

- немного вершин (концентраторов) имеют большое количество связей, а большинство вершин имеют лишь несколько связей, рис. 2. Такая структура довольно типична для распределенной информационно-телекоммуникационной системы с пакетной передачей данных для труднодоступных объектов, которая соединяет множества узлов связи, используя концентраторы (например, АПК-КРС) в качестве промежуточных станций для соединения маршрутов, рис. 1.
4. Важное отличие между экспоненциальной и безмасштабной сетью — это различная реакция на повреждение. Под повреждением понимает-

ся устранение некоторых вершин и всех связей, идущих от вершины. Интуитивно ясно, что безмасштабные сети весьма устойчивы по отношению к случайным повреждениям, однако очень чувствительны к намеренным повреждениям, направленным на концентраторы, которые приводят к разрушению большого количества связей и нарушению взаимодействия между различными частями сети. Если агрессивное воздействие будет направлено на уничтожение концентраторов, то даже если устранить менее 10 % таких узлов, сеть связи распадется на несвязанные между собой кластеры.

СПИСОК ЛИТЕРАТУРЫ

1. Бусленко Н.П. Моделирование сложных систем. — М.: Наука, 1978. — 400 с.
2. Сонькин М.А., Слядников Е.Е. Архитектура и общая технология функционирования территориально распределенных аппаратно-программных комплексов с пакетной передачей данных // Известия Томского политехнического университета. — 2006. — Т. 309. — № 5. — С. 131–139.
3. Сонькин М.А., Слядников Е.Е. Об одном подходе к оптимизации функционирования многоканальной системы связи для труднодоступных объектов // Вычислительные технологии. — 2007. — Т. 12. — Спец. вып. 1. — С. 17–22.
4. Watts D.J., Strogatz S.H. Collective dynamics Small-World Networks // Nature. — 1998. — V. 393. — № 4. — P. 440–442.
5. Хакен Г. Синергетика. — М.: Мир, 1980. — 404 с.

Поступила 30.09.2008 г.

УДК 004.056.55

МОДЕЛЬ НАДЕЖНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В ЗАЩИЩЕННОЙ РАСПРЕДЕЛЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

А.Ю. Крайнов, Р.В. Мещеряков*, А.А. Шелупанов**

Томский государственный университет

*Томский государственный университет систем управления и радиоэлектроники

**Томский научный центр СО РАН

E-mail: office@security.tomsk.ru

Рассмотрены подходы к построению модели надежности защищенности распределенной телекоммуникационной сети. Предлагается использовать классическую теорию надежности для формирования показателей качества работы системы.

Ключевые слова:

Надежность, критерий, защищенная сеть, телекоммуникационная система.

Разрабатываемая сеть на основе пакетного контроллера [1] предполагает проектирование на концептуальном уровне и формирование некоторой модели распределения узлов обработки и передачи данных. В виду того, что предполагаемое использование сети определяется обработкой сведений ограниченного распространения, требуется повышенное внимание к защищенности и надежности функционирования сети, обеспечению информационной безопасности.

При создании сложной иерархической структуры распределенной сети передачи данных необходимо уделить большое внимание надежности ее работы [2]. Принципиальным моментом является то,

что в условиях значительной удаленности населенных пунктов, отсутствия развитой инфраструктуры нет возможности заменить или быстро наладить сеть. Проектируемая сеть, как правило, может работать в режимах «точка-точка» и «центр — широковещательная передача из центра».

Рассматривая схемы по повышению надежности, можно выделить следующие из них, которые подходят для построения надежной распределенной сети передачи данных:

- параллельная работа;
- дублирование;
- резервирование.

Под параллельной работой подразумевается создание в регионе по крайней мере двух центров, работающих независимо друг от друга, с одинаковыми правилами резервирования аппаратуры, архивирования и хранения данных, а также согласованных регламентных мероприятиях по взаимодействию между ними, предполагающих координацию действий по развертыванию подчиненных центров на уровне компетентностного подхода, а также отлаженного четкого механизма взаимодействия.

Дублирование – параллельная работа центров и клиентских мест независимо друг от друга с обменом базами данных по единым правилам резервирования аппаратуры, архивирования и хранения данных.

Резервирование – создание в регионе двух центров с одинаковыми правилами работы резервирования аппаратуры и архивирования и хранения данных. Работа ведется основным центром, резервный центр работает в случае отказа основного.

Очевидно, что программно-аппаратную часть центра следует рассматривать как электронно-вычислительную систему, имеющей те же особенности, что и данного вида система.

