допомогою запропонованих програмних продуктів можливо здійснити розробку фінансової модель галузі, запрограмувати задачі по створенню балансу коштів, автоматизувати контроль дохідної частини, їх розподілу для проведення, наприклад, якісних ремонтів.

Стійка і безпечна робота рухомого складу значною мірою залежить від рівня технічного стану й ефективного використання, своєчасного і якісного його технічного обслуговування, що забезпечує третій комплекс інформаційних технологій "Керування інфраструктурою депо" та четвертий комплекс - "Керування невиробничою сферою".

Для реалізації усього комплексу задач необхідно значно прискорити реальне впровадження інформаційних технологій при експлуатації та ремонту міського електротранспорту, забезпечити комплексність інформатизації інфраструктури.

Застосування вищевказаного програмного забезпечення дозволяє оптимізувати роботу організації, спроектувати будь-яку організаційну структуру, сформувати бази даних, що приводить до економії ресурсів, зниження витрат, виключенню непотрібних технологічних операцій, підвищенню гнучкості і ефективності роботи міського електротранспорту .

Висновки

1. Визначено важливість інформатизації та автоматизації міського електротранспорту, які сприяють оптимізації його експлуатації та раціональному використанню матеріальних, енергетичних, трудових і фінансових ресурсів.

2. Запропоновано використання сучасного програмного забезпечення CASE та Bpwin, які дозволяють управляти проектами та сприяють підвищенню ефективності роботи міського електротранспорту, а також технічного обслуговування і ремонту рухомого складу, що в цілому впливає на ресурсозбереження.

Література

1. Канарчук В.Е., Курников И.П. Научная концепция программы формирования транспортного комплекса Украины // Автошляховик України. –№2.– К.– 1993. - С.2-7.

2. Крат В.І. Проблеми реформування міського електротранспорту // Комунальне господарство міст. – Вип.17.– К.: Техніка, 1998. – С.18-35.

3. Маклаков С.В. Bpwin и Epwin. CASE – средства разработки информационных систем. - М.: ДИАЛОГ – МИФИ, 2001. – 304 с.

УДК 001.891:65.011.56

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ПРОИЗВОДИТЕЛЬНОСТИ АНАЛИЗАТОРОВ ЛИНИЙ СИГНАЛИЗАЦИИ

А.В. Персиков

Аспирант.
Контактный тел.:+38(0572)27-44-96
e-mail:w_seal@mail.ru

А.С. Еременко

Магистрант.
e-mail:alexere@ukr.net

Л.Н. Холод

Соискатель.

Кафедра телекоммуникационных систем Харьковского Национального Университета Радиоэлектроники, просп. Ленина, 14, Харьков, Украина, 61166

В статье рассмотрееys вопросы разработки и внедрения комплексов для анализа содержимого потоков данных системы сигнализации №7. Были обсуждены практические вопросы по реализации анализаторов на базе инфраструктуры CORBA и исследованы показатели, влияющие на скоростные характеристики системы. Комплекс был рекомендован для защиты инфраструктуры АТС в максимально уязвимых режимах функционирования. Были даны рекомендации по удешевлению системы и возможностям ее интеграции в глобальные сети.

1. Введение

Система общеканальной сигнализации № 7 (ОКС7) представляет собой многофункциональный протокол управления доставкой сообщений переменной длины в пакетной форме[1]. Протокол ОКС7 поддерживает обмен сигнальными сообщениями с целью предоставления услуг доставки информации в сетях с коммутацией каналов, обмен пользователей, имеющих оконечное оборудование пакетного типа, обмен элементов интеллектуальной сети, элементов системы централизованной эксплуатации и технического обслуживания, элементов системы управления сетью электросвязи. Такое разнообразие применений ОКС7 позволяет считать этот протокол универсальным, способным обеспечивать транспортировку любых данных в сети с пакетной коммутацией.

