# О методе предотвращения DDoS атаки на контроллер в программно-конфигурируемых сетях

***Пашков Василий Николаевич,***
***Антипина Анна Вячеславовна***
*Ассистент кафедры АСВК, студент*
*Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия*
*E-mail:* pashkov@lvk.cs.msu.su, anya_antipina@lvk.cs.msu.su

***Научный руководитель*** *— Пашков В.Н.*

Одной из серьезнейших угроз безопасности для программно-конфигурируемых сетей (ПКС) является DDoS атака на контроллер [1]. Инициатором DDoS атаки выступает злоумышленник, имеющий точки присутствия в ПКС сети в виде *зараженных хостов* с установленным на них специальным вредоносным программным обеспечением (ВПО). ВПО позволяет злоумышленнику удаленно инициировать большое количество новых потоков (*фиктивных потоков*) трафика в сети. Отсутствие соответствующих правил в таблицах потоков коммутаторов для них приводит к формированию запросов к ПКС контроллеру на их установление. Это влечет за собой существенный рост задержек на установление правил для легитимных пользовательских потоков, истощение вычислительных ресурсов и перегрузку сервера контроллера, нарушение работоспособности всей сети с соответствующими прерываниями и отказами в работе пользовательских сетевых сервисов. Поэтому задача своевременного обнаружения, предотвращения и устранения последствий DDoS атаки на контроллер является актуальной и важной задачей, без решения которой внедрение технологий ПКС в реальных сетях невозможно.

В работе предполагается, что топология и структура ПКС сети зафиксирована и не изменяется, контроллер управляет коммутаторами посредством протокола OpenFlow не ниже версии 1.3 [2].

Предлагаемый метод основан на двухэтапной фильтрации потоков трафика на граничных коммутаторах доступа пользователей к сети и на контроллере с целью выявления зараженных хостов.

В методе предотвращения DDoS атак на контроллер выделены три фазы: фаза инициализации, фаза мониторинга и фаза противодействия атаки. В фазе инициализации контроллер формирует «таблицу привязок», содержащую MAC и IP адреса всех хостов в сети, номера физических портов и идентификаторы коммутаторов их под-

ключения. В таблицах потоков граничных коммутаторов устанавливаются правила для первого этапа фильтрации: пакеты сбрасываются, если их MAC и IP адреса источника, входной порт и/или MAC адрес коммутатора не совпадают или отсутствуют в таблице привязок.

В фазе мониторинга осуществляется контроль количества инициируемых потоков для каждого хоста. При превышении заранее установленного порогового значения фиксируется факт обнаружения атаки в сети.

В фазе противодействия атаки выполняется второй этап фильтрации с целью предотвращения DDoS атаки, на котором для каждого хоста осуществляется оценка надежности и поведения хоста и производится корректировка оценки с помощью фактора забывания. В результате каждый хост классифицируется как зараженный, пользовательский или неопределенный.

Метод предотвращения DDoS атак на контроллер был реализован в виде приложения на языке C++ для контроллера RUNOS [3]. Экспериментальное исследование метода проводилось на топологиях с количеством хостов от 4 до 128 и с долей зараженных хостов до 50%. В результате экспериментов было выявлено, что метод позволяет уменьшить утилизацию CPU сервера контроллера до 50% во время атаки, уменьшить задержку на установление новых потоков для пользовательского трафика до 6 раз и увеличить пропускную способность каналов до 2 раз во время атаки.

**Литература**

1. Сычева Е. А., Пашков В. Н. Исследование и разработка алгоритмов обнаружения и предотвращения DDoS атак на контроллер в программно-конфигурируемых сетях // Программные системы и инструменты. — Т. 16 из Тематический сборник № 16. — М: Издательский отдел факультета ВМиК МГУ МАКС Пресс, 2016. — С. 19–29.
2. Open Networking Foundation. OpenFlow Switch Specification. Version 1.3.0 (Protocol version 0x04).
3. RUNOS SDN/OpenFlow Controller. URL: `https://github.com/ARCCN/runos`