Подход к способу распределения информационного обмена в сети передачи данных оперативно-технологического назначения

Е. В. Скуднева

Санкт-Петербургский политехнический университет Петра Великого

skykatty@gmail.com

А. А. Привалов, А. М. Болдинов

Петербургский государственный университет путей сообщения Императора Александра I

Аннотация. **Рассмотрен принцип построения подпрограммы распределения информационного обмена в сети передачи данных оперативно-технологического назначения. В статье предложен алгоритм распределения частоты и объема данных во времени между узлами передачи данных. Этот способ является частью методики формирования «информационных портретов» в СПД-ОТН.**

Ключевые слова: информационный обмен, сеть передачи данных

I. Введение

Исследования и разработки в области передовых технологий и способов обеспечения информационной безопасности представляются особенно актуальными в современной геополитической обстановке. Отличительной особенностью сетей передачи данных оперативно-технологического назначения является свойство стационарности распределения частоты и объема передаваемой информации во времени между узлами при нормальной эксплуатации. Таким образом, выявление аномалий и различных отклонений от стационарных значений в сети передачи данных, с высокой вероятностью позволяет обнаруживать злонамеренные воздействия и внештатные ситуации эксплуатации, являющиеся целевыми по применяемым моделям угроз.

Для построения нормального стационарного расчетного состояния существует ряд подходов, которые базируются на особенностях сетей передачи данных. Эти подходы определяются функциональными возможностями оборудования, установленного на узлах, режимом эксплуатации, возможностью выделения сеансового доступа для обмена статистической информации. Рассматриваемая сеть передачи данных оперативно-технологического назначения позволяет организовать такого рода информационный обмен в виду того, что не имеет полной нагрузки. В свободное время между узлами коммутации может осуществляться обмен статистической информацией.

Для исследования особенностей поведения участников информационного обмена и выделения характерных свойств стационарного состояния сетей передачи данных оперативно-технологического назначения при их нормальной эксплуатации коллективом авторов была разработана модель информационного обмена. Эта модель позволяет определить характер работы узлов в ходе информационного обмена с использованием параметров, задаваемых алгоритмом. Исходные данные получены расчетным образом и на основе реальных статистических данных с узлов сети.

II. Описание алгоритма

Для реализации алгоритма построения матриц статистик описывающих сеть передачи данных ОТН в стационарном состоянии при нормальной эксплуатации реализуется посредством генерации тестовой последовательности, рассылки по всей топологии сети и построения матрицы дисперсии временных характеристик передачи данных между узлами. Блок-схема работы алгоритма приведена на рис. 1.

Построение матриц выполняется в три этапа:

На первом этапе вводятся следующие исходные данные

- x – число линий связи, в рассматриваемой модели;
- N – число узлов, рассматриваемой модели;

  матрица A – размерностью [N, N], определяющая маску допустимых информационных обменов между узлами, представляющая собой статическую таблицу маршрутизации в соответствии с общепринятыми технологиями построения сетей передачи данных;
- матрица B [x, 2] – определяет дисперсию времени при заданной скорости на пространстве разрешённых маршрутов передачи потока данных. При этом маршруты упорядочены по возрастанию дисперсии времени.
- $\Delta\varepsilon$ – допустимая погрешность измерений. [1]

На втором этапе (блок 3, рис. 1) осуществляется генерация тестовой последовательности размерности n бит на основе заранее определенного алфавита.

Третий этап (блок 4–8, рис. 1) производится измерение характеристик на основе передачи тестовой последовательности, которые заранее известны на принимающей и передающей стороне. При этом фиксируются значения TTL в заголовке IP-пакета и

производится вычисление дисперсии временных характеристик.

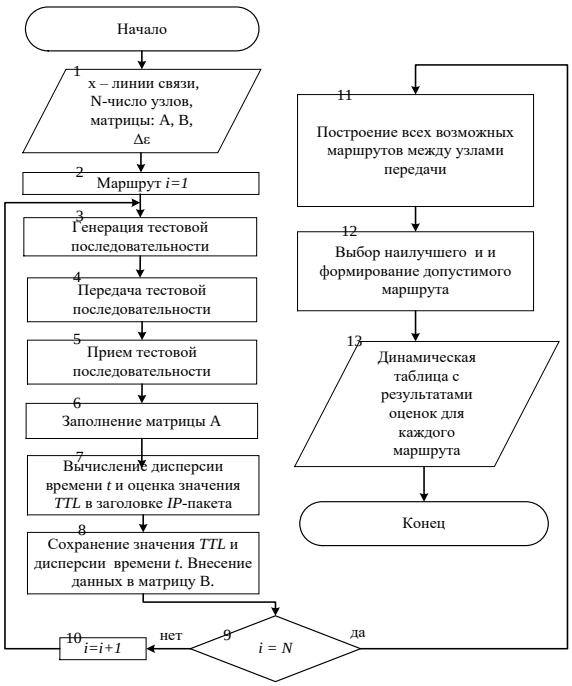

Рис. 1. Блок-схема распределения информационного обмена и формирования динамической таблицы для сети передачи данных

Для обеспечения заданных параметров ошибки эксперимент повторяется необходимое количество раз, значения усредняются между узлами по каждому из допустимых маршрутов. Расчет на каждом шаге производится по (1). [1]

$$\bar{t} = \frac{t_1(B)+t_2(B)+\ldots+t_{N_{\text{общ}}}(B)}{N_{\text{общ}}}, \qquad (1)$$

В результате осредненная дисперсии $\bar{t}$ прохождения пакета всеми известными путями, установленная в результате серии экспериментов определяет информационные портреты характерных видов взаимодействия между определёнными узлами. При нормальном функционировании сети передачи данных ОТН информационные портреты обладают свойством стационарности, сохраняют его во времени и являются теоретической основой высокой эффективности предлагаемого метода.