Для обмена сообщениями по протоколу ОКС7 создаётся сигнальная сеть, состоящая из пунктов сигнализации и связывающих их звеньев сигнализации. Ответственность такой сети за правильность предоставления услуг пользователям исключительно велика. Даже небольшие нарушения функционирования именно этой части системы могут оказать существенное влияние на качество рабо-

ты всей сети электросвязи. Поэтому необходимы высокоэффективные средства оперативного контроля за сигнальной сетью и управления её ресурсами.

Все операции по контролю выполняются в режиме работы, наиболее благоприятном для злоумышленника, целью которого является дестабилизация работы телефонной сети или, вообще, ее отказ. Пока инфраструктура АТС управляется с помощью удаленного доступа с использованием специальных, недокументированных программ, возможен перехват управляющего трафика и подчинение всей внутренней системы (АТС). Этого, конечно, не следует допускать, поэтому необходимо внедрять средства тестирования и контроля управляющих линий[2]. Именно о методах и проблемах разработки, а также внедрения средств защиты, и пойдет речь в данной статье.

2. Обзор возможных угроз

Как правило, доступ к специальным функциям АТС, создаваемым производителем, реализуется по незадокументированному адресу источника и направлен к инструментам эксплуатационного управления АТС. Такими незадокументированными функциями являются:

- функция загрузки/выгрузки станционной базы данных (БД). Существование данной функции позволяет злоумышленнику выгрузить БД системы, модифицировать ее или вставить программную закладку;
- функция проверки/модификации станционной БД. Функция позволяет дистанционно исследовать и модифицировать БД системы для устранения неисправностей из-за неправильной конфигурации, ошибки конструкции и т.п.
- функция отладки/обновления программного обеспечения (ПО). Функция предоставляет возможность дистанционно обновлять системы с обнаруженными дефектами. Это место наиболее уязвимо, так как доступ злоумышленника к ПО дает практически неограниченный доступ к АТС и сети.

Средства защиты системы необходимо применять не только в режиме отладки, но и во время функционирования в штатном режиме. Это позволит:

- маршрутизировать все запросы только на конкретные санкционированные адреса;
- фильтровать требования, поступающие в сеть;
- предотвращать несанкционированный доступ к существующим соединениям и разговорам;
- предотвращать несанкционированный контроль или управление абонентской БД в пределах памяти коммутатора;
- предотвращать несанкционированное отключение соединений и поддерживать разрешенные отключения;
- ограничивать использование своих ресурсов и функций для пользователей и позволять только санкционированным пользователям модифицировать атрибуты БД и коммутатора, регистрируя все попытки доступа несанкционированных пользователей, а также попытки санкционированных пользователей выполнить несанкционированные функции;
- вести БД контроля всех инцидентов, относящихся к безопасности и возникающих в рамках сети; такая информация защищена от несанкционированного доступа, модификации или уничтожения;
- определять и контролировать логический доступ к объектам сети;
- гарантировать, что ее ПО, осуществляющее безопасность, защищено от внешнего вмешательства.

3. Разработка анализатора линий сигнализации

Подключение анализатора в качестве активного монитора должно производится в «разрыв» стандартного цифрового потока (скорость предположительно 2,048 Мбит/с). При этом разумно предусматривать возможность подключения нескольких цифровых потоков (рисунок 1).

Любое современное телекоммуникационное устройство должно отвечать набору требований:

- соответствие современным телекоммуникационным стандартам;
- возможность интеграции устройства в современные вычислительные сети;
- децентрализованное удаленное управление и администрирование;

