Модель процесса мониторинга корректности фрагментации пакетов в ведомственной сети передачи данных

В.В. Починок, Р.С. Шерстобитов, А.П. Теленьга, Т.В. Лебедкина, В.В. Кучуров
Краснодарское высшее военное училище им. генерала армии С.М. Штеменко

Аннотация: В статье описывается модель, позволяющая провести исследование и обоснование выбора режимов работы ведомственных сетевых информационных объектов, функционирующих в распределенных сетях передачи данных, в условиях несанкционированных воздействий, направленных на перегрузку сетевых информационных объектов некорректно фрагментированными пакетами сообщений. Разработанная модель, за счет мониторинга сбоев (отказов) дефрагментации пакетов сообщений и адаптации параметров маршрута связи к изменению структуры (параметров) сети передачи данных, позволяет сформулировать требования по улучшению показателей своевременного предоставления сервисных возможностей абонентам ведомственных сетей передачи данных, а также обеспечению доступности обрабатываемой информации в условиях высокой интенсивности обмена пакетами сообщений с некорректными параметрами фрагментации.

Ключевые слова: сеть передачи данных, ведомственные сетевые информационные объекты, *IP*-дейтаграммы, фрагментация пакетов.

При организации связи между ведомственными сегментами сети передачи данных (далее СПД) через сеть связи общего пользования, передаваемые *IP*-дейтаграммы, могут быть фрагментированы по критерию значения *MTU* (*MTU, maximum transmission unit* – максимально возможная длина дейтаграммы, которую та или иная технология может поместить в поле данных своей единицы передачи). Протокол *TCP* разбивает исходящий поток байтов (у отправителя) на сегменты нужного размера. Фрагменты передают по адресу назначения, где приемник выполняет их сборку. На пути доставки фрагментированных пакетов они могут подвергаться неоднократной фрагментации, если необходима их передача через сегмент

сети с еще меньшим *MTU*. Транзитный трафик фрагментируется на маршрутизаторе, когда пакет необходимо передать из сети с большим значением *MTU* в сеть с меньшим значением *MTU*, протоколом *IP* [1].

Значения *MTU* для различных технологий передачи данных отличаются, а это значит, что в территориально распределенных СПД фрагментация необходима. Процессы фрагментации пакетов сообщений достаточно хорошо описаны, и сама по себе фрагментация является абсолютно нормальным явлением, однако, из теории массового обслуживания известно, что передача нормализованного трафика, включающего пакеты одинаковой длины, увеличивает скорость передачи данных в СПД. Поэтому фрагментации на транзитных узлах стараются избежать [2].

Избежать фрагментации в процессе ретрансляции можно, реализуя процедуры *Path MTU Discovery* [3] и *TCP MSS* [4].

Суть процедуры *Path MTU Discovery* заключается в том, что при отправке пакетов сообщений в заголовке устанавливается флаг *DF* (*Do Not Fragment* – не фрагментировать), который запрещает фрагментацию пакетов на транзитных узлах СПД. Это приводит к тому, что узел, значение *MTU* которого меньше размера пакета, отклоняет передачу пакета и отправляет *ICMP*-сообщение отправителю «*fragmentation needed and DF set*» (необходима фрагментация, но установлен флаг её запрета). Узел-отправитель уменьшает размер пакета и отсылает его заново. Такая операция происходит до тех пор, пока пакет не будет достаточно мал, чтобы дойти до хоста-получателя без фрагментации (см. рис. 1). В процессе выполнения *Path MTU Discovery* узел-отправитель запоминает значения *MTU* транзитных узлов, создавая строчки в таблице маршрутизации до соответствующего узла-получателя [3].

Данный способ не лишен недостатка, заключающегося в том, что при предустановленной блокировке ответов по протоколу *ICMP* выполнение процедуры *Path MTU Discovery* невозможно, а данная ситуация получила название *MTU Discovery Black Hole*.

