Инфокоммуникационные технологии и системы

УДК 621.396.677.49 **DOI: 10.14529/ctcr170304**

МОДЕЛЬ РАСПРЕДЕЛЕННЫХ АТАК В ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ СВЯЗИ

Ю.Ю. Коляденко[1], И.Г. Лукинов[1, 2]

[1] Харьковский национальный университет радиоэлектроники, г. Харьков, Украина,
[2] Харьковский государственный региональный научно-технический центр по вопросам технической защиты информации, г. Харьков, Украина

Показано, что архитектура SDN не лишена потенциальных уязвимостей с точки зрения информационной безопасности. Контроллер как ключевой компонент в управлении всей инфраструктурой SDN является наиболее уязвимым элементом, атака на который может повлечь критичные для всей инфраструктуры последствия. Основными угрозами, возникающими со стороны сетевых устройств, работающих по принципу программно-конфигурируемой сети, остаются вариации таких атак, как «отказ в обслуживании», подмена контроллера и т. д.

Предложено реакцию SDN-сети на потоки различных пакетов, в том числе и на атаки, рассматривать как функционирование некоторой системы массового обслуживания, которая обрабатывает требования на обработку пакетов. Разработана математическая модель SDN-сети в виде системы массового обслуживания. Получена математическая зависимость среднего числа заявок при появлении атак. Получены графики зависимости среднего числа заявок при наличии атак от вероятности потери пакетов. Достоинствами предлагаемой модели являются возможность своевременного (раннего) обнаружения атаки, ее способность адаптироваться к реальным параметрам сети.

Ключевые слова: SDN-сети, контроллер, коммутатор, протокол OpenFlow, информационная безопасность, атаки, теория массового обслуживания.

Введение

Сеть сотовой связи характеризуется огромной стоимостью и большими сроками строительства. Изменения в стандартах связи происходят регулярно, но переход к новому стандарту требует новых вложений и замены оборудования, которое часто еще не выработало свой ресурс. Сейчас для запуска сети нового поколения всё становится проще благодаря технологии программных конфигурируемых сетей (SDN). В сетях SDN основные функции коммутаторов и маршрутизаторов перенесены на центральный сетевой контроллер, что упрощает применение сетевых политик и мониторинг состояния сети [1].

При таком подходе передающие устройства отвечают только за передачу данных, опираясь на таблицу потоков, которая строится централизованным сетевым контроллером, взаимодействующим с передающим устройством [2].

Взаимодействие между сетевым контроллером и передающими устройствами реализуется посредством программного интерфейса, который используется для прямого управления группами устройств. Наиболее развитым программным интерфейсом на данный момент является протокол OpenFlow [1, 3]. Архитектура OpenFlow-коммутатора базируется на одной или нескольких таблицах правил, определяющих механизм обработки потоков сетевого трафика. Каждое правило является записью в таблице OpenFlow-коммутатора. Запись сопоставляется с определенным потоком трафика. В зависимости от результата сопоставления применяется соответствующее действие (блокирование, передача, модификация и т. д.) к пакетам из данного потока.

Архитектура SDN, предполагая существенно иной подход к реализации сетевой инфраструктуры, не лишена потенциальных уязвимостей с точки зрения информационной безопасности.

Необходимость разделения доступа сетевых приложений при работе с контроллером, вопросы аутентификации и авторизации при работе приложений с контроллером – это лишь немногие аспекты безопасности, которые приходится принимать во внимание при проектировании SDN-сетей [1].

Контроллер как ключевой компонент в управлении всей инфраструктурой SDN является наиболее уязвимым элементом, атака на который может повлечь критичные для всей инфраструктуры последствия [4]. Таким образом, разработка модели распределенных атак в программно-конфигурируемых сетях связи является актуальной научной задачей.

1. Основные угрозы архитектуры SDN

Основными угрозами, возникающими со стороны сетевых устройств, работающих по принципу программно-конфигурируемой сети, остаются вариации таких атак, как «отказ в обслуживании», подмена контроллера и т. д. Перенос «аналитической» компоненты сети на контроллер естественным образом переносит акцент многих атак с сетевого оборудования на обеспечивающее функционирование сети программное обеспечение (ПО): контроллер сети и сетевые приложения, обращающиеся к контроллеру [5].