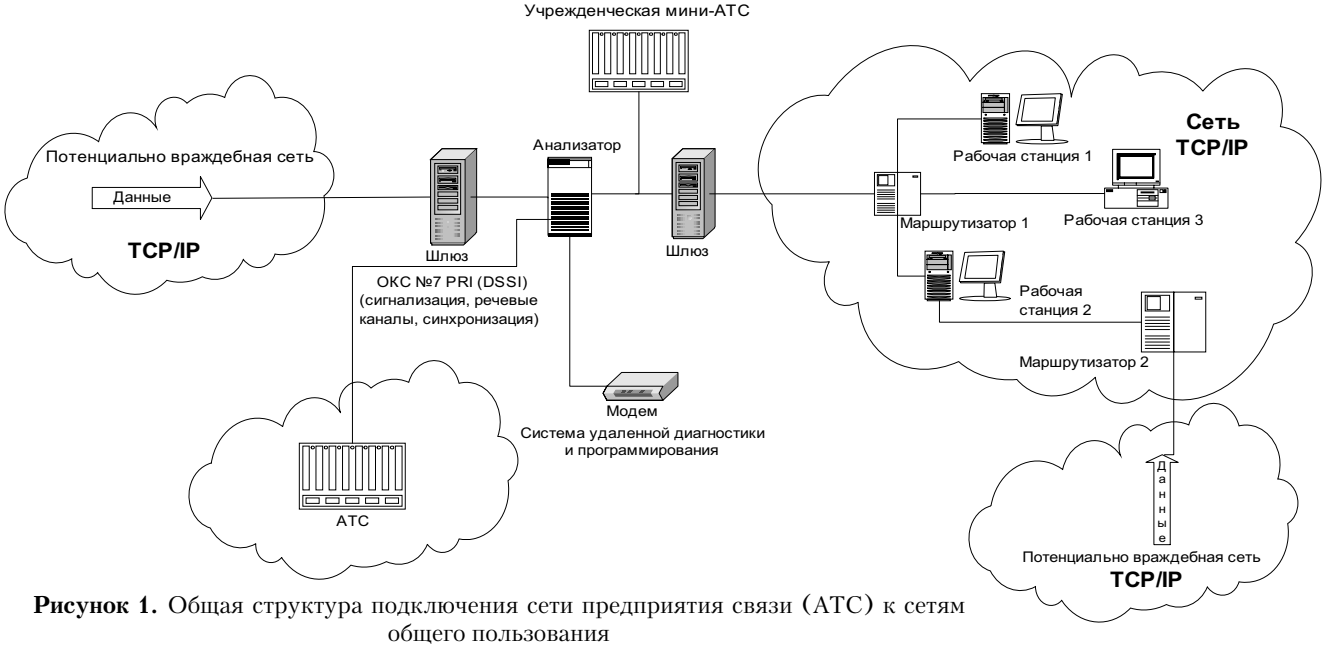

Рисунок 1. Общая структура подключения сети предприятия связи (АТС) к сетям общего пользования

- простота развертывания проектов, использующих данные устройства;
- низкая стоимость.

Конкретизировав требования к устройству, мы предложили следующие рекомендации для построения системы анализа сигнальных линий:

- использование анализаторов для всех возможных сигнальных линий сети, в целях предотвращения масштабной атаки, направленной на эти линии, – соответствие требованию, по которому защита должна быть комплексной; централизованное управление фильтрацией;
- перенесение нагрузки по обработке данных от оконечного устройства блоку обработки (в простейшем случае – ЭВМ). Это позволяет удешевить систему в целом за счет упрощения оконечного устройства и использования одной ЭВМ для обработки данных от множества устройств;
- использование по возможности бесплатного и условно-бесплатного программного обеспечения (Linux, MySQL) для уменьшения совокупной стоимости комплекса;
- обеспечение максимального соответствия архитектуры системы регистрации и фильтрации трафика концепции TMN (Telecommunication Management Network, сеть управления телекоммуникациями);
- использование технологии CORBA (Common Object Request Broker Architecture, общая архитектура брокеров объектных запросов) в качестве базовой технологии, а в качестве информационной магистрали – ORB (Object Request Broker) [3].

