МЕТОД ПОВЫШЕНИЯ ДОСТУПНОСТИ ТЕХНИЧЕСКИХ СИСТЕМ С САМОПОДОБНЫМ ПОТОКОМ

A METHOD OF INCREASING THE AVAILABILITY OF TECHNICAL SYSTEMS WITH SELF-SIMILAR FLOW

S. Platunova
E. Avksentieva

Summary. The article considers the problem of designing technical systems maintenance with self-similar flow, provides a specified availability, and requires consideration when designing and developing. The subject of research is a reduced risk of loss of availability of technical service systems with self-similar flow. The aim of this work is to assess the reduction in risk of availability loss from an attack of self-similar flow, flooding and loss of availability of technical systems.

Keywords: engineering, technical service systems, self-similar flow, accessibility, risk, loss of availability, protection, attack, vulnerability of technical systems, the coefficient of self-similarity, the number of channels redundancy.

Платунова Светлана Михайловна
Старший преподаватель, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург, Россия
platunowasweta@mail.ru
Авксентьева Елена Юрьевна
К.п.н., доцент, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, г. Санкт-Петербург, Россия,
avksentievaelena@rambler.ru

Аннотация. В работе рассматриваются задачи проектирования технических систем с самоподобным потоком, обеспечивающих заданную доступность и требующие учета при проектировании и разработке. Предметом исследования является снижение рисков потери доступности технических систем с самоподобным потоком. Целью работы является оценка снижения риска потери доступности от атаки самоподобного потока, приводящей к перегрузке и потере доступности технических систем.

Ключевые слова: проектирование, технические системы, самоподобный поток, доступность, риск, потеря доступности, защита, атака, уязвимость, коэффициент самоподобия, число каналов, резервирование.

Введение

Известными мерами безопасности технических систем являются идентификация, аутентификация, авторизация, разграничение доступа, шифрование, защита периметра, локальные и глобальные политики безопасности, цифровые подписи, сертификаты. Но эти меры не обеспечивают защиту от характера потока, который может перегрузить систему, вызвать потерю доступности технических систем (ТС), после чего известные меры безопасности окажутся невостребованными.

Уровень информационной безопасности ТС достигается обеспечением приемлемого уровня рисков нарушения конфиденциальности, целостности и доступности информационных ресурсов. В частности, нарушение доступности информационных ресурсов и услуг может произойти в результате: планирования и разработки ТС без учета требований безопасности, появления новых угроз при динамической эволюции ТС, масштабировании, построении демилитаризованных зон, функциональных структурных изменениях, угроз безопасности ТС, вызванных перегрузкой от влияния самоподобного потока.

Структура системы защиты от угроз [1] нарушения доступности при передаче информации включает в себя следующие меры: дублирование каналов связи, дублирование «узких мест» (шлюзов, межсетевых экранов), запас в пропускной способности сетевого оборудования.

Самоподобный поток — это разновидность атаки на отказ в обслуживании и угроза доступности услуг проектируемых технических систем

Самоподобие трафика — это угроза свободному ресурсу, потому что трафик поступает неравномерно, и по сравнению с классическими случаями, нужно больше ресурса, чтобы обслужить одинаковое количество трафика.

Самоподобие — это свойство потока, которое следует учитывать в модели системы при больших нагрузках. Угрозы атаки на отказ в обслуживании провоцируют отказ в обслуживании путем чрезмерной загрузки канала [2].

Самоподобный поток обладает некоторой структурой между интервалами поступления заявок, повторяющейся во времени, которую можно назвать кластеризацией кластеров запросов на обслуживание крайне отрицательно влияющих на оперативность ТС.

Автором В. И. Нейман введен учет самоподобной нагрузки. Для учета влияния самоподобия введена функ-

ция, зависящая от коэффициента самоподобия H, причем при $H=0,5$ свойство самоподобия отсутствует, а при увеличении коэффициента самоподобия H до единицы влияние самоподобности нагрузки усиливается. В формулах появляется функция $f(H)$, учитывающая влияние самоподобности нагрузки. Если использовать линейный закон и значение данной функции для $H=0,5$ равное 1, то можно представить $f(H)$ в виде: $f(H)=2H$.

Интенсивность поступающих на обслуживание заявок можно представить в виде: $\lambda_h=\lambda_0 f(H)$, где λ_0 — интенсивность поступающего на обслуживание потока заявок при отсутствии самоподобия.

$$\lambda_h = f(H)\ \lambda_0=2H\lambda_0=2\lambda_0, \quad (1)$$

Авторами Сычев К. И., Батенков К. А.показано, что увеличением размера буфера нельзя добиться значительного снижения очередей в случае пикового характера (кластеризованности) потока даже при использовании системы с приоритетами.