Наиболее простым и одновременно эффективным способом нарушения целостности работы сети SDN являются атаки типа «отказ в обслуживании». Опасность атаки следует из самого алгоритма работы SDN-коммутатора при получении неизвестного (т. е. не подходящего под имеющиеся в flow-таблице правила) пакета. В такой ситуации возможны два варианта:

1. Пакет целиком отправляется на контроллер для анализа.

2. Пакет остается в памяти коммутатора, на контроллер отправляются исключительно заголовки пакета.

Оба способа оставляют для атакующего широкое поле для эффективной реализации отказа в обслуживании путем формирования потока различных пакетов в SDN-сети. Рассмотрим реакцию сети в обоих вышеприведенных случаях [1].

1. Коммутатор начинает формирование большого количества сообщений для передачи неизвестных пакетов на контроллер. Расходуются процессорные ресурсы коммутатора, увеличивается расход памяти. Особенно сильно расходуется память в том случае, если коммутатор буферизирует сами пакеты и пересылает контроллеру только их заголовки.

2. Поток пакетов от коммутатора на контроллер нагружает канал связи между контроллером и коммутатором. Если среда связи является разделяемой, то снижение оперативности доставки сообщений могут ощутить на себе все коммутаторы. Повышенное влияние на канал связи будет оказано в ситуации, когда коммутатор пересылает пакеты для анализа целиком.

3. Контроллер принимает и обрабатывает поток сообщений, расходуя процессорное время и память своей среды исполнения. Формирование очередей сообщений заставит легитимные сообщения ожидать своей очереди и снизит оперативность принятия решений в сети.

4. Контроллер генерирует поток различных сообщений в ответ на запросы атакованного коммутатора. Расходуются ресурсы канала связи между коммутатором и контроллерами.

5. Коммутатор принимает команды от контроллера и выполняет их, расходуя ресурсы процессора и память. Если команды содержат в себе создание новых правил таблиц потоков, то происходит их лавинообразное увеличение, время проверки каждого нового пакета по таблице увеличивается, растут расходы на обслуживание такой таблицы, а также возможно переполнение таблиц потоков.

В результате реализация атаки может привести к следующим последствиям [1]:

1. Исчерпание ресурсов коммутатора. Легитимные пакеты либо вообще не будут обработаны данным сетевым узлом, либо их обработка будет сопровождаться задержками.

2. Канал связи между контроллером и коммутатором не обеспечит доставки управляющих сообщений, будучи загруженным потоками данных.

3. Контроллер будет перегружен приходящими запросами и не сможет обрабатывать управляющие сообщения, вызванные легитимным трафиком.

Угрозы безопасности, актуальные для большинства информационных систем, такие как сканирование портов и определение сетевых служб, являются критическими для архитектуры SDN по причине уязвимости канала OpenFlow и наличия большого количества трафика управления, передаваемого между коммутаторами и сетевыми контроллерами. Отметим уязвимость архитек-

туры SDN к DoS/DDoS-атакам – одним из самых опасных для архитектуры с централизованной точной управления.

Одной из причин уязвимости OpenFlow-сетей к атакам подмены является чрезмерная гибкость стандарта OpenFlow. Стандарт позволяет реализовать взаимодействие между сетевым контроллером и коммутаторами на базе протокола TCP без шифрования, а поддержка протокола TLS является необязательной для реализации.

Реакцию SDN-сети на потоки различных пакетов, в том числе и на атаки можно рассматривать как функционирование некоторой системы массового обслуживания (СМО), которая обрабатывает требования на обработку пакетов.

2. Математическая модель системы массового обслуживания

Под СМО [6] обычно понимается совокупность обслуживающих приборов и обслуживаемых требований (заявок) из некоторого входящего потока требований.

Число приборов в СМО может быть любым. Основной характеристикой прибора является время обслуживания одного требования этим прибором. Этот показатель характеризует не качество обслуживания, а пропускную способность прибора. Время обслуживания обычно непостоянно и зависит от различных факторов, поэтому в общем случае эта величина является случайной [7]. При этом считается, что продолжительность обслуживания различных требований одним прибором есть независимые случайные величины с одним и тем же законом распределения. Наиболее часто предполагают, что этот закон является показательным. Его применяют в тех случаях, когда время обслуживания подавляющего большинства требований мало и только для сравнительно небольшой части требований оно велико. При показательном распределении времени обслуживания требований теоретические рассуждения существенно упрощаются, а многие окончательные результаты оказываются справедливыми и для произвольного закона распределения, но с тем же средним временем обслуживания [8].

