УДК 004.728.49(045)

Жуков И.А., д-р техн. наук
Дрововозов В.И., канд. техн. наук

СПОСОБЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ СБОРА ИНФОРМАЦИИ В СИСТЕМАХ УПРАВЛЕНИЯ РЕАЛЬНОГО ВРЕМЕНИ

Институт компьютерных технологий
Национального авиационного университета

Рассмотрено использование гибридной многопроходной схемы сбора информации в системах управления реального времени, которая позволяет повысить уровень безопасности и надежности обмена информацией в беспроводной сенсорной сети. Предложены способы повышения надежности и безопасности сбора информации

Введение

Системой управления реального времени называется система, быстродействие функционирования которой адекватно скорости протекания физических процессов на объектах контроля или управления. При этом имеются ввиду те процессы, которые непосредственно связаны с функциями, выполняемыми конкретной системой реального времени. То есть система управления осуществляет сбор и передачу данных, производит их обработку в соответствии с заданными алгоритмами и формирует и выдает управляющие воздействия за такой промежуток времени, который обеспечивает успешное решение поставленных перед системой задач. Быстродействие системы реального времени должно быть тем больше, чем больше скорость протекания процессов на объектах контроля и управления. Большинство систем управления технологическими процессами относятся к так называемым системам «жесткого» реального времени, в которых неспособность обеспечения реакции на какие либо события в заданное время обычно приводит к невозможности решения поставленной задачи. Для своевременной выработки управляющих воздействий в системах «жесткого» реального времени крайне важно обеспечение необходимого уровня надежности и безопасности сбора информации и ее передачи в центр обработки и управления системы.

Постановка проблемы

Специальные авиационные и ракетно-космические, транспортные, энергетические и другие системы относятся к информационно-управляющим системам критического применения (ИУС КП). Вполне естественно отнести к ИУС КП системы навигации и управления воздушным движением (УВД). Такие системы работают в экстремальных условиях, непрерывно в течение всего периода эксплуатации управляемого объекта и, как правило, информационный обмен в них осуществляется в реальном времени. Поэтому требования к надежности, живучести, безопасности и производительности сбора и сетей передачи данных в ИУС КП значительно выше, чем в обычных производственных или коммерческих системах. Перепады вычислительной и сетевой нагрузки в ИУС КП при возникновении нештатных ситуаций достигают нескольких порядков. Простое увеличение ресурсов системы дает эффект только на короткое время – при внедрении новых приложений, повышении степени автоматизации систем УВД эти ресурсы истощаются. Автоматизированные системы УВД (АС УВД), имеют большое разнообразие (как по числу, так и по качеству) звеньев прохождения информации (в том числе и каналов передачи данных) и различную достоверность информации в каждом из этих звеньев. Некоторые звенья АС УВД, такие как комплексы обработки различных видов информации (радиолокационной, плановой, метеорологической и др.), должны иметь свои вычислительные сети и ресурсы. Раздельное проектирование каждого из звеньев АС УВД приводит к излишней избыточности всей системы и

ухудшению показателей безопасности из-за увеличения числа аппаратуры, завышению требований к надежности или помехоустойчивости отдельных узлов и звеньев системы, к техническим параметрам (в том числе ресурсам) вычислительных средств. Поэтому необходимо выработать системный подход к проектированию, который позволит повысить эффективность и качество работы АС УВД. Одним из принципов такого подхода может быть использование разделения средств и систем сбора и передачи информации, перераспределение вычислительных ресурсов как внутри сети, где возникла критическая ситуация, так и между сетями [1, 12, 13, 14].

Использование различных систем и средств сбора и передачи информации осуществляет определенную степень дублирования (в ИУС КП такое дублирование предусмотрено) и всегда обеспечивает повышение уровня надежности систем сбора и передачи информации в центр управления ИУС КП. При этом, решая задачу повышения уровня надежности функционирования каждой из систем, можно обеспечить требуемый уровень надежности и безопасности сбора и передачи информации для конкретной ИУС КП.

Пути решения проблемы

Внедрение беспроводных сенсорных сетей (БСС) в системах управления реального времени является одним из способов решения задачи повышения надежности и безопасности сбора информации в системах управления реального времени. БСС состоит из большого количества датчиков, с помощью которых осуществляется сбор информации для решения задач управления в реальном времени внутри определенной области и может обеспечить решения многих задач сбора и передачи информации в ИУС КП. Хотя некоторые технологии беспроводных сетей *ad hoc* (*MANET*) применимы к БСС, однако БСС отличаются от мобильных сетей *ad hoc* во многих аспектах.

Важными задачами, которые должны решаться в БСС, являются задачи обеспечения необходимого уровня надежности при сборе и передаче информации и обеспечения соответствующего уровня защиты информации, поскольку беспроводная передача информации между узлами доступна для многих видов вмешательств. Наиболее эффективной стратегией повышения надежности является многопроходное рассредоточение трафика [2].

Для решения задачи более надежного и более безопасного сбора данных в БСС предлагается гибридная многопутевая схема с использованием нового распределенного протокола многопроходного обнаружения *N-to*-1 (*multipath discovery protocol*). В то время как большинство протоколов многопутевой маршрутизации инициализированы источником и стремятся находить многократные непересекающиеся или частично непересекающиеся дорожки между единственной парой исходных адресатов, многопутевой *N-to*-1 протокол обнаружения инициализирован получателем (то есть, инициализирован БС) и находит каждый узел датчика и набор непересекающихся дорожек к БС одновременно в конце одного процесса обнаружения маршрута.

Это очень эффективно со средним распределением меньше одного направленного сообщения на один путь. Результаты исследования гибридной многопутевой схемы сбора данных, объединяющей постоянное параллельное многопутевое рассредоточение для сбора данных сквозного шифрования и маршрутизацию обходными путями для каждой отдельной передачи пакета, показывают, что гибридная схема *Hybrid-SPREAD* (*H-SPREAD*) может достигнуть значительно лучшей надежности и безопасности с малой избыточностью или даже отсутствием таковой. Предлагаемая схема БСС является чрезвычайно удобной для БСС, где главная задача – одновременный сбор данных от всех узлов датчиков для базовой станции.

Для повышения уровня надежности можно использовать множество кодирующих схем для уменьшения трафика при многопутевой маршрутизации. В качестве примера можно привести код Ри-

да-Соломона, разнесенный прием кодирования [4], кодирование многократного описания и т.д. В схеме распространения *SPREAD* [3] используется схема порогового способа разделения секрета для разбиения информации. Схема порогового способа разделения секрета *threshold secret sharing scheme* (*T, N*) делит информацию на оптимальное количество частей *N*, названных долями (*shares or shadows*). Хорошим качеством долей *N* является то, что, имея любое количество частей менее *T*, нельзя получить никаких данных о сути информационного содержания, в то время как, используя эффективный алгоритм, можно восстановить информацию, имея любое количество *T* из долей *N*. В схеме гибридного распространения *H-SPREAD*, выбран метод разделения секрета как схема кодирования.

