УДК 004.032.26
DOI: 10.15827/0236-235X.128.613-627
Дата подачи статьи: 29.04.19
2019. Т. 32. № 4. С. 613–627

Разработка импульсной нейронной сети с возможностью скоростного обучения для нейтрализации DDoS-атак

Е.В. Пальчевский [1], *аспирант, teelxp@inbox.ru*
О.И. Христодуло [1], *д.т.н., профессор, o-hristodulo@mail.ru*

[1] *Уфимский государственный авиационный технический университет, г. Уфа, 450008, Россия*

Эффективное обеспечение доступности данных является одной из ключевых задач в области информационной безопасности. Зачастую доступность информации нарушают DDoS-атаки. Несовершенство современных методов защиты от атак внешним несанкционированным трафиком приводит к тому, что многие компании, ресурсы которых имеют выход в сеть Интернет, сталкиваются с недоступностью собственных сервисов, предоставляющих различные услуги/информацию. Как следствие – финансовые потери компании от простоя оборудования. Для решения данной проблемы разработана импульсная (спайковая) нейронная сеть для защиты от атак внешним несанкционированным трафиком.

Основными преимуществами разработанной спайковой нейронной сети являются высокая скорость самообучения и быстрое реагирование на DDoS-атаки (в том числе и на неизвестные). Разработан новый метод самообучения импульсной нейронной сети, в основу которого входит равномерная обработка спайков каждым нейроном. За счет этого нейронная сеть в кратчайшие сроки обучается, как следствие – быстро и эффективно отфильтровывает атаки внешним несанкционированным трафиком. Также проведено сравнение разработанной спайковой нейронной сети с аналогичными решениями по защите от DDoS-атак. В результате сравнения выявлено, что разработанная нейронная сеть более оптимизирована под высокие нагрузки и способна в кратчайшие сроки обнаружить и нейтрализовать DDoS-атаки.

Проведена апробация разработанной импульсной нейронной сети в условиях простоя и в режиме защиты от DDoS-атак. В результате данного тестирования получены нагрузочные значения на ресурсы вычислительного кластера. Длительное тестирование импульсной нейронной сети показывает достаточно низкую нагрузку на центральный процессор, оперативную память и твердотельный накопитель при массивных DDoS-атаках. Таким образом, оптимальная нагрузка не только повышает доступность каждого физического сервера, но и предоставляет возможность параллельного запуска ресурсоемких вычислительных процессов без какого-либо нарушения функционирования рабочей среды.

Тестирование проводилось на серверах вычислительного кластера, где импульсная нейронная сеть показала стабильную работу и эффективно защищала от DDoS-атак.

Ключевые слова: *информация, передача данных, сети, спайковая нейронная сеть, самообучение нейронной сети, DDoS-атаки, вредоносный трафик, информационная безопасность.*

Информационные технологии являются неотъемлемой частью современного мира: внедрение различных инновационных решений повышает производительность труда и позволяет автоматизировать рабочие процессы [1]. Соответственно, в любой организации, активно использующей решения в области IT-сферы, существует определенный внутренний регламент по внедрению инновационных технологий в рабочий процесс с учетом политики информационной безопасности предприятия, закладывающей следующие основные аспекты [2]:

– цели обеспечения информационной безопасности;

– задачи, решаемые для достижения цели в области защиты информации;

– основные принципы обеспечения информационной безопасности;

– ответственность за нарушение политики информационной безопасности предприятия.

Как правило, в задачи обеспечения защиты информации предприятия входит предотвращение нарушения целостности, доступности и конфиденциальности данных. Например, доступность информации зачастую нарушают атаки внешним несанкционированным трафиком (DDoS-атаки) [3]. Данные киберугрозы подразделяются на однонаправленные (DoS) и распределенные (DDoS) [4–7]. Если рассматри-

вать однонаправленные атаки несанкционированным трафиком, то необходимо отметить, что на данный момент подобные кибератаки потеряли свою актуальность из-за достаточно быстрого и эффективного противодействия на уровне *центров обработки данных* (ЦОД), например, блокировка 123-го порта (network time protocol, NTP), позволяющая отразить NTP-усиление. Структурная схема работы DoS-атак представлена на рисунке 1.

Рис. 1. Структурная обобщенная схема работы однонаправленных атак

Fig. 1. A structural generalized scheme of unidirectional attacks

Как правило, на атакующем сервере (рис. 1) установлено специализированное ПО (например, панель управления троянской программой) для удаленного контроля уязвимых устройств. В свою очередь, данные троянские программы распространяются во внешней глобальной сети и заражают различные устройства: начиная от персональных компьютеров и заканчивая камерами наблюдения. После заражения злоумышленник получает удаленный контроль над устройством, имеющим выход во внешнюю глобальную сеть. Все зараженные устройства объединяются в сеть ботнет. Таким образом, происходит усиление трафика за счет большого количества хостов. Например, троянская программа произвела несанкционированный взлом 100 физических серверов (канал каждой ЭВМ – 1 Гбит/сек.). Таким образом, в случае с DoS будет произведена атака емкостью 100 Гбит/сек. на определенные порты физического сервера. Необходимо отметить, что ранее для DoS-атаки использовали именно одно зараженное удаленное устройство. На данный момент ситуация совершенно иная: для однонаправленных атак стали использовать большое количество устройств с целью доведения оборудования до отказа в удаленном обслуживании.

В случае с DDoS-атаками все не так однозначно: их частое использование приводит к тому, что фактически каждой компании приходится тратить дополнительные финансовые средства на обеспечение доступности информации. Как правило, данные атаки внешним несанкционированным трафиком гораздо эффективнее DoS и поэтому направлены на ресурсы, имеющие сетевой канал с большой пропускной способностью. Способ заражения и объединения устройств в единую сеть ботнет полностью идентичен с DoS. Структурная схема работы DDoS-атак показана на рисунке 2.

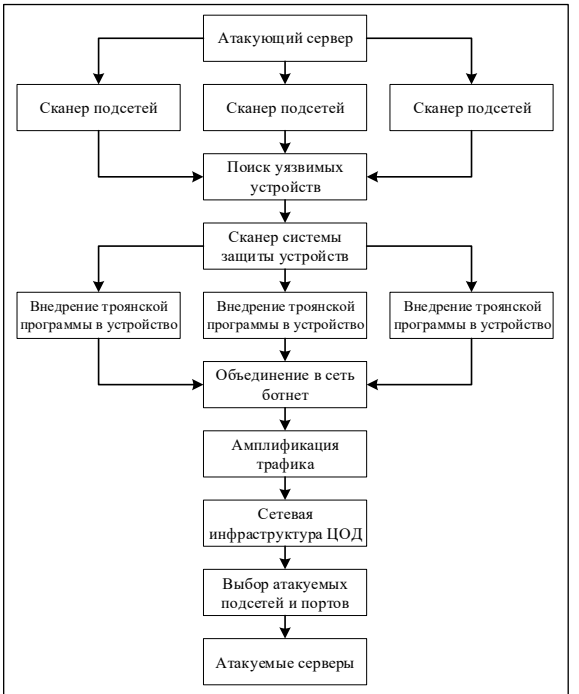

Рис. 2. Структурная обобщенная схема работы DDoS-атак

Fig. 2. A structural generalized scheme of DDoS attack operations

Изначально на атакующем сервере запускается панель управления сетью ботнет. Далее троянская программа распространяется по внешней глобальной сети, одновременно сканируя подсети IP-адресов. После сканирования подсетей и распространения данного вредоносного ПО происходит поиск уязвимых устройств (рис. 3). Следующими шагами являются выполнение сканирования и обход системы защиты от вредоносного ПО (в том числе и методом полного перебора) с последующим внедрением троянской программы. По завершении взлома в панель управления приходят данные для удаленного доступа к

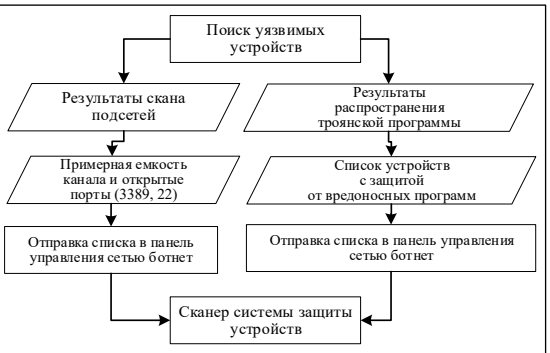

Рис. 3. Алгоритм поиска уязвимых устройств для включения в сеть ботнет

Fig. 3. Algorithm for searching vulnerable devices to include into the botnet network

устройству с дальнейшим включением его в сеть ботнет. Таким образом, при DDoS-атаке происходит усиление трафика с предварительным сканированием и исследованием сетевой инфраструктуры ЦОД, выбором атакуемых подсетей, портов и, как следствие, серверов.

