения вторжений в SDN.

В [10] представлена модель обнаружения DDoS и система защиты на основе глубокого машинного обучения в среде программно-конфигурируемой сети. Проведено сравнение работоспособности нескольких нейронных сетей (LSTM, CNN/LSTM, GRU, 3LSTM). Измерение точности проводилось на наборе данных ISCX. Лучший результат продемонстрировала модель 3LSTM - 99%.

По результатам экспериментов можно сделать вывод что схема обнаружения DDoS-атак, основанная на глубоком машинном обучении, обладает следующими преимуществами:

1. высокая точность обнаружения
2. слабая зависимость от аппаратных и программных устройств
3. простое обновление сетевой модели

Данный метод компенсирует недостатки существующих схем обнаружения DDoS-атак.

В [11] рассмотрен новый подход к построению сетей и управлению с использованием технологий SDN и Big Data, а также выделены основные преимущества их совместного использования. Рассмотрена архитектура технологии SDN. Выделены ее ключевые особенности (разделение уровня передачи данных от уровня управления, централизация логики управления сетью), которые могут быть полезны при решении задач обработки данных в облачных дата-центрах, доставки данных для BigData-приложений, эффективного планирования задач в Фреймворке Hadoop.

Предложен метод обнаружения сетевых атак с помощью конечных автоматов, генерируемых на основе генетических алгоритмов [15].В работе представлены два метода. В основе первого метода лежит модель «флиба»[15], способная предсказывать изменения сетевой активности на основе поступательного анализа сетевых записей в формате KDD-99. Второй метод является адаптацией классического конечного автомата.

В [12] был построен и исследован прототип автономной системы для обеспечения безопасности и качества обслуживания облачных платформ. В основу разработанной системы положена модель анализа трафика, основанная на нейронной сети. Предложена гибридная архитектура нейронной сети на основе многослойного персептрона и самоорганизующейся сети Кохонена. Такой подход позволил более точно классифицировать и обнаруживать вредоносный трафик. Проведенные экспериментальные исследования показали, что использование предлагаемого решения позволяет повысить эффективность обнаружения таких атак как отказ в обслуживании, а также во время атаки обеспечить требуемое качество обслуживания.

В [13] разработан основанный на нечеткой логике прототип системы обнаружения вторжений для SDN. Прототип состоит из двух модулей:

1. модуль сбора и обработки статистики
2. модуль принятия решений.

Исследования проводились с использованием среды моделирования Mininet [14] для оценки работы модулей. Предложенный алгоритм решения, основанный на нечеткой логике, показал лучшие результаты, чем алгоритмы безопасности, используемые отдельно.

Нейронные сети также могут использоваться для интеллектуальной обработки сетевого трафика. Они способны анализировать трафик и отличать подозрительное поведение от нормы [16],[17]. Для задач классификации чаще всего используют сети прямого распространения. В решении задач, связанных с прогнозированием, наиболее хорошо зарекомендовали себя рекуррентные нейронные сети. Помимо этого, они могут использоваться в задачах снижения размерности и классификации. Для фильтрации входящего в систему трафика тоже могут применяться алгоритмы на основе рекуррентных нейронных сетей.

В SDN машинное обучение также может применяться для анализа трафика с учетом QoS (Quality of Service «качество обслуживания»). QoS - технология предоставления различным классам трафика различных приоритетов в обслуживании. Обеспечение качества обслуживания в традиционных сетевых архитектурах является важной задачей. Хотя исследователи из академических кругов и промышленности предложили множество решений для устранения ограничений QoS в существующих сетях, многие из них либо потерпели неудачу, либо не были реализованы. Парадигма программно-определяемой сети возникла в ответ на ограничения традиционных сетевых архитектур. Ее основными преимуществами являются централизованное представление глобальной сети, программируемость и разделение плоскости данных и плоскости управления. Эти функции привлекли внимание исследователей для улучшения обеспечения QoS различных современных сетевых приложений. В работе [43] представлен обзор, в котором авторы

сгруппировали различные исследования в соответствии с категориями, в которых QoS может извлечь выгоду из концепции SDN:

- механизмы маршрутизации мультимедийных потоков,
- механизмы междоменной маршрутизации,
- механизмы резервирования ресурсов,
- механизмы управления очередями и планирования,
- механизмы мониторинга сети и другие QoS-ориентированные механизмы, такие как обеспечение QoS на основе виртуализации, управление политикой QoS и т. д.