Сделаем оценку надежности предлагаемой схемы сбора информации. Определим насколько надежно, сгенерированное с требуемой степенью надежности сообщение в одном узле датчика, может быть доставлено к базовой станции (БС). Фактически, в сети БСС, и узлы датчика и беспроводные связи подвержены ошибкам. Отказ узла может быть вызван физической неисправностью узла или тяжелой перегрузкой в узле, что вызывает потерю пакета в связи с буферным переполнением. Отказ связи может быть вызван проблемой конкуренции доступа, вмешательством множества пользователей или любым вмешательством, которое вызывает радиосигнал, неправильно декодируемый предназначенным получателем. Если предположить, что каждый узел имеет равную вероятность p_{n0} передачи пакета с необходимой степенью надежности, и каждая связь имеет равную вероятность p_{l0} степени надежности доставки пакета, то вероятность P успешной доставки пакета по пути состоящего из H шагов, будет равна $p = p_{n0}^{H} p_{l0}^{H}$ при условии, что прием адресатом пакета осуществляется с требуемой степенью надежности.

В предложенной в [2] аналитической модели для оценки надежности многопутевой маршрутизации в мобильных сетях *ad hoc* рассматривается потеря пакета ввиду топологических изменений, поэтому выполняется моделирование каждого пути как чистого канала со стиранием (*pure erasure channel*), а именно, в том случае, если путь неудачен, все переданные этим путем части, будут потеряны, в ином случае – все доли на части пути будут получены. Эта модель может рассматриваться как модель проблемы отказа узла. Для вычисления надежности в [2] предложено использование Гауссова приближения (*Gaussian approximation*). Результаты аналитических исследований показали, что многопутевая маршрутизация более стойка к проблеме отказа узла и доставка пакета может быть выполнена с большей степени надежности. Однако увеличение степени надежности очень полагается на определенной избыточности (введение дополнительных путей), которая будет определенным образом препятствовать достижению цели обеспечения необходимого уровня безопасности.

Оценим надежность с позиции наличия отказа связи. Пусть имеем сеть с идеально надежными узлами, но ненадежными связями. При этом потеря пакета при передаче вызвана отказом связи и независима от других передач. В этом случаи проблема отказа связи влияет на надежность многопутевой маршрутизации. Кроме того, неориентированная проблема отказов узлов может быть преобразована в направленную проблему без отказов узлов [5].

Предположим, что было отобрано M непересекающихся путей, каждый из которых с требуемой степенью надежности доставляет пакеты с вероятностью p_i ($i=1,2,...,M$). Используем вектор $\bar{n} = [n_1, n_2, ...n_M]$, обеспечивающий распределение частей n_i пакетов на i-ом пути. Пусть $x_i(j)$ определяет функцию индикатора на i-ом пути, при этом значение $x_i(j)=0$ указывает, что j-ый пакет доставлен успешно, а значение $x_i(j)=1$ указывает, что j-ый пакет потерян. Таким образом, $p_i = Pr\{x_i(j)=0\}$, а число пакетов,

потерянных на i-ом пути равно $\sum_j^{n_i} x_i(j)$. Основываясь на этом предположении и том факте, что пока общее количество потерянных пакетов из числа N пакетов меньше или равно значению $N-T$, первичная информация может быть правильно восстановлена БС, получаем вероятность успешной доставки P_R, определяемую следующим выражением:

$$P_R(\underline{n}) = \Pr\{L \le N-T\} = Pr\left\{\sum_{i=1}^{M}\sum_{j=1}^{n_i} x_i(j) \le N-T\right\},$$

где L – общее количество потерянных пакетов из числа N пакетов, доставленных M путями.

Имея вероятность надежной доставки пакета $\overline{p}$, можно эту вероятность максимизировать, отправив как можно больше частей самыми надежными путями и как можно меньше – наименее надежными путями. Этот результат подразумевает то, что с учетом неустойчивой модели отказа пакетов более высокая надежность достигается распределением всех пакетов по наиболее надежным путям. Однако многопутевое рассредоточение трафика в данной ситуации не обеспечивает повышение надежности.

Сделаем оценку общей безопасности и надежности работы предлагаемой схемы распространения *H-SPREAD*, а именно, набора параллельной многопутевой маршрутизации при сборе информации с использованием сквозного шифрования и дополнительной маршрутизации пути на каждой доставке пакета по определенному пути. Используем протокол многопутевого обнаружения *N-to-1*. Рассмотрим воздействие отказа узла, отказа связи как проблему компрометации узла. Предположим, что отказ узла постоянен. При отказе узела он не может быть использован для передачи пакетов. Отказ связи неустойчивый и не зависит от передачи каждого пакета. Когда ошибка связи происходит с пакетом, никакая повторная передача не будет выполнена для этого пакета. Компрометация узла также постоянна. Если узел компрометирован, все части/пакеты, переданные этим узлом, тоже считаются компрометированными.

Из-за пространственного ограничения сообщаются результаты в сетях, где диапазон передачи – 20 м. Каждый узел, который находится по крайней мере в двух шагах от узла *Sink*, инициализирует 100 сообщений. Каждое сообщение разделяется на $N=10$ частей и распространяется на M путях ($M=1,\cdots,7$). Если $M=1$, должен быть вектор распределения $n=[10]$, при этом все 10 частей должны проходить первичный путь. Соответственно:

$M=2$, $n=[5\ 5]$; $M=3$, $n=[4\ 3\ 3]$;

$M=4$, $n=[3\ 3\ 2\ 2]$; $M=5$, $n=[2\,2\,2\,2\,2]$;

$M=6$, $n=[2\ 2\ 2\ 2\ 1\ 1]$;

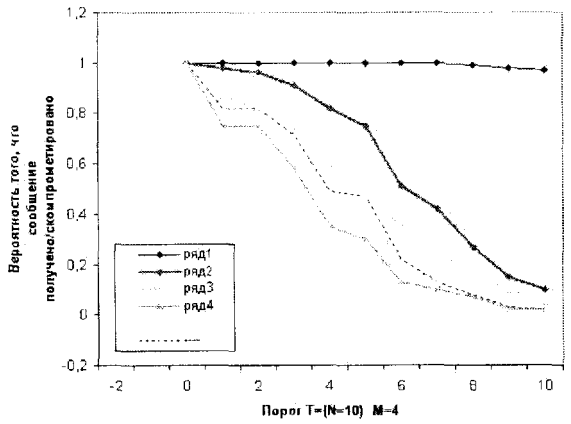
$M=7$, $n=[2\ 2\ 2\ 1\ 1\ 1\ 1]$.

Получены результаты моделирования в среднем более чем с 300 беспорядочно сгенерированными сетями.

