УДК 621.392

АНАЛИЗ РЕЗУЛЬТАТОВ ИСПЫТАНИЙ ДЕЙСТВУЮЩЕЙ СЕТИ НОВОГО ПОКОЛЕНИЯ (NGN) НА УЯЗВИМОСТЬ К АТАКАМ DoS

В.А. Матвеев[1], **А.М. Морозов**[2]

[1]МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
e-mail: v.a.matveev@bmstu.ru

[2]Региональный центр управления сетями связи Московского филиала ОАО "Ростелеком", Московская область, г. Люберцы, Российская Федерация
e-mail: a.m.morozov@gmal.com

Описаны испытания, проведенные в целях получения данных для оценки устойчивости сети связи следующего поколения NGN к некоторым типам атак "отказ в обслуживании" DoS, а также данных, необходимых для выработки мер противодействия таким атакам. Эксперимент проведен на тестовом участке действующей сети NGN. Полученные результаты имеют высокую практическую ценность. Приведен краткий анализ особенностей сети связи следующего поколения NGN с точки зрения информационной безопасности и рассмотрена специфика атак DoS на сеть NGN, являющаяся следствием названных особенностей. Определены условия, необходимые для реализации раннего обнаружения атак на сеть NGN. Приведена общая классификация атак "отказ в обслуживании" DoS в сетях связи нового поколения NGN. Предложены схемы и сценарии испытаний, в ходе которых имитируются различные типы атак "отказ в обслуживании" на один из элементов сети NGN. Проведен краткий анализ последствий таких атак для сети. В заключение в качестве одного из возможных алгоритмов по раннему обнаружению DoS-атаки рассмотрен алгоритм кумулятивной суммы CUSUM и приведен пример применения названного алгоритма для детектирования DoS-атаки.

Ключевые слова: "отказ в обслуживании", атака, связи нового поколения NGN, передачи голоса по IP-сетям, угроза, коммутируемая сеть связи общего пользования, ТфОП, протокол инициирования сеанса, система сигнализации № 7, программный коммутатор, флуд-атака, атаки "затоплением".

ANALYZING RESULTS OF TESTS OF THE FUNCTIONING NEW GENERATION NETWORK FOR VULNERABILITY TO DOS ATTACKS

V.A. Matveev[1], **A.M. Morozov**[2]

[1]Bauman Moscow State Technical University, Moscow, Russian Federation
e-mail:

[2] Regional Center for Management of Communication Networks of Moscow Branch of OAO "Rostelekom", Moscow region, Russian Federation
e-mail: a.m.morozov@gmal.com

The tests aimed at obtaining the data to assess the stability of the next generation network (NGN) to certain types of denial of service (DoS) attacks, as well as the data needed to develop measures to counter such attacks are described. The experiment has been conducted for a test part of the operating NGN and the results obtained are of great practical value. The NGN features are briefly analyzed from the data security standpoint, and the specificity of DoS attacks on a NGN, which is the consequence of these features, is considered. The conditions necessary for the implementation of early detection of attacks on a NGN are determined. The classification of DoS attacks

is given. The schemes and scenarios of tests are proposed, in which different types of DoS attacks are simulated on one of the NGN elements. Consequences of such attacks for the network are analyzed briefly. The cumulative sum (CUSUM) algorithm is considered as one of the possible algorithms for early detection of a DoS attack, and an example of application of this algorithm for detecting a DoS attack is given.

Keywords: denial of service, attack. new generation network (NGN), voice over IP networks, threat, public switched telephone network, PSTN, session initiation protocol, signaling system No. 7, program switcher, flood attack.

Настоящая работа посвящена анализу угрозы "отказ в обслуживании" DoS (Denial of service) информационной безопасности (ИБ) сети связи нового поколения NGN (new generation network). Такой тип атак относится к одной наиболее часто встречающейся и наиболее критичной по последствиям атаке в сети NGN, опирающейся на технологию передачи голоса по IP-сетям (Voice over IP, VoIP) [1, 2].

Для таких сетей присущи следующие характерные особенности [3], которые определяют специфику угроз DoS:

- использование протоколов нескольких классов — протоколов управления соединением (SIP, протоколы группы SIGTRAN), медиашлюзами (MGCP, MEGACO/H.248), медиапотоками (RTP/RTCP) и протоколов передачи медиаданных;
- распределенная архитектура сети. Это означает, что отдельные элементы сети NGN могут быть разнесены географически, находиться в разных административных доменах сети или быть разделены такими доменами;
- возможность наличия у каждого элемента архитектуры NGN нескольких сетевых интерфейсов к разным по своему назначению и принятым политикам безопасности сетям (такими сетями, как правило, являются сети управления, передачи медиаданных и сообщений сигнализации).