Также в теории массового обслуживания принято считать, что входящий поток требований распределен по пуассоновскому закону распределения. По определению пуассоновский поток должен удовлетворять трем следующим требованиям: стационарности, отсутствию последствия и ординарности.

Поток называется стационарным, если вероятность поступления k требований в течение промежутка времени t не зависит от момента начала этого промежутка.

Под отсутствием последствия понимается то, что вероятность поступлений k требований в систему после произвольного момента времени t_0 не зависит от того, когда и сколько поступило требований до этого момента времени. Из этого следует взаимная независимость поступления того или иного числа требований на обслуживание в непересекающиеся промежутки времени.

Свойство ординарности означает практическую невозможность одновременного поступления двух или более требований.

Стоит отметить, что многие реальные потоки являются приближенно пуассоновскими. Пуассоновский поток полностью определяется одним параметром – интенсивностью потока λ.

Математический аппарат теории массового обслуживания позволяет определить основные параметры системы: среднее число занятых приборов, вероятность отказа в обслуживании требования, среднюю длину очереди, среднее время простоя требования в очереди и т. д.

В данном случае наибольший интерес представляет среднее число занятых приборов [6]:

$$N = \sum_{k=1}^{n} k \cdot p_k = p_0 \sum_{k=1}^{n} \frac{\alpha^k}{(k-1)!} = \alpha\left(1 - p_n\right), \quad (1)$$

где n – количество приборов в системе; $\alpha = \lambda/\mu$; λ – интенсивность потока требований; $1/\mu$ – математическое ожидание времени обслуживания одного требования; p_k – вероятность нахождения в системе ровно k требований:

$$p_k = \frac{a^n}{k! \sum_{i=0}^{n} \frac{a^i}{i!}}. \quad (2)$$

3. Поток требований СМО

Будем рассматривать множество пакетов или их заголовков, поступающих от коммутатора к контроллеру, в качестве входящего потока заявок. Покажем, что в определённых условиях этот поток можно считать пуассоновским.

Интенсивность этого потока может зависеть от времени, если рассматривать его в течение достаточно больших промежутков времени. Например, в течение суток в дневное время его интенсивность может быть больше, чем ночью. Тем не менее, при уменьшении продолжительности рассматриваемого промежутка интенсивность поступающих заявок стабилизируется и может рассматриваться как некоторая постоянная величина. Для различных сетей продолжительность такого промежутка может быть разной (как правило, от нескольких минут до нескольких часов) и может быть установлена экспериментально.

В этом случае вероятность поступления k требований в интервале времени $(0, t)$ равна вероятности поступления k требований в любом другом интервале той же длительности $(a, a+t)$ в пределах заданного промежутка. Таким образом, рассматриваемый поток обладает свойством стационарности.

Далее будем считать, что коммутаторы обращаются к ресурсам контроллера независимо друг от друга. Если при одном обращении коммутатора к контроллеру устанавливается одно соединение, то поток требований обладает свойством отсутствия последствия [6].

Покажем, что поток требований является ординарным. Рассмотрим контроллер с одним сетевым интерфейсом. По такому подключению одновременно не могут прийти сразу несколько пакетов. Соответственно, существует некоторый малый промежуток времени, в течение которого может поступить не более одной заявки. Следовательно, для контроллера с одним сетевым интерфейсом входной поток пакетов является ординарным.

Таким образом, поток заявок, содержащих пакеты, поступающие на сервер с одним сетевым интерфейсом, обладает свойствами стационарности, ординарности и отсутствия последствия, и в соответствии с определением такой поток является пуассоновским.

4. SDN-сеть в виде системы массового обслуживания

Так как поток поступающих на контроллер пакетов в заданных условиях является пуассоновским, то его можно рассматривать как поток требований, поступающих в СМО. В нормальном режиме работы в ответ на каждый полученный пакет контроллер должен отправить сгенерированное сообщение на коммутатор [6, 8]. Из того, что существует взаимнооднозначное соответствие между входящими и исходящими пакетами следует эквивалентность потоков. Далее в качестве требований СМО будем рассматривать отправляемые коммутатором пакеты. Множеством обслуживающих приборов будем считать ресурсы коммутатора и контроллера, предназначенные для хранения параметров TCP соединений. В такой интерпретации обслуживание требования – это резервирование соответствующих ресурсов либо до успешного установления TCP соединения, либо до истечения отведенного таймаута.