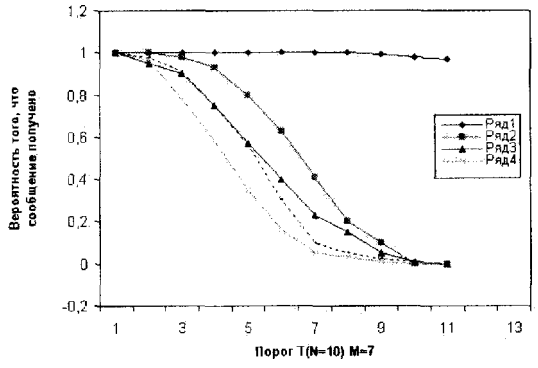
Существенное усовершенствование надежности наблюдается, когда используется спасение данных (*salvaging*). Результаты для $M=4,7$ представлены на рис. 1 (а, б). По оси абсцисс указаны значения порога T (с набором N к 10 во всех симулированиях), который может интерпретироваться как уровень избыточности. Уровень надежности представлен вероятностью того, что сообщение будет успешно доставлено и данная вероятность вычисляется как отношение общего количества сообщений, полученных в узле *Sink* к общему количеству сообщений, инициализированных от всех узлов датчиков. Сообщение считается полученным, если по крайней мере T частей достигают узел *Sink*. Точно так же уровень безопасности представлен вероятностью, того что сообщение компрометировано и вычисляется как отношение общего количества компрометированных сообщений к общему количеству сообщений, инициализированных всеми узлами датчиков. Сообщение скомпрометировано в том случае, когда, по крайней мере, T частей скомпрометировано.

Поэтому значение $i=10$ определяет отсутствие избыточности. В этом случае БС либо должна получить все 10 частей, либо осуществляется перехват всех этих

частей с целью восстановления сообщения.



а

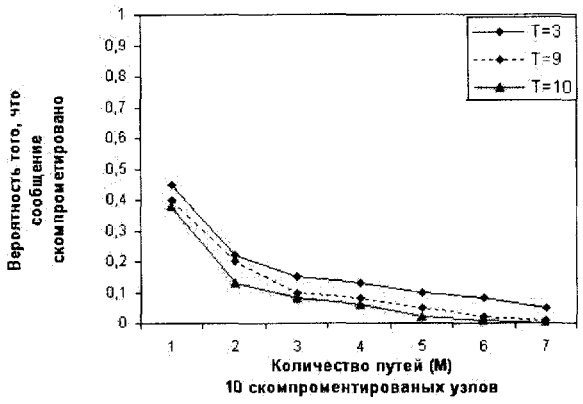


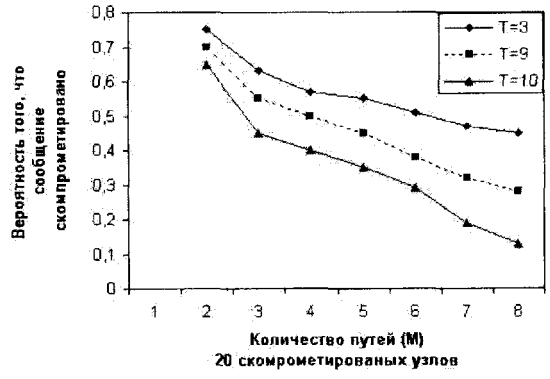
б

Рис. 1. Графики вероятностей безопасной и надежной передачи информации со спасением или без спасения пакетов (неисправных узлов – 10%, компрометированных узлов – 10%, вероятность неисправности связи – 1%); а) при $M = 4$; б) при $M = 7$

Наблюдается, что без метода спасения норма потери пакетов чувствительна к уровню избыточности и недопустимо высока даже с чрезмерной избыточностью (малые значения i). Однако, спасение пакетов проходящих по дополнительным путям, эффективно поддерживает очень высокий (близко к 100%) процент доставки на всех уровнях избыточности. С другой стороны, наблюдается, что безопасность очень чувствительна к избыточности, при этом, чем меньше избыточность, тем большую безопасность обеспечивает предлагаемая схема распространения. Уровень безопасности достигаемый в том случае, когда все узлы и связи имеют требуемый уровень надежности показан пунктирной линией на рис. 1 (а, б). Метод спасения при этом не осуществляется. Метод спасения немного уменьшает уровень безопасности из-за возможного перекрытия пути. Однако, данное взаимодействие несущественно по сравнению со значительно улучшенной надежностью. Это наиболее предпочтительное свойство, которое позволяет предложенной схеме распространения обеспечить одновременно повышение уровня безопасности, и надежности.

Значения вероятностей, характеризующих уровень надежности и безопасности при передаче пакетов данных, представлены на рис. 2, 3.





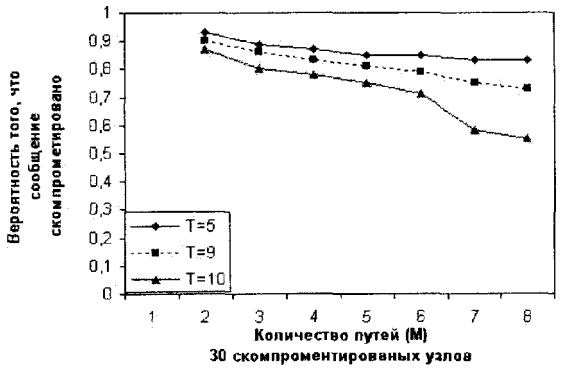


Рис. 2. Графики вероятностей, характеризующих уровень безопасности передачи пакетов данных

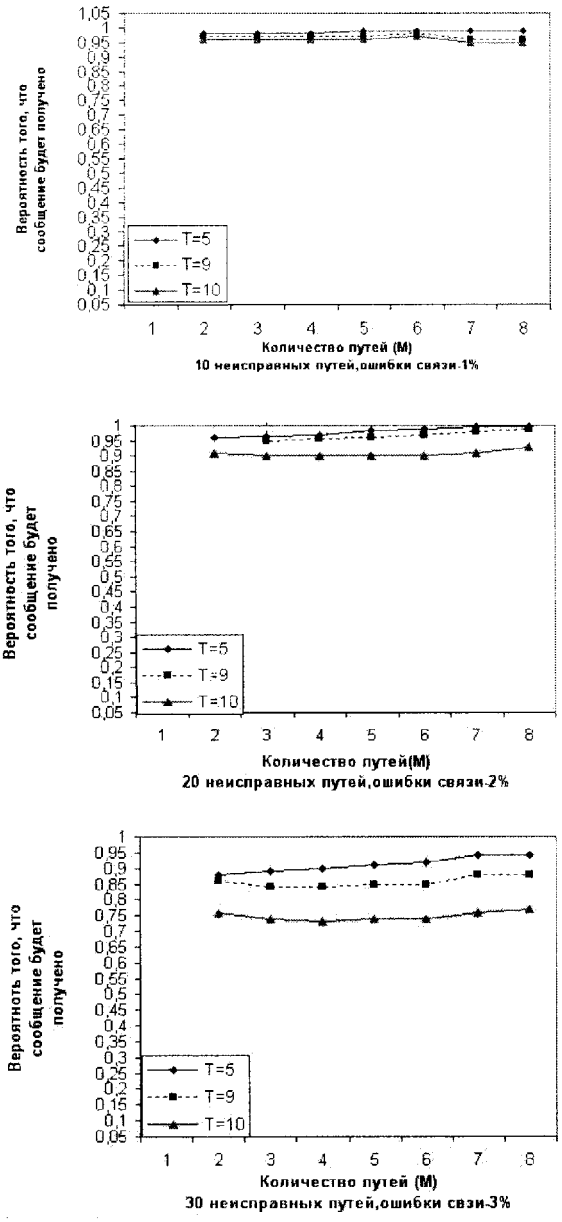


Рис. 3. Графики вероятностей, характеризующих уровень надежности передачи пакетов данных