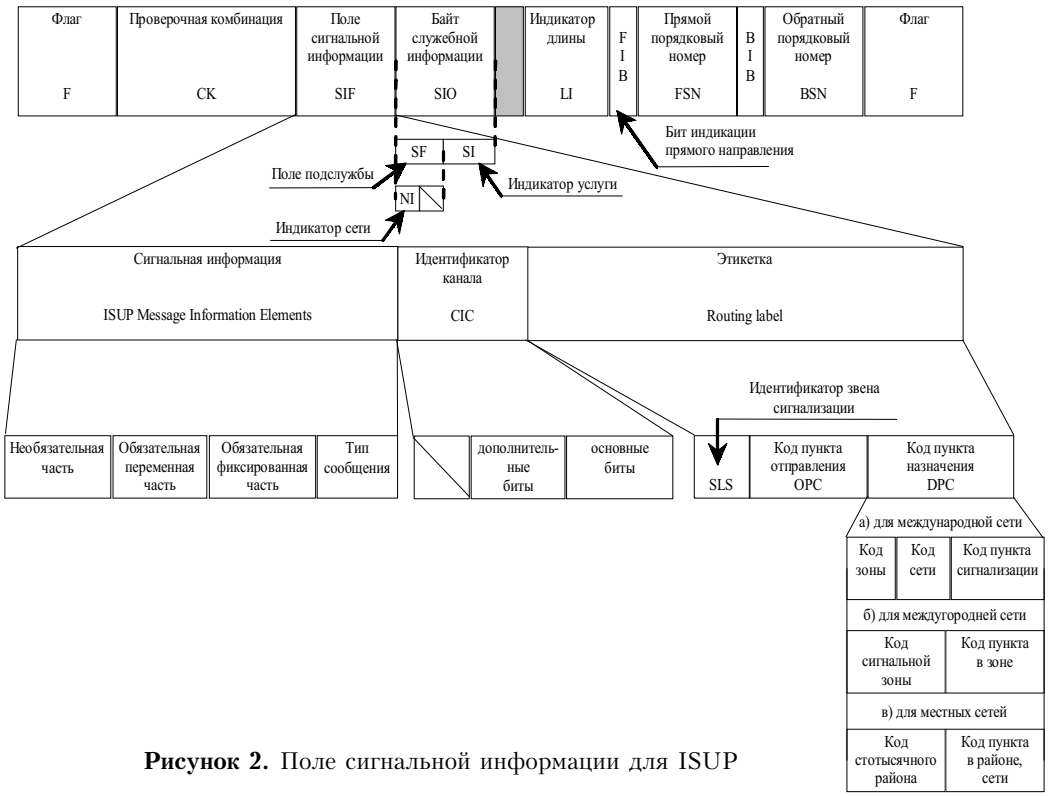

Рисунок 2. Поле сигнальной информации для ISUP

Данные рекомендации не являются исчерпывающими и все, в конечном счете, зависит от конкретной реализации.

4. Сбор информации и передача ее для обработки, интегрируемость в существующие системы

Сбор информации должен происходить на четвертом уровне протокола ОКС7 (подсистема ISUP) (рисунок 2).

Обмен данными подсистемы сбора информации с подсистемой анализа, мониторинга и принятия решений (ПАМПР) предлагается организовать по протоколу IIOP (Internet Inter-ORB Protocol). Преимуществами данного протокола являются минимум ресурсных затрат при взаимодействии компонент CORBA и «прозрачность» взаимодействия с сетями TCP/IP (рисунок 3).

В анализатор поступает поток сообщений, который разбирается на составляющие, которые далее подвергаются фильтрации.