При проектировании распределенной сети особо выделяются работы по исследованию и обеспечению надежности, которые должны иметь единое руководство и четко планироваться. В процессе проектирования непрерывно анализируются характеристики надежности компонент и прогнозируется надежность системы сети передачи данных в целом [3, 4].

Ошибки часто носят субъективный характер и их трудно формализовать. Для описания ошибок необходимо изучать факторы, влияющие на их появление, и принимать возможные предупредительные меры против их возникновения на всех стадиях разработки аппаратуры и программного обеспечения. Это позволяет использовать приближенные методы расчета показателей надежности системы сети передачи данных. Строгие методы не удастся применять из-за отсутствия достоверных исходных данных. Проблема обеспечения и расчета надежности может быть решена для сложных систем на основе системного анализа [5, 6].

Вероятность безотказной работы $P(t)$ есть функция времени, это вероятность того, что при заданных условиях эксплуатации в течение времени t не возникнет отказ:

$$P(t) = P(T \geq t),$$

где T – период работы системы.

Тогда вероятность отказа:

$$Q(t) = P(T < t) = 1 - P(t).$$

Свяжем среднее число отказов $n(\Delta t)$, произошедшее за малый интервал времени Δt , с количеством элементов системы N_0 и вероятностью безотказной работы $P(t)$:

$$\begin{aligned} n(\Delta t) &= N_0 \cdot P(t) - N_0 \cdot P(t + \Delta t) = \\ &= N_0 \cdot (P(t) - P(t + \Delta t)), \end{aligned}$$

разделив это выражение на Δt , получим количество отказов в единицу времени:

$$\frac{n(\Delta t)}{\Delta t} = N_0 \cdot \left[\frac{P(t) - P(t + \Delta t)}{\Delta t} \right],$$

но $(P(t) - P(t + \Delta t))/\Delta t$ при $\Delta t \rightarrow 0$ есть производная $-P'(t)$, или, если речь идет надежности – это частота отказов:

$$a(t) = -P'(t).$$

Частота отказов $a(t)$ определяется как:

$$a(t) = Q'(t) = -P'(t),$$

отсюда:

$$P(t) = \int_0^{\infty} a(t) dt.$$

Количество отказов за время Δt составит:

$$n(\Delta t) = N_0 \cdot a(t) \cdot \Delta t.$$

Для пуассоновского распределения длительность интервалов наступления событий есть случайная величина с плотностью распределения $f(x) = \lambda e^{-\lambda x}$, где:

- первый момент $M(x) = 1/\lambda$,
- второй момент $D(x) = 1/\lambda^2$.

Среднее время безотказной работы:

$$T_0 = M[T_0] = \int a(t) \cdot t dt.$$

Отказы обычно характеризуются интегральным критерием – интенсивностью потока отказов $\lambda(t)$:

$$\lambda(t) = \frac{a(t)}{P(t)} = -\frac{P'(t)}{P(t)} = \frac{d \cdot \ln P(t)}{dt},$$

отсюда вероятность безотказной работы:

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

при $t=0$ вероятность того, что система исправна $P(0)=1$, и, следовательно, $c=0$.

Если допустить, что $\lambda(\tau) = \text{const}$, то

$$P(t) = e^{-\lambda t}.$$

Время наработки на отказ составит:

$$T(t) = \frac{t}{N(t)},$$

где $N(t)$ – среднее число отказов за время t .

При условии постоянства потока отказов (что справедливо во многих случаях), т. е. $\lambda = \text{const}$, среднее время наработки на отказ можно определить как:

$$T_0 = M[T_0] = \frac{1}{\lambda},$$

Предположим, что сеть передачи данных исправно работала в момент времени t_0 . Вероятность безотказной работы в течение времени t после этого представляет собой условную вероятность:

$$P(t_0, t) = P(T \geq t_0 + \frac{t}{T} \geq t_0),$$

она определяется из выражения:

$$P(t_0 + t) = P(t_0) \cdot P(t_0, t), \quad (2)$$

откуда следует

$$P(t_0, t) = \frac{P(t_0 + t)}{P(t_0)}.$$

Оценим вероятность отказа в интервале времени от t до $t + \Delta t$, если сеть передачи данных до момента времени t была исправна:

$$Q(t < T < t + \frac{\Delta t}{T} > t) = 1 - P(t, \Delta t) = 1 - \frac{P(t + \Delta t)}{P(t)}, \quad (3)$$

отсюда:
$$Q(\Delta t) = \frac{P(t) - P(t + \Delta t)}{P(t)},$$

или
$$Q(\Delta t) = \frac{P(t) - P(t + \Delta t)}{\Delta t \cdot P(t)} \cdot \Delta t = -\frac{P'(t)}{P(t)} \cdot \Delta t.$$

Но из выражения (3) следует:

$$Q(\Delta t) = \frac{a(t) \cdot \Delta t}{P(t)},$$

учитывая, что $a(t) = \lambda P(t)$, получим:

$$Q(\Delta t) \approx \lambda \cdot \Delta t.$$

Таким образом, предложенная методология позволяет получать искомые оценки.