При этом надежность и безопасность рассматриваются как функции количества путей, используемых соответственно с условиями различных ошибок и угроз сети. Схема эффективна при сокращении вероятности того, что сообщение может быть скомпрометировано. Наблюдается, что при использовании активного спасения пакетов разрушается независимость путей а также вероятность того, что сообщение может быть скомпрометировано уменьшается с увеличением числа путей, используемых для распространения информации. Стоит обратить внимание, что ситуации, которые рассмотрены, очень спорные при наличии 10%, 20%, и 30% компрометированных узлов. Фактически, в менее спорных ситуациях, усовершенствование будет более существенным. Результаты подтверждают эффективность предложенной схемы, поскольку она более стойкая к организованным атакам компрометированных узлов. Соответственно, эксплуатационные характеристики надежности показывают, что предложенная схема в состоянии поддержать довольно хороший уровень доставки сообщений относительно отказов и связи, и узла. Можно сделать вывод, что предложенная схема и метод активного спасения дополнительного пути более устойчивы к проблеме отказов узлов.

Эффективная поставка данных в *WSNs* – стимулирующая задача. Прямое рассредоточение [6, 7] и *SPIN* являются двумя парадигмами распространения образцовых данных. Как метод центральных данных, прямое рассредоточение использует лавинную маршрутизацию низкого уровня для установки градиентов и использует постепенное укрепление лучших дорожек, для приспособления определенных уровней сети к динамике *sink*. *SPIN* принимает согласование метаданных для устранения избыточной передачи данных и является подходящим в тех случаях, когда отдельный датчик распространяет свои наблюдения по всем датчикам в сети. Некоторые подходы к распространению данных в сетях БСС включают распространение, основанное на лавинной маршрутизации, вероятностной лавинной маршрутизации, иерархии *TTDD* и т.д.

Многопутевая маршрутизация является хорошей методикой в сетях *MANET*, которая может объединить ограниченную пропускную способность, чтобы уменьшить трафик пакетной передачи с целью уменьшения перегрузки сети, улучшения отказоустойчивость, и, что наиболее важно, повышения надежности.

Использование беспроводных сенсорных сетей обеспечивает повышение уровня надежности и безопасности сбора и передачи информации в ИУС КП. Однако в настоящее время в качестве основных средств и систем сбора и передачи

информации в центр управления ИУС КП используются проводные сети к которым предъявляются высокие требования к производительности, уровню надежности функционирования, поскольку потери а также несвоевременное поступление пакетов данных в центр обработки и управления может привести к понижению уровня надежности функционирования ИУС КП и даже к невыполнению определенных функций.

Главными задачами сети является обеспечение возможности совместного использования ресурсов в реальном времени, выполнение соответствующих требований производительности и надежности функционирования и обеспечение своевременной доставки пакетов данных с допустимо минимальной их потерей.

В сетях ИУС КП весь трафик сети с разнородными потоками не может считаться «эластичным», т.е. не имеющим ограничений на время ожидания. Теоретически при превышении порога ожидания заявка может уйти из очереди (так называемые «нетерпеливые» заявки). Практически, конечно, в системах ИУС КП такая ситуация, как правило, недопустима. Для систем массового обслуживания (СМО) с «нетерпеливыми» заявками понятие «вероятность отказа» не имеет смысла – каждая заявка становится в очередь, но может и не дождаться обслуживания, уйдя раньше времени. Для предотвращения потери таких «нетерпеливых» заявок и, соответственно, ухудшения качества обслуживания целесообразно применять алгоритмы обслуживания с приоритетами типа маркировки потоков [8] или ранжирования пакетов по длительности [9].

Необходимо учесть также, что существует ненулевая вероятность исчерпания буферной памяти узла коммутации (УК) – маршрутизатора, обычного или программного коммутатора. Иными словами, число мест в очереди нельзя считать неограниченным. При этом вновь поступающим заявкам будет отказано в обслуживании. Вероятность отказа в обслуживании зависит от соотношения интенсивностей поступления и обслуживания заявок. Не обслуженные заявки (пакеты, кадры, сообщения) просто теряются. Придется передавать их повторно, поскольку источник не получит квитанцию – подтверждение о доставке.

Рассмотрим характеристики нагрузки на сеть при наличии «нетерпеливых» заявок и ограниченном объеме буферной памяти.

Если все каналы обслуживания заняты и имеется очередь заявок, то, как известно [8], поток обслуженных заявок можно считать простейшим. Сделаем также допущение о простейшем характере потока «нетерпеливых» заявок в общем потоке. Относительная пропускная способность системы q вычисляется из предположения, что будут обслужены все заявки, кроме тех, которые уйдут из очереди досрочно. Для нахождения среднего числа таких заявок вычислим среднее число заявок в очереди:

$$\bar{r} = 1 \cdot p_{n+1} + 2 \cdot p_{n+2} + ... + r \cdot p_{n+r} + ...$$

На каждую из них действует «поток уходов» с интенсивностью ν. Значит, из среднего числа $\bar{r}$ заявок в очереди в среднем будет уходить, не дождавшись обслуживания, $\nu \bar{r}$ заявок в единицу времени; всего в единицу времени в среднем будет обслужено $A = \lambda - \nu \bar{r}$ заявок.

Относительная пропускная способность СМО будет $q_p = 1 - \frac{\nu}{\lambda}\bar{r}$, среднее число занятых каналов (из общего числа n) $\bar{z} = \rho - \beta \bar{r}$, среднее число заявок в очереди $\bar{r} = \frac{\rho}{\beta} - \frac{\bar{z}}{\beta}$. Здесь λ, μ – интенсивности потока заявок и обслуживания соответственно; $\rho = \frac{\lambda}{\mu}$, $\beta = \frac{\nu}{\mu}$.

Примем допущение, что все каналы обслуживания УК имеют общую буферную память объемом N_b ячеек. Каналы взаимно независимы, дисциплина доступа к каждому каналу одинакова (например, *FIFO – first in – first out*, «первый пришел – первый вышел», *LIFO – last in – first out*, «последний пришел – первый вышел» или

FIRO – first in – random out, «первый пришел – случайный вышел»). Тогда можно рассматривать любой канал УК как одноканальную СМО с числом мест в очереди $N_Q = N_b / K$, где K – число каналов. Строго говоря, N_Q является случайной величиной, однако при условии $N_b >> K$ (что обычно выполняется на практике) можно рассматривать N_Q как некоторое усредненное значение числа мест в очереди для каждого канала.

Заявки обслуживаются при следующих условиях.

1. В современных УК время обслуживания, как правило, не зависит от характеристик заявки (длины пакета). Поэтому можно считать, что интенсивность обслуживания в каждом канале одинакова и постоянна: $\mu_i = \mu = const$, $i = \overline{1, K}$.