В настоящее время исследованиями в области защиты от атак внешним несанкционированным трафиком (DDoS) занимаются многие российские и зарубежные ученые. Например, методика обнаружения низко- и высокоактивных DDoS-атак на веб-приложения, использующих IPv6, описана в [8], защита от атак внешним несанкционированным трафиком для DNS-инфраструктуры – в [9], метод раннего обнаружения низкоактивных DDoS-атак на сети ЦОД с использованием технологии программно-конфигурируемой сети (software defined networking, SDN) – в [10], инфраструктурный метод обнаружения DDoS-атак, основанный на байесовской модели множественных изменений, – в [11]. Интеллектуальная система защиты от DDoS-атак в сетях связи, состоящая из двух компонентов – монитора для обнаружения DDoS-атак и дискриминатора для выявления пользователей в системе со злонамеренными планами описана в [12], распределенная, гибкая, автоматизированная и универсальная система защиты (D-FACE) уровня ISP, позволяющая обнаруживать атаки внешним несанкционированным трафиком на их раннем этапе, – в [13], использование искусственной нейронной сети для обнаружения DDoS-атак на основе определенных характерных особенностей (шаблонов), отделяющих вредоносный трафик от пользовательского (легитимного), – в [14].

Современные функциональные спецификации и технические возможности в настоящее время позволяют разрабатывать и альтернативные нейронные сети для защиты от DDoS-атак. Это способствует не только совершенствованию существующих разработок, но и созданию полностью инновационных и уникальных продуктов в области искусственного интеллекта, которые повышают производительность серверного оборудования, снижают затраты на закупку и обслуживание физических серверов, а также автоматизируют решение каких-либо задач в различных организациях.

Целью данного научного исследования является разработка *импульсной (спайковой) нейронной сети* (ИмНС) для равномерного распределения сетевой нагрузки при DDoS-атаках в UNIX-подобных системах. Достижение поставленной цели позволит:

– в автоматическом режиме выявлять, анализировать и нейтрализовывать атаки внешним несанкционированным трафиком;

– в зависимости от конфигурации физического сервера/кластера рассчитывать количество ресурсов и их текущую загруженность;

– создавать БД с различными видами и типами DDoS (в том числе и с обнаружением новых атак вредоносным трафиком), что позволит нейронной сети более точно составлять правила фильтрации в режиме реального времени;

– повысить доступность информации объекта (физического сервера/кластера).

Анализ существующих решений по защите от DDoS-атак

Существует множество способов для противодействия DDoS-атакам: распределенные сети фильтрации, SDN, стандартные программные решения на стороне клиента, решения операторов связи.

Распределенные сети фильтрации, общая схема которых представлена на рисунке 4, позволяют распределять имеющуюся сетевую нагрузку по достаточно большому количеству узлов, исключая возможность ее концентрации в одном ЦОД.

Изначально атакующий сервер отправляет специализированные запросы троянским программам, которые заражают различное оборудование, имеющее выход во внешнюю глобальную сеть. Далее происходит усиление трафика, как следствие – емкая и интенсивная DDoS-атака. Если подсеть, в которой расположен IP-адрес атакуемого сервера, входит в рас-

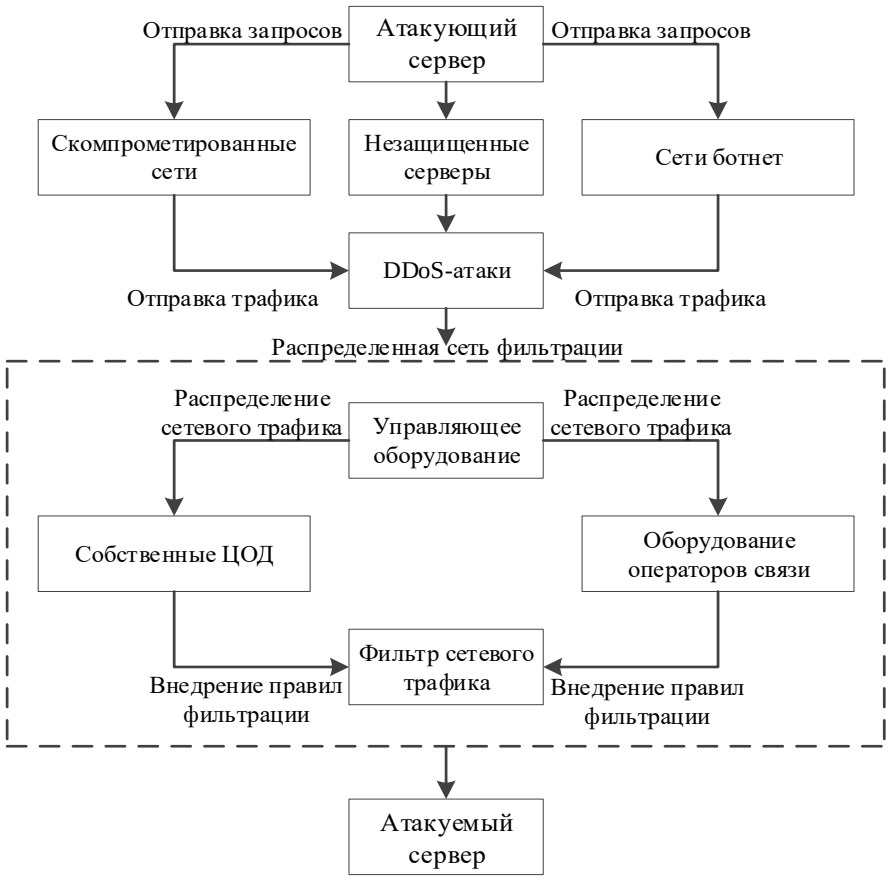

Рис. 4. Структурная обобщенная схема работы распределенных сетей фильтрации

Fig. 4. A structural generalized scheme of distributed filtering networks

пределенную сеть фильтрации, то происходит отделение вредоносного трафика от пользовательского (нормального):

– управляющее оборудование производит анализ и распределение сетевого трафика по собственным ЦОД и оборудованию операторов связи, с которыми заключен договор у компании, осуществляющей защиту от DDoS-атак;

– как правило, каждый ЦОД представляет собой одну или несколько точек фильтрации трафика; фильтрация сетевого трафика происходит и на оборудовании операторов связи;

– на основе расчета мощностей оборудования и емкостей каналов связи выполняется внедрение правил фильтрации сетевого трафика (в зависимости от DDoS-атаки правила могут кардинально отличаться друг от друга).

Таким образом, основным преимуществом распределенных сетей фильтрации является эффективная защита от DDoS-атак, а в качестве основных недостатков можно отметить сложность конфигурации сети (необходимо грамотно настроить каждый элемент узла (точки) фильтрации во избежание каких-либо проблем, например, ложное срабатывание системы фильтрации на пользовательский (легитимный) трафик) и цену (подобное решение для защиты от DDoS-атак является дорогостоящим из-за высоких цен на оборудование, реализацию и обслуживание данной сети фильтрации).

SDN представляет собой одну из форм виртуализации сети, в которой уровень управления работает отдельно от каких-либо устройств передачи данных и реализуется на программном уровне. Создание данных сетей обусловлено сразу несколькими факторами:

– стремительный рост объемов сетевого трафика;

– изменение структуры и направленности трафика;

– необходимость адаптации к растущему числу пользователей, активно использующих мобильный Интернет;

– формирование высокопроизводительных вычислительных кластеров для обработки большого объема данных;

– реализация облачных сервисов для предоставления различных услуг.

