DOI: 10.34020/2073-6495-2021-3-031-036
УДК 004.72

МОДЕЛЬ ОТКАЗОУСТОЙЧИВОСТИ ПРОГРАММНО-КОНФИГУРИРУЕМОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Хрусталев С.А.
Российская академия народного хозяйства и государственной службы
при президенте Российской Федерации
E-mail: s.khrustaliov@gmail.com

В публикации рассматривается проблематика проектирования и моделирования отказоустойчивости защищенных программно-конфигурируемых сетей передачи данных. Предлагается методика оценки параметров отказоустойчивости программно-конфигурируемой сети передачи данных. Обоснована организационная модель построения программно-конфигурируемой сети передачи данных на основе проектирования конфигурации по принципу динамической защиты с применением селективной трансформации, учитывающей вероятности сбоев и позволяющей обеспечить высокие заданные параметры отказоустойчивости.

Ключевые слова: инфраструктура вычислительных сетей, безопасность сетевой инфраструктуры, программно-конфигурируемые сети, сети передачи данных, отказоустойчивость, модель отказоустойчивости.

MODEL OF FAILURE RESOLUTION OF SOFTWARE-DEFINED CONFIGURABLE DATA NETWORK

Khrustalyev S.A.
Russian Academy of National Economy and Public Administration
under the President of the Russian Federation
E-mail: s.khrustaliov@gmail.com

The publication deals with the design and modeling of fault tolerance for secured software-defined data transmission networks. A technique for evaluating the parameters of fault tolerance of a software-defined data transmission network is proposed. An organizational model for building a software-configurable data transmission network based on the design of a configuration based on the principle of dynamic protection with the use of selective transformation, taking into account the probability of failures and allowing to ensure high specified parameters of fault tolerance.

Keywords: computer network infrastructure, network infrastructure security, software-defined networks, data transmission networks, fault tolerance, fault tolerance model.

ВВЕДЕНИЕ

В условиях существенного роста загруженности сетей передачи данных, в сочетании с сохранением высокого уровня вероятности реализации рисков злонамеренного вмешательства в их нормальное функционирование, актуализируются аспекты разработки сетевых конфигураций, основанных на неуклонном обеспечении высокой отказоустойчивости работы сетей.

Заявленная проблематика дополнительно усиливается вследствие воздействия пиковых нагрузок на большинство сетей передачи данных в условиях активного использования дистанционных коммуникационных технологий в контексте социальных мер, предпринятых для минимизации угроз и рисков, связанных с пандемией заболеваний, вызванных новой коронавирусной инфекцией COVID-19.

Для достижения соответствующих целей с высокой долей успешности может применяться технология защищенных программно-конфигурируемых сетей передачи данных (ПКС, англ. software-defined networks, SDN) с высокой степенью отказоустойчивости и защищенности от негативных внешних воздействий. Речь идет о перспективных разработках в сфере проектирования сетей и их инфраструктуры, отдельным вопросам которого, а именно разработке организационной модели отказоустойчивости ПКС передачи данных, посвящено настоящее исследование.

ТЕОРЕТИЧЕСКИЙ АНАЛИЗ

Концепция ПКС была сформулирована сравнительно недавно (предложена в исследованиях специалистов Стэнфордского университета M. Casado, N. McKeown в 2007 г. [5]), теоретические и прикладные разработки в данной сфере осуществляются лишь в последнее десятилетие, когда от лабораторных проектов идеи ПКС постепенно переводятся в плоскость практического исполнения, в том числе в промышленных масштабах.

Применение ПКС призвано оказать воздействие на следующие ключевые проблемы классической сетевой архитектуры:

– обеспечение безопасности и отказоустойчивости сетей при росте нагрузок в геометрической прогрессии (проблематика особо актуальна в контексте социальных ограничений в период пандемии и связанных с ними пиковых нагрузок на сети передачи данных;

– проприетарность, закрытость «классических» сетей, затруднения при конфигурации оборудования различных производителей;

– необходимость управления количеством сетевых протоколов и их стеков, что связано, помимо прочего, с обеспечением производительности сети передачи данных на заявленном уровне.