2. На вход УК поступают как обычные, так и «нетерпеливые» заявки.

3. Время ожидания «нетерпеливой» заявки в очереди не превышает $t_{w\max}$. После этого заявка уходит из очереди.

4. Обычная («терпеливая») заявка отбрасывается, т.е. уходит из очереди, если истекло время ожидания квитанции (тайм-аута) t_{out}.

5. «Нетерпеливая» заявка уходит из очереди и больше не появляется на данном УК, поскольку источник – терминальный узел или промежуточный УК – перемаршрутизирует ее. При этом $t_{w\max} << t_{out}$. Данное условие вытекает из следующего требования. Необходимо повторно (а, возможно, и дважды) передать «нетерпеливую» заявку по другому маршруту, причем общее время передач не должно превышать максимально допустимого времени задержки для данного вида трафика.

6. «Терпеливая» заявка, у которой истекло время тайм-аута, может появиться на этом же УК через некоторое, в общем случае недетерминированное время. Это время зависит от задержек прохождения заявки от источника до рассматриваемого УК и является достаточно малым. Логично предположить, что за это время статистические характеристики входящего трафика на данном УК могут измениться весьма незначительно.

Состояния канала обслуживания могут быть такими:

– S_0 – канал свободен с вероятностью P_0; в случае поступления заявки ее обслуживание начинается немедленно;

– S_1 – канал занят, очереди нет; вероятность состояния S_1 равна P_1;

– S_2 – канал занят, одна заявка в очереди; вероятность состояния S_2 равна P_2;

– S_k – канал занят, $k-1$ заявка в очереди; вероятность состояния S_k равна P_k;

– S_{Nq+1} – канал занят, N_Q заявок в очереди, свободных мест в очереди нет; вероятность состояния S_{Nq+1} равна P_{Nq+1}.

События $S_0, S_1, \ldots, S_{Nq+1}$ представляют собой полную группу, следовательно, сумма вероятностей $P_0, P_1, \ldots, P_{Nq}$ равна единице. Вероятность того, что на каком-то конкретном временном интервале все места в очереди заняты обычными и «нетерпеливыми» заявками, при условии, что «нетерпеливые» заявки в данный момент не покидают очереди, равна $P_{откv} = \dfrac{\lambda - \nu}{\lambda - \nu + \mu} = P_{Nq+1}$. Обозначим разность между интенсивностями входного потока λ и потока уходов «нетерпеливых» заявок ν через $\lambda_0 = \lambda - \nu$. Напомним, что μ - интенсивность обслуживания.

Для того, чтобы не накладывать ограничения на вид вероятностных распределений интервалов между первичными и повторными заявками, используем модели потоков с ограниченным последействием. Тогда можно записать выражение для $P_{откv}$ в следующем виде: $P_{откv} = \dfrac{\lambda_0}{\lambda_0 + \mu}$. Вероятность $P_{откv}$, по существу, представляет собой долю не обслуженных заявок из общего числа

входящих заявок, как обычных, так и «нетерпеливых». Обозначим эту долю

$$q_{необсл}: P_{откv} = \frac{\lambda_0}{\lambda_0 + \mu} = q_{необсл}.$$

В соответствии с приведенными выше условиями обслуживания обычные заявки через некоторое время могут вернуться для повторного обслуживания на УК. Следовательно, они добавляются к вновь поступающим заявкам, и интенсивность входного потока возрастает на величину $\left(1+q_{необсл}\right)$. Новая величина интенсивности входного потока

$$\lambda_1 = \lambda_0\left(1+q_{необсл}\right) = \lambda_0 + \frac{\lambda_0^2}{\lambda_0+\mu}. \quad (1)$$

Примерно через такое же время на входе УК опять будут присутствовать первичные заявки, к которым добавятся ранее не обслуженные. По аналогии с (1) запишем выражение для вновь изменившейся интенсивности суммарного входного потока:

$$\lambda_2 = \lambda_1\left(1+q_{необсл}\right) = \lambda_1 + \frac{\lambda_1^2}{\lambda_1+\mu}.$$

По индукции запишем выражение для текущей интенсивности λ_i входного потока заявок в следующем виде:

$$\lambda_i = \lambda_{i-1} + \frac{\lambda_{i-1}^2}{\lambda_{i-1}+\mu}. \quad (2)$$

В данной рекуррентной последовательности (2) изменения интенсивности входного потока заявок учитываются все заявки, не обслуженные на предыдущих этапах. При стремлении $i \to \infty$ мы получим некие асимптотические оценки полезной пропускной способности сети при различных соотношениях $\rho = \lambda/\mu$ – *интенсивности поступления заявок и интенсивности их обслуживания.*

Рассмотрим далее задачу оценивания вероятности возникновения коллизии в сети *Ethernet*. Поскольку локальные сети ИУС КП, к которым относятся системы УВД, строятся, как правило, по технологии *Ethernet*, проблема ограничения коэффициента использования сети является еще более острой по причинам, связанным именно с принципами работы, заложенными в этой технологии.

При увеличении коэффициента использования сети $k_{исп}$ – отношения пропускной способности к интенсивности трафика – все большая часть ресурса тратится на обработку коллизий. При стремлении $k_{исп}$ к единице будет стремиться к единице вероятность коллизий и, соответственно, появление все новых и новых *jam*-последовательностей. Пытаясь обрабатывать коллизии, сеть перестанет пропускать полезную информацию и будет работать «на себя». При обосновании предельно допустимого коэффициента использования сети необходимо учитывать риск возникновения такой ситуации.

Пусть к сети подключено N компьютеров, которые выдают потоки пакетов с интенсивностями $\lambda_n(t)$, $n = 1, N$. Будем считать, что пакеты, выдаваемые n-м компьютером, имеют длительность τ_n. Чтобы не связывать себя необходимостью точного учета момента появления каждого пакета, предположим, что они происходят в случайные моменты времени с одинаковым вероятностным распределением, и на конечном отрезке времени $T >> \tau_n$ образуют поток Эрланга k-го порядка.

Как известно [8], задаваясь порядком потока Эрланга, можно получить любую степень последействия: от полной взаимной независимости между моментами появления событий при $k = 0$ до детерминированной функциональной связи при $k \to \infty$.

Пусть в точке t_j, находящейся внутри интервала анализа T, появился пакет f_j с длительностью τ_j. Вероятность появления этого пакета обозначим $P(t_j)$. Выведем выражение для условной плотности вероятности частичного перекрытия пакета f_j другим пакетом f_i с длительностью τ_i.