Таким образом, основной проблемой является статичность традиционных сетей: несоответствие требованиям современного бизнеса и уязвимость. Решить данную проблему позволяют SDN. Архитектура SDN состоит из трех уровней: сетевых приложений, управления и инфраструктуры. Уровень сетевых приложений содержит в себе специализированные SDN-приложения, взаимодействующие с SDN-контроллером через API и предназначенные для сбора, анализа, развертывания и управления сетевой инфраструктурой на уровне приложений. Уровень управления предоставляет возможность операторам согласованно управлять SDN любой сложности и ее устройствами. На инфраструктурном уровне SDN функционируют сетевое оборудование (например, коммутаторы) и каналы передачи данных. Более детальная архитектура SDN показана на рисунке 5.

Если рассматривать SDN-сети как способ для защиты от DDoS-атак, то необходимо отметить, что основная нагрузка ложится на управляющие (основные) сетевые коммутаторы, что может сказаться на работоспособности всей сети. Алгоритм работы SDN-сети во время DDoS-атаки представлен на рисунке 6.

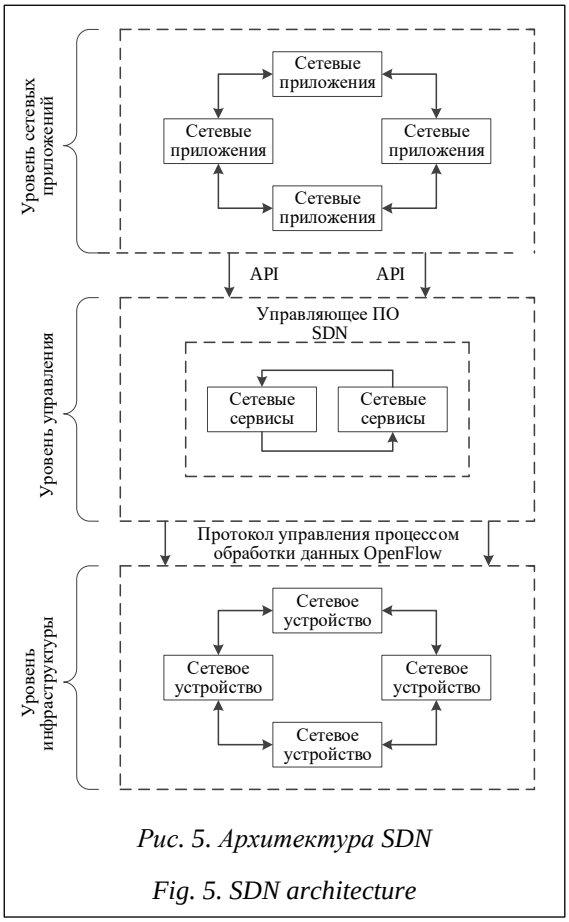

Рис. 5. Архитектура SDN

Fig. 5. SDN architecture

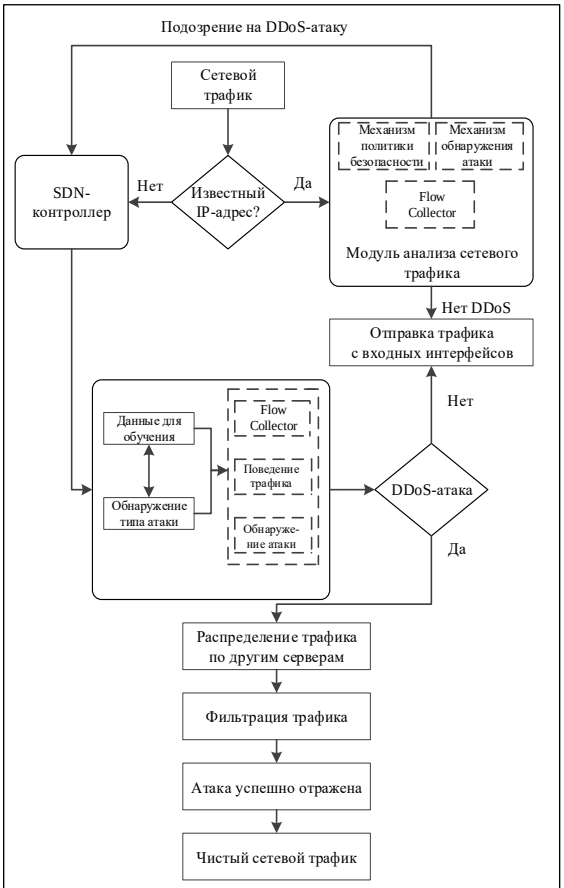

Рис. 6. Алгоритм работы SDN при DDoS

Fig. 6. SDN algorithm for DDoS

В качестве основных преимуществ данного решения по отражению DDoS-атак необходимо выделить:

– программное управление сетью: нет необходимости конфигурировать сетевое оборудование вручную, что существенно экономит время и упрощает решение каких-либо задач (в том числе и по нейтрализации DDoS);

– возможность предоставления приложения абстрактного вида сетевой инфраструктуры в силу чего сеть становится более динамичной и «умной»: реализованы самоанализ и принятие решения о форвардинге трафика (Traffic-forwarding) на основе требований определенных приложений.

Основными недостатками являются:

– высокая цена на оборудование: в сравнении с распределенными сетями фильтрации данное решение является относительно недорогим, но для малого и среднего бизнеса за-

купка оборудования для реализации SDN может оказаться проблемной из-за отсутствия необходимых финансов;

– конфигурация всей сети находится на персональном компьютере системного администратора, что довольно плохо сказывается на политике безопасности: в случае потери данных и отсутствия резервной копии администратору придется восстанавливать конфигурацию вручную;

– контроллер SDN является самой уязвимой точкой, а также главной целью для DDoS-атак;

– в случае отсутствия связи между контроллером и устройствами сети коммутаторы в автоматическом режиме переходят в исходное состояние, таким образом, сеть становится неуправляемой или нефункционирующей;

– неравномерное распределение сетевой нагрузки во время DDoS-атак.

Стандартные программные решения на стороне клиента представляют собой различные программные составляющие операционной системы, осуществляющие анализ, контроль и фильтрацию проходящего через него локального и внешнего сетевого трафика. Как правило, межсетевые экраны выполняют следующие функции:

– защита каких-либо сегментов сети, а также отдельных хостов от несанкционированного доступа;

– отделение пользовательского (нормального) сетевого трафика от вредоносного посредством внедрения правил фильтрации.

На сегодняшний день существуют межсетевые экраны (в стандартной комплектации) в двух вариантах:

– с графической оболочкой (например, стандартный брандмауэр Windows);

– с управлением через командную строку (например, Netfilter в Linux управляется при помощи IPTables).

Схема работы межсетевых экранов на стороне клиента представлена на рисунке 7.

Основным преимуществом данных решений является доступность: стандартные межсетевые экраны, как правило, внедрены в ядро операционной системы, что позволяет использовать файрвол сразу же после инсталлирования ОС. В качестве основных недостатков стандартных межсетевых экранов необходимо отметить:

– недостаточную эффективность (при больших объемах DDoS-атак файрвол может

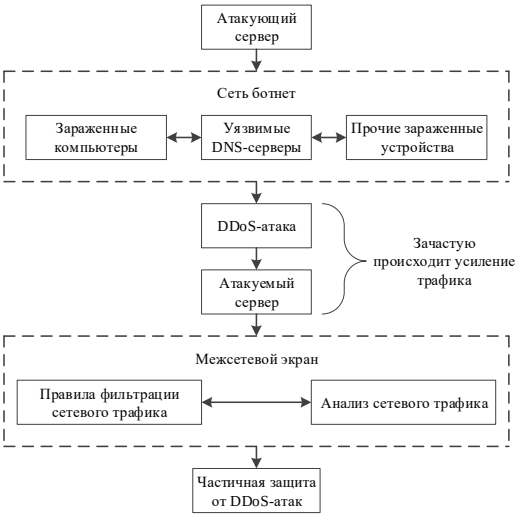

Рис. 7. Структурная стандартная схема работы файрвола в ОС

Fig. 7. The structural standard scheme of the firewall in the operation system

загрузить ресурсы ЭВМ до максимума, что может привести к ее зависанию и увеличению энергопотребления);

– невозможность распределения сетевой нагрузки при DDoS-атаках (например, если атака происходит на одно приложение, то нагрузка будет идти на все ядра, используемые данной программой, как следствие – существенное снижение производительности ЭВМ).