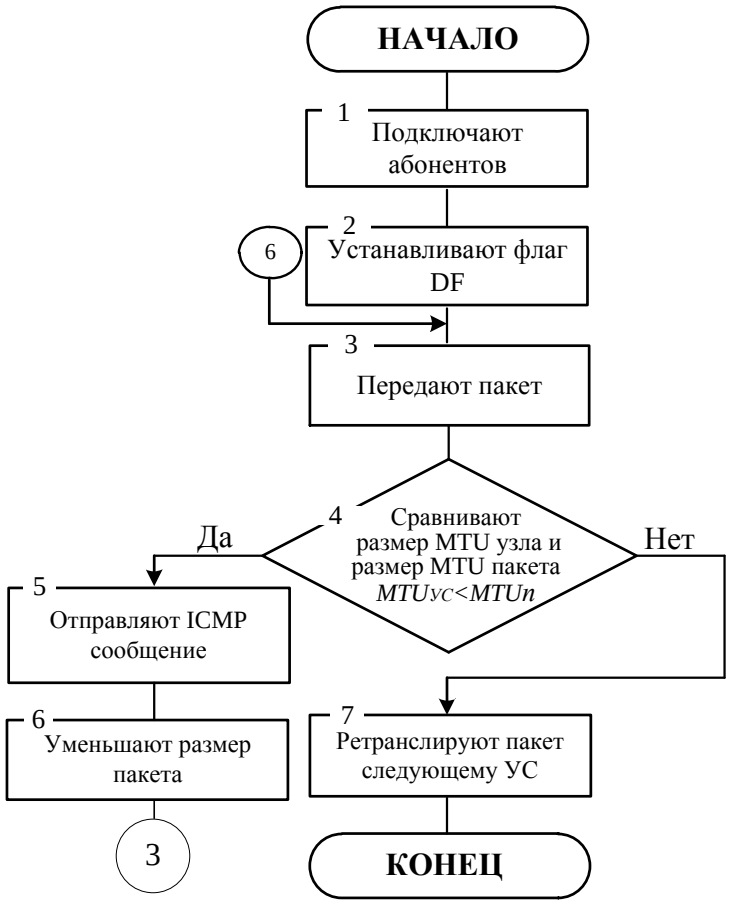

Рис. 1. – Алгоритм работы протокола *Path MTU Discovery*

Рассмотренные способы снижают процедурную нагрузку на СПД и принимающего абонента.

Однако, независимо от принятой политики продвижения трафика, существует возможность создания фрагментов пакетов, которые при их сборке на приемнике позволят привести к снижению доступности принимающего абонента [5].

Для реализации компьютерных атак такого типа злоумышленники используют два основных метода: *Tiny Fragments* («микрофрагменты») и

Fragment Overlapping («перекрытие фрагментов»). Такие компьютерные атаки и их интерпретации можно отнести к несанкционированным воздействиям процедурного типа. Даже при наличии инициализированной системы контроля таких атак, обеспечивающей защиту от них, неизбежна чрезмерная трата вычислительных ресурсов на атакованном сегменте СПД [6].

Цель разработки модели – исследование и обоснование выбора режимов работы ведомственных сетевых информационных объектов, функционирующих в распределенных сетях передачи данных (СПД), основанных на семействе коммуникационных протоколов *TCP*/*IP* в условиях несанкционированных воздействий, направленных на перегрузку сетевых информационных объектов некорректно фрагментированными пакетами сообщений.

Достижение сформулированной цели необходимо для своевременного предоставления сервисных возможностей абонентам ведомственных СПД, а также для обеспечения доступности обрабатываемой информации.

Значение коэффициента результативности дефрагментации $K_{ij}^{\text{РД}}$ пакетов сообщений для каждого маршрута связи удобно вычислять по формуле (1):

$$K_{ij}^{\text{РД}} = \frac{\Lambda_{ij}^{\text{ПС}} - \Lambda_{ij}^{\text{АФ}}}{\Lambda_{ij}^{\text{ПС}}}, \quad (1)$$

где $\Lambda_{ij}^{\text{ПС}}$ – значение интенсивности *IP*-пакетов сообщений, направленных *i*-м отправителем *j*-му получателю для каждого маршрута связи;

$\Lambda_{ij}^{\text{АФ}}$ – значение интенсивности *IP*-пакетов сообщений, содержащих признаки аномальных значений параметров фрагментации.