Будем считать, что перекрытие происходит уже при соприкосновении паке-

тов. Тогда необходимо вычислить совместную вероятность $P(t_i,t_j)$ того, что пакет f_i попадет в интервал $\lfloor t_1-\tau_i,\ t_1+\tau_j \rfloor$ при условии, что пакет f_j начинается в точке t_1. С учетом временных соотношений эта вероятность определяется как

$$P(t_i,t_j)=P(t_1-\tau_i\le t\le t_1+\tau_j/t_1=t_j).$$

Логично предположить, что процессы появления в сети пакетов, выдаваемых разными источниками, взаимно независимы, а моменты появления пакета f_j на интервале $[t_0,t_0+T]$ равновероятны. Тогда:

$$P(t_i,t_j)=P(t_1-\tau_i\le t\le t_1+\tau_j/t_1=t_j)=$$
$$=P(t_1-\tau_i\le t\le t_1+\tau_j)P(t_1),$$

где $P(t_1)=P(0\le t_j<t_j+\tau_j\le T)=\frac{\tau_j}{T}$, – вероятность того, что пакет f_j «накроет» интервал длительностью τ_j в какой-либо точке t_j.

Положим, что в момент времени $t_1-\tau_i$ пакет f_i не наблюдается. Вычислим вероятность $P(t_1-\tau_i\le t_i\le t_1+\tau_j)$ появления f_i-го пакета за отрезок времени $\lfloor t_1-\tau_i,\ t_1+\tau_j \rfloor$, используя выражения для закона Эрланга k-го порядка [8], в которых для учета нестационарности введем переменную интенсивность потока $\lambda_i(t)$:

$$P(t_1-\tau_i\le t\le t_1+\tau_j)=\frac{\lambda_i(t_1-\tau_i)\left(\lambda_i(t_1-\tau_i+t)\,t\right)^{k-1}}{(k-1)!}\exp\left(-\int_{t_1-\tau_i}^{t_1+\tau_j}\lambda_i(t)dt\right). \quad (3)$$

Если считать интенсивность потока $\lambda_i(t)$ медленно меняющейся величиной, то можно с приемлемой точностью усреднить ее на интервале интегрирования $\lfloor t_1-\tau_i,\ t_1+\tau_j \rfloor$: $\lambda_i(t)\approx\lambda_{icp}$. Тогда выражение (3) упрощается:

$$P(t_1-\tau_i\le t\le t_1+\tau_j)=\frac{\lambda_{icp}\left(\lambda_{icp}\,t\right)^{k-1}}{(k-1)!}\exp\left(-\lambda_{icp}\right). \quad (4)$$

После несложных, но громоздких преобразований выражение (4) преобразуется для случая самоподобного трафика таким образом:

$$P(t_1-\tau_i\le t\le t_1+\tau_j)=\frac{\lambda_{icp}^{1/2(1-H)}\left(\lambda_{icp}^{1/2(1-H)}\,t\right)^{k-1}}{(k-1)!}\exp\left(-\lambda_{icp}H/(1-H)\right), \quad (5)$$

где H – параметр Херста.

По формулам (3–5) могут рассчитаны зависимости полезной пропускной способности сети от коэффициента использования для Пуассоновского трафика и самоподобного трафика с разными параметрами Херста.

Под идеальным трафиком понимается отсутствие коллизий. Производительность сети заметно убывает уже при коэффициенте использования, превышающем значение 0,3…0,4 (особенно для самоподобного трафика).

Таким образом, коэффициент использования сетей, построенных как по *ATM*-технологии, так и по технологии *Ethernet*, не может быть слишком близок к единице, иначе полезная пропускная способность сети резко упадет. Сеть будет или повторно передавать утерянные пакеты и квитанции, или обрабатывать коллизии, т.е. работать «на себя». Ни в коем случае нельзя допускать неконтролируемую перегрузку сети, потому что восстановление параметров заявленной производительности сети идет намного медленнее, чем их падение. Сетевые специалисты говорят, что «сеть быстро ло-

жится, но медленно встает». Такие ситуации тем более недопустимы для систем критичного применения. Поэтому для управления ресурсами и поддержания пропускной способности сети в целом на требуемом уровне необходимо перераспределять нагрузку на отдельные сегменты уже при появлении самых первых симптомов перегрузки, пока она еще контролируема.

Логическая структуризация сетей любого масштаба – один из основных способов преодоления ограничений, которые возникают при использовании общей разделяемой среды [10]. Крупные сети, как правило, строятся на основе структуры с общей магистралью (*Backbone*). К магистрали через УК и сети доступа присоединяются автономные подсети. Это подсети отдельных аэродромно-районных АС УВД (АРАС УВД) или районных АС УВД (РАС УВД). Подсети, в свою очередь, делятся на сегменты, предназначенные для обслуживания структурных подразделений, групп автоматизированных рабочих мест (АРМ) или отдельных АРМ, которые входят в состав АРАС УВД или РАС УВД.

Для сегментации магистральной сети наиболее целесообразно использовать шлюзы, поскольку с их помощью успешно решаются задачи объединения подсетей с различными типами системного (сетевого) и прикладного программного обеспечения. Кроме того, с помощью шлюзов локализуется трафик отдельных участков магистральной сети [10]. Перечисленные задачи еще эффективнее и с более высоким быстродействием решаются с помощью программных коммутаторов (*Softswitch*) [11], однако эти устройства значительно дороже шлюзов.

При сегментации сетей достигаются следующие преимущества.

1. Сегментированные сети более гибко адаптируются к потребностям отдельных групп пользователей. В разных подсетях могут использоваться различные сетевые технологии, операционные системы и прикладное программное обеспечение. Это не исключает возможностей обмена данными между подсетями через УК.

2. Улучшается контроль иерархии и распределения прав доступа к сетевым ресурсам.

3. Упрощается управление сетью в целом. Общая задача управления распадается на совокупность локальных задач, более простых и зачастую слабо связанных между собой. Поэтому при разрешении проблем внутри одной подсети условия работы других подсетей практически не изменяются.

Естественно, структуризация и сегментация сетей не может быть доведена до вырожденного состояния, когда каждый терминальный узел фактически представляет собой отдельный сегмент. Тогда число УК будет практически равно числу терминальных узлов. Помимо существенного удорожания системы в целом, это может привести к отрицательным последствиям. Из-за задержек прохождения данных (кадров, пакетов) через УК, потерь данных при переполнении буферов и вынужденных повторов пересылки потерянных данных пропускная способность сети может резко уменьшиться. Кроме того, будут утрачены такие очевидные преимущества сети со стандартной технологией разделяемой среды:

– простота топологии и легкость наращивания числа терминальных узлов в пределах, которые определяются стандартом технологии;

– простота регулирования потока данных и доступа пользователей к общей разделяемой среде (например, с помощью арбитра сети);

– простота и полная унификация протоколов обмена, что обеспечивает простоту конструкции, а, следовательно, низкую стоимость и высокую надежность сетевого оборудования.

Поэтому, очевидно, существует разумный оптимум в выборе числа сегментов сети и числа терминальных узлов в каждом сегменте. При этом, естественно, вовсе не обязательно, чтобы каждый сегмент имел одинаковое число узлов – все определяется интенсивностями потоков данных в отдельном сегменте.