Помимо этого, авторы описывают в общих чертах потенциальные проблемы, которые необходимо решать в дальнейшем для улучшения QoS в сетях SDN.

В работе [44] авторы демонстрируют подход к качеству обслуживания, который управляется и определяется централизованным сетевым контроллером в SDN.

В работе [45] авторы представляют систему под названием QoS Controller (Q-Ctrl), для программного достижения требуемых пользователем ограничений QoS в облачной инфраструктуре на основе SDN. В своей статье они описывают:

1) проектирование и реализацию системы Q-Ctrl,
2) как поддерживается QoS сети для виртуальных машин с помощью Q-Ctrl,
3) пример того, как приложение потокового видео использует Q-Ctrl систему для достижения необходимого QoS в облачной инфраструктуре на основе SDN.

При решении задач, связанных с качеством обслуживания, также актуально использование методов машинного обучения. В работе [1] предлагается метод классификации трафика с учетом QoS для программно-конфигурируемых сетей. Данный подход классифицирует сетевой трафик по разным классам в соответствии с требованиями QoS, которые предоставляют важную информацию для обеспечения детального проектирования трафика. Предложенная структура полностью расположена в сетевом контроллере. Она использует методы проверки пакетов и машинное обучение, что позволяет реализовать точную классификацию трафика. Моделирование проводилось на основе данных, которые были получены исследовательской группой по широкополосной связи в UPC (Universitat Politècnica de Catalunya, Политехнический университет Каталонии, Барселона, Испания). Набор данных представляет собой файл трассировки трафика объемом 59 ГБ. Результаты моделирования показывают, что предлагаемая классификационная структура может обеспечить хорошую производительность с точки зрения точности классификации и затрат на связь.

Еще одним примером является платформа Atlas [3], которая обеспечивает детальную, точную и масштабируемую классификацию приложений в SDN. В ней используется метод классификации трафика на основе машинного обучения.

В [8] авторы описывают простую архитектуру, развернутую в корпоративной сети, которая собирает данные о трафике с использованием протокола OpenFlow. Представлены наборы данных, которые можно получить, и демонстрируется, как несколько методов машинного обучения могут быть применены к ним для классификации трафика. Результаты показывают, что с такими наборами данных может быть получена высокая точность классификации, при использовании контролируемого обучения.

VI. Заключение

В результате исследования был проведен обзор существующих работ, посвященных решению задачи обнаружения вторжений в программно-конфигурируемых сетях. Удалось выяснить, что решать задачу обнаружения вторжений в SDN можно с помощью методов машинного обучения. Представлен обзор различных исследований и экспериментов по использованию этих методов для выявления и предотвращения потенциальных атак в SDN. Специфика программно-конфигурируемых сетей позволяет использовать методы защиты, отличные от методов, свойственных сетям с традиционной архитектурой, так как наличие OpenFlow позволяет использовать саму сеть как сенсор. Методы машинного обучения также могут применяться для анализа трафика с учетом QoS. Это позволит увеличить эффективность распределения ресурсов сети.

Дальнейшие работы будут посвящены анализу методов обнаружения вторжений, а также исследованию и разработке системы обнаружения вторжений (IDS), которая служит для обнаружения несанкционированных действий в программно-конфигурируемых сетях с использованием методов машинного обучения.

Библиография

[1] Wang P., Lin S. C., Luo M. A framework for QoS-aware traffic classification using semi-supervised machine learning in SDNs //2016 IEEE International Conference on Services Computing (SCC). – IEEE, 2016. – С. 760-765.

[2] Nanda S. et al. Predicting network attack patterns in SDN using machine learning approach //2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). – IEEE, 2016. – С. 167-172.

[3] Qazi Z. A. et al. Application-awareness in SDN //ACM SIGCOMM computer communication review. – ACM, 2013. – Т. 43. – №. 4. – С. 487-488.

[4] Kokila R. T., Selvi S. T., Govindarajan K. DDoS detection and analysis in SDN-based environment using support vector machine classifier //2014 Sixth International Conference on Advanced Computing (ICoAC). – IEEE, 2014. – С. 205-210.

[5] Tang T. A. et al. Deep learning approach for network intrusion detection in software defined networking //2016 International Conference on Wireless Networks and Mobile Communications (WINCOM). – IEEE, 2016. – С. 258-263.