Созданная программная модель позволяет осуществлять оценку функционирования суперпозиции допустимых информационных портретов. Рассчитывать теоретическими способами пространство допустимых состояний стационарного поведения сети передачи данных ОТН при ее нормальном функционировании.

Расчет суммарной дисперсии времени $t_{\text{п}}$ осуществляется по (2). [2, 3]

$$t_{\text{п}} = \sqrt{{t_1}^2 + {t_2}^2 + \ldots + {t_i}^2}\ , \qquad (2)$$

$t_{\text{iп}}$ – значение времени передачи данных на i-ом участке пути; i – количество участков, по которым проходит поток данных. [1]

Хранение динамической таблицы осуществляется в отсортированном виде по убыванию.

Характеристики всех возможных маршрутов и их суперпозиции получаемые таким образом сохраняются в динамической таблице путей, свойственных режимам эксплуатации исследуемой сети.

В ходе разработки данного подхода коллектив авторов исходит из того, что скорость изменения динамической таблицы мала по отношению к степени повторяемости видов коммуникации возникающих при нормальной эксплуатации сети передачи данных оперативно-технологического назначения.

Таким образом, любая аномалия рассматривается, как потенциальная угроза информационной безопасности или аварийная ситуация. Только при отсутствии подтверждения по указанным двум факторам осуществляется дополнение динамической таблицы путей. Далее формируется модель стационарных характеристик сети передачи данных при её нормальном функционировании, которая пригодна для дальнейшего моделирования различных состояний.

На основе построенной модели осуществляется анализ фактических данных о нагрузках на узлах сети передачи данных ОТН от времени, которые собираются при ее реальной эксплуатации. В рамках сбора статистической информации производится передача системных данных и статистик с узлов в моменты времени с низкой загруженностью сети.

Таким образом, скорость выявления аномалий напрямую зависит от режима эксплуатации и при отсутствии полной загрузки позволяет организовать оперативно-технические меры реагирования в соответствии с применяемой моделью угроз с достаточной эффективностью.

При эксплуатации сети передачи данных ОТН в режимах не позволяющих использовать сеансовое времени для передачи статистик, возможно накопление этой информации на узлах и ретроспективный анализ соответствия статистической информации о происходящей коммуникации допустимым информационным портретам.

При этом данные передаются в аналитический центр в соответствии с организационно методическими решениями принятыми ответственными лицами с отчуждаемых носителей. Аналогичным способом может производиться модельное исследование аномалий по статистикам, сгенерированным с целью совершенствования применяемых алгоритмов.

III. Заключение

Коллективом авторов были использованы собранные данные с участка железнодорожной сети передачи данных оперативно-технологического назначения.

На рис. 2 отображен график, где 95 % процентов трафика сгенерировано на основе допустимых информационных портретов динамической таблицы, а 5 %, как коммуникация двух узлов выбираемых случайным образом. Трафик соответствует реальной среде эксплуатации.

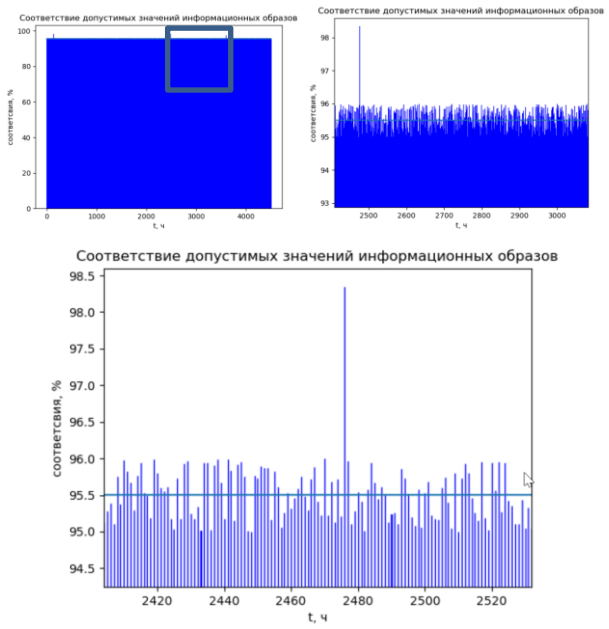

Рис. 1. Соответствие допустимых информационных образов

По оси ординат указано распределение количества данных от времени. Процент соответствия допустимых информационных образов по оси абсцисс.

Полученные результаты подтверждают, что использование методов информационных портретов является высокоэффективной мерой по обеспечению противодействия угрозам в оперативном режиме, в случае использования сети передачи данных оперативно-технологического назначения для передачи статистической информации или в ретроспективном режиме при отсутствии такой возможности.

Таким образом, любое использование таких методов позволяет с высокой степенью достоверности выявлять аномалии и осуществлять реагирование в соответствии с организационно техническими мерами, применяемыми на предприятии.

Список литературы

[1] Скуднева Е.В. Методика маскирования информационного обмена в сетях передачи данных оперативно-технологического назначения ОАО "РЖД": дис. … канд. тех. наук / Государственный университет морского и речного флота имени адмирала С.О. Макарова. СПб.: Изд-во ГУМРФ им. адм. С.О. Макарова, СПб., 2017. 141 с.

[2] Привалов А.А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ. СПб: ВМА, 2000. 166 с.

[3] Юркин Ю.В. Оперативно-технологическая телефонная связь на железнодорожном транспорте: учебник для вузов железнодорожного транспорта / Ю.В. Юркин, А.К. Лебединский, В.А. Прокофьев, И.Д. Блиндер. М.: УМЦ ЖДТ, 2007, 264 с.