Разработка эффективного алгоритма безопасности для программно-конфигурируемой сети

Ю. Г. Чашин, email: chashin@bsu.edu.ru
Д. Г. Азизова, email: diana_azizova94@mail.ru
А. А. Бабенко, email: nastas.petrova@yandex.ru

Белгородский государственный национально – исследовательский университет

Аннотация. *В статье рассмотрены особенности обеспечения безопасности программно-конфигурируемой сети. В процессе исследования предложен алгоритм безопасности сети SDN на основе вставки маскирующих элементов.*

Ключевые слова: *сеть, конфигурация, маршрутизатор, защита, сервер, шифрование.*

Введение

Оргкомитет Международной конференции «Информатика: проблемы, методология, технология» рад приветствовать своих участников и потенциальных участников. Данный документ представляет собой шаблон оформления и описание требований оформления работ для участников данной конференции. Программно-конфигурируемая сеть – Software Defined Network (SDN) – это архитектура, разработанная для того, чтобы сделать сеть более гибкой и простой в управлении. SDN централизует управление, разделяя плоскость управления от функции пересылки данных в дискретных сетевых устройствах. [1]. Таким образом, сеть становится программируемой, создаваемой из явных (открытые стандарты SDN, протокол OpenFlow) ресурсов под конкретные программы и приложения, но в тоже время такие особенности делают ее более открытой. Очевидно, что в таких условиях выдвигаются повышенные требования к безопасности SDN сетей и защите данных в них, в том числе особый акцент делается на ключевых (коэффициент готовности, надежность, латентность) характеристиках их восстановления после отказа.

С учетом вышеизложенного конфигурирование сетей превращается в достаточно сложную задачу, которая требует серьезных трансформаций принципов построения системы безопасности (контроль над всеми операциями, разграничение доступа) и методов управления

ею. Это в свою очередь актуализирует необходимость разработки эффективных алгоритмов безопасности для SDN сетей, которые позволят обеспечить сбалансированное использование доступного сетевого ресурса, будут способствовать улучшению отказоустойчивости и сетевой безопасности.

Таким образом, обозначенные обстоятельства подтверждают теоретическую и практическую значимость темы данной статьи, а также обуславливают целевую направленность проводимого исследования..

1. Разработка алгоритма безопасности для программно-конфигурируемой сети

Весомый вклад в решение задач защиты SDN сети, управления сетевым ресурсом и обеспечения сетевой безопасности внесли такие специалисты как: Olakanmi Olufemi; Odeyemi Oluwasesan; Fosić Igor; Žagar Drago; Saleem Kashif; Коротаев В.О., Козлов С.А., Березина Е.О., Виткова Л.А.

По результатам их исследования установлено, что для обеспечения высокого уровня сетевой безопасности необходимо использовать все технологические и протокольные средства управления трафиком.

Опираясь на уже имеющиеся наработки и достижения, существующие методы обеспечения безопасности в сетях SDN можно подразделить на два самостоятельных класса [3]: резервирование или защитное переключение и перемаршрутизация (восстановление). В таблице 1 представлено краткое описание этих методов, а также обозначены их достоинства и недостатки.

Таблица

Преимущества и недостатки методов защиты сети SDN

Методы	Недостатки	Преимущества
Восстановление	Необходимы значительные временные затраты на восстановление связи, высокий риск нестабильной работы сети	Оптимизация пропускной способности SDN сети
Защитное переключение	Сеть нуждается в дополнительной пропускной способности	SDN сеть быстро восстанавливается

В тоже время, необходимо отметить, что перспективным методом защиты и обеспечения безопасности сети SDN является метод

шифрования информации с использованием маскирующих элементов на основе блочных шифров.

На первом этапе процедуры шифрования перед (или после) определенных символов ОТ вставляются дополнительные маскирующие элементы. Необходимо вставлять такое количество маскирующих элементов, чтобы в каждый блок шифрования попадал хотя бы один маскирующий элемент. Маскирующие элементы выбираются таким образом, чтобы статистический анализ ОТ до вставки и после вставки маскирующих элементов изменялся в сторону равномерной частоты употребления символов. Если при перемножении в матрицу символов ОТ вставляется хотя бы один маскирующий элемент, то изменяются все результирующие символы шифрованного текста (ШТ). В этом случае ОТ с маскирующими элементами будет иметь следующую конфигурацию: в каждом блоке (если $\mu = 3$) будет один маскирующий элемент перед символом ОТ, символ ОТ и один маскирующий элемент после символа ОТ. Блок выглядит так: $\{m_i; v_i; m_i\}$, где m_i – маскирующий элемент, v_i – символ ОТ. Если конфигурация ОТ с маскирующими элементами будет такая, которая рассматривалась выше, а $\mu = 4$, тогда блоки будут иметь следующий вид: первый – $\{m_i; v_i; m_i; m_i\}$, второй – $\{v_i; m_i; m_i; v_i;\}$, третий – $\{m_i; m_i; v_i; m_i\}$, четвертый – $\{m_i; v_i; m_i; m_i\}$, пятый – $\{m_i; v_i; m_i; m_i\}$ – аналогичный первому, и весь цикл с периодом 4 повторяется.

2. Достоинства разработанного алгоритма

Достоинством данного алгоритма является тот факт, что предлагаемый способ шифрования информации несложно реализуется аппаратным, программным или комбинированным способом. Кроме того, сама процедура вставки маскирующих элементов и их извлечение является процедурой, не уменьшающей производительность работы криптографа. При этом маскирующие элементы подбираются с помощью генератора случайных чисел из наименее употребляемых символов в тексте. Таковой метод подбора маскирующих частей можно считать дополнительным ключом для формирования ШТ. Сложность извлечения маскирующих элементов не определяется их номером или названием, так как изымаются символы на соответствующих позициях ШТ..

Заключение

Таким образом, использование маскирующих элементов имеет широкую перспективу в направлении создания шифров повышенной эффективности. Расшифровка ШТ, не имея ключа, методом перебора

всех возможных вариантов ключа, не позволяет получить читаемый ОТ, поскольку имела место модификация ОТ перед шифрованием.

В предложенном методе шифрования решающим является искажение информации о повторениях, которые могли бы возникнуть вновь в ШТ по аналогии с ОТ. И эта задача успешно решается благодаря использованию блочного шифра на основе маскирующих элементов. Эта особенность предложенного алгоритма обеспечивает скрытие использованного метода шифрования, имеющего важный эффект для защиты SDN.

Список литературы

1. Березина Е .О. Анализ угроз безопасности для программно-конфигурируемых сетей // Вестник молодых ученых Санкт-Петербургского государственного университета технологии и дизайна. 2020. № 1. С. 24-32.

2. Fosić, Igor; Žagar, Drago Security Features in a Hybrid Software-Defined Network // Tehnicki vjesnik- Strojarski Fakultet. 2021. Number 4; pp 1371-1379.

3. Смелянский Р. Л., Пилюгин П. Л. Современные проблемы обеспечения безопасности в SDN // REDS: Телекоммуникационные устройства и системы. 2017. Т. 7. № 4. С. 523-526.

4. Иванов В. В. Алгоритм создания и конфигурация сетей // Вестник молодых ученых Санкт-Петербургского государственного университета технологии и дизайна. 2020. № 1. С. 48-52.

5. Бело А. В., Селеванов Д. Е. Проектирование сетей безопасности в SDN // REDS: Телекоммуникационные устройства и системы. 2017. Т. 7. № 4. С. 635-678.