[6] Niyaz Q., Sun W., Javaid A. Y. A deep learning based DDoS detection system in software-defined networking (SDN) //arXiv preprint arXiv:1611.07400. – 2016.

[7] Sultana N. et al. Survey on SDN based network intrusion detection system using machine learning approaches //Peer-to-Peer Networking and Applications. – 2019. – Т. 12. – №. 2. – С. 493-501.

[8] Amaral P. et al. Machine learning in software defined networks: Data collection and traffic classification //2016 IEEE 24th International Conference on Network Protocols (ICNP). – IEEE, 2016. – С. 1-5.

[9] Abubakar A., Pranggono B. Machine learning based intrusion detection system for software defined networks //2017 Seventh International Conference on Emerging Security Technologies (EST). – IEEE, 2017. – С. 138-143.

[10] Li C. et al. Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN //International Journal of Communication Systems. – 2018. – Т. 31. – №. 5. – С. e3497.
[11] Савина О. А. и др. К вопросу о совместном применении технологий SDN и big data //д-ра экон. наук, канд. техн. наук, проф. ПВ Терелянского, д-ра экон. наук СА Лукьянова. – 2017. – С. 74.
[12] Болодурина И. П., Парфёнов Д. И. Исследование модели нейронной сети для обеспечения безопасности и качества обслуживания мультиоблачной платформы //Информационные и математические технологии в науке и управлении. – 2018. – №. 3. – С. 18-26.
[13] Dotcenko S., Vladyko A., Letenko I. A fuzzy logic-based information security management for software-defined networks //16th International Conference on Advanced Communication Technology. – IEEE, 2014. – С. 167-171.
[14] Lantz B., Heller B., McKeown N. A network in a laptop: rapid prototyping for software-defined networks //Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks. – ACM, 2010. – С. 19.
[15] Фраленко В. П. Обнаружение сетевых атак с помощью генетически создаваемых конечных автоматов // Вестник РУДН. Серия: Математика, информатика, физика. 2012. №4.
[16] Кондратьев А. А. Распределённая система обнаружения и предотвращения сетевых атак на системы облачных вычислений // Вестник РУДН. Серия: Математика, информатика, физика. 2014. №1.
[17] Иванов В. Г., Киреев С.Х., Лыжинкин К.В. Применение методов искусственного интеллекта для обнаружения компьютерных атак // Труды ЦНИИС. Санкт-Петербургский филиал. 2017. Т. 1. № 4. С. 109-116.
[18] Yan Q. et al. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges //IEEE communications surveys & tutorials. – 2015. – Т. 18. – №. 1. – С. 602-622.
[19] Семеновых А. А., Лапонина О. Р. Сравнительный анализ SDN-контроллеров. // International Journal of Open Information Technologies ISSN: 2307-8162. - 2018. - vol. 6. - №. 7.
[20] Ошкина Е. В. Сетевая технология SDN (обзор, современные тенденции) [Текст] // Технические науки: проблемы и перспективы: материалы V Междунар. науч. конф. (г. Санкт-Петербург, июль 2017 г.). — СПб.: Свое издательство, 2017. — С. 3-6. — URL https://moluch.ru/conf/tech/archive/231/12628/ (дата обращения: 30.05.2019).
[21] Коломеец А. Е., Сурков Л. В. Программно-конфигурируемые сети на базе протокола OpenFlow //Инженерный вестник. – 2014. – №. 5. – С. 2-2.
[22] Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы [Текст] // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). — Уфа: Лето, 2011. — С. 8-13. — URL:https://moluch.ru/conf/tech/archive/5/1115/ (дата обращения: 12.03.2019).
[23] Захаров А. А., Попов Е. Ф., Фучко М. М. Аспекты информационной безопасности архитектуры SDN //Вестник СибГУТИ. – 2016. – №. 1. – С. 83-92.
[24] Логинов С.С. Об уровнях управления в программно-конфигурируемой сети (SDN) // T-Comm: Телекоммуникации и транспорт. 2017. Том 11. No3. С. 50-55.
[25] Martin Casado, Tal Garfinkel, Aditya Akella, Michael J. Freedman Dan Boneh, Nick McKeown, Scott Shenker. SANE: A Protection Architecture for Enterprise Networks //15-th Usenix Security Symposium. Vancouver, Canada. 2006.