Рассмотрим переход от детерминированной постановки задачи к постановке задачи в условиях неопределенности. Тогда финальную

вероятность состояния S_i СПД можно будет интерпретировать как среднее относительное время пребывания системы в этом состоянии.

На рис. 2 представлен размеченный граф состояний моделируемой системы.

В таблице №1 перечислены необходимые для математического моделирования состояния S_1 – S_5 мониторинга сбоев (отказов) дефрагментации пакетов на приемнике и адаптации параметров маршрута связи.

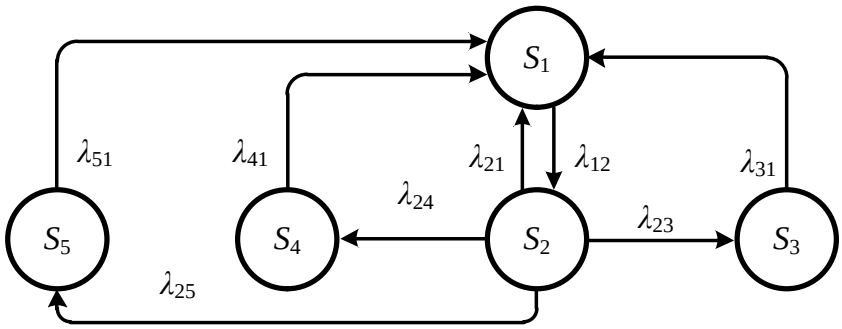

Рис. 2. – Граф состояний процесса мониторинга корректности фрагментации пакетов в СПД

Таблица №1

Дискретные состояния процесса мониторинга корректности фрагментации пакетов в СПД

S_1	Оценка корректности параметров фрагментации, вычисление коэффициента результативности $K_{ij}^{РД}$
S_2	Трассировка маршрутов в ССОП и определение значений *MTU* узлов ССОП (*Path MTU Discovery*)
S_3	Изменение структуры ведомственной СПД вследствие ее масштабирования (подключение новых абонентов)
S_4	Несанкционированные воздействия на процессы фрагментации пакетов
S_5	Изменение структуры сети связи общего пользования (действия операторов связи), непреднамеренные воздействия

Моменты возможных переходов моделируемой СПД при информационном обмене из состояния в состояние неопределенны, случайны и происходят под действием событий, характеризующиеся их интенсивностями λ, являющимися важной характеристикой потоков событий и характеризующими среднее число событий, приходящееся на единицу времени. При построении и использовании математической модели задаются значения интенсивностей событий, перечисленных в таблице №2.

Таблица №2

Интенсивности потоков событий в системе мониторинга СПД

Интенсивность	Обозначение
заявок на трассировку маршрутов в ССОП и определение значений *MTU* узлов ССОП (*Path MTU Discovery*)	λ_{12}
заявок на оценку достоверности определения значений *MTU* узлов ССОП	λ_{21}
заявок на масштабирование структуры СПД связи, вызванное появлением новых абонентов	λ_{23}
целенаправленных деструктивных воздействий злоумышленников	λ_{24}
воздействия случайных (непреднамеренных) помех	λ_{25}
заявок на вычисление коэффициента результативности $K_{ij}^{РД}$ при масштабировании структуры СПД	λ_{31}
заявок на вычисление коэффициента результативности $K_{ij}^{РД}$ при целенаправленных деструктивных воздействиях злоумышленников	λ_{41}
заявок на вычисление коэффициента результативности $K_{ij}^{РД}$ при воздействии случайных (непреднамеренных) помех	λ_{51}