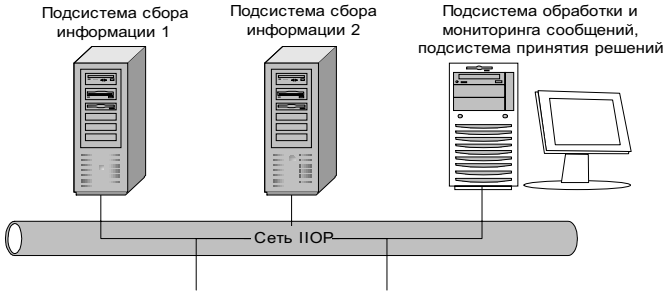

Рисунок 3. Образование единой системы анализа

Выбор алгоритма фильтрации зависит от следующих параметров:

- адресов источника и получателя;
- категории пользователя;
- поступающей команды;
- истории команд и соединений.

Самым простым видом фильтрации является фильтрация по адресам. Организуется БД, в которой регистрируются адреса санкционированных (СП) и несанкционированных (НСП) пользователей. Сообщения от НСП не анализируются (хотя возможен статистический анализ команд, посылаемых такими пользователями) и сразу отбрасываются.

Фильтрация по категориям пользователей является более сложной, поскольку предполагает анализ не только адресной части сообщения, но и прав доступа к определенным службам внутренней сети. Данный алгоритм фильтрации применяется в том случае, когда пользователь запрашивает информацию, необходимую для инициализации услуги (установление соединения, опрос доступности службы, опрос маршрутов).

Анализ поступающих команд является следующей стадией анализа. На данной стадии анализируется возможность настройки соединения после подключения, переведение системы в режим отладки, запросов передачи/при-

ема данных, фильтрации ошибочных команд и т.п. Для данного типа фильтрации характерен анализ одношаговых, несвязанных команд.

Анализ истории команд и сообщений является самым сложным процессом. Здесь проводится долгосрочная выборка команд из БД, после чего происходит анализ взаимосвязанных действий на интервале, меньшем или равном времени соединения. Такой вид анализа необходим при работе системы в режиме виртуальной частной сети или в режиме отладки. Поскольку анализ является сложным, то для него необходимо значительное количество вычислительных ресурсов. Поэтому требуются модифицированные алгоритмы анализа и мощные вычислительные машины.

Взаимодействие с «внешней средой» происходит через дополнительное подключение ПАМПР к сети IIOP или TCP/IP. Сюда входят функции удаленного администрирования, взаимодействия с БД и подачи сигналов оператору. Возможно также подключение к внешней биллинговой системе. Интегрируемость в другие системы становится возможной, если при разработке анализатора используются общепринятые стандартизированные протоколы и были приняты во внимание рекомендации ITU для TMN.

5. Хранение данных и протоколирование событий в сети

Для хранения данных могут применяться различные схемы. Основным различием схем является местоположение данных (рисунок 4).

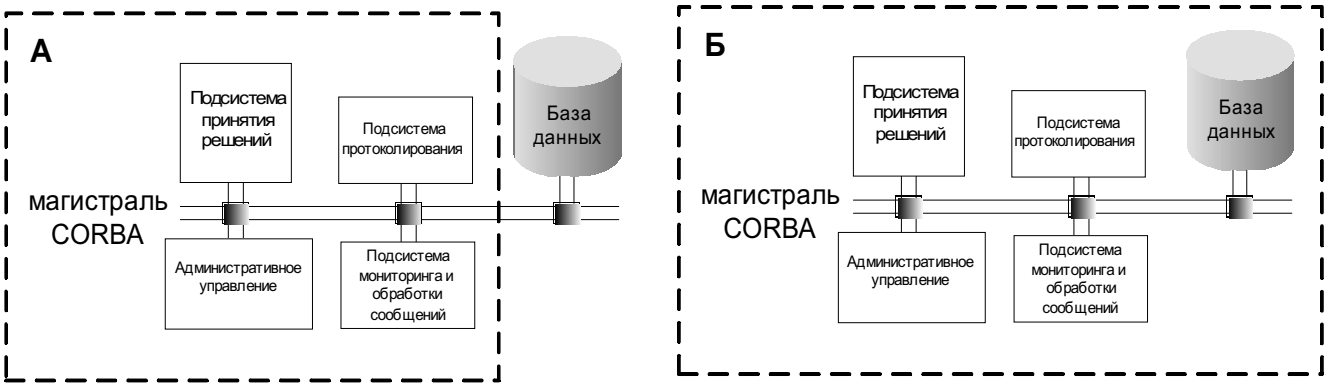

Рисунок 4. Подсистемы анализатора в соответствии с используемыми механизмами взаимодействия CORBA