Для такой модели признаком атаки является резкое увеличение количества заявок в СМО. Находясь под воздействием атаки, коммутатор и контроллер выделяют соответствующие ресурсы, которые остаются занятыми в течение отведенного таймаута. Времени таймаута (от десятков секунд до нескольких минут) достаточно, чтобы занять все доступные ресурсы коммутатора и контроллера, предназначенные для хранения параметров TCP соединений. Для рассматриваемой модели это означает резкое увеличение занятых обслуживающих приборов.

Рассмотрим более детально ресурсы коммутатора и контроллера, выступающие в качестве обслуживающих приборов. Параметры TCP соединений хранятся в соответствующем буфере [8], который можно представить в виде массива размерности L, элементы которого хранят параметры TCP соединений. Их можно разделить на три типа: содержащие параметры установленных соединений, полуоткрытых соединений и свободные. Пусть B – количество открытых в данный момент TCP соединений. Тогда $n = L - B$ – количество элементов второго и третьего типов, совокупность которых будем рассматривать в качестве множества обслуживающих приборов СМО. При этом занятые обслуживанием требований приборы – это элементы второго типа. На рис. 1

изображен описанный массив, а на рис. 2 показано представление ресурсов контроллера в качестве множества обслуживающих приборов.

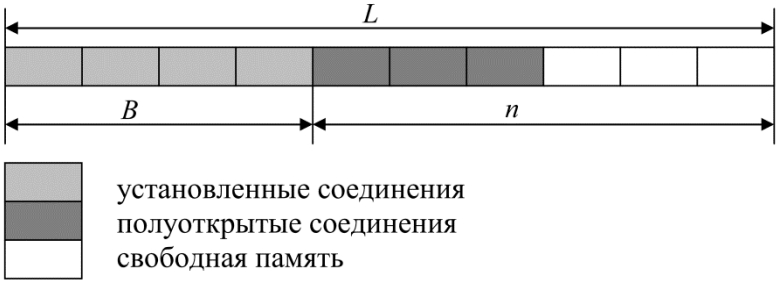

Рис. 1. Буфер для хранения соединений

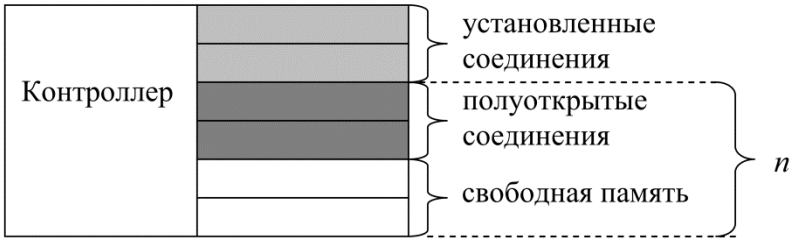

Рис. 2. Контроллер как система массового обслуживания

В зависимости от соотношения интенсивности входящего потока требований λ и размерности массива L можно рассматривать два типа СМО. Если интенсивность входящего потока заявок значительно меньше возможностей контроллера, то целесообразно рассматривать СМО с бесконечным числом обслуживающих приборов. В противном случае можно рассматривать СМО с отказами. Ввиду того, что на практике в нормальном режиме работы возможности контроллера со значительным запасом покрывают входящие требования, то рассмотрение системы с отказами является неактуальным. В дальнейшем будем рассматривать систему первого типа.

5. СМО с бесконечным количеством обслуживающих приборов

Обозначим отношение интенсивности входящего потока требований λ к среднему времени обслуживания заявки μ коэффициентом $\alpha = \lambda/\mu$. Так как поток требований является пуассоновским, то вероятность того, что в системе находится ровно k требований, определяется как

$$p_k = \frac{\alpha^k e^{-\alpha}}{k!}. \tag{3}$$

Подставив это значение в соотношение (2), описывающее среднее число приборов, занятых обслуживанием (общее число полуоткрытых соединений), получим

$$N = \sum_{k=1}^{\infty} k \cdot p_k = p_0 \sum_{k=1}^{\infty} \frac{\alpha^k}{(k-1)!} = \alpha(1 - p_\infty). \tag{4}$$