[26] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner. Openflow: Enabling innovation in campus networks // SIGCOMM Computer Communication Review. vol. 38. № 2. pp. 69–74, 2008.
[27] SDN Technical Specifications [Электронный ресурс]. URL:https://www.opennetworking.org/software-defined-standards/specifications/ (дата обращения: 10.10.2019)
[28] Hu Y. N. et al. On the placement of controllers in software-defined networks //The Journal of China Universities of Posts and Telecommunications. – 2012. – Т. 19. – С. 92-171.
[29] Hu Y. et al. Reliability-aware controller placement for software-defined networks //Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on. – IEEE, 2013. – С. 672-675.
[30] Чугреев Д.А., Шкребец А.Е., Шевель А.Е., Власов Д.В., Грудинин В.А., Каирканов А.Б., Садов О.Л., Титов В.Б., Хоружников С.Э., Сомс Л.Н. Разработка интерфейса взаимодействия с контроллером программно-конфигурируемых сетей //Современные проблемы науки и образования - 2013. - № 3. - С. 83.
[31] Власов Д.В., Грудинин В.А., Каирканов А.Б., Садов О.Л., Сомс Л.Н., Титов В.Б., Хоружников С.Э., Чугреев Д.А., Шевель А.Е., Шкребец А.Е. Разработка прототипов средств управления сетевыми ресурсами и потоками данных на основе программно-конфигурируемых сетей OpenFlow //Современные проблемы науки и образования. - 2013. - № 3. - С. 86.
[32] Садов О.Л., Власов Д.В., Грудинин В.А., Каирканов А.Б., Сомс Л.Н., Титов В.Б., Хоружников С.Э., Чугреев Д.А., Шевель А.Е., Шкребец А.Е. Исследование сети хранения данных, построенной с использованием программно-конфигурируемых сетей OpenFlow //Современные проблемы науки и образования. - 2013. - № 4. - С. 64.
[33] Лапонина О.Р., Сизов М.Р. Лабораторный стенд для тестирования возможностей интеграции ПКС-сетей и традиционных сетей //International Journal of Open Information Technologies. 2017. Т. 5. № 9. С. 3-12.
[34] Амелянович А.В., Шпаков М.Н., Мутханна А.С., Буйневич М.В., Владыко А.Г. Централизованное управления потоками трафика в беспроводных локальных сетях на базе концепции SDN //Системы синхронизации, формирования и обработки сигналов. 2017. Т. 8. № 2. С. 31-35.
[35] Маньков В.А., Краснова И.А. Алгоритм динамической классификации потоков в мультисервисной SDN-сети // T-Comm: Телекоммуникации и транспорт. 2017. Том 11. No12. С. 37-42.
[36] Смелянский Р.Л., Пилюгин П.Л. Современные проблемы обеспечения безопасности в SDN //REDS: Телекоммуникационные устройства и системы. 2017. Т. 7. № 4. С. 523-526..
[37] Wang H., Xu L., Gu G. Floodguard: A dos attack prevention extension in software-defined networks //2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. – IEEE, 2015. – С. 239-250.
[38] Shin S. et al. Enhancing network security through software defined networking (sdn) //2016 25th International Conference on Computer Communication and Networks (ICCCN). – IEEE, 2016. – С. 1-9.
[39] Hong S. et al. Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures //NDSS. – 2015. – Т. 15. – С. 8-11.
[40] Lee S. et al. DELTA: A Security Assessment Framework for Software-Defined Networks //NDSS. – 2017.
[41] An Overview of Misuse / Attack Cases [Электронный ресурс]. URL: http://www.sdnsecurity.org/vulnerability/attacks/ (дата обращения: 10.10.2019)
[42] Tang T. A. et al. Deep recurrent neural network for intrusion detection in sdn-based networks //2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft). – IEEE, 2018. – С. 202-206.
[43] Karakus M., Durresi A. Quality of service (QoS) in software defined networking (SDN): A survey //Journal of Network and Computer Applications. – 2017. – Т. 80. – С. 200-218.
[44] Wallner R., Cannistra R. An SDN approach: quality of service using big switch's floodlight open-source controller //Proceedings of the Asia-Pacific Advanced Network. – 2013. – Т. 35. – С. 14-19.
[45] Govindarajan K. et al. Realizing the quality of service (QoS) in software-defined networking (SDN) based cloud infrastructure //2014 2nd International Conference on Information and Communication Technology (ICoICT). – IEEE, 2014. – С. 505-510.