Активное применение SDN-технологий происходит в 2010 годах и по настоящее время, в эпоху цифровизации, и связано с тотальным обеспечением высокой безопасности и отказоустойчивости сетей передачи данных [6]. Особое внимание необходимо уделять вопросам проектирования программно-конфигурируемых сетей, от корректного осуществления которого в немалой степени зависит соответствие ПКС поставленным задачам и заданным параметрам функционирования.

В результате можно констатировать, что исследовательская задача моделирования отказоустойчивости программно-конфигурируемых сетей сводится к решению следующих аспектов:

– выбор релевантного способа математической оценки ключевых параметров отказоустойчивости сети;

– проектирование конфигурации ПКС, обеспечивающее максимально высокие параметры отказоустойчивости.

Соответствующие вопросы стали предметом ряда научных исследований; рассмотрим некоторые из них.

В частности, в публикации [1] предложена математическая модель надежности защищенной распределенной телекоммуникационной сети на основе пакетного контроллера, основанная на связи интенсивности потоков отказов и восстановления и вероятностных аспектов состояния ЗРТС в любой отдельно взятый промежуток времени. В работе [3] предложена математическая модель надежности сетей, которая может быть использована для цели расчета вероятностных значений аварии распределенных сетей передачи данных. В [4] предлагается математическая модель коммутатора ПКС, обеспечивающего управление сетевой конфигурацией с высоким уровнем отказоустойчивости.

Отдельные исследования посвящены вопросам мониторинга отказоустойчивости сетей передачи данных. Э.М. Мехтиев и соавторы [2] предлагают концептуальное решение по организации мониторинга сетевой инфраструктуры и информационных систем на основе модели оценки эффективности выбранного пакета программ, используемых для построения подсистем корпоративной вычислительной сети, включаемых в единый комплекс мониторинга.

R. Sahay., W. Meng, C.D. Jensen [7] предлагают практическое решение по повышению отказоустойчивости ПКС на основе комплексного учета сетевых параметров при анализе вероятности отказов канала.

РЕЗУЛЬТАТЫ

Представляется целесообразным развивать исследования в сфере моделирования отказоустойчивости ПКС на основе совершенствования конфигурации с учетом вероятности отказов. Соответственно, в основе проектирования ПКС должны быть положены математические модели вероятности отказов сети на основе ключевых сетевых параметров. Данные модели должны быть положены в основу цифрового мониторинга состояния сети при управлении сетевой операционной системой.

В качестве варианта решения может быть предложена представленная в [1] модель оценки вероятности безотказной работы ПКС:

$$P(t) = e^{-\int_0^{\tau} \lambda(\tau) d\tau} + c, \quad (1)$$

где t – период времени безотказной работы, $\lambda(\tau)$ – интенсивность потока отказов.

Вероятность безотказной работы ПКС, включающей N элементов, может быть выражена через время работы i-го элемента сети при условии, если поток отказов не меняется во времени, по формуле:

$$P(t) = e^{-t \cdot \sum_{i=1}^{N} \lambda_i}. \quad (2)$$

При большом числе элементов сети и одинаковых значениях вероятности отказов в малые интервалы времени, вероятность безотказной работы