Специфика атак DoS в сетях NGN выражается в следующем:

- атаки DoS на сети NGN приводят к различным негативным последствиям — от снижения качества обслуживания легитимных пользователей до полной потери доступа легитимных пользователей к услугам NGN-сети. Специфично то, что атака DoS в сети NGN может негативно отразиться также на смежные с ней сети (ТфОП, сети мобильных операторов);
- атака на один из действующих протоколов отражается последствиями и для остальных протоколов;
- атака на один из элементов распределенной архитектуры может иметь негативные последствия для участка сети или всей сети;
- атака на один из сетевых интерфейсов элемента сети NGN имеет последствия для всего элемента сети.

С учетом названных особенностей математическая оценка уязвимости сети NGN в целом и степени риска реализации угроз DoS в

частности является достаточно сложной задачей, к решению которой существует несколько подходов, в том числе использование для оценки уязвимости NGN-сети математического аппарата теории нечетких множеств. В работе [4] описывается использование этого аппарата для решения вопросов безопасности беспроводных сетей стандарта IEEE 802.11.

Одной из основных задач противодействия угрозам DoS или минимизации последствий от реализации таких угроз является своевременное обнаружение факта начала атаки. Важными шагами в решении данной задачи являются:

— выбор параметров, наблюдение за которыми позволит получить достоверную и достаточную информацию о текущем уровне угрозы информационной безопасности сети. Такими параметрами могут быть данные об использовании сетевых ресурсов и аппаратных ресурсов элементов сети, данные об интенсивности и характере сигнального обмена и прочее;

— выбор алгоритма анализа данных, который позволит с высокой скоростью и при низком коэффициенте ошибки принять решение о наличии угрозы информационной безопасности.

Одним из наиболее эффективных способов, позволяющим точно оценить уязвимость сети NGN, найти наиболее информативные параметры, отражающие уровень угрозы информационной безопасности, выбрать алгоритм и оценить его эффективность, являются испытания, в ходе которых имитируются атаки на компоненты сети.

Классификация атак DoS в сетях NGN. Существуют различные подходы к классификации атак DoS [1, 5]. По своему характеру атака DoS может быть непреднамеренной (вызванной сбоем в работе оборудования или программного обеспечения, возникшим либо в результате неисправности, либо в результате ошибок в эксплуатации, или сбоями, вызванными просчетами в проектировании сети связи) и преднамеренные. Следует отметить, что в сетях операторов связи именно непреднамеренные атаки DoS являются наиболее частыми, сложно прогнозируемыми, зачастую достаточно сложно локализуемыми. Они могут нанести значительный ущерб. Устранение непреднамеренной угрозы DoS нередко сопряжено с проведением длительного и сложного анализа на этапе локализации источника и определения причин атаки, с необходимостью модернизации или замены программного или аппаратного обеспечения части компонентов сети, длительного тестирования после устранения причин.

По месту воздействия угрозы DoS можно классифицировать следующим образом.

1. Атаки, использующие особенности и уязвимости транспортной сетевой инфраструктуры. К таким особенностям можно отнести выб-

ранную топологию IP-сети, используемые протоколы в IP-сети, пропускную способность IP-сети, эксплуатационные особенности сети и др.

2. Атаки, использующие особенности и уязвимости аппаратного обеспечения и системного программного обеспечения компонентов NGN сети. К таким особенностям и уязвимостям можно отнести различные особенности операционных систем, под управлением которых работают компоненты NGN-сети, объем оперативной памяти, производительность центрального процессора и др.

Компонентами сети NGN являются: медиашлюзы — сетевые элементы, обеспечивающие доступ пользователей к услугам сети VoIP, а также выполняющие функцию сопряжения сетей VoIP и ТфОП; шлюзы сигнализации, обеспечивающие трансляцию управляющих сообщений сигнализации из сети ТфОП в сеть VoIP; программный коммутатор (softswitch), реализующий функции обработки сообщений сигнализации, управления вызовами, управления медиашлюзами.

3. Атаки, использующие специфические уязвимости протоколов, применяемых в сети NGN.

4. Атаки, использующие уязвимости программного обеспечения, реализующего функции обработки вызовов, различные функции по управлению и обслуживанию компонента NGN.

По способу реализации атаки DoS принято классифицировать следующим образом:

— атаки, реализуемые посредством передачи большого числа сообщений сигнализации или медиасообщений (в англоязычной литературе для обозначения данного вида атаки DoS используются термины flood attacks, depletion attacks, brute force attacks); далее в тексте работы эту атаку будем называть флуд-атакой;

— компрометация сигнальных сообщений; такие атаки реализуются в результате ошибочной (вследствие сбоев в программном обеспечении или ошибок в конфигурации) или преднамеренной передачи сигнальных сообщений, препятствующих установлению сеанса связи или преждевременно завершающих сеанс связи. Например, в сети сигнализации SIP [6] такими сообщениями могут быть запросы CANSEL, BUY, а также фиктивные сообщения-ответы об ошибках в ходе установления соединения;

— компрометация полезной нагрузки сигнальных сообщений. Атаки такого типа реализуются в результате передачи в сигнальных сообщениях некорректных или ошибочных данных, необходимых для установления медиасессии. В результате реализации атаки происходит срыв установления медиасессии или возникает ситуация, при которой соединение устанавливается, но обмен данными в рамках этой сессии невозможен или возможен с существенными ограничениями.