По размеченному графу состояний (рис. 2) согласно правилам, изложенным в [7], составлены уравнения Колмогорова – дифференциальные уравнения с неизвестными функциями $p_i(t)$:

$$\left.\begin{aligned}
\frac{dp_1(t)}{dt} &= \lambda_{21}p_2(t) + \lambda_{31}p_3(t) + \lambda_{41}p_4(t) + \lambda_{51}p_5(t) - \lambda_{12}p_1(t),\\
\frac{dp_2(t)}{dt} &= \lambda_{12}p_1(t) - (\lambda_{21} + \lambda_{23} + \lambda_{24} + \lambda_{25})p_2(t),\\
\frac{dp_3(t)}{dt} &= \lambda_{23}p_2(t) - \lambda_{31}p_3(t),\\
\frac{dp_4(t)}{dt} &= \lambda_{24}p_2(t) - \lambda_{41}p_4(t),\\
\frac{dp_3(t)}{dt} &= \lambda_{25}p_2(t) - \lambda_{51}p_5(t),\\
\sum_{i=1}^{5} p_i(t) &= 1.
\end{aligned}\right\}$$

Данное уравнение – математическая модель процесса мониторинга корректности фрагментации пакетов в ведомственной СПД. Порядок решения таких уравнений известен, и описан, например, в [8]. В процессе решения производится расчет приближенных значений p_i для заданных значений интенсивностей событий $\lambda_{ij} = const$ (марковский однородный процесс), что позволяет получить числовую таблицу искомых решений $p(t)$ на некотором интервале $t \in [t_0, t_1]$. Расчет произведен с помощью пакета математического программирования «*MathCAD* 15».

Вероятностные и временные характеристики, описывающие состояния моделируемого процесса определяются значениями интенсивностей событий λ_{ij}, в зависимости от следующих условий функционирования (ситуаций) СПД.

Ситуация №1 – интенсивности масштабирования структуры СПД и целенаправленных деструктивных воздействий злоумышленников минимальны, $\lambda_{31} = \lambda_{41} = min$, интенсивность воздействия случайных (непреднамеренных) помех постоянна, $\lambda_{51} = const$.

Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующих ситуации №1 представлены на рис. 3.

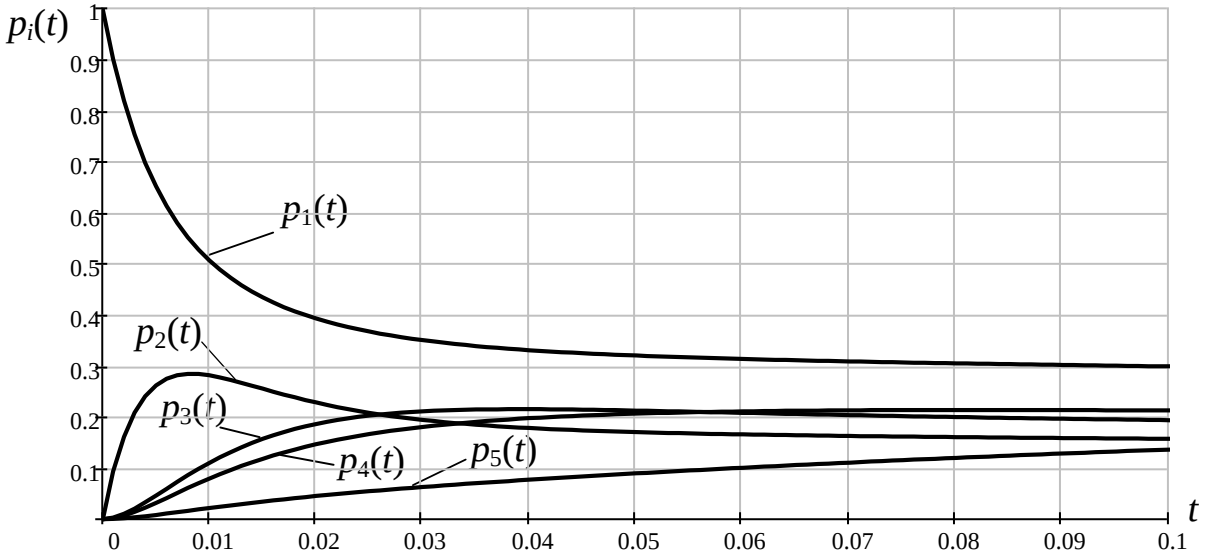

Рис. 3. – Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, ситуация №1

После установления в моделируемой системе стационарного режима финальная вероятность нахождения системы в состоянии S_1 максимальна, регулярное воздействие случайных (непреднамеренных) помех после начального всплеска $p_2(t)$, характеризующего необходимость адаптации параметров маршрута связи за счет инициализации процедуры *Path MTU Discovery*, не приводит к доминированию дестабилизирующих факторов [9].

