DOI 10.37882/2223–2966.2020.07.38

ЗАЩИТА МОБИЛЬНОЙ СЕТИ ОТ DDOS-АТАК С ПРИМЕНЕНИЕМ СПИСКА IP-АДРЕСОВ

Храмцов Илья Александрович
Аспирант, Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева, г. Красноярск
ilia.khramcov@yandex.ru

Аннотация. Масштабное использование мобильных сетей поднимает вопрос обеспечения защиты персональных данных от злоумышленников. Несмотря на текущий уровень обеспечения безопасности мобильных сетей, до сих пор актуальными проблемами являются угрозы кражи, хищения, перехвата и прослушивания конфиденциальной и личной информации оператора и абонента сети. Реализация данных угроз в сети дает возможность злоумышленнику получать контроль над базовыми станциями и необходимую информацию об абоненте, а также влиять на работу оборудования мобильной сети.

Ключевые слова: информационная безопасность, информационно-телекоммуникационная сеть, DDoS-атака.

PROTECTING THE MOBILE NETWORK FROM DDOS ATTACKS USING A LIST OF IP ADDRESSES

I. Khramtsov

Summary. The large-Scale use of mobile networks raises the issue of ensuring the protection of personal data from hackers. Despite the current level of security of mobile networks, threats of theft, theft, interception and listening to confidential and personal information of the network operator and subscriber are still relevant problems. Implementation of these threats in the network allows an attacker to gain control over the base stations and the necessary information about the subscriber, as well as influence the operation of mobile network equipment.

Keywords: information security, information and telecommunications network, DDoS attack.

Введение

Ключевой особенностью современных мобильных сетей связи является использование вычислительных распределенных систем, которые позволяют обеспечить быстрый и гибкий доступ к информационным ресурсам сети оператора. При этом необходимо учитывать тот факт, что вместе с развитием технических средств, обрабатывающих информацию, также развиваются методы и средства реализации воздействия на оператора и пользователя мобильной сети со стороны злоумышленников.

В данный момент одним из основных видов атак являются атаки типа «отказ в обслуживании» (DDoS-атаки), которые оказывают сильное воздействие на информационные системы мобильной сети [4–5]. Основной принцип воздействия DDoS-атаки на мобильную сеть основан на большом количестве отправляемых запросов на сервер сети, в результате чего реализуется максимальная нагрузка на вычислительные ресурсы сервера, что приводит к тому, что сервер не справляется с обработкой данных и в дальнейшем не дает обратной связи на запросы пользователей [1].

Рассматривая современные методы систем защиты, следует констатировать, что они не в полной мере справляются с обеспечением защиты мобильной сети от DDoS-атак, так как данным методам нужно значительное время для восстановления работоспособности сетевых элементов. Также это связано с отсутствием дополнительного анализа служебной информации сети, что приводит к тому, что имеющиеся на сегодняшний момент методы не всегда приводят к нужному и желаемому результату [2–3].