Соответственно,

$$p_\infty = \lim_{k\to\infty} \frac{\alpha^k e^{-\alpha}}{k!} = e^{-\alpha} \lim_{k\to\infty} \frac{\alpha^k}{k!} = 0. \tag{5}$$

Из соотношений (4) и (5) для СМО с бесконечным числом обслуживающих приборов имеем [6]:

$$N = \alpha(1 - p_\infty) = \alpha(1 - 0) = \alpha. \tag{6}$$

Предложенная модель описывает работу контроллера в нормальном режиме и позволяет учитывать такие параметры, как интенсивность обращений к контроллеру и среднее время обслуживания заявки. Однако такая СМО недостаточно полно описывает работу контроллера, так как не учитывает возможность потери легитимных пакетов при появлении DoS/DDoS-атак.

Для усовершенствования предложенной модели целесообразно разделить рассматриваемую СМО на две системы, обслуживающие заявки на нормальное установление соединения (когда все пакеты доставлены) и полуоткрытые соединения, удаляемые по таймауту. Для разделения исходного потока требований на множества заявок для каждой из систем необходимо ввести критерий, позволяющий определить принадлежность заявок к вышеописанным типам. Для этого в дальнейшем будет использован тот факт, что в большинстве случаев время прохождения пакета между произвольными коммутаторами не превосходит некоторого порогового значения [1].

6. Модель, учитывающая потерю пакетов в сети

Разделим СМО на две системы: СМО1 и СМО2. Будем считать, что первая система описывает обслуживание заявок, для которых полуоткрытые соединения будут успешно установлены после получения коммутатором ответа контроллера, а вторая – требования, для которых соединения не будут установлены и после истечения отведенного таймаута будут удалены.

В большинстве случаев время обмена парой пакетов между коммутатором и контроллером не превосходит порог $T_{\text{п}}$. К требованиям второго типа будем относить заявки, для которых TCP соединение находится в полуоткрытом состоянии дольше чем $T_{\text{п}}$. Обозначим через s и l – количества соединений первого и второго типов соответственно. Такое представление контроллера изображено на рис. 3.

Рис. 3. Контроллер как система массового обслуживания

Определим соотношения, описывающие состояние такой системы. Аналогично (6) определим среднее количество полуоткрытых соединений:

$$N = s + l = \alpha_1 + \alpha_2 = \frac{\lambda_1}{\mu_1} + \frac{\lambda_2}{\mu_2}. \qquad (7)$$

Как следует из соотношения (7), среднее число полуоткрытых соединений является случайной величиной, равной сумме двух случайных величин, имеющих пуассоновский закон распределения. Первая из них описывает среднее количество полуоткрытых соединений, которые не представляют собой угрозу с точки зрения атаки. Вторая составляющая представляет собой полуоткрытые соединения, которые не будут установлены и через заданный промежуток времени (определяемый таймаутом) будут удалены, до этого занимая ресурсы контроллера. Увеличение количества таких соединений является признаком атаки.

Далее будем рассматривать в качестве заявки не все пакеты, для которых коммутатор ожидает ответный пакет от контроллера, а только те, для которых время ожидания превышает пороговое значение $T_{\text{п}}$. Интенсивность поступления таких заявок определяется соотношением

$$\lambda_2 = \lambda \cdot P_{\text{по}}, \qquad (8)$$

где λ – интенсивность поступающих пакетов; $P_{\text{по}}$ – вероятность появления полуоткрытого соединения, которое не будет установлено.

Параметр $P_{\text{по}}$ зависит от качества работы сети, которое характеризуется вероятностью потери пакета в сети $P_{\text{пп}}$. Найдем зависимость $P_{\text{по}}$ от $P_{\text{пп}}$. Пусть событие A заключается в том, что был потерян пакет в направлении от коммутатора к контроллеру, а событие B представляет собой

потерю пакета от контроллера к коммутатору. Вероятность события A равна вероятности потери пакета в сети:

$$P(A) = P_{\text{пп}}. \quad (9)$$

Так как событие B может наступить только тогда, когда не наступило событие A, то его вероятность равна

$$P(B) = P(\overline{A}) \cdot P_{\text{пп}} = (1 - P_{\text{пп}}) \cdot P_{\text{пп}}. \quad (10)$$