Таким образом, стандартные межсетевые экраны операционных систем не способны справиться с массивными DDoS-атаками, что позволяет атакующему достигнуть поставленной цели.

Решения операторов связи представляют собой специализированные сети фильтрации с оборудованием, способным пропускать большие объемы трафика. Необходимо отметить, что особенность реализации решений по анализу, выявлению и фильтрации DDoS-атак для оператора связи неразрывно связана с архитектурой построения его сетей, а также с возможностями сетевого оборудования. Обобщенная структура решений операторов связи по фильтрации сетевого трафика показана на рисунке 8.

Весь трафик от ботнета и обычных пользователей Интернета (рис. 8) проходит через пограничный маршрутизатор (могут быть как один, так и несколько). Как правило, в качестве пограничных маршрутизаторов ставится мощное сетевое оборудование, например, Juniper M320i или Huawei NE40E-X8. Далее маршру-

тизатор пропускает трафик к фильтру AntiDDoS. Соответственно, AntiDDoS в автоматическом режиме распознает и отфильтровывает DDoS-атаку, а также при необходимости направляет трафик на дополнительную фильтрацию в специализированный сектор (структура представлена на рисунке 9). Таким образом, конечный (отфильтрованный) сетевой трафик попадает в клиентский сектор (атакуемые физические серверы).

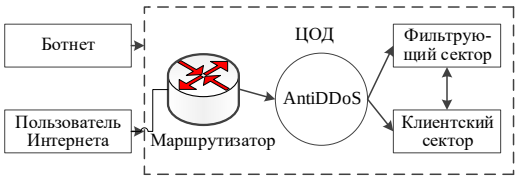

Рис. 8. Структура решений операторов связи по защите от DDoS-атак

Fig. 8. A solution structure of telecom operators for protection against DDoS attacks

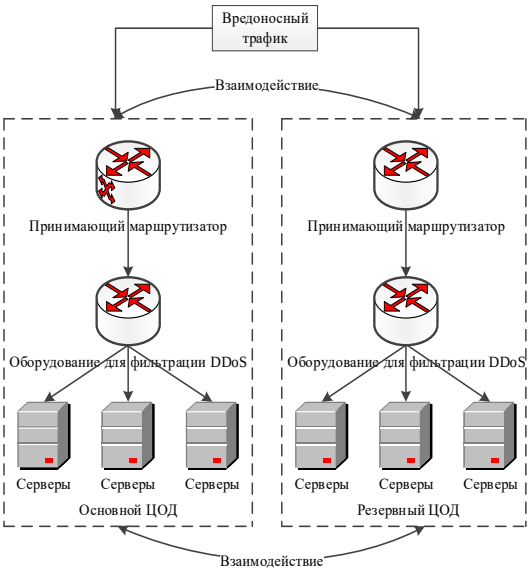

Рис. 9. Структура фильтрующего сектора

Fig. 9. A filter sector structure

Если AntiDDoS направляет сетевой трафик на дополнительную фильтрацию в специализированный сектор, то изначально все действия происходят в основном ЦОД: принимающий трафик маршрутизатор (основной) в автоматическом режиме перенаправляет его на специализированное оборудование по защите от DDoS-атак (например, Arbor APS).

Основные преимущества операторских решений по DDoS-атакам:

– независимость (если у оператора неарендованные каналы, то возможно их полное использование для защиты от DDoS-атак; например, если канал арендован у вышестоящего оператора связи, то при массивной DDoS-атаке арендодатель может временно приостановить предоставление данной услуги в рамках договора);

– эффективность обнаружения и нейтрализации низкоактивных атак внешним несанкционированным трафиком;

– возможность обработки большого количества сетевых пакетов (до 500 миллионов в секунду).

В качестве основных недостатков операторских решений по DDoS-атакам необходимо отметить:

– дорогое оборудование (как правило, малый и средний бизнес не могут позволить себе такой способ защиты от DDoS-атак по финансовым соображениям);

– неэффективность при массивных атаках внешним несанкционированным трафиком (как правило, операторские решения по нейтрализации DDoS имеют не слишком большую емкость сетевого канала; на сегодняшний день уже фиксировались атаки со скоростью больше 1 Тбит/сек. (например, DDoS-атака на веб-сервис GitHub), а средняя емкость DDoS возрастает с каждым днем);

– невозможность распределения сетевой нагрузки на физических серверах клиентов по ядрам (в случае, если DDoS-атака достигнет ЭВМ, то высока вероятность отказа в удаленном обслуживании из-за перегруженности сетевого канала и процессорных ресурсов);

– ручное редактирование правил фильтрации (в случае нового вида DDoS-атаки системному администратору придется вручную конфигурировать защиту от атак внешним несанкционированным трафиком для нейтрализации данной киберугрозы).

Таким образом, защита от атак внешним несанкционированным трафиком на уровне операторов связи является дорогостоящим решением, которое эффективно при низкоактивных DDoS-атаках.

Приведенные аналогичные методы защиты от атак внешним несанкционированным трафиком, несмотря на дорогостоящее оборудование, достаточно широко используются и сегодня по следующим причинам:

– простота в реализации и доступность (например, в стандартных межсетевых экранах

операционных систем достаточно легко внедрить правило фильтрации трафика);

– наличие необходимого базового функционала для отражения низкоактивных DDoS-атак.

Существенными минусами приведенных аналогичных решений являются невозможность равномерного распределения сетевой нагрузки по атакуемым физическим серверам и автоматическое обнаружение новых типов DDoS-атак. Решение данных проблем позволит не только снизить загруженность ресурсов ЭВМ, одновременно повышая ее общую производительность и позволяя запускать ресурсоемкие процессы для решения каких-либо задач, но и повысить доступность информации, что положительно скажется на работоспособности каждого физического сервера в кластере. Таким образом, разработка новых способов защиты от атак внешним несанкционированным трафиком является сегодня важной задачей.

Разработка импульсной нейронной сети для защиты от DDoS-атак и равномерного распределения сетевой нагрузки

Спайковая нейронная сеть представляет собой *искусственную нейронную сеть* (ИНС) третьего поколения, основное отличие которой от скоростных/частотных и бинарных ИНС заключается в обмене нейронами короткими импульсами одинаковой амплитуды. Разработка способа защиты от DDoS-атак на основе *импульсной нейронной сети* (ИмНС) обусловлена тем, что она является динамичной, многозадачной, высокоскоростной и быстрообучаемой. Это позволит не только анализировать, обнаруживать и нейтрализовывать DDoS-атаки, но и равномерно распределять сетевую нагрузку по физическим и логическим ядрам процессора каждого физического сервера в кластере, что дает преимущество в производительности всей системы. Общая структура ИмНС показана на рисунке 10. Структура разработанной спайковой нейронной сети для защиты от атак внешним несанкционированным трафиком и его распределением по ресурсам каждого сервера в кластере представлена на рисунке 11.