Задачу оптимизации топологической структуры сети поставим следующим образом. Имеются следующие векторы:

$\vec{U}$ – вектор параметров сетевой нагрузки: интенсивности потоков данных между каждой парой соседних узлов коммутации, статистические характеристики трафика, приоритеты или некоторые весовые функции отдельных потоков данных;

$\vec{Q}$ – вектор параметров качества сервиса сети: быстродействие, достоверность и пр., характеризующих качество передачи данных или, в традиционной трактовке – качество сервиса QoS;

$\vec{W}$ – вектор эксплуатационных характеристик сети: пропускная способность каналов передачи данных, быстродействие и объёмы буферной памяти узлов коммутации, надежность и время восстановления оборудования, весовые коэффициенты, с помощью которых даются сравнительные оценки параметров логических связей между узлами сети.

Накладываются (векторные) ограничения на предельные характеристики сетевого оборудования, в том числе на общую стоимость и структуру сети:

$$C_i\left(\vec{U},\vec{Q},\vec{W}\right) \le C_{i\max},\ i=\overline{1,N_c}, \quad (6)$$

где N – число элементов множеств C_i и $C_{i\max}$.

Наконец, накладываются ограничения на техническую архитектуру сети, вытекающие из условий физической и практической реализуемости: предельно достижимая скорость передачи данных, максимально допустимые расстояния между узлами, минимально достижимые задержки в коммутационном оборудовании, уровень взаимных помех и т.д. Обозначим множество этих ограничений через $R_{\max}$:

$$R\left(\vec{U},\vec{Q},\vec{W}\right) \in R_{\max}. \quad (7)$$

Требуется найти такой набор векторов $\left\{\vec{U},\vec{Q},\vec{W}\right\}$, который доставлял бы экстремум функционалу нормированной эффективности:

$$\Psi_{en}\left(\vec{U},\vec{Q},\vec{W}\right) \underset{\substack{\vec{U}=\vec{U}_{opt}\\ \vec{Q}=\vec{Q}_{opt}\\ \vec{W}=\vec{W}_{opt}}}{\rightarrow} \max, \quad (8)$$

при ограничениях вида (6 – 8).

Общий алгоритм адаптивной логической структуризации сети представляет собой такую последовательность действий.

1. Ввод исходных данных:

– количество активных терминальных узлов N_i и их принадлежность к i-му сегменту;

– усредненные объемы загрузки буферов УК;

– условия работы системы (штатный режим – режим обработки экстремальных ситуаций; тип экстремальной ситуации E_i);

– начальное соотношение $V_{вп i}/V_{мс i}$ каждого сегмента;

– среднее время тайм-аута t_{out} при межсетевом обмене (в экстремальной ситуации меньше, чем в штатной, в 2 – 3 раза);

– средний коэффициент использования каждого сегмента $k_{исп i}$.

2. Имеется ли экстремальная ситуация (ЭС)?

Если да, то переход на шаг 3. Иначе – переход на шаг 6.

3. Распознавание типа ЭС.

4. Выбор из базы данных (БД) оптимальной схемы сегмента для обработки данной ЭС.

5. Переход на шаг 2.

6. Выбор из БД схемы начальной сегментации.

7. Подсчет числа *jam*-последовательностей в каждом сегменте.

8. Подсчет числа обнаруженных превышений постоянной составляющей в физическом канале каждого сегмента.

9. Расчет полезной пропускной способности.

10. Расчет $k_{испi}$.

11. $k_{испi} < k_{испmax}$? Если да, то переход к шагу 2. Иначе – к шагу 12.

12. Поиск экстремума – наилучшей структуры по критерию $k_{испi} \le k_{испmax}$.

13. Расчет новой структуры i-го сегмента.

14. Переход к шагу 2.

Алгоритм является циклическим с незаданным числом повторений. Для поиска экстремума – оптимальной структуры – целесообразно использовать методы рекуррентного статистического поиска. В базах данных (БД) хранятся конфигурации сегментов, организуемых при наличии той или иной экстремальной ситуации, а также исходная конфигурация сети. Наличие перегрузки фиксируется по числу *jam*-последовательностей и по числу превышений постоянной составляющей напряжения в общей разделяемой среде U_{const}. Число *jam*- последовательностей не связано жесткой функциональной зависимостью с коэффициентом использования i-го сегмента $k_{в\,i}$, поэтому его можно табулировать и выбирать данные из БД, с учетом ранее накопленных априорных данных о характере трафика в каждом сегменте. Простейший подход – расчет $k_{в\,i}$ по соотношению между числом *jam*-последовательностей и числом полезных переданных кадров. Последнее определяется по числу переданных квитанций о приёме кадра j-м терминальным узлом.

Задача поиска экстремума функционала (8) принадлежит к классу задач системного анализ, как и любая задача теории больших систем. Решение задачи (8) может быть получено путем поиска компромиссов между противоречивыми критериями (например, методами Парето или анализа иерархий Саати).

Ограничения вида (6) и, отчасти, (7) трудно формализовать и описать с использованием строгого математического аппарата. Тем более трудно, практически невозможно решить задачу (8) в целом, пытаясь остаться в рамках формального математического подхода. Поэтому необходимо использовать некие процедуры декомпозиции – разложения общей задачи на совокупность частных задач и поиска для них оптимальных решений с учетом функциональных или статистических (корреляция и регрессия) связей между этими задачами.

Представим исследуемую корпоративную сеть в виде иерархической структуры «магистраль – подсети – сегменты». Такое представление вполне соответствует реальной структуре систем УВД, которые всегда строятся по древовидно-иерархической схеме. Можно с достаточной уверенностью утверждать, что при оптимизации, например, отдельного сегмента сети характеристики других сегментов, как минимум, не ухудшатся, а характеристики всей сети улучшатся. Поэтому, оставаясь в рамках глобальной проблемы (8) оптимального проектирования корпоративной сети для системы критичного применения, рассмотрим частную задачу оптимизации отдельного ее сегмента – локальной вычислительной сети структурного подразделения АС УВД. Поскольку размерность задачи может меняться в широких пределах, используем алгоритм рекуррентного статистического поиска.

1. На основе $K+1$ случайных независимых опытов имеем векторную сумму

$$\vec{W}_m = \sum_{k=1}^{K} \Xi_k \left[\Psi_{ne}\left(\vec{W} + r\,\Xi_k \right) - \Psi_{ne}\left(\vec{W} \right) \right], \quad (9)$$

где r – длина случайного шага; Ξ_k – случайная величина R, имеющая равномерное распределение на $[0,1]$, K – число узлов коммутации. Напомним, что $\vec{W}$ – вектор эксплуатационных характеристик сети, компонентами которого в данном случае являются коэффициент использования и полезная пропускная способность сегмента.

2. Сумму (9) представим в рекуррентной форме:

$$\vec{W}_m = a\vec{W}_{m-1} + \Xi \Delta \Psi_{пет}, \quad 0 \le a \le 1,$$

где a – коэффициент убывания последействия. Этот коэффициент выбирается опытным путем для конкретного сегмента сети с учетом средней нагрузки в штатной ситуации.