Далее приводится описание испытаний по исследованию уязвимости сети NGN отдельно по каналам сигнализации (по протоколу SIP) к атакам DoS (типа флуд-атака).

Анализ испытаний уязвимости к атакам DoS сети NGN по каналам сигнализации. Атака посредством передачи большого числа сообщений протоколов или медиасообщений — наиболее просто реализуемый злоумышленником и часто реализуемый тип атаки. Цель — исчерпать имеющиеся ресурсы объекта атаки. Обработка каждого сигнального сообщения занимает ресурсы системы (процессорное время, оперативную память, полосу пропускания). При одновременном поступлении большого числа сообщений ресурсы системы могут быть исчерпаны, что приведет к сбоям или полной остановке ее работы.

Такая ситуация может возникнуть непреднамеренно, в результате ошибок программного обеспечения или как следствие аварий в IP-сети (например, возврат сервера в работу после вре́менной недоступности может привести к лавинообразному росту запросов на регистрацию, в результате которого может возникнуть атака DoS).

Для оценки устойчивости действующего оборудования к атакам DoS типа флуд-атака на тестовом участке сети одного из операторов связи был проведен ряд тестов, в ходе которых имитировались эти атаки. Тестовый участок приведен на рис. 1. Тестовый участок имеет подключения к сети ТфОП по протоколу общеканальной сигнализации SSN7 и к смежному сегменту сети NGN по протоколу SIP.

На схеме приняты следующие обозначения: ssw1 — программный коммутатор (softswitch) действующего сегмента сети; sswtest — программный коммутатор (softswitch) тестового сегмента сети; smg —

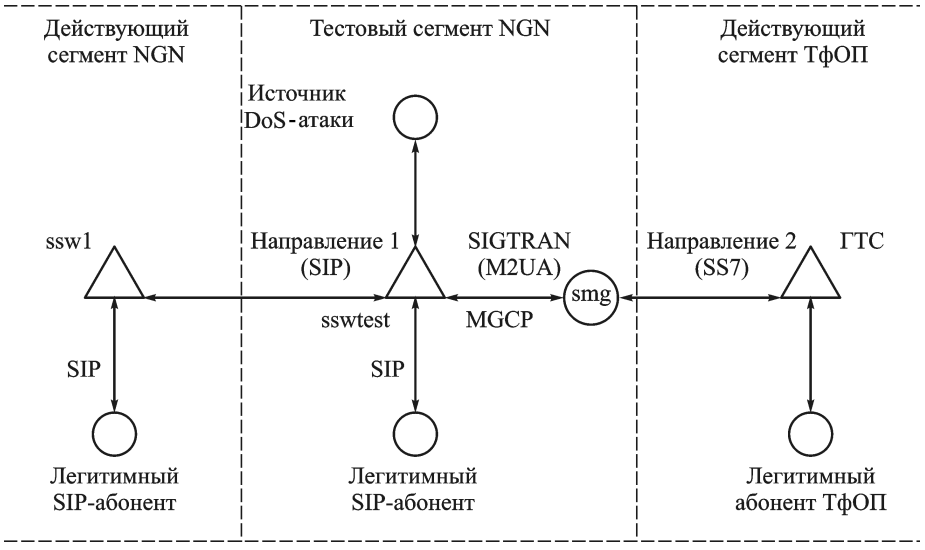

Рис. 1. Схема тестового участка сети NGN при тестировании уязвимости к атакам DoS типа флуд-атака

шлюз сигнализации и медиашлюз (signaling media gateway). ГТС — городская телефонная станция. Источник атаки DoS — терминал SIP с утилитой для генерации большого потока вызовов и медиапотоков (SIPp [7]).

В ходе испытаний исследованы следующие варианты реализации атаки DoS:

1. Инициация большого числа одновременных соединений.

2. Атака посредством передачи большого числа сообщений инициации соединения INVITE.

3. Атака посредством передачи большого числа сообщений REGISTER.

При этом ставились следующие задачи:

— показать с помощью предлагаемого метода тестирования возможность получить реальную картину уязвимости к указанным атакам DoS в действующей сети связи NGN общего пользования по протоколу сигнализации SIP;

— дать рекомендации по раннему обнаружению этих атак в действующей сети связи;

— провести исследование эффективности алгоритма обнаружения DoS-атаки;

— показать необходимость продолжения работ по другим типам атак DoS, приведенным в разделе “Классификация атак DoS в сетях NGN”.