Изначально (рис. 11) данные считываются с внешнего сетевого интерфейса каждого физического сервера в кластере (при этом нейроны генерируются в зависимости от свободных ресурсов на кластере). Далее в автоматическом режиме происходит кодирование

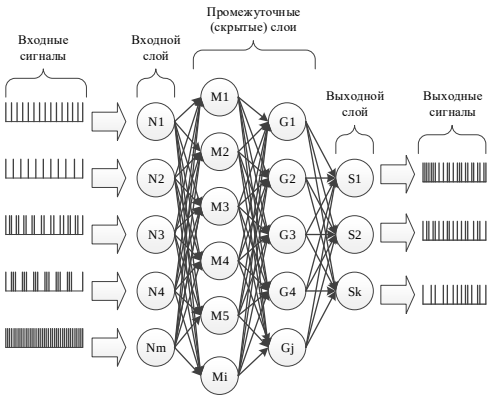

Рис. 10. Структура спайковой нейронной сети

Fig. 10. A spiking neural network structure

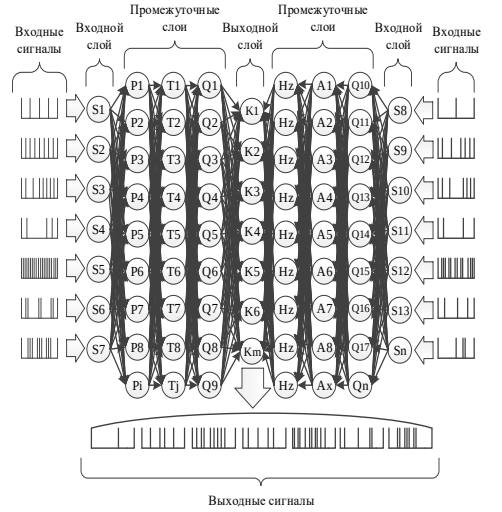

Рис. 11. Структура разработанной ИмНС

Fig. 11. The structure developed by a spiking neural network

информации (для ее последующего представления в ИмНС), полученной с внешнего сетевого интерфейса методом порядка следования импульсов (рис. 12): от расположения того или иного спайка (после преобразования и генерации) зависят скорость передачи данных и их обработка нейронной сетью. После кодирования информации спайковая ИНС в автоматическом режиме самообучается для выполнения следующих задач:

– анализ, распознавание и нейтрализация DDoS-атак с последующей записью атак и полученных правил фильтрации сетевого трафика в БД;

– распределение сетевой нагрузки по вычислительным ресурсам каждого физического сервера в кластере.

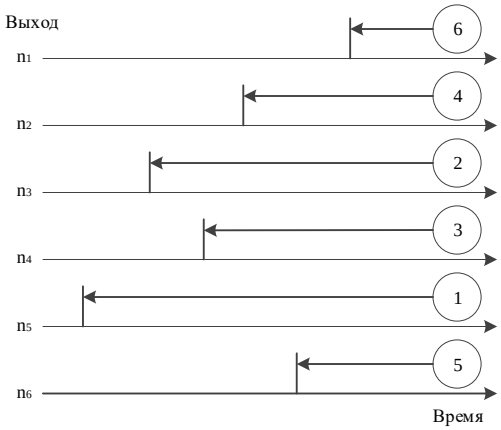

Рис. 12. Порядковый способ представления информации в разработанной ИмНС

Fig. 12. The ordinal way of presenting information in the developed by a spiking neural network

В конечном итоге на выходе получаем преобразованное правило фильтрации для защиты доступности информации всего вычислительного кластера.

Структура нейрона. Для защиты от атак внешним несанкционированным трафиком в ИмНС за основу берется модель ФитцХью–Нагумо [15, 16], измененная авторами статьи. Отличие от оригинальной модели состоит в том, что добавлена возможность реагирования каждого *i*-го и *j*-го нейронов на внешние воздействия (в данном случае – на изменение видов и типов DDoS-атак). Структура нейрона представлена на рисунке 13 (*k*1 – коэффициент реагирования на тип и вид атаки в диапазоне от 0 до 1).

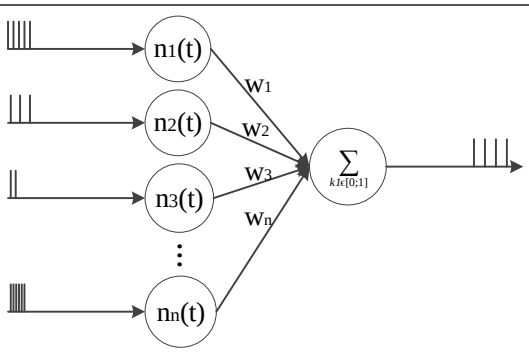

Рис. 13. Структура нейрона в разработанной ИмНС

Fig. 13. The neuron structure in the developed spiking neural network

Данная модель нейрона описывается следующей системой уравнений:

$$\begin{cases} \nu = \dfrac{\alpha}{2} + I_{ext}, \\ \tau \dfrac{dw}{dt} = \nu + k1 + \alpha, \end{cases} \quad (1)$$

где α – потенциал нейрона; I_{ext} – коэффициент внешнего стимула (воздействия); w – восстановление входного тока; ν – динамика мембранного потенциала; t – время угасания сигнала импульса.

Таким образом, реагирование на изменение вида и типа DDoS-атак (табл. 1) позволяет в кратчайшие сроки обнаружить их, проанализировать и нейтрализовать. Соответственно, после обнаружения неизвестного типа DDoS-атаки происходит ее нейтрализация в виде выработки специализированных правил фильтрации трафика с последующим занесением данной атаки в БД и присвоением ей коэффициента реагирования.

Таблица 1

Обозначения коэффициента реагирования *k*1

Table 1

***k*1 response rate designations**

Тип DDoS-атаки	Коэффициент
UDP-флуд	0,001
DNS-усиление	0,002
HTTP-флуд	0,003
Все виды ICMP-флуда	0,004–0,120
MAC-флуд	0,121
SYN-флуд	0,122
NTP-усиление	0,123
TCP-флуд (Reset)	0,124
Source-флуд	0,125
VoIP-флуд	0,126
Неизвестные типы DDoS-атак	0,127–0,999

Разработка метода самообучения ИмНС для защиты от DDoS-атак и равномерного распределения сетевой нагрузки по вычислительным ресурсам кластера. Данный метод самообучения ИмНС позволит в кратчайшие сроки нейтрализовать атаки внешним несанкционированным трафиком, а также равномерно распределить сетевую нагрузку по ресурсам кластера как во время DDoS-атак, так и в обычном режиме. Структура самообучения спайковой нейронной сети представлена на рисунке 14 и состоит из пяти этапов.

Первый этап: прием данных с входного слоя. Необходимо отметить, что данные принимаются в импульсах, поэтому нейрон генерирует их в том случае, когда его внутреннее состояние (потенциал) пересекает предел α (от 0 до 1). Таким образом, соотношение между

Рис. 14. Поэтапное обучение спайковой нейронной сети для защиты от DDoS-атак

Fig. 14. Step-by-step training of a spiking neural network to protect against DDoS attacks

полученными импульсами и изменением потенциала нейрона будет следующим:

$$x_n(t) = \sum_{i=0} \sum_{j=1} \sum_{k=1} b_{ij}^k \cdot s_{ij}^k(t), \quad (2)$$

где i и j – нейрон каждого слоя; k – состояние синапса при возбуждении нейрона; b_{ij}^k – вес каждого синапса при взаимодействии между нейронами i и j; $s_{ij}^k(t)$ – количество импульсов при отправке информации от i-го нейрона к j-му:

$$s_{ij}^k(t) = \eta \cdot (t_i - t_j), \quad (3)$$

где t_i и t_j – время генерации импульса нейронами i и j; η – импульсный ответ (функция, рис. 15):

$$\eta(t) = \frac{t_j}{t_j} \cdot \sigma^{1-\frac{t_i}{t_j}}, \quad (4)$$

где t_i и $t_j > 0$; σ – определяемое автоматически время угасания спайка (импульса).