Исходя из краткого обзора, можно сделать вывод, что самоподобный поток является разновидностью атаки на отказ в обслуживании, т.к. с вероятностью, которой нельзя пренебречь, может появляться большое и очень большое число запросов, поступающих в систему, что может перегрузить систему и вызвать отказ в обслуживании.

Атака самоподобного потока проявляется в том, что запросы на обслуживание, пакеты самоподобного потока, которые могут поступать кластерами, пачками, могут занять все приборы обслуживания, порты, линии связи, вызвав отказ в обслуживании.

В ГОСТ Р ИСО/МЭК 13335–2007 4 п. 10.4.15 указано, что перегрузка трафика угрожает доступности информации, передаваемой через предоставляемые услуги. Защитные меры в этой области включают в себя, в частности, резервирование. Внедрение резервирования компонентов коммуникационных услуг может применяться для снижения вероятности перегрузки трафика.

В ГОСТ Р ИСО/МЭК 13335–1–2006 и ИСО/МЭК 7498–2 понятие доступность (availability) определено как свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта.

Угроза (причина) потери доступности ТС или уязвимость (слабость) ТС — это отсутствие запаса ресурса (пропускной способности), например, наличия числа каналов n_0.

Устраняется угроза потери доступности или уязвимость, в частности, путем увеличения числа каналов обслуживания пакетов самоподобного трафика с учетом коэффициента самоподобия H.

Так как коэффициент самоподобия $H\in[0,5;\ 1]$, то $2H\in[1;\ 2]$, причем при $H=0,5$ самоподобие потока отсутствует, то суть СЗД от перегрузки самоподобного потока состоит в удваивании (ресурса) числа каналов $n0$ ТС, спланированных без учета коэффициента самоподобия потока.

$$n_h=f(H)n_0=2Hn_0=2n_0, \quad (2)$$

где n_0 — число каналов (количество ресурса) при отсутствии самоподобия потока.

Предлагается метод снижения риска потери доступности, который позволяет устранить атаки на доступность путем разгрузки ТС. Метод снижения риска потери доступности от атаки самоподобного потока заключается в учете коэффициента самоподобия путем удваивания числа каналов и памяти (количество ресурса ТС) относительно числа каналов n_0, спланированного без учета коэффициента самоподобия потока по другим критериям (требованиям задержки, надежности).

Интенсивность атак на ТС СП λ_h — это интенсивность поступления пакетов самоподобной нагрузки, которые ТС должна обработать для отражения потери доступности: $\lambda_h=2\lambda_0$, где λ_0 — предположительная интенсивность нагрузки ТС без учета коэффициента самоподобия.

Доля успешной атаки самоподобного потока на доступность — это вероятность потери доступности от перегрузки самоподобным трафиком $p_{пд}$.

Авторы [3], [4], [5], [6] мотивированно считают атаку самоподобного потока актуальной и реализуемым метод снижения риска потери доступности ТС от перегрузки самоподобным трафиком.

Метод снижения риска потери доступности технических систем от перегрузки самоподобным потоком

Метод заключается в применении резервирования каналов для обработки атаки самоподобного потока.

Отказы СЗД — это обнаружение уязвимости ТС, перегрузка, потеря доступности ТС.

Интенсивность λ отказов мер защиты доступности от атаки самоподобного трафика — это частота успешной атаки самоподобного потока, вызвавшего перегрузку —

Таблица 1. Вероятность $P_s(t)$ увеличивается при применении параллельно включенных элементов (мер) защиты относительно не применения системы защиты

	P0a	Ps
2 параллельных меры (элемента) защиты	0.333	0.555
2 параллельных меры (элемента) защиты	0.13	0.243
4 параллельных меры (элемента) защиты	0.333	0.802
4 параллельных меры (элемента) защиты	0.13	0.427

потерю доступности $\lambda=2\lambda_0$, где λ_0 — предположительная интенсивность нагрузки ТС без учета коэффициента самоподобия.

Для экспоненциального распределения интенсивности λ отказов СЗД вероятность $p(t)$исправной работы канала системы защиты доступности (ВБР СЗД) в течение произвольного интервала времени t определяется следующим образом:

$$p(t)=e_{-\lambda\, tv}$$

Среднее время tv восстановления СЗД — это время занятости ресурса ТС — время обслуживания пакетов самоподобного потока — перегрузка ТС, разгрузка каналов ТС обработки атаки самоподобного трафика.