Рассмотрим событие C, заключающееся в появлении полуоткрытого соединения второго типа. Оно равно сумме событий A и B. Отсюда, с учетом (9) и (10), получим

$$P_{\text{по}} = P(C) = P(A+B) = P(A) + P(B) = P_{\text{пп}} + (1 - P_{\text{пп}}) \cdot P_{\text{пп}} = P_{\text{пп}} + P_{\text{пп}} - P_{\text{пп}}^2 = 2P_{\text{пп}} - P_{\text{пп}}^2. \quad (11)$$

Из соотношений (8) и (11) найдем интенсивность потока требований второго типа

$$\lambda_2 = \lambda \cdot P_{\text{по}} = \lambda \cdot (2P_{\text{пп}} - P_{\text{пп}}^2). \quad (12)$$

Коммутатор может отсылать несколько копий пакетов до тех пор, пока не будет получен ответ контроллера. Обозначим количество таких копий параметром N_{kontr}. Тогда интересующее нас событие заключается в том, что ни для одной из копий не дойдет ответный пакет, и соотношение (12) принимает следующий вид:

$$\lambda_2 = \lambda \cdot P_{\text{по}}{}^{N_{kontr}} = \lambda \cdot (2P_{\text{пп}} - P_{\text{пп}}^2)^{N_{kontr}}. \quad (13)$$

Так как интенсивность потока требований второго типа (наличие атак) пропорциональна интенсивности первоначального потока, то он так же является пуассоновским.

Среднее число таких заявок, находящихся на обслуживании в СМО, определяется вторым слагаемым формулы (7):

$$l = \frac{\lambda_2}{\mu_2} = \frac{\lambda \cdot P_{\text{пп}}{}^{N_{kontr}}}{\mu_2} = \frac{\lambda (2P_{\text{пп}} - P_{\text{пп}}^2)^{N_{kontr}}}{\mu_2}, \quad (14)$$

где $1/\mu_2$ – таймаут, отведенный на коммутаторе на установление TCP соединения; P_{nn} – вероятность потери пакета в сети; N_{kontr} – количество копий пакетов, отправляемых коммутатором.

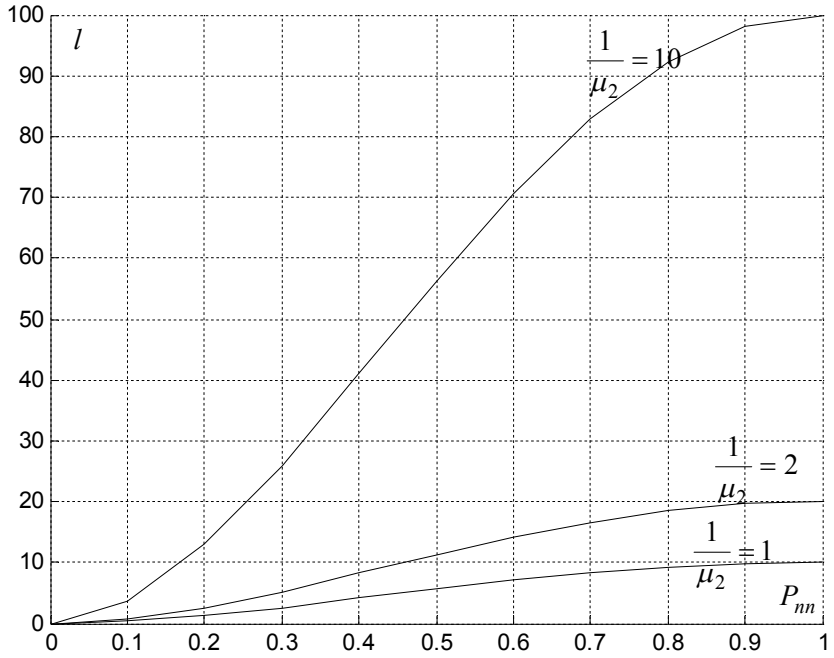

Рис. 4. Зависимость среднего числа заявок при наличии атак от вероятности потери пакетов

На рис. 4 представлены графики зависимости среднего числа заявок при наличии атак от вероятности потери пакетов. Данные графики получены при $N_{kontr} = 2$ и $\lambda = 10$. Верхняя кривая на рис. 4 соответствует $1/\mu_2 = 10$, средняя кривая – $1/\mu_2 = 2$ и нижняя кривая – $1/\mu_2 = 1$. Из данных

графиков видно, что с увеличением вероятности потери пакетов количество заявок при наличии атак увеличивается. Также видно, что с увеличением времени тауймаута количество заявок также увеличивается.