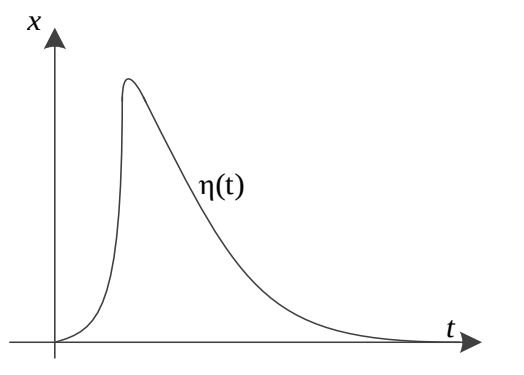

Рис. 15. Функция ответа импульсов

Fig. 15.A pulse response function

Также для следующих этапов самообучения спайковой нейронной сети учитывается условие: если у нейрона потенциал входит в предел α (от 0 до 1), то он подвергается дальнейшему обучению и принимает ровно столько импульсов для обработки, сколько позволяют выделенные ресурсы. Ресурсы под каждый нейрон рассчитываются по формуле

$$L = \sum_{R=1}^{P1} \frac{R}{N1}, \quad (5)$$

где L – выделяемые под нейрон ресурсы; R – свободные ресурсы кластера; $N1$ – количество нейронов в промежуточных слоях. Количество скрытых слоев определяется следующим образом:

$$P1 = M1 - (V1 - Q1), \quad (6)$$

где $M1$ – общее количество слоев в нейронной сети; $V1$ – входной слой; $Q1$ – выходной слой.

Второй этап: равномерное распределение импульсов по нейронам. В разработанной ИмНС для ускоренного обучения у каждого нейрона генерируется определенное количество входов, зависящее от размера входных данных:

$$A_{ij}(t) = \left(\sum_{i=1} \sum_{j=1} \sum_{N1 \in P1}^{M1} \frac{L}{\vartheta \cdot (b_{ij}^k \cdot ((t_i) - (t_j)))} - 1 \right) - \int_R \frac{\partial \sigma}{\partial \vartheta} \cdot s_{ij}^k(t), \quad (7)$$

где ϑ – размер входных данных (измеряется автоматически и записывается на входном слое нейронной сети). Таким образом, распределение импульсов в промежуточных слоях нейронов происходит следующим образом:

$$Z_{ij}(t) = A_{ij}(t) \cdot \left(\sum_{N1 \in P1}^{M1} \frac{L - (t_i \cdot t_j)}{1 - s_{ij}^k(t)} \right). \quad (8)$$

Третий этап: равномерное распределение промежуточных слоев спайковой нейронной сети по свободным ресурсам кластера для повышения скорости обучения:

$$W1 = R \cdot \frac{P1}{(C1 \cdot R1 \cdot S1)}, \quad (9)$$

где $C1$ – количество физических и логических ядер в кластере; $R1$ – размер оперативной памяти в кластере; $S1$ – нагрузочная способность SSD, объединенных в RAID 10.

Четвертый этап: понижение информационной энтропии. Необходимо отметить, что зачастую данный этап обучения в ИмНС используется в обучении с подкреплением. Но в разработанной ИмНС для защиты от DDoS-атак и равномерного распределения сетевой нагрузки

именно спайки запускают самообучение: изменяются веса в сенсорных каналах нейрона. Соответственно, вес нейрона изменяется следующим образом:

$$\frac{dt_i}{dt_j} = \lambda \cdot A_{ij}(t) \cdot (V1 + Q1), \quad (10)$$

$$H1 = \frac{d\sigma}{d\vartheta} + \left(\sum_{k=1} \sum_{i=1} \sum_{j=1} \sum_{N1 \in P1} \frac{\lambda \cdot \left(Z_{ij}(t) \cdot \int_{k}^{A_{ij}(t)} \frac{d\sigma}{d\vartheta} \right)}{V1 + Q1} \right), \quad (11)$$

где λ – коэффициент скорости обучения.

Таким образом, решение уравнения для функции $A_{ij}(t)$

$$H2 \frac{d\sigma}{d(t_i \cdot t_j)} = A_{ij}(t) + \vartheta \quad (12)$$

является сверткой градиента информационной энтропии с фильтром e^{-t_i/t_j}:

$$H2 = \frac{1}{\lambda} e^{-t_i/t_j}. \quad (13)$$

Итак, при разработанной структуре спайковой нейронной сети (рис. 11) вес каждого синапса изменяется в зависимости от прихода/ухода импульса от одного нейрона к другому. Как следствие – правила фильтрации вредоносного трафика генерируются быстрее, но с разной частотой.

Пятый этап: подача данных на выходной слой. Необходимо отметить, что преобразование импульсов в правило для фильтрации DDoS-атак происходит после получения данных на выходном слое. Таким образом, после финальной (понижение информационной энтропии) стадии самообучения ИмНС импульсы отправляются на выходной слой:

$$V1_j^i = \sum_{i=1}^{\lambda} \sum_{j=1}^{\lambda} N1 \cdot s_{ij}^k(t). \quad (14)$$

Сравнение и апробация

Для выявления эффективности предлагаемого авторами статьи решения по защите от DDoS-атак был проведен анализ функционала и возможностей аналогичных программных продуктов, результаты которого представлены в таблице 2.

Таким образом, исходя из результатов анализа (табл. 2), необходимо отметить, что ИмНС для защиты от DDoS-атак не только более оптимизирована под высокие нагрузки и способна обрабатывать большие объемы данных, но и в автоматическом режиме обнаруживает новые виды и типы атак внешним несанкционированным трафиком с их дальнейшей нейтрализацией.

Далее в рамках реализации защиты от DDoS-атак была произведена апробация разработанной ИмНС в режиме простоя – без DDoS (табл. 3) и при массивных атаках внешним несанкционированным трафиком (табл. 4).

Таблица 2

Сравнение функциональных возможностей с аналогами

Table 2

Comparing functionality with analogues

Общий функционал и возможности	**ИмНС авторов статьи**	**Примеры работ [8–14]**	**Стандартные файрволы**	**Решения DPI (Deep Packet Inspection)**
Работа с большими объемами данных	Да	Нет	Нет	Да
Скоростное обучение	Да	Нет	Нет	Нет
Реагирование на внешние ситуации	Да	Нет	Нет	Да
Равномерное распределение сетевой нагрузки	Да	Нет	Нет	Нет
Возможность автоматического выявления новых видов DDoS	Да	Нет	Нет	Нет
Высокое время реагирования (до 20 сек.)	Да	Нет	Нет	Нет
Повышение задержки	Нет	Да	Да	Да
Сохранение новых видов атак в БД	Да	Нет	Нет	Нет
Подробный анализ сетевых пакетов	Да	Нет	Нет	Да
Большое потребление физических ресурсов при DDoS-атаках	Нет	Да	Да	Да

Таблица 3

Потребление ресурсов в режиме простоя

Table 3

Idle resource consumption

Ситуация	День									
	1	2	3	4	5	6	7	8	9	10
	Количество входящего трафика, Гбит/сек.									
	1,0	1,2	1,8	2,0	2,5	2,6	2,7	2,8	2,9	3,5
	Нагрузка на центральный процессор, %									
Старт	0,1	0,1	0,1	0,1	0,1	0,1	0,2	0,2	0,2	0,3
Перезагрузка	0,2	0,3	0,2	0,1	0,2	0,2	0,3	0,3	0,3	0,4
Анализ трафика	0,4	0,4	0,5	0,5	0,5	0,6	0,7	0,7	0,8	0,9
	Загруженность SSD, %									
Старт	0,1									
Перезагрузка	0,1	0,2	0,2	0,3	0,3	0,4	0,5	0,6	0,7	0,8
Анализ трафика	0,3	0,4	0,6	0,7	0,8	1,0	1,1	1,2	1,4	1,5
	Потребление ОЗУ, %									
Старт	0,1									
Перезагрузка	0,2	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1,0
Анализ трафика	0,5	0,6	0,7	0,8	0,9	1,0	1,1	1,2	1,3	1,4

Таблица 4

Потребление ресурсов в режиме защиты от DDoS-атак

Table 4

Resource consumption in the DDoS protection mode

Ситуация	День									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
	Емкость DDoS-атаки, Гбит/сек.									
	2,3	3,5	4,0	4,4	4,8	5,8	6,4	7,9	8,3	9,9
	Количество сетевых пакетов, млн шт./сек.									
	0,5	1,0	1,5	2,0	2,5	3,0	4,5	7,0	9,5	9,9
	Нагрузка на центральный процессор, %									
Старт	3,1	4,2	4,6	4,9	5,6	6,0	7,5	8,0	9,0	9,3
Перезагрузка	4,1	4,8	5,2	6,3	7,0	7,5	8,7	9,0	9,5	9,7
Анализ трафика	5,2	5,6	6,0	6,5	7,3	8,2	8,6	8,9	9,3	9,9
	Загруженность SSD, %									
Старт	1,1	1,2	1,3	1,4	1,5	1,6	1,7	1,8	1,9	2,3
Перезагрузка	2,0	3,2	4,1	4,3	4,8	5,0	5,5	6,0	6,7	7,5
Анализ трафика	2,4	3,0	3,5	4,0	4,7	5,6	7,0	8,2	8,6	9,3
	Потребление ОЗУ, %									
Старт	0,8	0,9	1,3	1,5	1,9	2,3	2,8	3,0	3,2	3,7
Перезагрузка	1,3	1,6	1,9	2,5	2,9	3,8	4,0	5,1	5,7	5,9
Анализ трафика	1,7	1,9	2,3	2,7	3,6	4,0	4,5	5,2	5,7	6,4

На основе данных таблиц 3 и 4 определим среднюю загруженность ресурсов кластера (табл. 5).