Защитоспособность мер характеризуется вероятностью P_s безотказной защиты за время t и определяется для основных средств защиты (n_h каналов) ТС вероятностью P_c.

Использование дополнительных механизмов защиты — это увеличение размера буфера для буферизации пакетов самоподобного трафика с целью избегания потерь и последующих перезапросов на обслуживание, обеспечивающих резервирование основных средств защиты (m_h), и характеризуемых вероятностью P_e:

$$P_s(t) = (1-(1-P_c(t))(1-P_b(t)))$$

В связи с тем, что пакеты потока или находятся в серверах (каналах) обслуживания или ожидают обслуживания в буферах ТС, то основная защитная мера — серверы (каналы) ТС резервируется дополнительной защитной мерой в виде увеличения буфера (для буферизации пакетов самоподобного трафика с целью уменьшения потерь и последующих перезапросов на обслуживание), при этом атака самоподобного потока направлена или на каналы или на буферы.

Вероятность защитоспособности $P_s(t)$ СЗД для параллельного соединения элементов защиты равна:

$$P_s(t) = (1-(1-P_c(t))(1-P_b(t))) \quad (3)$$

где $P_c(t)$ — вероятность защитоспособности (безотказной (работы) защиты) средствами увеличения числа каналов, $P_m(t)$ вероятность защитоспособности системы буферов.

$$P_c(t) = \left(\frac{(c\lambda t_v)^c}{c!(1-\lambda t_v)} + \sum_{i=0}^{c-1} \frac{(c\lambda t_v)^i}{i!} \right)^{-1},$$

где c — число серверов (каналов) ТС

$$P_b(t) = \left(\frac{(b\lambda t_v)^b}{b!(1-\lambda t_v)} + \sum_{i=0}^{b-1} \frac{(b\lambda t_v)^i}{i!} \right)^{-1},$$

где b — число мест в буфере ТС

$P_c(t)$, $P_b(t)$ показывают вероятность того, что в серверах (каналах, буферах) нет клиентов (заявок на обслуживание), т.е. в ТС СП нет угроз.

Коэффициент K_{rs} готовности мер защиты оценивает вероятность того, что средства защиты в любое время защищают доступность ТС или оценивает долю времени, в течение которого Средства Защиты Доступности (СЗД) защитоспособны, и рассчитывается из выражения:

$$K_{rs} = \frac{1}{1+\lambda t_v} \quad (4)$$

Далее Вводим коэффициент оперативной защищенности СЗД — характеристику защищенности, которая оценивает вероятность или долю времени того, что СЗД будут готовы к защите доступности ТС от перегрузки СП в произвольный момент времени, кроме периодов восстановления СЗД и, начиная с этого момента, будет обрабатывать атаки СП безотказно в течение заданного интервала времени.

Введем оценки СЗД и покажем варианты применения от атаки самоподобного потока.

Коэффициент оперативной защищенности

Для экспоненциального распределения интенсивности отказов СЗД (для постоянной интенсивности от-

Таблица 2. Уменьшение риска в защищенной системе защиты доступности по сравнению с незащищенной системой защиты доступности

Число каналов системы n	R_s (n)	1- R_s (n)	$R_{защ}$/ $R_{нез}$ (выигрыш от применения СЗД)	Коэффициент защищенности D =(1- $R_{защ}$/ $R_{нез}$) *100%
1	0.9406	0,0594		
2	0.9982	0,0018	0,030303	96,97%
4	0.9993	0,0007	0,388889	61,11%

Таблица 3. Повышение доступности ТС СП при удваивании числа каналов, учитывающих самоподобия потока.

Число каналов системы n	Доступность системы P_s(n)	Риск потери доступности: Q(n) =1- P_s(n)	Снижение риска потери доступности системы от угрозы перегрузки самоподобным потоком G_Q= Qs(n_h)/Q_s(n_0)
1	0.9406	0,0594	
2	0.9982	0,0018	0,0303
4	0.9993	0,0007	0,01178

казов) и восстановления СЗД коэффициент оперативной защищенности системы $Rs\ (t)$ будем рассчитывать по формуле:

$$R_s\left(t\right) = K_{rs} P_s\left(t\right) \quad (5)$$

Этот показатель предлагается считать пессимистическим, когда СЗД наносится наибольший вред и стоимость недоступности информации не учитывается при расчете коэффициента защищенности D системы (таблица 2).

$$D = 1 - \frac{\left(1 - R_{sn_h}\left(t\right)\right)}{\left(1 - R_{sn_0}\left(t\right)\right)} 100\%$$

В таблице 2 представлены результаты исследования тестовой технической системы обслуживания в виде агрегированной линии связи без применения и с применением системы защиты доступности ТС от перегрузки самоподобным трафиком при одинаковых исходных условиях.