Machine learning in SDN

S. S. Volkov, I. I. Kurochkin

***Аннотация*—Increase in demand for network connectivity has challenged traditional network architectures. To match demand, SDN (Software-Defined Network) was proposed as a new architecture. Since SDN technology provides network virtualization capabilities, separates control and data planes, implements logically centralized control and opens up network capabilities for higher-level applications, it is especially suitable for implementing data center networks. This network will be distinguished by functionality that supports centralized management. This article provides an overview of software-defined network technology. The features of the architecture of these networks are described, as well as the main advantages of this technology over the architecture of traditional networks. The issue of security in the SDN is considered. The authors concluded that it is possible to solve the security problem of software-defined networks using machine learning methods. A review of various studies and experiments on the use of these methods to detect and prevent potential attacks in the SDN is presented. Machine learning methods also can be used to analyze traffic taking into account QoS (Quality of Service). Several works on ensuring the quality of service for software-defined networks are considered. Among them there are works that also use machine learning methods.**

***Ключевые слова* — Software-defined network, SDN, information security, machine learning.**

REFERENCES

[1] Wang P., Lin S. C., Luo M. A framework for QoS-aware traffic classification using semi-supervised machine learning in SDNs //2016 IEEE International Conference on Services Computing (SCC). – IEEE, 2016. – С. 760-765.

[2] Nanda S. et al. Predicting network attack patterns in SDN using machine learning approach //2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). – IEEE, 2016. – С. 167-172.

[3] Qazi Z. A. et al. Application-awareness in SDN //ACM SIGCOMM computer communication review. – ACM, 2013. – Т. 43. – №. 4. – С. 487-488.

[4] Kokila R. T., Selvi S. T., Govindarajan K. DDoS detection and analysis in SDN-based environment using support vector machine classifier //2014 Sixth International Conference on Advanced Computing (ICoAC). – IEEE, 2014. – С. 205-210.

[5] Tang T. A. et al. Deep learning approach for network intrusion detection in software defined networking //2016 International Conference on Wireless Networks and Mobile Communications (WINCOM). – IEEE, 2016. – С. 258-263.

[6] Niyaz Q., Sun W., Javaid A. Y. A deep learning based DDoS detection system in software-defined networking (SDN) //arXiv preprint arXiv:1611.07400. – 2016.

[7] Sultana N. et al. Survey on SDN based network intrusion detection system using machine learning approaches //Peer-to-Peer Networking and Applications. – 2019. – Т. 12. – №. 2. – С. 493-501.

[8] Amaral P. et al. Machine learning in software defined networks: Data collection and traffic classification //2016 IEEE 24th International Conference on Network Protocols (ICNP). – IEEE, 2016. – С. 1-5.

[9] Abubakar A., Pranggono B. Machine learning based intrusion detection system for software defined networks //2017 Seventh International Conference on Emerging Security Technologies (EST). – IEEE, 2017. – С. 138-143.

[10] Li C. et al. Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN //International Journal of Communication Systems. – 2018. – Т. 31. – №. 5. – С. e3497.

[11] Savina O. A. et al. K voprosu o sovmestnom primenenii tekhnologiy sdn i big data [to the question of joint application of sdn and big data technologies] // Doctor of Economic Sciences, Candidate of Technical Sciences, Professor of PV Terelyanskiy, Doctor of Economic Sciences SA Lukianova. – 2017. – С. 74.

[12] Bolodurina I. P., Parphenov D. I. Issledovaniye modeli neyronnoy seti dlya obespecheniya bezopasnosti i kachestva obsluzhivaniya mul'tioblachnoy platformy [research of a neural network model to ensure the safety and quality of service of the multi-cloud platform] // Informatsionnyye i matematicheskiye tekhnologii v nauke i upravlenii [Information and mathematical technologies in science and control]. – 2018. – №. 3. – С. 18-26.

[13] Dotcenko S., Vladyko A., Letenko I. A fuzzy logic-based information security management for software-defined networks //16th International Conference on Advanced Communication Technology. – IEEE, 2014. – С. 167-171.

[14] Lantz B., Heller B., McKeown N. A network in a laptop: rapid prototyping for software-defined networks //Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks. – ACM, 2010. – С. 19.

[15] Fralenko V. P. Obnaruzheniye setevykh atak s pomoshch'yu geneticheski sozdavayemykh konechnykh avtomatov [Genetic state machine detection of network attacks] // Herald of the RUDN University. Series: Mathematics, Computer Science, Physics. 2012. №4.