1. Инициация большого числа одновременных соединений. Оборудование операторов связи, как правило, имеет ограничения по числу одновременных соединений. Это может быть продиктовано ограничениями конструктивными (например, числом цифровых потоков E1), административными (конечное число соединительных линий, как правило, определяется межоператорским договором о присоединении сетей) лицензионными (производитель или поставщик аппаратного и программного обеспечения устанавливает ограничение на число одновременных соединений). Административно число одновременных соединений на IP-направлениях может регулироваться, например, ограничением диапазона портов UDP, необходимых для организации медиасессий. Число инициированных вызовов и установленных соединений может превысить существующие ограничения и создать перегрузку на данном направлении, создав атаку DoS. Следует отметить, что вызовы должны быть корректными и завершаться установлением соединения, а также, что при возникновении подобной ситуации в одном из направлений связи другие направления могут оставаться в работе.

Данная ситуация может возникнуть в результате просчетов при проектировании, когда реальная загруженность направления превышает расчетную, в результате вызванных объективными причинами всплесков нагрузки или может быть следствием действий злоумышленника (как правило, это связано с попыткой нелегитимного использования направления связи).

В ходе тестирования имитировались следующие три сценария:

А. Число соединительных линий на направлении 1 (SIP) превышает число соединительных линий на направлении 2 (SS7). Источник атаки DoS от имени программного коммутатора ssw1 инициирует транзитные вызовы в направлении ТфОП через программный коммутатор ssw test. Число одновременных вызовов превышает число соединительных линий в направлении 2, но не превышает числа соединительных линий в направлении 1. В результате атаки направление 2 было перегружено. Легитимным абонентам программных коммутаторов ssw1 и ssw test стали недоступны вызовы в направлении ТфОП, также абонентам ТфОП стали недоступны вызовы в направлении абонентов программных коммутаторов ssw1 и ssw test. При этом сохранилась доступность вызовов между абонентами программных коммутаторов ssw1 и ssw test.

Б. Число соединительных линий на направлении 2 превышает число соединительных линий на направлении 1. Злоумышленник от имени программного коммутатора ssw1 инициирует транзитные вызовы в направлении ТфОП через программный коммутатор ssw test. Число одновременных вызовов превышает число соединительных линий в направлении 1, но не превышает числа соединительных линий в направлении 2. В результате атаки направление 1 было перегружено. Легитимным абонентам программных коммутаторов ssw1 стали недоступны вызовы в направлении ТфОП, также абонентам ТфОП и абонентам программного коммутатора ssw test стали недоступны вызовы в направлении абонентов программного коммутатора ssw1. При этом сохранилась доступность вызовов между абонентами программного коммутатора ssw test и ТфОП.

В. Злоумышленник от имени легитимных абонентов программного коммутатора ssw test инициирует большое число вызовов в направлении абонентов ssw1 и абонентов ТфОП. Число инициированных вызовов в обоих направлениях превышает число соединительных линий в этих направлениях. В результате этой атаки направления 1 и 2 были перегружены. Легитимным абонентам программного коммутатора ssw1 стали недоступны вызовы в направлении ТфОП и в направлении абонентов ssw test, абонентам ТфОП стали недоступны вызовы в направлении абонентов программных коммутаторов ssw1 и ssw test,

абонентам программного коммутатора ssw test стали недоступны вызовы в направлении ТфОП и в направлении абонентов ssw 1.

Во всех трех сценариях реализованная угроза не повлияла на возможность абонентов ssw test выполнять локальные вызовы.

Методика контроля возникновения описанных атак DoS сводится к мониторингу числа активных сессий на направлениях связи. В ходе проведенных испытаний при достижении числа административно установленного предела одновременных вызовов в тестовом направлении связи в сигнальном обмене каждая попытка установить очередной сеанс связи завершалась ответами программного коммутатора *480 Временно недоступен (Temporarily Unavailable)* и *503 Служба недоступна (Service Unavailable.*

2. Атака посредством передачи значительного числа сообщений инициации соединения INVITE. Данная атака DoS имеет ряд отличий от рассмотренной ранее атаки.

Во-первых, целью данной атаки является не перегрузка одного из действующих направлений, а перегрузка аппаратных ресурсов оборудования.

Во-вторых, адресная информация, передаваемая в таких запросах, может быть некорректной.

В-третьих, для реализации данной угрозы требуется генерировать значительно большее число запросов INVITE.

В ходе тестирования реализована атака на программный коммутатор ssw test. Были имитированы следующие сценарии атаки:

— передача большого числа запросов INVITE от имени зарегистрированного легитимного пользователя;

— передача большого числа запросов INVITE от имени программного коммутатора ssw 1;

— передача большого числа запросов INVITE велась с узла, не зарегистрированного на программном коммутаторе ssw test.