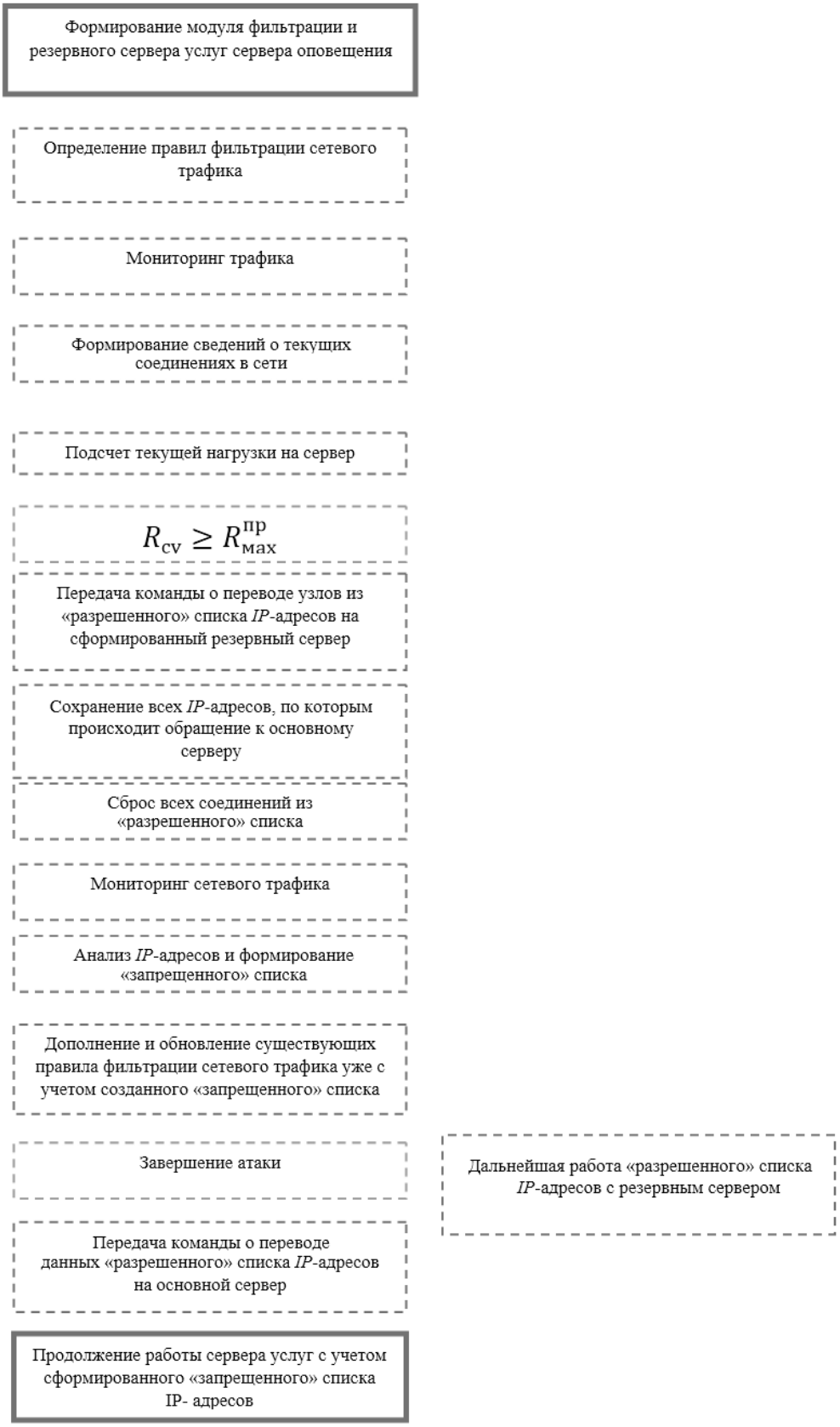

Рис. 1. Алгоритм, реализующий метод защиты сервера услуг от DDoS-атак

Алгоритм предлагаемого метода

Рассмотрим вариант реализации метода защиты с использованием IP-адресов, который может быть использован для защиты серверов от потенциальной угрозы DDos-атаки.

Схема предлагаемого метода представлена на рисунке 1, где на первом этапе формируется модуль управления, который в дальнейшем применяет «разрешенные» и «запрещенные» списки IP-адресов, а также корректируются правила фильтрации, по которым список «разрешенных» IP-адресов задаётся первоначально, а «запрещенный» список адресов формируется на шаге № 11. Также, помимо этого, задаётся максимальная производительность сервера услуг и формируется «дополнительный» резервный сервер услуг и сервер оповещения, который служит для рассылки служебных команд, которые формируются при переключении на дополнительный сервер.

На следующем шаге создаются правила фильтрации сетевого трафика. Данные правила основываются на выбранном режиме безопасности сети для каждого сетевого интерфейса, а также списка сетевых фильтров системы устранения атак. Фильтрация трафика происходит при установлении соединения в сети, то есть соединений, образующихся на основании разрешенного правилами входящего или исходящего пакета передачи данных в сети. При получении пакета данных на основании правил записываются параметры разрешенного фильтрами входящего или исходящего пакета данных. На основании этих данных в сети формируется временное разрешенное соединение для дальнейшего пропуска пакета данных. Данное правило действует, пока есть трафик, соответствующий данному соединению в сети.

Далее происходит мониторинг сетевого трафика. Программы мониторинга сети позволяют выполнять захват пакетов и их реассемблирование для дальнейшего анализа. Параллельно с этим идет обработка полученных данных обо всех запросах к серверу сети с последующим агрегированием полученных данных.