Таким образом, повышалась загруженность ресурсов в режиме защиты от DDoS-атак:

- центральный процессор в 23 раза;
- SSD в 10 раз;
- оперативная память в 6,2 раза.

Нагрузка на ресурсы всех физических серверов кластера достаточно низкая, несмотря на массивные DDoS-атаки. Данный эффект достигается за счет равномерного распределения сетевой нагрузки по физическим и логическим ядрам каждого сервера в кластере. Все физические серверы во время атак внешним несанкционированным трафиком были доступны по внешней глобальной сети и работали без перебоев за счет быстрого обучения, реагирования и ликвидации атак типа DDoS разработанной ИмНС.

Таблица 5

Средняя нагрузка на ресурсы вычислительного кластера, %

Table 5

The average load on computing cluster resources, %

Ресурс	Режим простоя	Режим защиты от DDoS-атак	Разница, раз
Центральный процессор	0,3	6,9	23,0
Твердотельный накопитель	0,4	4,0	10,0
Оперативная память	0,5	3,1	6,2

Тестирование проводилось на следующем оборудовании:

– количество физических серверов – 30;

– процессор Intel Xeon 5690 (CPU – 60, физических ядер – 360, потоков – 720);

– оперативная память – 960 Гб;

– SSD – RAID 10 (Samsung 850 pro 1 Тб каждый);

– внешний сетевой канал – 20 Гбит/сек.;

– внутренний сетевой канал (локальная сеть) – 100 Гбит/сек.

Данный кластер соответствует современным требованиям и позволяет обрабатывать большие объемы данных.

Интерфейс разработанного ПО

Стоит отметить, что данная нейронная сеть является частью управляемого через веб-интерфейс аппаратно-программного комплекса Protection и функционирует в следующих разделах панели управления: «Основная статистика» (см. http://www.swsys.ru/uploaded/image/2019-4/2019-4-dop/6.jpg), «Управление и нагрузка АПК» (см. http://www.swsys.ru/uploaded/image/2019-4/2019-4-dop/7.jpg) и «DDoS на картах» (см. http://www.swsys.ru/uploaded/image/2019-4/2019-4-dop/8.jpg).

Реализация веб-интерфейса для управления аппаратно-программным комплексом (и нейронной сетью соответственно) обусловлена возможностью постоянного доступа с любой точки, в которой есть доступ к внешней глобальной сети. Управление может происходить как с мобильного устройства (у веб-части адаптивный дизайн), так и с компьютера.

Таким образом, быстрый доступ к панели управления позволяет не только следить за состоянием физических серверов кластера и управлять аппаратно-программным комплексом (и нейронной сетью соответственно), но и нейтрализовывать некоторые виды DDoS-атак вручную и в кратчайшие сроки.

Заключение

В ходе проведенных исследований были получены следующие результаты.

Предложен метод обучения ИмНС, позволяющий реализовать структуру самообучения (без учителя) ИНС на программном уровне. Данные берутся с внешнего сетевого интерфейса (ip-адреса, сетевые пакеты, загруженность сетевого канала) и преобразуются в спайки (импульсы) на входном слое. После самообучения спайки передаются на выходной слой и преобразуются в правила фильтрации с последующим сохранением в БД.

Разработана ИмНС для отражения атак внешним несанкционированным трафиком, основными преимуществами которой являются быстрое самообучение (в случае нового вида DDoS-атаки обучение без учителя может достигать 20 сек.) и скорость реагирования (срабатывания) во время DDoS.

Проведено множество тестирований, доказывающих целесообразность использования разработанной спайковой нейронной сети. Средняя нагрузка на центральный процессор варьируется от 0,3 до 6,9 %. Достаточно низкая загруженность CPU позволяет запускать многочисленные ресурсоемкие процессы как во время DDoS-атак, так и в режиме простоя без каких-либо потерь производительности. Средняя загруженность SSD-накопителей, объединенных в массив RAID-10 (1+0), колеблется от 0,4 до 4,0 %. Столь небольшая нагрузка на твердотельный накопитель позволяет использовать SSD другими ресурсоемкими процессами. Среднее потребление ресурсов оперативной памяти варьируется в диапазоне 0,5–3,1 %. Небольшое потребление ресурсов ОЗУ также говорит о целесообразности использования разработанной ИмНС для защиты от DDoS-атак. Таким образом, низкая нагрузка на вычислительные ресурсы позволяет не только в кратчайшие сроки защитить каждую ЭВМ кластера от атак внешним несанкционированным трафиком, но и повысить их доступность наряду с производительностью, а также равномерно распределить сетевую нагрузку по физическим и логическим ядрам каждого процессора во всех серверах вычислительного кластера.

Литература

1. Пальчевский Е.В., Халиков А.Р. Автоматизированная система защиты доступности информации от атак внешним несанкционированным трафиком в UNIX-подобных системах // Программные продукты и системы. 2018. Т. 31. № 3. С. 548–556. DOI: 10.15827/0236-235X.123.548-556.
2. Пальчевский Е.В., Халиков А.Р., Христодуло О.И. Разработка системы защиты от DDoS-атак на основе картографических данных // Инновации в науке и практике: сб. матер. IV Междунар. науч.-практич. конф. Барнаул, 2017. С. 34–39.
3. Воробьева Ю.Н., Катасева Д.В., Катасев А.С., Кирпичников А.П. Нейросетевая модель выявления DDoS-атак // Вестн. технолог. ун-та. 2018. Т. 21. № 2. С. 94–98.
4. Краснов А.Е., Надеждин Е.Н., Никольский Д.Н., Репин Д.С., Галяев В.С. Детектирование DDoS-атак на основе анализа динамики и взаимосвязи характеристик сетевого трафика // Вестн. УдГУ: Математика. Механика. Компьютерные науки. 2018. Т. 28. № 3. С. 407–418.
5. Тарасов Я.В. К вопросу противодействия целенаправленным компьютерным атакам // Защита информации. Инсайд. 2018. № 4. С. 48–53.
6. Кляус Т.К., Наумов А.Д., Гатчин Ю.А., Бондаренко И.Б. Сравнительное исследование применимости деревьев атак-контрмер и метода куста событий для оценки безопасности информационных систем // Вестн. РФО: Безопасность в информационной сфере. 2018. № 2. С. 36–42.
7. Чинаев В.Ю. Преимущества применения технологии блокчейна в информационной безопасности промышленных предприятий // Экономические аспекты технологического развития современной промышленности: сб. матер. Междунар. науч.-практич. конф. М., 2018. С. 240–242.
8. Aleesa A.M., Hassan R. A proposed technique to detect DDoS attack on IPv6 web applications. Proc. 4th Intern. Conf., 2016, pp. 118–121. DOI: 10.1109/PDGC.2016.7913127.
9. Zheng W. An elastic and resiliency defense against DDoS attacks on the critical DNS authoritative infrastructure. J. of Computer and System Sciences, 2019, vol. 99, pp. 1–26. DOI: 10.1016/j.jcss.2017.05.012
10. Kshira S.S., Deepak P., Mayank T., Joel R., Bibhudatta S., Ratnakar D. An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. Future Generation Computer Systems, 2018, vol. 89, pp. 685–697.
11. Barış K., Çağatay Y., Taha Y.C., Bülent S., Ali T.C. A Bayesian change point model for detecting SIP-based DDoS attacks. Digital Signal Processing, 2018, vol. 77, pp. 48–62. DOI: 10.1016/j.dsp.2017.10.009.
12. Murat S., Ali T.C., Bülent S. An intelligent cyber security system against DDoS attacks in SIP networks. Computer Networks, 2018, vol. 136, pp. 137–154. DOI: 10.1016/j.comnet.2018.02.025.
13. Behal S., Krishan K., Sachdeva M. D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events. J. of NCA, 2018, vol. 111, pp. 49–63. DOI: 10.1016/j.jnca.2018.03.024.
14. Saied A., Overill R., Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing, 2016, vol. 172, pp. 385–393.
15. FitzHugh R. Impulses and physiological states in theoretical models of nerve membrane. Biophys. J., 1961, vol. 1, pp. 446–466.
16. Nagumo J., Arimoto S., Yoshizawa S. An active pulse transmission line simulating nerve axon. Proc. IRE, 1962, vol. 50, iss. 10, pp. 2061–2070. DOI: 10.1109/JRPROC.1962.288235.