В случае *А* модуль для хранения базы данных находится отдельно от других частей анализатора и, вероятнее всего, является разделяемым ресурсом. В случае *Б* БД хранится на накопителях вместе с другими подсистемами. Однако для всех подсистем физическое местоположение БД не играет роли, так как используется архитектура CORBA, которая предусматривает «прозрачный» доступ к объектам (сгенерированный код программы-заготовки доставляет запрос БД в виде обычного вызова метода). Используемая модель запросов, обладающих функциональными возможностями вызова методов, предполагает, что все запросы характеризуются точкой назначения, операциями и набором параметров.

Типы полей БД должны быть примитивными, и это позволит быстро проводить сортировки и выборки. Ни в коем случае не следует использовать объектные БД. В качестве адаптера CORBA следует выбирать BOA – он проще и поддерживается большим количеством фирм-производителей ПО. Также имеются различные бесплатные реализации адаптера.

Протоколирование событий, происходящих в сети, позволяет вести статистику по соединениям, пользователям, командам и внутрисетевым маршрутам. Данная статистика позволяет, при расширении возможностей анализатора дополнительными функциями, оптимизировать алгоритмы обработки входящих запросов, маршруты продвижения трафика. Собственно, возможно использование анализатора не как средства защиты, а как устройства сбора статистики для внутренних сетей. Это позволит выяснить сложившуюся ситуацию в сети и провести ряд технических и организационных мероприятий по ее реконструкции.

6. Временные характеристики анализатора, проблема производительности

Важнейшим аспектом работы анализатора является согласование с удаленными сторонами отправителя и получателя. Такое согласование накладывает жесткие нормы на время пребывания информации в модуле, являющемся системой массового обслуживания реального времени. В основе расчета максимально допустимого времени пребывания кадра или сигнальной единицы в анализаторе используются следующие глобальные стандарты ITU-T:

- рекомендации Q.706, определяющие нормируемые задержки для оконечного и транзитного пунктов сигнализации;
- рекомендации E.721 и E.723, нормирующие число пунктов коммутации и транзитных пунктов сигнализации, а также нормы сквозных задержек для типовых сигнальных соединений при различных видах связи.

Однако максимально допустимое время пребывания сигнальной единицы в системе будет существенно меньше указанных выше значений, поскольку необходимо учитывать время передачи в транзитном пункте сигнализации, время распространения по звену данных сигнализации и т.д.

Максимально допустимое время пребывания значащей сигнальной единицы в комплексе $T_ф$ не должно приводить к превышению общего времени передачи сообщений при отсутствии искажений $T_{ои}$, которое определяется:

$$T_{ои} = T_{запр} + T_{проверки} + T_{ответа} \quad (1)$$

где $T_{запр}$ – время, затрачиваемое на передачу сообщения из потока к системе принятия решений;

$T_{проверки}$ – время, затрачиваемое системой принятия решения для генерации ответа;

$T_{ответа}$ – время, необходимое системе для возврата сообщения в цифровой поток. В случае фильтрации $T_{ответа} \approx 0$. В случае работы анализатора в сквозном режиме (только лишь ведение статистики) $T_{ои}=0$.