Анализ проведенной имитации выявил, что при атаке с не зарегистрированного на программном коммутаторе узла (сценарий 3) и высокой интенсивности атаки (максимальная скорость передачи запросов INVITE составляла 1000 запросов/с) процент загрузки процессора программного коммутатора не превышал 70. . . 80 %. При этом загрузка оперативной памяти была незначительной. Данная атака не отражалась на функционировании программного коммутатора, легитимные пользователи могли инициировать и принимать вызовы беспрепятственно. Факт начала атаки данного типа характеризовался резким ростом числа сообщений *403 Запрещено* (*Forbidden*) и *503 Служба недоступна* (*Service Unavailable*) в сигнальном обмене.

При реализации атаки по сценариям 1 и 2 и при достижении интенсивности передачи сообщений INVITE 400 запросов/с загрузка процессора SIP сервера приближалась к 100 %, объем свободной оперативной памяти приближался к нулю. Данная ситуация приводила к остановке работающих на программном коммутаторе сервисов с последующим рестартом программного коммутатора. В результате абоненты ТфОП не могли осуществлять вызовы абонентов обоих сегментов сети NGN и абоненты обоих сегментов сети NGN не могли осуществлять вызовы абонентов сети ТфОП. Абонентам программного коммутатора ssw test любые сервисы были недоступны.

Факт реализации атаки данного типа характеризовался появлением в сигнальном обмене и резким ростом числа сообщений *480 Временно недоступен* (*Temporarily Unavailable*) и *503 Служба недоступна* (*Service Unavailable*). При реализации данной атаки запросами INVITE, содержащими некорректную адресную информацию в сигнальном обмене, наблюдался резкий рост сообщений *404 Не найдено* (*Not found*).

При выбранном на программном коммутаторе механизме авторизации запросов INVITE в реализации атаки по сценарию 1 появляется вариант, когда в запросах INVITE, реализующих атаку, передается некорректная информация авторизации. В этом случае в сигнальном обмене наблюдается резкий рост числа сообщений *401 Несанкционированный* (*Unauthorized*) и *403 Запрещено* (*Forbidden*).

3. Атака посредством передачи большого числа сообщений REGISTER. Идея данной атаки аналогична атаке посредством передачи большого числа сообщений INVITE — исчерпать ресурсы системы. В ходе имитации атаки flood REGISTER на программный коммутатор ssw test реализованы следующие сценарии атаки:

— передача большого числа запросов REGISTER от имени абонента, отсутствующего в абонентской базе программного коммутатора;

— передача большого числа запросов REGISTER от имени легитимного пользователя (тело запроса содержит корректные регистрационные данные легитимного пользователя).

В результате тестирования выявлено следующее. При реализации атаки по сценарию 1 вне зависимости от интенсивности атаки (предельная скорость передачи запросов REGISTER в ходе испытаний 5000 запросов/с) загрузка процессора программного коммутатора не превышала 40. . . 50 %. Загрузка оперативной памяти была незначительной. Данная атака не отражалась на функционировании программного коммутатора, легитимные пользователи могли инициировать и принимать вызовы беспрепятственно. Факт реализации атаки данного типа характеризовался резким ростом числа сообщений *404 Не найдено (Not found)* в сигнальном обмене.

При реализации атаки по сценарию 2 и достижении интенсивности атаки 1000 запросов/с загрузка процессора коммутатора приближалась к 100 %, объем свободной оперативной памяти приближался к нулю. Данная ситуация приводила к остановке работающих на программном коммутаторе сервисов с последующим рестартом программного коммутатора.

При реализации на программном коммутаторе механизме авторизации запросов REGISTER возможны два варианта атаки по сценарию 2:

— в запросах REGISTER передаются корректные данные авторизации (такая атака характеризуется резким ростом интенсивности успешных запросов на регистрацию и резким сокращением периода перерегистрации SIP-абонентов программного коммутатора);

— в запросах REGISTER передаются некорректные данные авторизации (атака характеризуется резким ростом числа ответов *401 Требуется авторизация (Unauthorized)* и *403 Запрещено (Forbidden)* на запросы REGISTER).

Проведенные тесты позволили экспериментально определить признаки реализации исследуемых флуд-атак на сети NGN. Такими признаками являются: рост числа ошибок в сигнальном обмене; увеличение загрузки процессора программного коммутатора и уменьшение объема свободной памяти программного коммутатора.

Контроль за изменениями этих параметров позволит получить информацию, необходимую для анализа уровня угрозы и для принятия решения о наличии угрозы атаки DoS.

Таким образом, задачу детектирования атаки DoS можно сформулировать как задачу детектирования момента времени, в который названные признаки достигнут определенного порогового значения.