На шаге № 4 алгоритма идет сбор сведений о текущих соединениях сервера. Далее происходит процесс инвентаризации соединений на сервере и IP-адресов пользователя, а также подсчитывается количество IP-пакетов, которые были переданы между этими парами. Далее с учетом подсчитанных данных идет расчет текущей нагрузки на сервер. В общем случае представим подсчет нагрузки на сервер в виде произведения количества абонентов, подключенных к серверу услуг, и объема передаваемой абонентами информации:

$$R_{инф}^{уз} = N_{аб} * V_{инф}^{аб}$$

Где $R_{инф}^{уз}$ — общая нагрузка на сервер;

$N_{аб}$ — количество абонентов;

$V_{инф}^{аб}$ — объем передаваемой абонентами информации.

При рассмотрении ситуации в условиях сетевых атак общую нагрузку на сервер сети можно представить как сумму нагрузки DDoS-атаки и информационной нагрузки от узлов связи сети:

$$R_{су} = \sum_{j=1}^{I} R_{инф}^{уз} * R_{ат}$$

Где $R_{су}$ — общая нагрузка на сервер услуг;

$R_{инф}^{уз}$ — нагрузка от узлов связи, подключённых к серверу услуг;

$R_{ат}$ — нагрузка на сервер, производимая DDoS-атакой.

На шаге № 6 идет проверка выполнения условия $R_{су} \geq R_{\max}^{пр}$. Если условие выполняется, то алгоритм переходит к шагу № 7 и передает команды о переводе узлов связи из «разрешенного» списка IP-адресов на резервный сервер услуг. Если условие не выполняется, то алгоритм возвращается к шагу № 3 и продолжает дальнейший мониторинг сетевого трафика. На шаге № 8 производится запись всех IP-адресов, с которых происходило обращение к основному серверу сети (кроме IP адресов «разрешенного» списка), на основании полученных данных обо всех запросах к серверу услуг выделяют IP-адреса и записывают их в массив памяти M_1.

На шаге № 9 происходит сбрасывание всех соединений из «разрешенного» списка IP-адресов. Все соединения из «разрешенного» списка IP-адресов, установленные с сервером сети, сбрасываются, после чего сервер услуг перезагружают.

На шаге № 10 осуществляют мониторинг сетевого трафика основного сервера услуг. На данном этапе идет обработка полученных данных обо всех запросах к серверу сети с последующим агрегированием полученной информации.

На шаге № 11 происходит анализ IP-адресов, а также формируется «запрещенный» список IP-адресов. Из полученных данных обо всех запросах к серверу сети выделяют IP-адреса, с которых было сформировано обращение к серверу, и сохраняют их в массив памяти M_2. Далее идет сравнение массивов M_1 и M_2. Если IP-адреса в массивах совпали, то они записываются в массив памяти M. Данный массив памяти M и будет считаться

«запрещённым» списком IP-адресов. IP-адреса, которые присутствовали только в одном из массивов, не считаются угрозой сети и в данный список не попадают.

Также следует указать, что запрещенный список IP-адресов принято разделять на статический и динамический списки. Ключевым недостатком статических списков является то, что для обращения к выбранной службе «запрещенных» списков установленные программы фильтрации создают специальный запрос DNS, который передаётся на сервер DNS оператора «запрещенных» списков. Динамический список «запрещенных» IP-адресов представляет собой сетевую службу, которая предоставляется оператором. Задача этих операторов непосредственно направлена на поиск IP-адреса, скомпрометированного возможным злоумышленником.

В предложенном алгоритме «запрещенный» список IP-адресов создаётся непосредственно при осуществлении атаки и позволяет выяснить актуальные для конкретной атаки IP-адреса. При этом данные списка постоянно обновляются в режиме реального времени, а также отсутствует необходимость обращения к оператору «запрещённых» списков IP-адресов.

На шаге № 12 происходит обновление правил фильтрации сетевого трафика на основании скорректированного «запрещенного» списка IP-адресов. На шаге № 13 данного алгоритма происходит проверка окончания атаки на основании сервера сети. Если данная атака продолжается, то алгоритм переходит на шаг № 14 и продолжает взаимодействие узлов «разрешённого» списка IP-адресов с резервным сервером услуг. Если нет, то алгоритм переходит к шагу № 15 и передает служебные команды о переводе узлов «разрешенного» списка IP-адресов на основной сервер услуг сети. На шаге № 16 осуществляется функционирование сервера услуг с учетом уже скорректированного «запрещенного» списка IP-адресов.