Вероятность неготовности

Введем еще один показатель защищенности исходя из следующих соображений. Риск потери доступности ТС от угрозы самоподобия потока заключается в том, что на стадии разработки не учитывается угроза перегрузки самоподобным потоком. Целесообразно риск потери доступности оценивать с помощью вероятности неготовности ТС, рассчитанной для числа каналов n_0 без учета угрозы самоподобия потока.

$$Q(n_h) = 1 - P_s(n_h) \quad (9)$$

Снижение риска потери доступности ТС от угрозы самоподобия потока заключается в учете влияния самоподобного потока путем удваивания числа каналов ТС относительно числа каналов n_0, спланированного без учета влияния самоподобия потока по другим критериям (требованиям задержки, надежности).

Снижение риска потери доступности вычисляется как отношение G_Q риска потери доступности системы с числом каналов, учитывающих самоподобие потока к риску потери доступности для числа каналов, не учитывающих самоподобие потока:

$$G_Q = Q_s(n_h)/Q_s(n_0) \quad (10)$$

Снижение риска потери доступности, число каналов и среднее время пребывания запроса в тестовой системе до и после применения предложенного метода при одинаковых исходных условиях представлены в таблице 1.

Заключение

Рассмотрены модели самоподобного потока, показывающие, что самоподобный поток является разновидностью атаки на отказ в обслуживании, ведущей к перегрузке ТС и потере доступности ТС. Предложена система защиты, позволяющая повысить доступность ТС от перегрузки самоподобным потоком с учетом коэффициента самоподобия на этапе проектирования и разработки ТС. Показана эффективность средств защиты доступности, которая оценивается коэффициентом защищенности (выигрышем) от применения СЗД. Показана эффективность системы защиты доступности, которая оценивается Вероятностью неготовности СЗД.

ЛИТЕРАТУРА

1. Авксентьева Е.Ю., Авксентьев С. Ю. Рекомендации по защите информации при использовании сервисов облачного хранения в учебном заведении // Электронное обучение в ВУЗе и в школе /Материалы сетевой международной научно-практической конференции –2014.— С. 20–24 http://istina.msu.ru/media/publications/article/57e/b48/7483836/Sbornik_razv.pdf
2. Шелухин О.И., Моделирование информационных систем [Текст]: учеб. пособие для вузов «Сети и системы коммутации», «Многоканал. телекоммунакац. системы» / О. И. Шелухин.— [2-е изд., перераб. и доп.].— М.: Горячая линия-Телеком, 2014.— 516 с.: ил., табл.— (Специальность для высших учебных заведений).— Библиогр.: с. 508–509.— ISBN**9**78–5–9912–0193–3 (в пер.)
3. Платунова С. М. Исследование метода повышения доступности вычислительной сети с самоподобным трафиком // Международный научно-исследовательский журнал Успехи современной науки и образования № 11, том 2, 2016 год, С. 70–73 http://elibrary.ru/item.asp?id=27430594, http://modernsciencejournal.org/release/USNO_2016_11_2_tom.pdf
4. Авксентьева Е.Ю., Платунова С. М. Методы и модели проектирования системы материально-технического обеспечения учебного процесса // Современная наука: актуальные проблемы теории и практики. Серия: Гуманитарные науки — 2016.— № 1.— С. 72–80, http://www.nauteh-journal.ru/index.php/—gn16–01/1779-a
5. Платунова С.М., Модель корпоративной сети при агрегировании каналов и резервировании линий, Научно-технический и производственный журнал «Вестник компьютерных и информационных технологий», № 22011, ISSN1810–7206, DOI: 10.14489/issn.1810–7206**,** http://vkit.ru/index.php/archive-rus/134–02
6. Платунова С.М., Модель корпоративной сети при настройке ip-доменов, Научно-технический журнал Информационные системы и технологии № 4 (60) июль-август 2010, Государственное Образовательное Учреждение высшего профессионального образования «Орловский государственный технический университет», С. 130–134, http://gu-unpk.ru/public/file/archive/isit%204–2010.pdf

Журнал «Современная наука: актуальные проблемы теории и практики»