С задачей обнаружения момента изменения контролируемого параметра успешно справляется алгоритм кумулятивной суммы (cumulative sum, CUSUM) [8]. В работе [9] описываются различные подходы к использованию алгоритма CUSUM для обнаружения изменения в контролируемом параметре.

Общее представление алгоритма описывается следующим образом. Из последовательности независимых случайных величин Y_k с плотностью вероятности $P_\Theta(y)$, зависящей только от скалярного параметра Θ, берутся выборки размером N. Известно, что до момента времени t_0 параметр $\Theta = \Theta_0$. После момента времени t_0 $-$ $\Theta = \Theta_1$, $(\Theta_1 \neq \Theta_0)$. Значения Θ_0 и Θ_1 известны априори. Значение t_0 неизвестно. Для обнаружения момента изменений параметра Θ в конце каждой выборки проводится проверка истинности одной из двух гипотез:

$$H_0 : \Theta = \Theta_0;$$

$$H_1 : \Theta = \Theta_1.$$

Если в результате проверки принимается решение об истинности гипотезы H_0, проверке подвергается следующая выборка из последовательности Y_k. Если принимается решение об истинности гипотезы H_1, то тест останавливается.

Правило принятия решения описывается так:

$$d = \begin{cases} 0, \text{ если } S_1^k < h; \text{ выбрана гипотеза } H_0; \\ 1, \text{ если } S_1^k \geq h; \text{ выбрана гипотеза } H_1, \end{cases}$$

где h — пороговое значение;

$$S_1^k = \sum_{i=1}^{k} S_i$$

— функция принятия решения;

$$S_i = \ln \frac{P_{\theta 1}(y_i)}{P_{\theta 0}(y_i)}$$

— статистический параметр алгоритма.

Из приведенных выражений следует, что пока параметр Θ находится в пределах контролируемого диапазона ($\Theta = \Theta_0$, $P_{\Theta 0}(y_i) > P_{\Theta 1}(y_i)$), значение S_{1k} равно нулю или меньше нуля. В момент изменения параметра ($\Theta = \Theta_1$, $P_{\Theta 0}(y_i) < P_{\Theta 1}(y_i)$) значение S_{1k} резко возрастает.

Время остановки теста t_0 (другими словами, время обнаружения изменения параметра Θ) определяется выражением

$$t_0 = N \cdot \min\{k : d_k = 1\},$$

что можно сформулировать как правило остановки наблюдений при обнаружении изменения параметра Θ: наблюдения останавливаются после первой выборки N, для которой принято решение об истинности гипотезы H_1.

Исследования [10–12] показывают возможность использования алгоритма CUSUM для детектирования флуд-атак DoS различных типов. Эффективность алгоритма CUSUM при детектирования атак DoS во многом зависит от релевантности выбранного контролируемого параметра. В работе [12] предлагается в качестве такого параметра использовать гибридное значение, отражающее соотношение запросов и ответов:

$$\Theta_i = \Theta_i^{\text{INVITE/ACK}} + \Theta_i^{\text{INVITE/200 OK}} + \Theta_i^{\text{REGISTER/200 OK}}.$$

В работе [10] рассматривается возможность использования в качестве такого параметра разности REGISTER – 200 OK.

На основании проведенных испытаний можно предложить в качестве контролируемого параметра при использовании алгоритма

CUSUM для детектирования флуд-атак DoS использовать гибридный параметр, отражающий процент загрузки процессора и число сообщений об ошибках в сигнальном обмене.

Рассмотрим пример использования алгоритма CUSUM для обнаружения изменений числа ошибок *503 Служба недоступна* в ответ на запрос INVITE в сети сигнализации SIP. Как было показано ранее, увеличение таких ошибок в сигнальном трафике может свидетельствовать о начале флуд-атаки. Для использования в примере взят образец сигнального обмена длительностью 30 с, полученный при проведении теста по имитации флуд-атаки посредством передачи большого числа запросов INVITE. В течение этого периода осуществлено две флуд-атаки разной интенсивности, длительностью 5 с каждая. В качестве контролируемого параметра выбрано среднее значение интенсивности ошибок *503 Служба недоступна* в сети сигнализации. Интенсивность измерялась путем подсчета числа ошибок за секунду. Подход, когда в качестве контролируемого параметра используется среднее значение, описан в работе [8]. В этом случае функция принятия решения принимает следующий вид:

$$S_i^k = \frac{\mu_i - \mu_0}{\sigma^2} \sum_i^k \Big(y_i - \frac{\mu_1 + \mu_0}{2} \Big),$$

где μ_1 и μ_0 — текущее и эталонное среднее значения параметра y_i, σ — среднеквадратическое отклонение параметра y_i от эталонного среднего.

Выбор значений μ_0 и σ может быть сделан с опорой на экспертные оценки или получен экспериментально. Данные значения определяют чувствительность алгоритма.