При использовании данной модели признаком атаки является превышение значения среднего числа заявок от текущего количества полуоткрытых соединений некоторого порогового значения $l_{\text{пор}}$, которое будет соответствовать вероятности верного обнаружения атаки.

Достоинствами предлагаемой модели являются возможность своевременного (раннего) обнаружения атаки, ее способность адаптироваться к реальным параметрам сети. При значительном увеличении интенсивности обращений к контроллеру количество потерянных пакетов увеличится пропорционально вероятности потери пакета в сети. Так как для современных сетей эта величина имеет небольшое значение, то эффективность обнаружения снизится незначительно. Недостатком является то, что неисправности сетевого оборудования, в результате которых увеличивается вероятность потери пакета в сети, будут интерпретированы как атака.

Для того, чтобы иметь возможность эффективно обнаруживать атаку на практике, необходимы средства, позволяющие определять значения исходных параметров модели.

Выводы

1. Архитектура SDN не лишена потенциальных уязвимостей с точки зрения информационной безопасности. Контроллер как ключевой компонент в управлении всей инфраструктурой SDN является наиболее уязвимым элементом, атака на который может повлечь критичные для всей инфраструктуры последствия. Основными угрозами, возникающими со стороны сетевых устройств, работающих по принципу программно-конфигурируемой сети, остаются вариации таких атак, как «отказ в обслуживании», подмена контроллера и т. д.

2. Предложено реакцию SDN-сети на потоки различных пакетов, в том числе и на атаки рассматривать как функционирование некоторой системы массового обслуживания, которая обрабатывает требования на обработку пакетов.

3. Разработана математическая модель SDN-сети в виде системы массового обслуживания. Получена математическая зависимость среднего числа заявок при появлении атак. Получены графики зависимости среднего числа заявок при наличии атак от вероятности потери пакетов. Достоинствами предлагаемой модели являются возможность своевременного (раннего) обнаружения атаки, ее способность адаптироваться к реальным параметрам сети.

Литература

1. Захаров, А.А. Аспекты информационной безопасности архитектуры SDN / А.А. Захаров, Е.Ф. Попов, М.М. Фучко // Вестник СибГУТИ. – 2016. – № 1. – С. 83–92.

2. Openflow: enabling innovation in campus networks / N. McKeown, T. Anderson, H. Balakrishnan et al. // ACM SIGCOMM Computer Communication Review. – 2008. – Vol. 38, iss. 4. – P. 69–74. DOI: 10.1145/1355734.1355746

3. OpenFlow Switch Specification Ver 1.5.1, 2016 – https://www.opennetworking.org/images/ stories/downloads/sdnresources/ onf-specifications/openflow/openflow-switch-v1.5.1.pdf (дата обращения: 11.01.2016).

4. Партыка, Т.Л. Информационная безопасность: учеб. пособие для студентов учреждений сред. проф. образования / Т.Л. Партыка, И.И. Попов. – М.: ФОРУМ: ИНФРА-М. – 2002. − 368 с.

5. Лукацкий, А. Информационная безопасность 2015 / А. Лукацкий // ИТ-безопасность. Стандарты. Средства защиты. Мероприятия. – 2013. – № 12. – С. 64–69.

6. Ложковский, А.Г. Теория массового обслуживания в телекоммуникациях: учеб. / А.Г. Ложковский. – Одесса: ОНАС им. А.С. Попова, 2012. – 112 с.

7. Ложковский, А.Г. Моделирование многоканальной системы обслуживания с организацией очереди / А.Г. Ложковский, Н.С. Салманов, О.В. Вербанов // Восточно-Европейский журнал передовых технологий. – 2007. – № 3/6 (27). – С. 72–76.

8. Корнышев, Ю.Н. Теория распределения информации: учеб. пособие для вузов / Ю.Н. Корнышев, Г.Л. Фань. – М.: Радио и Связь, 1985. – 184 с.

Коляденко Юлия Юрьевна, д-р техн. наук, профессор, профессор кафедры инфокоммуникационной инженерии, Харьковский национальный университет радиоэлектроники, г. Харьков; kolyadenko.home@rambler.ru.

Лукинов Иван Геннадьевич, аспирант кафедры инфокоммуникационной инженерии, Харьковский национальный университет радиоэлектроники; инженер, Харьковский государственный региональный научно-технический центр по вопросам технической защиты информации; lig-90@ukr.net.