Ситуация №2 – интенсивность масштабирования структуры СПД постоянна, $\lambda_{31} = const$, интенсивность целенаправленных деструктивных воздействий злоумышленников минимальна, $\lambda_{41} = min$, интенсивность воздействия случайных (непреднамеренных) помех максимальна, $\lambda_{51} = max$.

Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующих ситуации №2, представлены на рис. 4.

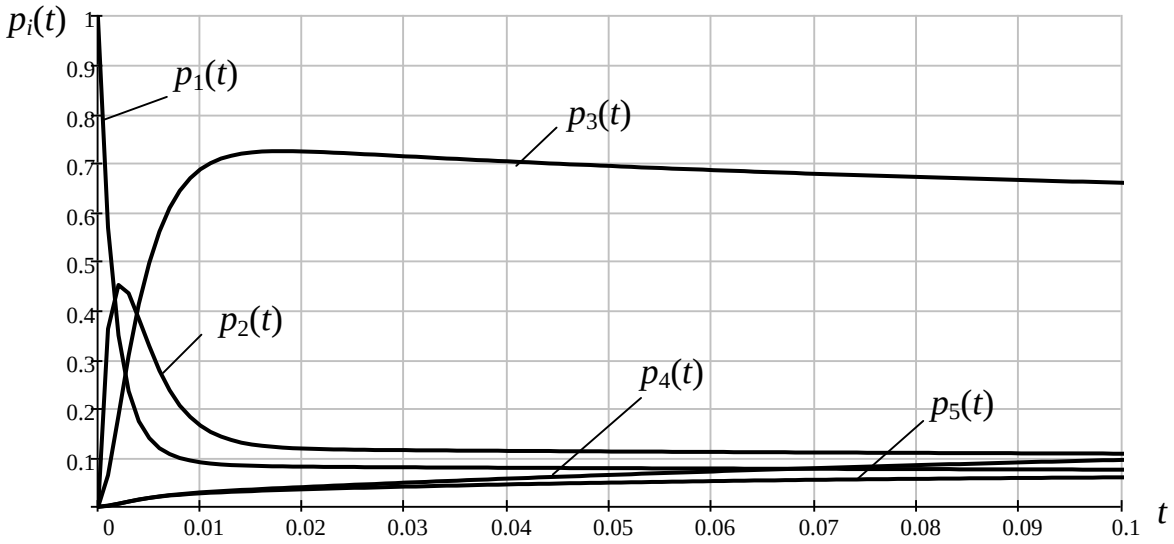

Рис. 4. – Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, ситуация №2

После установления в моделируемой системе стационарного режима финальная вероятность нахождения системы в состоянии S_2 существенно увеличивается, что характеризует адаптацию параметров маршрута связи с целью поиска альтернативного маршрута, свободного от источника помех. Финальная вероятность нахождения системы в состоянии S_1 минимальна. Снижение интенсивности воздействия случайных (непреднамеренных) помех $\lambda_{51} \to min$ приводит к увеличению финальной вероятности нахождения системы в состоянии S_1, то есть к ее адаптации за счет применения процедуры *Path MTU Discovery*. Ухудшение показателя своевременности доставки пакетов сообщений принимающему абоненту при высокой интенсивности дефектных пакетов сообщений устраняется за счет мониторинга интенсивности сбоев (отказов) дефрагментации пакетов сообщений [10].

Таким образом, использованием разработанной модели за счет мониторинга сбоев (отказов) дефрагментации пакетов сообщений и адаптации параметров маршрута связи к изменению структуры (параметров) СПД и сети связи общего пользования, достигают улучшения показателя

своевременного предоставления сервисных возможностей абонентам ведомственных СПД, а также обеспечивают доступность обрабатываемой информации при высокой интенсивности пакетов сообщений с некорректными параметрами фрагментации.