В рассматриваемом примере приняты следующие значения величин $\mu_0 = 0{,}01$; $\sigma = 1{,}97$.

Значение μ_1 вычислялось ежесекундно по выборке длительностью 5 с. Результаты сведены в таблицу.

На рис. 2 показан график функции S_i^k. На графике видно, что при $\mu_1 \le \mu_0$ функция S_i^k принимает близкие к нулю или даже отрицательные значения. При $\mu_1 > \mu_0$ значение S_i^k резко возрастает, сигнализируя об изменении контролируемого параметра.

Порог, при котором будет принято решение об имеющей место атаки DoS, может быть установлен экспериментальным путем.

Выводы. Результаты анализа уязвимостей действующей сети сигнализации по протоколу SIP к тестируемым атакам DoS показывают эффективность использования метода, описанного в статье, по всем типам атак DoS в плане:

— оценки возможности реализации различных сценариев атак DoS в целях выработки мер по противодействию таким атакам;

Таблица значений CUSUM

Время t_i, с	y_i	μ_i	S_i^k	Время t_i, с	y_i	μ_i	S_i^k
1	0	0	1,28836E-05	16	0	0,2	0,348578938
2	0	0	2,57672E-05	17	0	0,2	0,343438378
3	0	0	3,86508E-05	18	0	0,2	0,338297818
4	0	0	5,15344E-05	19	0	0	–0,017792265
5	0	0	6,4418E-05	20	0	0	–0,017779381
6	4	0,8	0,726712876	21	0	0	–0,017766497
7	2	1,2	1,52241748	22	0	0	–0,017753614
8	2	1,6	2,523744492	23	0	0	–0,01774073
9	3	2,2	4,545453374	24	0	0	–0,017727847
10	2	2,6	5,839495993	25	0	0	–0,017714963
11	0	1,8	3,618374604	26	9	1,8	6,90466129
12	0	1,4	2,557293411	27	10	3,8	22,5247623
13	0	1	1,692558427	28	10	5,8	44,99636682
14	1	0,6	1,114354918	29	10	7,8	72,77344173
15	0	0,2	0,353719498	30	10	9,8	104,3099539

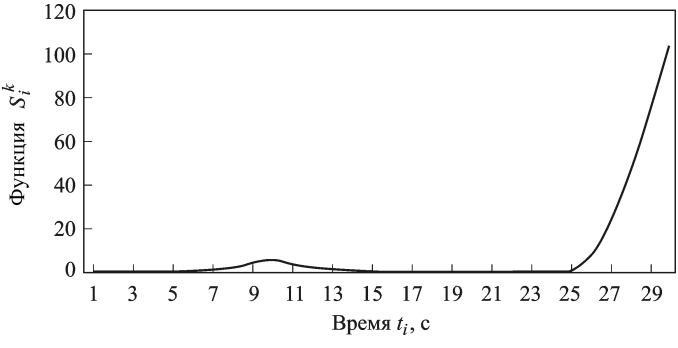

Рис. 2. Изменение значений функции принятия решения алгоритма CUSUM при детектировании DoS-атаки

— выявления признаков реализации атаки DoS, необходимых для поиска алгоритмов раннего обнаружения этих атак;

— оценки эффективности выбранных алгоритмов обнаружения атак DoS;

— возможности получения путем опроса экспертов достаточно достоверных субъективных показателей вероятностей реализации атаки и ущерба от реализации. Эти данные дают основание для использования математического аппарата нечетких множеств и нечеткой логики, который позволяет решать некоторые задачи количественной оценки риска безопасности в сетях связи;

— продолжения работ по проведению тестирования в целях получения экспериментальных данных об уязвимости компонентов сети

NGN к различным типам угроз информационной безопасности и поиска мер противодействия этим угрозам.

ЛИТЕРАТУРА

1. *Dorgham* Sisalem, et. al. SIP security. John Wiley & Sons, Ltd., 2009.
2. *Yao* Jiang, et. al. Evaluation model for DoS attack effect in softswitch network // International Conference on Communications and Intelligence Information // Security, 2010. P. 88–91.
3. *Гольдштейн А.Б.*, *Гольдштейн Б.С.* Softswitch. СПб.: БХВ – Санкт-Петербург. 2006.
4. *Щербаков В.Б.*, *Ермаков С.А.* Безопасность беспроводных сетей: стандарт IEEE 802.11. М.: РадиоСофт, 2010.
5. *Ehlert S.*, *Geneiatakis D.*, *Magedanz T.* Survey of network security systems to counter SIP-based denial-of-service attacks, Elsevier, 2009.
6. *Schulzrinne H.*, et. al. SIP: Session Initiation Protocol, RFC 3261, June 2002.
7. *SIPp* официальный сайт. http://sipp.sourceforge.net/
8. *Page E.S.* (June, 1954). Continuous Inspection Scheme. Biometrika 41 (1/2): 100–115.
9. *Basseville M.* and *Nikiforov I.V.* Detection of abrupt changes: Theory and application. Prentice-Hall Inc, 1993.
10. *Kim H.*, *Rozovskii B.* and *Tartakovsky A.* A nonparametric multichart cusum test for rapid intrusion detection // International Journal of Computing and Information Science, 2(3):149–158, December, 2004.
11. *Chen Z.*, et. al. Detecting SIP flooding attacks on IP multimedia subsystem (IMS) // Computing, Networking and Communications (ICNC), 2012 International Conference, Conference Publications, p. 154–158, Feb. 2012.
12. *Li W.*, et. al. On Sliding Window Based Change Point Detection for Hybrid SIP DoS attack // IEEE Asia-Pacific Services Computing Conference. 2010.