Поступила в редакцию 9 апреля 2017 г.

DOI: 10.14529/ctcr170304

MODEL OF DISTRIBUTED ATTACKS IN PROGRAM-CONFIGURABLE COMMUNICATION NETWORKS

***Yu.Yu. Kolyadenko*[1]**, *kolyadenko.home@rambler.ru,*
***I.G. Lukinov*[1, 2]**, *lig-90@ukr.net*
[1] *Kharkiv National University of Radio Electronics, Kharkiv, Ukraine,*
[2] *Kharkiv State Regional Scientific Technical Center of Technical Information Protection, Kharkiv, Ukraine*

It is shown that the architecture of SDN is not without potential vulnerabilities in terms of information security. The controller as a key component in the management of the entire SDN infrastructure is the most vulnerable element, the attack on which can entail consequences that are critical for the entire infrastructure. The main threats arising from network devices operating on the principle of a program-configurable network are variations of such attacks as “denial of service”, replacement of the controller, and so on.

The SDN-network's reaction to the flows of various packets, including attacks, is considered as the functioning of some queuing system that processes processing requirements for packets. A mathematical model of the SDN-network in the form of a queuing system was developed. A mathematical dependence of the average number of applications is obtained upon the appearance of attacks. The graphs of the average number of applications are obtained in the presence of attacks against the probability of packet loss. Advantages of the proposed model are the possibility of timely (early) detection of an attack, its ability to adapt to the real parameters of the network.

Keywords: SDN-network, controller, switch, OpenFlow protocol, information security, attacks, queuing theory.

References

1. Zakharov A.A., Popov Ye.F., Fuchko M.M. [Aspects of Information Security of Architecture of SDN/A]. *Bulletin of Siberian State University of Telecommunications and Information Science*, 2016, no. 1, pp. 83–92. (in Russ.)

2. McKeown N., Anderson T., Balakrishnan H., Parulkar G., Peterson L., Rexford J., Shenker S., Turner J. Openflow: Enabling Innovation in Campus Networks. *ACM SIGCOMM Computer Communication Review*, 2008, vol. 38, iss. 4, pp. 69–74. DOI: 10.1145/1355734.1355746

3. OpenFlow Switch Specification Ver 1.5.1, 2016. Available at: https://www.opennetworking.org/images/stories/downloads/sdnresources/onf-specifications/openflow/openflow-switch-v1.5.1.pdf (accessed 11.01.2016).

4. Partyka T.L., Popov I.I. *Informatsionnaya bezopasnost': uchebnoye posobiye dlya studentov uchrezhdeniy srednego professional'nogo obrazovaniya* [Information Security: Manual for Students of Secondary Vocational Education Institutions]. Moscow, FORUM: INFRA-M. Publ., 2002. 368 p.

5. Lukatskiy A. [Information Security 2015]. *IT-Safety. Standards. Means of Protection. Actions*, 2013, no. 12, pp. 64–69. (in Russ.)

6. Lozhkovskiy A.G. *Teoriya massovogo obsluzhivaniya v telekommunikatsiyakh: uchebnik* [The Theory of Mass Service in Telecommunications: Textbook]. Odessa, Odessa National Academy of Telecommunications Publ., 2012. 112 p.

7. Lozhkovskiy A.G., Salmanov N.S., Verbanov O.V. [Modeling of Multichannel System of Service with the Organization of Turn]. *East European Journal of Advanced Technologies*, 2007, no. 3/6 (27), pp. 72–76. (in Russ.)

8. Kornyshev Yu.N., Fan' G.L. *Teoriya raspredeleniya informatsii: ucheb. posobiye dlya vuzov* [Theory of Dstribution of Information: Manual for Higher Education Institutions]. Moscow, Radio i Svyaz' Publ., 1985. 184 p.

Received 9 April 2017

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Коляденко, Ю.Ю. Модель распределенных атак в программно-конфигурируемых сетях связи / Ю.Ю. Коляденко, И.Г. Лукинов // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2017. – Т. 17, № 3. – С. 34–43. DOI: 10.14529/ctcr170304

FOR CITATION

Kolyadenko Yu.Yu., Lukinov I.G. Model of Distributed Attacks in Program-Configurable Communication Networks. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*, 2017, vol. 17, no. 3, pp. 34–43. (in Russ.) DOI: 10.14529/ctcr170304