Для ускорения поиска экстремума применим типовой алгоритм одномерной минимизации вдоль выбранного направления. Как известно, наиболее эффективными алгоритмами одномерного поиска являются метод Фибоначчи и метод золотого сечения. Поскольку число вычислений функции, необходимое для достижения требуемой степени дробления интервала неопределенности, заранее неизвестно, используем метод золотого сечения, который менее чувствителен к недостатку априорных сведений, чем метод Фибоначчи.

Рассмотрим структуру алгоритма локальной одномерной минимизации вдоль направления статистического градиента. Пусть имеются N терминальных узлов локальной сети. Между терминальными узлами имеются УК, которые присоединены к корневому УК (КР УК) для данного сегмента. УК могут работать как в обычном режиме, так и в «прозрачном» режиме. В обычном режиме работы УК строятся таблицы маршрутизации и изолируются отдельные сегменты друг от друга, вплоть до перехода в режим «микросегментации», когда каждый терминальный узел присоединен к КР УК через свой УК. В «прозрачном» режиме УК работает как простой повторитель, без переадресации поступающих пакетов. Формируется общая разделяемая среда, для которой задержки передачи данных минимальны, алгоритм обмена данными наиболее прост, а, следовательно, надежность работы сегмента наиболее высока.

В исходном состоянии, при отсутствии признаков перегрузки сегмента сети, все УК работают в «прозрачном» режиме. Данные через них передаются транзитом. Сегмент представляет собой общую разделяемую среду и один домен коллизий.

Алгоритм поиска точки разбиения сегмента на подсегменты работает следующим образом.

1. При обнаружении перегрузки сегмента разбиваем его на две части $N_1 + N_2 = N$ по методу золотого сечения в соотношении $\frac{N_1}{N} \approx \frac{N_2}{N_1}$.

2. Отыскиваем значения Ψ_{ne1} для N_1 и Ψ_{ne2} для N_2 .

3. По полученным значениям Ψ_{ne1}, Ψ_{ne2} сокращаем интервал неопределенности $\min(N_1, N_2)$.

4. Представим величину интервала неопределенности в виде $N_{k-2} \approx N_{k-1} + N_k$, $1 < k < K$.

5. Коэффициент дробления интервала неопределенности на k-м этапе $\Delta N_k \approx N \times 0{,}618^{k-1}$. Если интервал неопределенности на очередном этапе дробления становится меньше единицы (правильной дробью), операция поиска точки разбиения заканчивается.

Алгоритм одномерной минимизации реализуется на шаге 12 общего алгоритма и включается по команде, которая вырабатывается на шаге 11. Такая структура алгоритма дает возможность быстрой адаптации к изменяющейся обстановке, перераспределения сетевых ресурсов, сосредоточения их на разрешении нештатных ситуаций [1].

Выводы

1. Сети новых поколений – беспроводные сенсорные, ковергентные, мультисервисные, интеллектуальные – необычайно расширяют возможности информационного обмена, особенно в системах критичного применения. Однако возникает множество новых проблем. Необходимость сочетания в одних сетевых устройствах и узлах новых технологий передачи данных с существующими технологиями требует совершенных и весьма сложных технологических и алгоритмических решений. Для обеспечения требуемой эффективности функционирования сети и качества обслуживания необходим постоянный контроль пропускной способности и предотвращение перегрузок на отдельных фрагментах и во всей сети.

2. Для повышения одновременно и надежности, и безопасности предлагается эффективный *N-to*-1 протокол многопутевого обнаружения, который периодически или по требованию инициализирует обновление маршрута на базовой станции и в конце каждого процесса обнаружения, находит каждый узел датчика, набор непересекающихся путей к базовой станции. Основываясь на наличии множества путей на каждом узле, предлагается гибридная схема многопутевой маршрутизации для выполнения задачи безопасного и надежного сбора данных. Результаты симулирования показывают, что предложенный протокол многопутевого обнаружения очень эффективен с менее, чем одним сообщением на найденный путь. Предложенная гибридная схема многопутевого сбора данных более эластична к отказам узла/связи и организованным атакам компрометированных узлов.

3. Алгоритм адаптивной логической структуризации автономных локальных сетей основаны на оптимизации соотношения внутрисегментного и межсегментного трафика. Достоинством предложенного подхода является простота диагностики перегрузки отдельного сегмента и возможность обнаружения перегрузки на самой ранней стадии, пока она ещё контролируема и есть возможность её устранения в реальном времени.

Список литературы

1. *Жуков И.А., Кубицкий В.И., Дрововозов В.И., Халимон Н.Ф.* Адаптивная структуризация информационно-вычислительных сетей системы управления воздушным движением и навигации // Проблемы организации воздушного движения. Безопасность полетов. Науч. вестник ГосНИИ «Аэронавигация». – М.: ГосНИИА, 2007. – №7. – С. 100 – 105.

2. *A. Tsirigos, Z.J. Haas,* "Multipath routing in the presence of frequent topological changes", IEEE Communication Magazine, Nov 2001.

3. *W. Lou, W. Liu, Y. Fang,* "SPREAD: Enhancing data confidentiality in mobile ad hoc networks, IEEE INFOCOM 2004, HongKong, China, March 2004.

4. *E. Ayanoglu, C-L. I, R.D. Gitlin, J.E Mazo,* "Diversity coding for transparent self-healing and fault-tolerant communication networks", IEEE Transactions on Communications,41(11):1677-1686, Nov 1993.

5. *C.J. Colbourn,* The Combinatorics of Network Reliability, Oxford University Press, 1987.

6. *C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann,* "Directed diffusion for wireless sensor networks", IEEE/ACM Transactions on Networking, 11(1):2-16, Feb 2003.

7. *D. Ganesan, R. Govindan, S. Shenker, D. Estrin,* "Highly-resilient, energy-efficient multipath routing in wireless sensor networks", Mobile Computing and Communication Review, 5(4):10-24, Oct 2001.

8. *Гнеденко Б.В., Коваленко И.Н.* Введение в теорию массового обслуживания. 2-е изд. – М.: Наука, 1987. – 336 с.

9. . *Столингс В.* Современные компьютерные сети. 2-е изд. – С.Пб.: Питер, 2003. – 783 с.

10. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. – С.Пб.: Питер, 2003. – 864 с.

11. *Виноградов Н.А.* Анализ потенциальных характеристик устройств коммутации и управления сетями новых поколений // Зв'язок. – К.: – 2004. – № 4. – С. 10 – 17.

12. *Жуков І.А., Дрововозов В.І., Гузій М.М.* Підвищення ефективності системи керування рухом повітряних суден застосуванням комплексних систем навігації, зв'язку і керуванням повітряним рухом. Зб. наук. пр. КІ ВПС. – К.: КІВПС 1999. – Вип. 6 – С. 34 – 40.

13. *Жуков І.А., Дрововозов В.І., Карпушин Ю.П.* Визначення навантаження обчислювального комплексу системи керування повітряним рухом. Вісник: – К.: КМУЦА, 2000 Вісник 3-4 (7) – С. 124 – 127.

14. *Жуков І.А., Гуменюк В.О., Альтман І.Є.* Комп'ютерні мережі та технології: Навч. посібн. – К.: НАУ, 2004. – 276 с.