Сеть передачи данных состоит из многих элементов на каждом уровне ее анализа. Если время работы i -го элемента характеризуется интенсивностью потока отказов $\lambda_i(t)$, то из выражений (1) и (2) следует, что вероятность правильной работы определится как:

$$P_i(t) = 1 - \int_0^t \lambda_i(\tau) \cdot e^{-\lambda_i \tau} d\tau.$$

В предположении, что поток отказов не меняется во времени, вероятность безотказной работы сети, содержащей N элементов в сети, составит:

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

Выход из строя одного элемента сети означает общий отказ. Тогда время наработки на отказ сети:

$$T_0 = \min\{T_{0i}\}, \quad i=1, \dots, N,$$

т. к. $T_0 > t$ в случае, если любое $T_{0i} > t$, то вероятность безотказной работы сети:

$$P(t) = \prod_{i=1}^N P_i(t).$$

Если предположить, что надежность всех клиентских мест сети одинакова и время наработки на отказ одного элемента много больше, чем всей сети, можно полагать, что при малых t вероятность отказа составит:

$$Q_{0i}(t) \approx \lambda \cdot t^a,$$

где $a > 0$ – некоторая положительная величина.

Вероятность правильной работы определится как

$$P(T_0 > t) = P(T_{0i} > t, i=1, \dots, N)$$

или
$$P(T_0 > t) = \prod_{i=1}^N (1 - F_{0i}).$$

Тогда при больших N и одинаковых $Q_{0i}(t)$ $P(T_0 > t) = [1 - NQ_{0i}(t)] \approx e^{-N \cdot Q_{0i}(t)}$, или вероятность безотказной работы сети из N элементов можно записать как:

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

Ремонтопригодность сети оценивается средним временем восстановления работоспособности после отказа – T_w .

Поскольку сеть занимается переработкой и передаче информации, то целесообразно использовать понятие «Достоверность». Достоверность оценивается средним временем наработки на один сбой T_s .

Время восстановления после сбоя складывается из времени идентификации ошибки, времени фиксации сбоя (для набора статистики) и времени рестарта. Это случайная величина с заданной функцией распределения [3]:

$$F_s(t) = P(T_s < t) \quad (4)$$

и плотностью распределения:

$$f_s(t) = \frac{dF_s(t)}{dt}. \quad (5)$$

Восстанавливаемость оценивается средним временем восстановления вычислительного процесса после сбоя (математическое ожидание T_s). Интенсивность потока восстановления μ_s – условная плотность распределения вероятностей времени до восстановления абонентского пункта при условии, что до времени t он был неработоспособен.

Можно считать, что T_s – случайная величина с экспоненциальным распределением и с постоянной интенсивностью:

$$f_s(t) = \mu_s e^{-\mu_s t}. \quad (6)$$

Среднее время восстановления после сбоя сети:

$$T_s = M[T_s] = \int_0^{\infty} t \mu_s e^{-\mu_s t} dt \quad \text{или} \quad T_s = \frac{1}{\mu_s}.$$

Время восстановления сети после сбоя зависит от времени поиска неисправности t_n и времени ее устранения t_u .

$$T_w = t_n + t_u.$$

При профилактических испытаниях увеличивается время наработки на отказ. Эффективность профилактики можно оценить как:

$$E_p = \frac{T_{op}}{T_0},$$

где T_{op} – время наработки на отказ при профилактике.

Коэффициент результативности профилактики:

$$K_p = \frac{N_p}{(N_p + N_r)}$$

Значения E_p и K_p зависят от периодичности и объема профилактических работ.

Проведем оценку вероятности нахождения сети в исправном состоянии при наличии потоков отказов и восстановления. Пусть λ_0 – параметр экспоненциального распределения длительности времени между двумя отказами; μ_w – аналогичный параметр для процесса восстановления и времени ожидания ремонта; $P_0(t)$ – вероятность нахождения сети в исправном состоянии; в начальный момент времени $P_0(0)=1$; $P_1(t)$ – вероятность нахождения сети в неисправном состоянии. Вычислим вероятность нахождения сети в исправном состоянии через малое время Δt .