[16] Kondratiev A. A. Raspredelonnaya sistema obnaruzheniya i predotvrashcheniya setevykh atak na sistemy oblachnykh vychisleniy [Distributed system for detecting and preventing network attacks on cloud computing systems] // Herald of the RUDN University. Series: Mathematics, Computer Science, Physics. 2014. №1.

[17] Ivanov V. G. Kireev S. H., Lyzhkin K. V. Primeneniye metodov iskusstvennogo intellekta dlya obnaruzheniya komp'yuternykh atak [The use of artificial intelligence to detect computer attacks]// Trudy CNIIS. Sankt-Peterburgskiy filial [Proceedings of CNIIS. St. Petersburg branch.]. 2017. Т. 1. № 4. С. 109-116.

[18] Yan Q. et al. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges //IEEE communications surveys & tutorials. – 2015. – Т. 18. – №. 1. – С. 602-622.

[19] Semenovykh A. A., Laponina O. R. Sravnitel'nyy analiz SDN-kontrollerov [Comparative analysis of SDN controllers]. // International Journal of Open Information Technologies ISSN: 2307-8162. - 2018. - vol. 6. - №. 7.

[20] Oshkina Ye. V. Setevaya tekhnologiya SDN (obzor, sovremennyye tendentsii) [Network technology SDN (review, current trends)] // Tekhnicheskiye nauki: problemy i perspektivy: materialy 5 Mezhdunarodnoy nauchnoy konferentsii [Engineering: problems and prospects: proceedings of the 5th International Scientific Conference] (St. Petersburg, July 2017.). — SPb.: Svoye izdatel'stvo [SPb .: Own publishing house], 2017. — С. 3-6. — URL https://moluch.ru/conf/tech/archive/231/12628/ (accessed: 30.05.2019).

[21] Kolomeyets A. Ye., Surkov L. V. Programmno-konfiguriruyemyye seti na baze protokola OpenFlow [Software-configured networks based on the OpenFlow protocol]// Inzhenernyy vestnik [Engineering Herald]. – 2014. – №. 5. – С. 2-2.

[22] Borshevnikov A. Ye. Setevyye ataki. Vidy. Sposoby bor'by [Network attacks. Kinds. Ways to deal with it.] // Sovremennyye tendentsii tekhnicheskikh nauk: materialy mezhdunarodnoy nauchnoy konferentsii [Current Trends in Engineering: Proceedings of an International Scientific Conference]. — Ufa: Summer, 2011. — С. 8-13. — URL:https://moluch.ru/conf/tech/archive/5/1115/ (accessed: 12.03.2019).

[23] Zakharov A. A., Popov Ye. F., Fuchko M. M. Aspekty informatsionnoy bezopasnosti arkhitektury SDN [Aspects of information security of the SDN architecture]// Vestnik SibGUTI [SibGUTI Herald]. – 2016. – №. 1. – С. 83-92.