REFERENCES

[1] Sisalem D., Floroiu J., Kuthan J., Abend U., Schulzrinne H. SIP security. Chichester, John Wiley & Sons, 2009. 350 p. doi: 10.1002/9780470516997

[2] Jiang Y., Zheng K., Yang Y., Luo S., Zhao J. Evaluation model for DoS attack effect in softswitch network. Proc. Int. Conf. Commun. Intell. Inf. Secur. (ICCIIS), 2010, pp. 88–91. doi: 10.1109/ICCIIS.2010.30

[3] Gol'dshteyn A.B., Gol'dshteyn B.S. Softswitch. St. Petersburg, BKhV–Peterburg Publ., 2006. 368 p. (in Russ.).

[4] Shcherbakov V.B., Ermakov S.A. Bezopasnost' besprovodnykh setey: standart IEEE 802.11 [Wireless security: standard IEEE 802.11]. Moscow, RadioSoft Publ., 2010. 255 p.

[5] Ehlert S., Geneiatakis D., Magedanz T. Survey of network security systems to counter SIP-based denial-of-service attacks. *Comput. Secur.*, 2009, vol. 29, no. 2, pp. 225–243.

[6] Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M., Schooler E. SIP: Session Initiation Protocol, RFC 3261, 2002. Available at: http://www.ietf.org/rfc/rfc3261.txt (Accessed 14 July 2013).

[7] SIPp website. Available at: http://sipp.sourceforge.net/ (Accessed 14 July 2013).

[8] Page E.S. Continuous inspection schemes. *Biometrika*, 1954, vol. 4, nos. 1–2, pp. 100–115. doi:10.1093/biomet/41.1-2.100

[9] Basseville M., Nikiforov I.V. Detection of abrupt changes: theory and application. Prentice-Hall Inc., Englewood Cliffs, 1993. 469 p.

[10] Kim H., Rozovskii B., Tartakovsky A. A nonparametric multichart cusum test for rapid intrusion detection. *Int. J. Comput. Inf. Sci.*, 2004, vol. 2, no. 3, pp. 149–158.

[11] Chen Z., Wen W.,Yu D. Detecting SIP flooding attacks on IP multimedia subsystem (IMS). Proc. Int. Conf. Comput. Networking Commun. (ICNC), 2012, pp. 154–158. doi: 10.1109/ICCNC.2012.6167401

[12] Li W., Guo W., Luo X., Li X. On sliding window based change point detection for hybrid SIP DoS attack. Proc. IEEE Asia-Pac. Serv. Comput. Conf., 2010, pp. 425–432. doi: 10.1109/APSCC.2010.84

Статья поступила в редакцию

Валерий Александрович Матвеев — д-р техн. наук, профессор, заведующий кафедрой “Информационная безопасность”, руководитель НУК “Информатика и системы управления” МГТУ им. Н.Э. Баумана. Автор более 200 научных работ и 23 патентов в области информатики, систем управления и навигации.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

V.A. Matveev — Dr. Sci. (Eng.), professor, head of "Information Security" department, chief of Scientific and Educational Complex for Information Technologies and Control Systems of the Bauman Moscow State Technical University. Author of more than 200 publications and 23 patents in the field of instrument engineering.
Bauman Moscow State Technical University, Vtoraya Baumanskaya ul., 5, Moscow, 105005 Russian Federation.

Алексей Михайлович Морозов — ведущий инженер отдела управления сетями Московского филиала ОАО “Ростелеком”, соискатель кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана, автор шести научных работ в области информационной безопасности.
Региональный центр управления сетями связи Московского филиала ОАО “Ростелеком”, Российская Федерация, 140000, Московская обл., г.Люберцы, ул. Московская, д. 17.

A.M. Morozov — leading engineer of department for network management of Regional Center for Management of Communication Networks of Moscow Branch of OAO “Rostelekom”. Author of six publications.
Regional Center for Management of Communication Networks of Moscow Branch of OAO “Rostelekom”, ul. Moskovskaya, 17, Lyubertsy, Moscow region, 140000 Russian Federation.