Вероятность нахождения в работоспособном состоянии исправной сети в начальный момент времени составит, согласно (2):

$$P_0(t + \Delta t) = P_0(t) \cdot e^{-\lambda_0 \cdot \Delta t}, \quad (7)$$

а для неисправной:

$$P(t + \Delta t) = P_1(t) \cdot (1 - e^{-\mu_w \cdot \Delta t}),$$

Итоговая вероятность:

$$P(t + \Delta t) = P_0(t + \Delta t) + P(t + \Delta t) = 1. \quad (8)$$

При малых Δt в соответствии с (7) можно записать:

$$e^{-\lambda_0 \Delta t} \approx 1 - \lambda_0 \Delta t,$$

$$e^{-\mu_w \Delta t} \approx 1 - \mu_w \Delta t.$$

Подставляя (5) и (6) в (8), получим:

$$P_0(t + \Delta t) = P(t) - \lambda_0 \cdot \Delta t \cdot P_0(t) + \mu_w P_1(t) \cdot \Delta t,$$

разделим на Δt :

$$\frac{P(t + \Delta t) - P(t)}{\Delta t} = -\lambda_0 \cdot P_0(t) + \mu_w P_1(t),$$

или при малых Δt :

$$\frac{dP(t)}{dt} = -\lambda_0 \cdot P_0(t) + \mu_w P_1(t).$$

Учитывая, что $P_0(t) + P_1(t) = 1$, получим в итоге уравнение Колмогорова:

$$\frac{dP_0(t)}{dt} = -[\lambda_0 + \mu_w] \cdot P_0(t) + \mu_w.$$

Аналитическое решение уравнения Колмогорова имеет вид:

$$P_0(t) = \frac{\mu_w}{\lambda_0 + \mu_w} \cdot [1 - e^{-(\lambda_0 + \mu_w)t}] + P_0(0) \cdot e^{-(\lambda_0 + \mu_w)t}.$$

При достаточно больших значениях t и постоянных во времени потоках отказов и восстановлений вероятность нахождения сети в исправном состоянии:

$$P_0 = \frac{\mu_w}{\lambda_0 + \mu_w},$$

в неисправном:

$$P_1 = \frac{\lambda_0}{\lambda_0 + \mu_w}.$$

Учитывая связь интенсивности потоков отказов и восстановления, а также вероятность состояния сети в произвольный момент времени t , получим:

$$P_0(t) = \frac{\left(\frac{1}{T_w}\right)}{\left(\frac{1}{T_0} + \frac{1}{T_w}\right)} = \frac{T_0}{T_w + T_0}. \quad (9)$$

Выводы

По разработанной модели надежности передачи информации в защищенной распределенной телекоммуникационной сети можно сформулировать систему требований к элементам сети как элементарным компонентам. Это требует выполнения критериев увеличения времени нахождения сети в работоспособном состоянии (4), (5), (7), (9), что приводит к обоснованию последовательного использования средств повышения надежности элементов сети и, как следствие, получению новых связей в этой сети. Очевидно, что конкретные требования в защищенной телекоммуникационной сети формулируются на основе системообразующих требований при оценке каждого элемента сети.

Работа выполнена при финансовой поддержке СО РАН (код проекта 1.10 «Разработка методов и средств создания распределенных информационно-телекоммуникационных систем» согласно постановления Президиума СО РАН № 54 от 09.02.2006).

СПИСОК ЛИТЕРАТУРЫ

1. Мешеряков Р.В., Росошек С.К., Шелупанов А.А., Сонькин М.А. Защищенная сеть передачи данных на основе пакетного контроллера // Вестник Сибирского государственного аэрокосмического университета им. акад. М.Ф. Решетнева. – 2006. – № 3 (10). – С. 171–175.
2. Мешеряков Р.В., Шелупанов А.А., Белов Е.Б., Лось В.П. Основы информационной безопасности. – М.: Горячая линия-Телеком, 2006. – 544 с.
3. Давыдов П.С. Техническая диагностика радиоэлектронных устройств и систем. – М.: Радио и связь, 1988. – 256 с.: ил.

4. Липаев В.В. Надежность программного обеспечения АСУ. – М.: Энергоиздат, 1981. – 240 с., ил.
5. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации. – М.: Гелеос АРВ, 2005. – 224 с.
6. Перегудов Ф.И., Тарасенко Ф.П. Основы системного анализа. – Томск: Изд-во ТГУ, 1997. – 396 с.

Поступила 23.10.2008 г.