УДК 004.715

Ячменев И.А.

студент РГУ нефти и газа (НИУ) имени И.М. Губкина

Сухов С.Д

студент РГУ нефти и газа (НИУ) имени И.М. Губкина

ИССЛЕДОВАНИЕ ВРЕМЕНИ СХОДИМОСТИ ПРОТОКОЛОВ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ ПРИ АТАКАХ ТИПА DOS

Аннотация: В статье исследуется влияние DoS-атак на время сходимости протоколов динамической маршрутизации в условиях изменения топологии сети. Рассматриваются проактивные (OLSR) и реактивные (AODV) протоколы, их различия по способу работы и определения маршрутов. Для проведения экспериментов использовался симулятор NS-3, обеспечивающий высокую детализацию моделирования. В качестве тестовой топологии использовалась сеть с маршрутизаторами и персональными компьютерами, где на одном из узлов инициировалась DoS-атака. Было выявлено, что OLSR обладает меньшим временем сходимости благодаря проактивному характеру, что делает его предпочтительным для сетей с высокими требованиями к отказоустойчивости. AODV показал большую задержку из-за реактивного подхода к обнаружению маршрутов. Разница во времени сходимости для обоих протоколов минимальна и практически не зависит от топологической удаленности разрыва

Ключевые слова: DoS-атаки, динамическая маршрутизация, время сходимости, NS-3, AODV, OLSR, сетевые протоколы, сетевые цифровые двойники.

Yachmenev I.A.

student of Gubkin Russian State University of Oil and Gas

Sukhov S.D

student of Gubkin Russian State University of Oil and Gas

RESEARCH CONVERGENCE TIME OF DYNAMIC ROUTING PROTOCOLS UNDER DOS-TYPE ATTACKS

Annotation: This article investigates the impact of DoS attacks on the convergence time of dynamic routing protocols under changing network topologies. Proactive (OLSR) and reactive (AODV) protocols are analyzed, focusing on their operational principles and route determination methods. The experiments were conducted using the NS-3 simulator, which provides high-detail network modeling capabilities. The test topology included routers and personal computers, with a DoS attack initiated at one of the nodes. The results show that OLSR has a shorter convergence time due to its proactive nature, making it preferable for networks requiring high resilience. AODV exhibited greater delays due to its reactive route discovery approach. The difference in convergence times for both protocols is minimal and is largely unaffected by the topological distance of the link failure.
Keywords: DoS attacks, dynamic routing, convergence time, NS-3, AODV, OLSR, network protocols, digital network twins.

Атаки типа DoS представляют собой один из наиболее распространенных и разрушительных методов воздействия на сетевую инфраструктуру. Их цель заключается в перегрузке целевой системы, что приводит к недоступности сетевых услуг и значительному ухудшению их качества.

Протоколы динамической маршрутизации можно квалифицировать на 2 категории [1]:

1) По способу работы с маршрутами

Проактивные протоколы поддерживают актуальную таблицу маршрутов ко всем узлам сети независимо от наличия текущей передачи данных. Пример: OLSR (Optimized Link State Routing Protocol).

Маршруты в реактивных протоколах обнаруживаются только при необходимости передачи данных. Пример: AODV (Ad hoc On-Demand Distance Vector).

2) По способу определения маршрутов

Векторные протоколы: Узлы передают информацию о маршрутах своим соседям, выбирая пути на основе метрики (например, количества хопов). Пример: AODV, RIP.

Протоколы состояния канала: Узлы поддерживают глобальное представление о топологии сети, что позволяет рассчитывать оптимальные маршруты. Пример: OLSR, OSPF.

Для измерения времени сходимости протоколов динамической маршрутизации важно учитывать влияние различных факторов, включая топологическое расположение разрыва связи. Сетевые цифровые двойники являются виртуальной моделью реальной сети, воспроизводящей ее структуру, функциональность и поведение. Благодаря этому администраторы совместно с инженерами имеют возможность проводить многочисленные эксперименты по модернизации сети, тестировать новые конфигурационные решения. Одной из задач двойника является тестирование настроек маршрутизации для выбора наиболее подходящих решений [2].

В процессе моделирования используются функциональные возможности NS-3. Это современный инструмент для моделирования сетей, широко используемый в исследованиях сетевых протоколов и механизмов их взаимодействия. NS-3 представляет собой симулятор событий с высокой степенью детализации, который позволяет анализировать работу сетевых устройств и протоколов в различных условиях. Его открытый исходный код, гибкость и мощные инструменты визуализации делают его идеальным выбором для исследования времени сходимости протоколов маршрутизации при воздействии DoS-атак.

Для изучения времени сходимости протоколов маршрутизации используется топология, представленная на рисунке (рис. 1). Сеть состоит из трех персональных компьютеров (PC1, PC2 и PC3). PC1 играет роль отправителя данных, генерируя трафик, который направляется на PC2, выступающий в роли получателя, PC3 атакующая машина. Компьютеры соединенных через пять маршрутизаторов (R1, R2, R3, R4, R5). Основной

маршрут для передачи данных проходит через узлы R1, R2 и R3. В случае разрыва связи резервный маршрут обеспечивает передачу данных через узлы R1, R4, R5 и R3.