[24] Loginov S.S. Ob urovnyakh upravleniya v programmno-konfiguriruyemoy seti (SDN) [About control levels in a software-configured network (SDN)]// T-Comm: Telekommunikatsii i transport [T-Comm: Telecommunications and transport]. 2017. Vol 11. No3. C. 50-55.
[25] Martin Casado, Tal Garfinkel, Aditya Akella, Michael J. Freedman Dan Boneh, Nick McKeown, Scott Shenker. SANE: A Protection Architecture for Enterprise Networks //15-th Usenix Security Symposium. Vancouver, Canada. 2006.
[26] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, J. Turner. Openflow: Enabling innovation in campus networks // SIGCOMM Computer Communication Review. vol. 38. № 2. pp. 69–74, 2008.
[27] SDN Technical Specifications. URL:https://www.opennetworking.org/software-defined-standards/specifications/ (accessed: 10.10.2019)
[28] Hu Y. N. et al. On the placement of controllers in software-defined networks //The Journal of China Universities of Posts and Telecommunications. – 2012. – T. 19. – C. 92-171.
[29] Hu Y. et al. Reliability-aware controller placement for software-defined networks //Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on. – IEEE, 2013. – C. 672-675.
[30] Chugreyev D.A., Shkrebets A.Ye., Shevel' A.Ye., Vlasov D.V., Grudinin V.A., Kairkanov A.B., Sadov O.L., Titov V.B., Khoruzhnikov S.E., Soms L.N. Razrabotka interfeysa vzaimodeystviya s kontrollerom programmno-konfiguriruyemykh setey [Development of interface for interaction with the program-configurable networks controller]// Sovremennyye problemy nauki i obrazovaniya [Modern problems of science and education]. - 2013. - № 3. - C. 83.
[31] Vlasov D.V., Grudinin V.A., Kairkanov A.B., Sadov O.L., Soms L.N., Titov V.B., Khoruzhnikov S.E., Chugreyev D.A., Shevel' A.Ye., Shkrebets A.Ye. Razrabotka prototipov sredstv upravleniya setevymi resursami i potokami dannykh [Development of prototypes of network resources and data flows based on openflow software configurated networks]// Sovremennyye problemy nauki i obrazovaniya [Modern problems of science and education]. - 2013. - № 3. - C. 86.
[32] Sadov O.L., Vlasov D.V., Grudinin V.A., Kairkanov A.B., Soms L.N., Titov V.B., Khoruzhnikov S.E., Chugreyev D.A., Shevel' A.Ye., Shkrebets A.Ye. Issledovaniye seti khraneniya dannykh, postroyennoy s ispol'zovaniyem programmno-konfiguriruyemykh [Researching a storage network built using openflow software-defined networks]// Sovremennyye problemy nauki i obrazovaniya [Modern problems of science and education]. - 2013. - № 4. - C. 64.
[33] Laponina O.R., Sizov M.R. Laboratornyy stend dlya testirovaniya vozmozhnostey integratsii PKS-setey i traditsionnykh setey [Laboratory bench for testing the integration capabilities of SDN and traditional networks]//International Journal of Open Information Technologies. 2017. T. 5. № 9. C. 3-12.
[34] Amelyanovich A.V., Shpakov M.N., Mutkhanna A.S., Buynevich M.V., Vladyko A.G. Tsentralizovannoye upravleniya potokami trafika v besprovodnykh lokal'nykh setyakh na baze kontseptsii SDN [Centralized traffic flow control in wireless LANs based on the SDN concept]// Sistemy sinkhronizatsii, formirovaniya i obrabotki signalov [Systems of synchronization, formation and processing of signals]. 2017. T. 8. № 2. C. 31-35.
[35] Man'kov V.A., Krasnova I.A. Algoritm dinamicheskoy klassifikatsii potokov v mul'tiservisnoy SDN-seti [The algorithm for dynamic classification of flows in a multi-service SDN network]// T-Comm: Telekommunikatsii i transport [T-Comm: Telecommunications and transport]. 2017. Том 11. No12. C. 37-42.
[36] Smelyanskiy R.L., Pilyugin P.L. Sovremennyye problemy obespecheniya bezopasnosti v SDN [Modern security problems in SDN]// REDS: Telekommunikatsionnyye ustroystva i sistemy [REDS: Telecommunication devices and systems]. 2017. T. 7. № 4. C. 523-526.
[37] Wang H., Xu L., Gu G. Floodguard: A dos attack prevention extension in software-defined networks //2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. – IEEE, 2015. – C. 239-250.
[38] Shin S. et al. Enhancing network security through software defined networking (sdn) //2016 25th International Conference on Computer Communication and Networks (ICCCN). – IEEE, 2016. – C. 1-9.
[39] Hong S. et al. Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures //NDSS. – 2015. – T. 15. – C. 8-11.
[40] Lee S. et al. DELTA: A Security Assessment Framework for Software-Defined Networks //NDSS. – 2017.
[41] An Overview of Misuse / Attack Cases. URL:http://www.sdnsecurity.org/vulnerability/attacks (accessed: 10.10.2019)
[42] Tang T. A. et al. Deep recurrent neural network for intrusion detection in sdn-based networks //2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft). – IEEE, 2018. – C. 202-206.
[43] Karakus M., Durresi A. Quality of service (QoS) in software defined networking (SDN): A survey //Journal of Network and Computer Applications. – 2017. – T. 80. – C. 200-218.
[44] Wallner R., Cannistra R. An SDN approach: quality of service using big switch's floodlight open-source controller //Proceedings of the Asia-Pacific Advanced Network. – 2013. – T. 35. – C. 14-19.
[45] Govindarajan K. et al. Realizing the quality of service (QoS) in software-defined networking (SDN) based cloud infrastructure //2014 2nd International Conference on Information and Communication Technology (ICoICT). – IEEE, 2014. – C. 505-510.