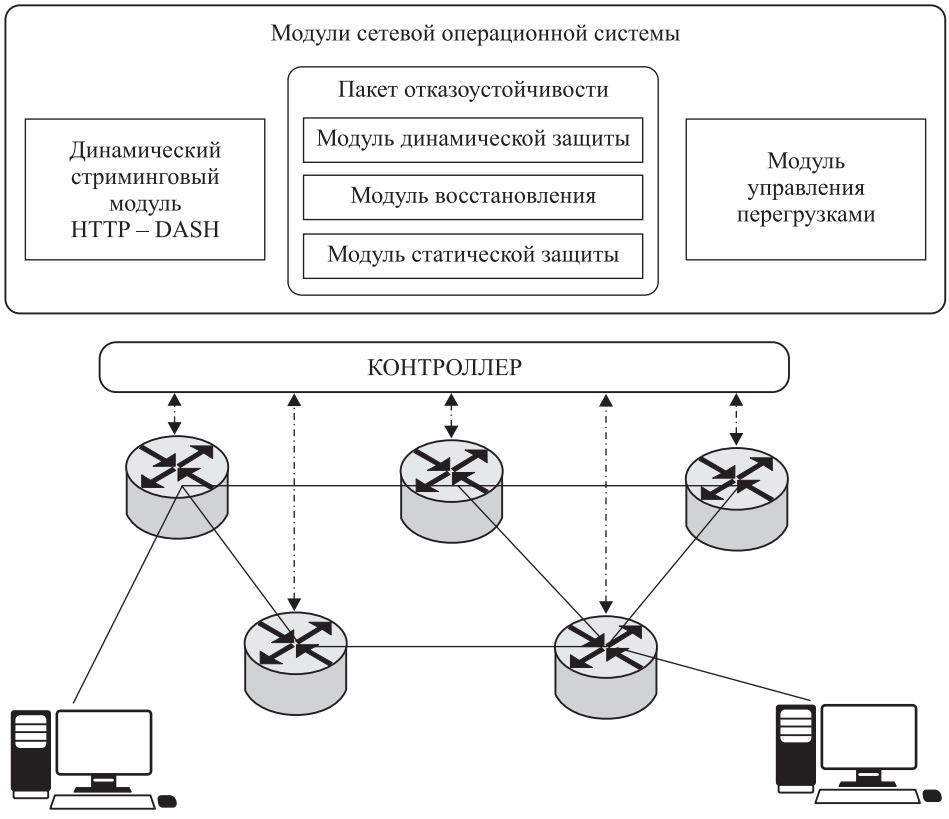
программно-конфигурируемой сети передачи данных может быть определена как

$$P(T_0 > t) = e^{-N\lambda t^a}, \quad (3)$$

где T_0 – время наработки на отказ, a – некоторая положительная величина.

При проектировании с учетом аспектов трансформаций внешней среды функционирования сетей передачи данных должны применяться решения, основанные на тотальной минимизации рисков отказов, за счет применения системы дублирования маршрутов, резервирования емкостей. Соответствующие цели могут быть достигнуты при организации параллельной работы ПКС, организационная модель которой представлена на рисунке.

Предлагаемое решение основано на применении принципа динамической защиты программно-конфигурируемой сети и предполагает применение альтернативных путей передачи данных, задействуемых при отказах элементов сети. Учитывается такой аспект перегрузки сетевого трафика, несбалансированного по времени, как кеширование стриминговых потоков, связанное с активным использованием стриминговых сервисов в развлекательных целях и в контексте осуществления удаленных коммуникаций. Модуль динамической защиты обеспечивает конфигурацию альтернативных путей передачи данных на основе прогнозирования вероятности отказов,



Организационный дизайн отказоустойчивости ПКС на основе параллельной работы элементов сети передачи данных

в том числе с учетом сетевого трафика. Выбор производится в пользу наилучших по качеству альтернативных путей передачи данных.

Модуль статической защиты также предназначен для резервирования путей на случай отказа. Модуль значительно снижает нагрузку на сам контроллер, но автоматическое переключение на альтернативные пути, в отличие от модуля динамической защиты, происходить не будет. В условиях сети передачи данных с большим количеством контроллеров такой метод не будет эффективен с точки зрения отказоустойчивости.

Модуль восстановления характеризуется тем, что информация о сбое связи принимается контроллером в качестве события. На основе этой информации определяется текущее состояние сети для вычисления нового маршрута на основе наименьшего количества переходов для потоков в связи со сбоем.

ОБСУЖДЕНИЕ

Высокая отказоустойчивость защищенных корпоративных и иных сетей передачи данных, конфигурируемых на основе SDN-технологии при их проектировании, обеспечивается за счет реализации принципов, отличающих программно-конфигурируемые сети от классической сетевой архитектуры:

– разделение функций (уровня) управления данными и передачи данных в сети;

– применение принципа управления сетью OpenFlow. Объединение коммутаторов и маршрутизаторов под общим управлением сетевой операционной системы, обеспечивающей непрерывный мониторинг сетевой конфигурации, а также доступ, управление сетью, принятие интеллектуальных решений по маршрутизации;

– оптимизация продвижения пакетов данных через центральный контроллер, управляющий потоками на основе комплексной достоверной информации о типологии и структуре сети;

– коммутация через контроллеры с применением уникальных таблиц коммутации – FlowTable;

– возможность успешного применения сетевого оборудования различных поставщиков без, в частности, рисков конфликта такого оборудования.