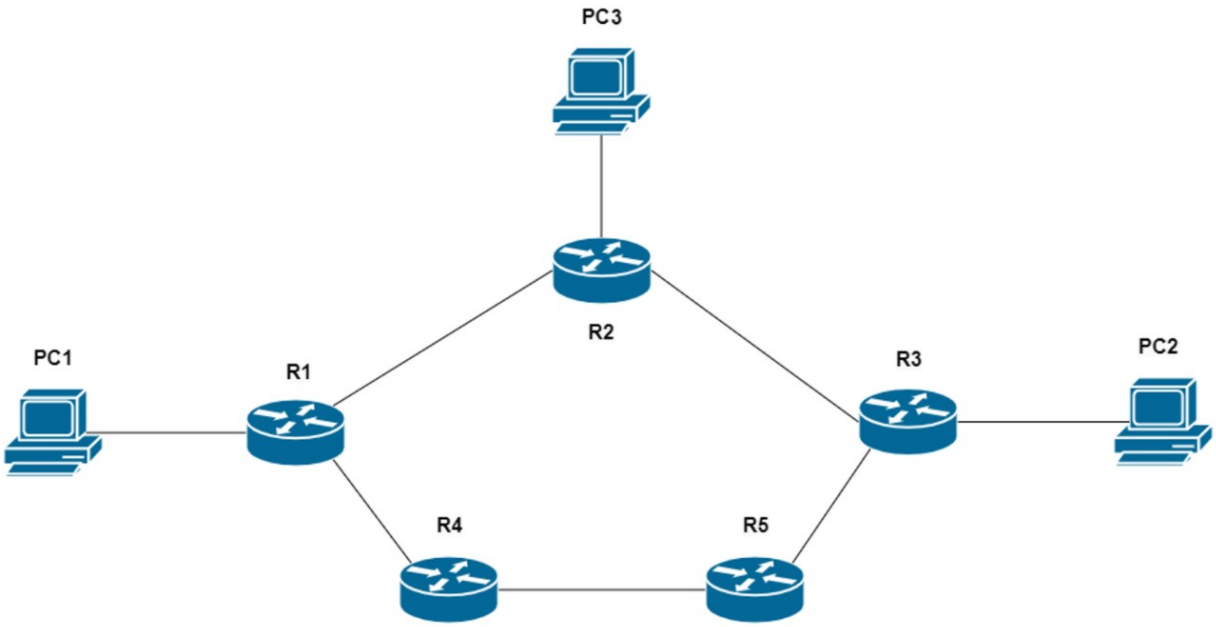

Рисунок 1 - Схема сети для проведения экспериментов

Для имитации DoS-атаки, с помощью метода Schedule класса Simulator запланируем отключение интерфейса на R2. В результате разрыва связи протоколы динамической маршрутизации автоматически инициируют процесс обновления таблиц маршрутов. После этого сетевой трафик начнет перенаправляться по резервному маршруту, обеспечивая восстановление передачи данных. Далее с помощью Callback-функции регистрируем время доставки пакета после сходимости.

Для полного измерения времени сходимости протоколов маршрутизации мы будем использовать поэтапный подход. Сначала будет производиться отключение сетевого интерфейса, расположенного ближе к источнику трафика. Это позволит оценить скорость восстановления маршрутов при минимальной дистанции до точки отказа. Затем эксперимент будет повторен с отключением интерфейса, расположенного дальше от источника. Такой подход обеспечит более глубокое понимание поведения

протоколов в различных сетевых условиях и позволит выявить, как удаленность разрыва связи влияет на их адаптацию к изменениям топологии.

Таблица 1 - Измерение времени сходимости для протоколов

Протокол	Время сходимости при разрыве связи, с	
	Ближе к отправителю	Дальше от отправителя
AODV	8.11529	8.15422
OLSR	6.07373	6.09216

Влияние топологической удаленности разрыва на время сходимости протоколов является минимальным. В обоих случаях разница в времени сходимости для AODV и OLSR составляет менее 0.05 секунды, что указывает на их способность адаптироваться к изменению топологии независимо от расположения разрыва. Однако, OLSR более эффективен в условиях разрыва связи благодаря своему проактивному характеру, что делает его предпочтительным выбором для сетей, требующих минимального времени отклика. AODV, как реактивный протокол, требует больше времени для восстановления маршрутов, так как процесс обнаружения маршрута инициируется только при необходимости.

Использованные источники:

1. Греков В.С. Перспективы кибербезопасности в нефтегазовой отрасли / В. С. Греков, А. Г. Уймин // Губкинский университет в решении вопросов нефтегазовой отрасли России : Тезисы докладов VI Региональной научно-технической конференции, посвященной 100-летию М.М. Ивановой, Москва, 19–21 сентября 2022 года. – Москва: Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, 2022. – С. 1108-1109.

2. Уймин, А. Г. Обзор систем моделирования: анализ эффективности на примере чемпионата AtomSkills-2023 / А. Г. Уймин, В. С. Греков // Автоматизация и информатизация ТЭК. – 2023. – № 11(604). – С. 25-34. – DOI 10.33285/2782-604X-2023-11(604)-25-34. – EDN QYQRCO.

3. Макаренко, С. И. Время сходимости протоколов маршрутизации при отказах в сети / С. И. Макаренко // Системы управления, связи и безопасности. – 2015. – № 2. – С. 45-98. – DOI 10.24411/2410-9916-2015-10203. – EDN TXOSKP.

4. Моисеев, О. В. Алгоритмы, обеспечивающие время сходимости протоколов маршрутизации в условиях реконфигурации или при отказах в сети / О. В. Моисеев, Т. Ф. Фам // Системы управления и информационные технологии. – 2017. – № 4(70). – С. 45-50. – EDN ZTDAYN.

5. Васильев, А. С. Сравнение протоколов динамической маршрутизации / А. С. Васильев // Молодой ученый. — 2020. — № 8 (298). — С. 10-14. — URL: https://moluch.ru/archive/298/67570/ (дата обращения 08.01.2025)