Software & Systems Received 29.04.19
DOI: 10.15827/0236-235X.128.613-627 2019, vol. 32, no. 4, pp. 613–627

Development of a spiking neural network with the possibility of high-speed training to neutralize DDoS attacks

E.V. Palchevsky [1], *Postgraduate Student, teelxp@inbox.ru*
O.I. Hristodulo [1], *Dr.Sc. (Engineering), Professor, o-hristodulo@mail.ru*

[1] *Ufa State Aviation Technical University, Ufa, 450008, Russian Federation*

Abstract. Effective data accessibility is one of the key challenges in information security. Often DDoS attacks violate information availability. The imperfection of modern protection methods against attacks by external unauthorized traffic leads to the fact that many companies with Internet access are faced with the inaccessibility of their own services that provide various services or information. This results in company financial losses from equipment downtime. To solve this problem, the authors have developed a spiking neural network to protect against attacks by external unauthorized traffic.

The main advantages of the developed spiking neural network are high self-learning speed and quick response to DDoS attacks (including unknown ones). A new method of a spiking neural network self-training is based on uniform processing of spikes by each neuron. Due to this fact, the neural network is trained in the shortest possible

time, therefore it quickly and efficiently filters attacks with external unauthorized traffic. The paper also compares the developed spiking neural network with similar solutions for protecting against DDoS attacks. As a result, it reveales that the developed neural network is more optimized for high loads and is able to detect and neutralize DDoS attacks as soon as possible.

The developed spiking neural network was tested in idle conditions and in protection against DDoS attacks. Load values were obtained on the resources of the computing cluster. Long-term testing of a pulsed neural network shows a rather low load on the central processor, RAM and solid state drive during massive DDoS attacks. Thus, the optimal load not only increases the availability of each physical server, but also provides the ability to simultaneously run resource-intensive computing processes without any disruption to the functioning of the working environment.

Testing was carried out on computing cluster servers, where a spiking neural network showed stable operation and effectively protected from DDoS attacks.

Keywords: information, data transfer, networks, spiking neural network, neural network self-training, DDoS attacks, malicious traffic, information security.

References

1. Palchevsky E.V., Khalikov A.R. An automated system of information accessibility protecting from attacks by unauthorized traffic in UNIX-like systems. *Software & Systems*. 2018, vol. 31, no. 3, pp. 548–556. DOI: 10.15827/0236-235X.123.548-556 (in Russ.).

2. Palchevsky E.V., Khalikov A.R., Khristodulo O.I. Development of DDoS protection system based on map data. *Proc. 4th Intern. Sci. and Pract. Conf. Innovations in Science and Practice*. Barnaul, Dendra, 2017, pp. 34–39 (in Russ.).

3. Vorobeva Yu.N., Kataseva D.V., Katasev A.S., Kirpichnikov A.P. Neural network model to detect DDoS attacks. *Bulletin of Technological Univ*. 2018, vol. 21, no. 2, pp. 94–98 (in Russ.).

4. Krasnov A.E., Nadezhdin E.N., Nikolsky D.N., Repin D.S., Galyaev V.S. Detection of DDoS attacks based on analysis of dynamics and interconnection of network traffic characteristics. *Bulletin of the Udmurt Univ. Mathematics. Mechanics. Computer Science*. 2018, vol. 28, no. 3, pp. 407–418 (in Russ.).

5. Tarasov Ya.V. On the issue of countering targeted computer attacks. *Information Protection. Inside*. 2018, no. 4, pp. 48–53 (in Russ.).

6. Klyaus T.K., Naumov A.D., Gatchin Yu.A., Bondarenko I.B. A comparative study of the applicability of attack-countermeasures trees and the event Bush method to assess the security of information systems. *UrFR Newsletter. Information Security*. 2018, no. 2, pp. 36–42 (in Russ.).

7. Chinaev V.Yu. The advantages of using the technology of the blockchain in the information security industry. *Proc. Intern. Sci. and Pract. Conf. Economic Aspects of Technological Development of Modern Industry*. Moscow, Moscow Polytechnic Univ. Publ., 2018, pp. 240–242 (in Russ.).

8. Aleesa A.M., Hassan R. A proposed technique to detect DDoS attack on IPv6 web applications. *Proc. 4th Intern. Conf. on Parallel, Distributed and Grid Computing*. Solan, 2016, pp. 118–121. DOI: 10.1109/PDGC.2016.7913127.

9. Zheng W. An elastic and resiliency defense against DDoS attacks on the critical DNS authoritative infrastructure. *J. of Computer and System Sciences*. 2019, vol. 99, pp. 1–26. DOI: 10.1016/j.jcss.2017.05.012.

10. Kshira S.S., Deepak P., Mayank T., Joel R., Bibhudatta S., Ratnakar D. An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. *Future Generation Computer Systems*. 2018, vol. 89, pp. 685–697.

11. Barış K., Çağatay Y., Taha Y.C., Bülent S., Ali T.C. A Bayesian change point model for detecting SIP-based DDoS attacks. *Digital Signal Processing*. 2018, vol. 77, pp. 48–62. DOI: 10.1016/j.dsp.2017.10.009.

12. Murat S., Ali T.C., Bülent S. An intelligent cyber security system against DDoS attacks in SIP networks. *Computer Networks*. 2018, vol. 136, pp. 137–154. DOI: 10.1016/j.comnet.2018.02.025.

13. Behal S., Krishan K., Sachdeva M. D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events. *J. of Network and Computer Applications*. 2018, vol. 111, pp. 49–63. DOI: 10.1016/j.jnca.2018.03.024.

14. Saied A., Overill R., Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing*. 2016, vol. 172, pp. 385–393.

15. FitzHugh R. Impulses and physiological states in theoretical models of nerve membrane. *Biophysical J*. 1961, vol. 1, pp. 446–466.

16. Nagumo J., Arimoto S., Yoshizawa S. An active pulse transmission line simulating nerve axon. *Proc. IRE*. 1962, vol. 50, iss. 10, pp. 2061–2070. DOI: 10.1109/JRPROC.1962.288235.

Для цитирования

Пальчевский Е.В., Христодуло О.И. Разработка импульсной нейронной сети с возможностью скоростного обучения для нейтрализации DDoS-атак // Программные продукты и системы. 2019. Т. 32. № 4. С. 613–627. DOI: 10.15827/0236-235X.128.613-627.

For citation

Palchevsky E.V., Hristodulo O.I. Development of a spiking neural network with the possibility of high-speed training to neutralize DDoS attacks. *Software & Systems*. 2019, vol. 32, no. 4, pp. 613–627 (in Russ.). DOI: 10.15827/0236-235X.128.613-627.