После перевода «разрешённого» списка IP-адресов на основной сервер сети пакеты данных проверяются с учетом «разрешённого» списка IP-адресов. Если принятые пакеты получены из списка «разрешённых» IP-адресов, то данный пакет обрабатывается. Если пакет принят с IP-адреса не из «разрешённого» списка, то далее данный IP-адрес сравнивается с «запрещенным» списком IP-адресов. Если обнаружиться, что данный пакет данных получен из списка «запрещенных» IP-адресов, то такой пакет будет отфильтрован в центр очистки с дальнейшим полным уничтожением.

Рассчитав примерную эффективность предлагаемого алгоритма, следует заключить, что в среднем DDoS-атака длится приблизительно 5 часов, при этом во время атаки нагрузка на сервер сети превосходит допустимую возможную нагрузку, что в дальнейшем приводит к отказу в обслуживании абонентов сети, также используются лишние ресурсы и время для восстановления оптимальной работы сервера. Таким образом, все время проведения DDoS-атаки и время, необходимое для восстановления работоспособности, сервер услуг не сможет предоставлять услуги пользователям.

$$t_{оу} = 5ч + t_{в}$$

где $t_{оу}$ — среднее время отказа в обслуживании;
$t_{в}$ — среднее время восстановления.

В предложенном алгоритме в начале DDoS-атаки за время t_1 все соединения, которые будут установлены с сервером услуг, будут переведены на резервный сервер, после чего за время t_2 происходит обработка сетевого трафика и формирование обновленного «запрещенного» списка IP-адресов. Время t_3 будет затрачено на перезагрузку сервера сети, а время t_4 — на восстановление работы сервера услуг сети (учитывая «запрещенный» список IP-адресов):

$$t_{оу} = t_1 + t_2 + t_3 + t_4$$

Подводя итоги, следует отметить, что данный метод позволит повысить защищенность сервера услуг за счет непрерывного обслуживания соединений из «разрешенного» списка IP-адресов, а также организации дополнительного анализа «запрещенного» списка IP-адресов.

Заключение

Приведенный метод защиты распределенных информационных систем за счет блокирования потенциально несущих угрозу исходящих потоков данных, осуществляющих реализацию DDoS-атак, даст возможность обеспечить безопасность информационной системы и ресурсов мобильной сети.

Основным шагом в выявлении DoS/DDoS-атак можно считать непосредственно обнаружение данной атаки. Поскольку число возможных атак и их видов растет, то их обнаружение становится главной проблемой. В настоящее время на практике сложно разработать и внедрить механизмы защиты от DDoS-атак. В современных мобильных сетях сейчас выполнение всех требований по обнаружению DDoS-атак становится очень затруднительным, потому что различные параметры информационной безопасности мобильной сети должны быть точно и надлежащим образом сбалансированы и быть полностью взаимосвязаны. Именно поэтому обсуждаемая проблема остается актуальной.

ЛИТЕРАТУРА

1. Бегаев А.Н., Добрышин М. М., Закалкин П. В. и др. Предложение по оценке способности узла компьютерной сети функционировать в условиях информационно-технических воздействий // Вопросы кибербезопасности. 2018. № 3 (27). С. 2–8.
2. Бегаев А.Н., Добрышин М. М., Закалкин П. В., Реформат А. Н., Рауткин Ю. В. Комплексный алгоритм мониторинга защищенности узлов VPN от компьютерной разведки и DDoS-атак // Электросвязь. 2018. № 7. С. 46–52.
3. Гречишников Е.В., Добрышин М. М., Закалкин П. В. Модель узла доступа VPN как объекта сетевой и потоковой компьютерных разведок и DDoS-атак // Вопросы кибербезопасности. 2016. № 3 (16). С. 4–12.
4. Карайчев С. Ю. Подход к формированию логических схем реализации угроз при визуализации информации в системах информационной безопасности / С. Ю. Карайчев, В. В. Бухарин // Защита информации Инсайд. 2017. № 2 (74). С. 52–57.
5. Коцыняк М.А., Лаута О. С., Иванов Д. А., Лукина О. М. Модель воздействия таргетированной кибернетической атаки на информационно-теле- коммуникационную сеть // Вопросы оборонной техники. Серия 16. 2019. Вып. 3–4 (129–130). С. 58–65.

© Храмцов Илья Александрович (ilia.khramcov@yandex.ru).

Журнал «Современная наука: актуальные проблемы теории и практики»