Предлагаемое решение обеспечивает ожидаемый высокий заданный уровень отказоустойчивости сети передачи данных за счет сочетания SDN-технологий и их конфигурации на основе вероятностных моделей отказов сети. Этой цели должны способствовать конфигурационные решения в сфере динамической защиты ПКС, основанные на принципах расширения дублирования, резервирования, параллельной работы элементов сети.

ЗАКЛЮЧЕНИЕ

Обеспечение надежности сетей передачи данных в современных условиях беспрецедентного роста сетевого трафика и прочих нагрузок на сеть в сочетании с сохраняющимися угрозами злонамеренного вмешательства в функционирование сетей представляется возможным на основе технологий ПКС, активно разрабатываемых и совершенствуемых в настоящее время.

При проектировании с учетом аспектов трансформаций внешней среды функционирования сетей передачи данных должны применяться решения, основанные на тотальной минимизации рисков отказов, за счет применения системы дублирования маршрутов, резервирования, параллельной работы ПКС, составляющих основу принципа динамической защиты сети.

Литература

1. *Крайнов А.Ю., Мещеряков Р.В., Шелупанов А.А*. Модель надежности передачи информации в защищенной распределенной телекоммуникационной сети // Известия Томского политехнического университета. 2008. Т. 313. № 5. С. 60–63.
2. *Мехтиев Э.М., Комагоров В.П., Фофанов О.Б., Марчуков А.В*. К вопросу о проектировании системы мониторинга корпоративной вычислительной сети // Доклады ТУСУР. 2012. № 2-1 (26). С. 184–188.
3. *Перегуда А.И., Перегуда А.А., Тимашев Д.А*. Математическая модель надежности компьютерных сетей // Надежность. 2013. № 4. С. 18–30.
4. *Самуйлов К.Е., Шалимов И.А., Бужин И.Г, Миронов Ю.Б*. Модель функционирования телекоммуникационного оборудования программно-конфигурируемых сетей // Современные информационные технологии и ИТ-образование. 2018. Т. 14. № 1. С. 13–26.
5. *Casado M. et al*. Ethane: Taking control of the enterprise // ACM SIGCOMM computer communication review. 2007. Vol. 37. № 4. P. 1–12.
6. *Feamster N., Rexford J., Zegura E*. The road to SDN: an intellectual history of programmable networks // ACM SIGCOMM Computer Communication Review. 2014. Vol. 44. № 2. P. 87–98.
7. *Sahay R., Meng W., Jensen C.D*. The application of Software Defined Networking on securing computer networks: a survey // Journal of Network and Computer Applications. 2019. Vol. 131. P. 89–108.

Bibliography

1. *Krajnov A.Ju., Meshherjakov R.V., Shelupanov A.A*. Model' nadezhnosti peredachi informacii v zashhishhennoj raspredelennoj telekommunikacionnoj seti // Izvestija Tomskogo politehnicheskogo universiteta. 2008. T. 313. № 5. P. 60–63.
2. *Mehtiev Je.M., Komagorov V.P., Fofanov O.B., Marchukov A.V*. K voprosu o proektirovanii sistemy monitoringa korporativnoj vychislitel'noj seti // Doklady TUSUR. 2012. № 2-1 (26). P. 184–188.
3. *Pereguda A.I., Pereguda A.A., Timashev D.A*. Matematicheskaja model' nadezhnosti komp'juternyh setej // Nadezhnost'. 2013. № 4. P. 18–30.
4. *Samujlov K.E., Shalimov I.A., Buzhin I.G., Mironov Ju.B*. Model' funkcionirovanija telekommunikacionnogo oborudovanija programmno-konfiguriruemyh setej // Sovremennye informacionnye tehnologii i IT-obrazovanie. 2018. T. 14. № 1. P. 13–26.
5. *Casado M. et al*. Ethane: Taking control of the enterprise // ACM SIGCOMM computer communication review. 2007. Vol. 37. № 4. P. 1–12.
6. *Feamster N., Rexford J., Zegura E*. The road to SDN: an intellectual history of programmable networks // ACM SIGCOMM Computer Communication Review. 2014. Vol. 44. № 2. P. 87–98.
7. *Sahay R., Meng W., Jensen C.D*. The application of Software Defined Networking on securing computer networks: a survey // Journal of Network and Computer Applications. 2019. Vol. 131. P. 89–108.