Литература

1. Ворончихин И. С., Иванов И. И., Максимов Р. В., Соколовский С. П. Маскирование структуры распределенных информационных систем в киберпространстве // Вопросы кибербезопасности. 2019. № 6 (34). С. 92-101. doi: 10.21681/2311-3456-2019-6-92-101.

2. Максимов Р. В., Соколовский С. П., Шарифуллин С. Р., Чернолес В. П. Инновационные информационные технологии в контексте обеспечения национальной безопасности государства // Инновации. 2018. № 3 (233). С. 28-35.

3. Request for Comments: 1191. Path MTU Discovery, Draft Standard, 1990. – URL: tools.ietf.org/html/rfc1191

4. Request for Comments: 879. The TSP Maximum Segment Size and Related Topics, 1983. – URL: tools.ietf.org/html/rfc879#section-3

5. Максимов Р. В., Орехов Д. Н., Соколовский С. П. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки // Системы управления, связи и безопасности. 2019. № 4. С. 50-99. doi: 10.24411/2410-9916-2019-10403.

6. Норткан С., Новак Д. Обнаружение нарушений безопасности в сетях, 3-е издание: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 448 с.: ил.

7. Вентцель Е.С., Исследование операций: задачи, принципы, методология. – 2-е изд., стер. – М.: Наука. Гл. ред. физ.-мат. лит., 1988. – 208 с.

8. Вержбицкий В.М., Основы численных методов: Учебник для вузов.. – М.: Высш. Шк., 2002. – 840 с.

9. Куринных Д.Ю., Айдинян А.Р., Цветкова О.Л. Подход к кластеризации угроз информационной безопасности предприятий // Инженерный вестник Дона, 2018, №1 URL: ivdon.ru/magazine/archive/n1y2018/4803.

10. Лыков Н.Ю. Методика управления ресурсами маскираторов информационных направлений распределенных интегрированных инфокоммуникационных систем ведомственного назначения // Инженерный вестник Дона, 2018, №4 URL: ivdon.ru/ru/magazine/archive/n4y2018/5377.

References

1. Voronchixin I. S., Ivanov I. I., Maksimov R. V., Sokolovskij S. P. Voprosy` kiberbezopasnosti. 2019. № 6 (34). pp. 92-101. doi: 10.21681/2311-3456-2019-6-92-101.

2. Maksimov R. V., Sokolovskij S. P., Sharifullin S. R., Chernoles V. P. Innovacii. 2018. № 3 (233). pp. 28-35.

3. Request for Comments: 1191. Path MTU Discovery, Draft Standard, 1990. URL: tools.ietf.org/html/rfc1191.

4. Request for Comments: 879. The TSP Maximum Segment Size and Related Topics, 1983. URL: tools.ietf.org/html/rfc879#section-3.

5. Maksimov R. V., Orexov D. N., Sokolovskij S. P. Sistemy` upravleniya, svyazi i bezopasnosti. 2019. № 4. pp. 50-99. doi: 10.24411/2410-9916-2019-10403.

6. Nortkan S, Novak D. Obnaruzhenie narushenij bezopasnosti v setyax [Network Security Detection], 3-e izdanie.: Per. s angl. M.: Izdatel`skij dom «Vil`yams», 2003. 448 p.

7. Ventcel` E.S., Issledovanie operacij: zadachi, principy`, metodologiya. [Operations research: tasks, principles, methodology]. 2-e izd., ster. M.: Nauka. Gl. red. fiz.-mat. lit., 1988. 208 p.

8. Verzhbiczkij V.M., Osnovy` chislenny`x metodov: Uchebnik dlya vuzov. [Fundamentals of Numerical Methods: Textbook for High Schools]. M.: Vy`ssh. Shk., 2002. 840 p.

9. Kurinny`x D.Yu., Ajdinyan A.R., Czvetkova O.L. Inzhenernyj vestnik Dona, 2018, №1. URL: ivdon.ru/magazine/archive/n1y2018/4803.

10. Ly`kov N.Yu. Inzhenernyj vestnik Dona, 2018, №4. URL: ivdon.ru/ru/magazine/archive/n4y2018/5377.