Расчет временных задержек анализатора для модели M/G/1 производится на основе рекомендации Q.706 ITU-T. Использование данной модели обусловлено необходимостью оценки средней задержки требования в системе, определяемой по формуле Полячека-Хинчина [4]. Отношение $T_ф / \overline{x}$, то есть времени, проведенного сообщением в системе, ко времени, которое необходимо в среднем на обслуживание одного требования, определяется как:

$$T_ф / \overline{x} = 1 + \rho \frac{(1 + C_b^2)}{2(1 - \rho)}, \quad (2)$$

где $\rho = \lambda \overline{x}$ – коэффициент использования анализатора, равный произведению интенсивности поступления требований в систему на среднее время обслуживания; $C_b^2 = \sigma_b^2 / \overline{x}^2$ – нормированная дисперсия времени обслуживания, равная отношению дисперсии промежутка времени между соседними требованиями ко второму моменту распределения времени обслуживания.

На время пребывания сообщения в анализаторе влияют следующие факторы: нестандартность команды, производительность выбранных технологий, выбор реализации алгоритма фильтрации и вычислительная сложность самой фильтрации.

Нестандартность – это отклонение от стандартов ITU. При реализации нестандартных функций сети используются дополнительные команды, передающиеся в необязательных параметрах сообщений ISUP. Чем больше параметров у команды, тем дольше она обрабатывается системой. Наибольшее время обработки сообщений наблюдается, например, при реализации функции частной виртуальной сети.

При использовании технологии CORBA на производительность распределенной системы сильное влияние оказывают следующие факторы:

- количество вызовов удаленных методов, проводимых в системе;
- объем данных, передаваемых с каждым вызовом удаленных методов;
- затраты на обработку различных типов IDL-данных, используемых в системе.

Эффективность брокера запросов во многом определяется набором следующих функций:

1. Функция кодирования–декодирования запроса.

Пусть $M(x)$ – функция кодирования запроса x, $DM(x)$ – функция декодирования. Тогда:

$$DM(x+y) = M(x+y)' = (M(x) + M(y) + R(x,y))' \quad (3)$$

где $x+y$ – конкатенация x и y; $R(x,y)$ – количество байтов, выравнивающих y до 4 байт после x.

Пусть $T_M(x)$ – время выполнения $M(x)$. Тогда можно условиться, что время кодирования линейно растет в соответствии с длиной запроса, поэтому можем заметить, что

$$T_M(x+y) = T_M(x) + T_M(y) + T_{R(x,y)} \quad (4)$$

где $T_{R(x,y)}$ – время, затрачиваемое на добавление выравнивающих байт. $T_{R(x,y)} << T_M(x)$. Размер GIOP последовательности также растет пропорционально размеру параметра:

$$|M(x)| = K_{SM} \times |x| \quad (5)$$

где K_{SM} – коэффициент преобразования запроса, показывающий, насколько в среднем увеличивается размер кодируемого запроса, $|x|$ – размер запроса x в байтах.

Заметим также, что время декодирования приблизительно равно времени кодирования.

2. Функция поиска в таблице объектов. Заметим, что основной параметр, от которого зависит эта функция – количество одновременно существующих объектов в системе. Пусть время выполнения этой функции:

$$T_{FO}(o, N_O) \quad (6)$$

(здесь o – объект, N_O – размер таблицы активных объектов в системе).

3. Функция поиска в таблице методов:

$$T_{F_m}(m, N_m(o)) \quad (7)$$

где m – метод, $N_m(o)$ – размер таблицы удаленных методов объекта o.

4. Функция активации объекта и вызова метода: $T_I(o,m)$, в которую входит время вызова сервера и инициализации, при необходимости, его потока исполнения. Эта функция зависит от загрузки операционной системы, стратегии обработки параллельных вызовов и от количества поддерживаемых соединений.

5. Функция сетевой среды, которая добавляет время на пересылку данных:

$$T_S(x) = K_S \times |M(x)| = K_S \times K_{SM} \times |x| = K_S' \times |x| \quad (8)$$

где K_S – среднее время пересылки одного байта.

Таким образом, мы можем построить следующую аналитическую модель выполнения CORBA вызова:

Пусть имеется программный код $y = m(x)$, выполняемый в контексте c. Тогда приближенное время вызова в нашей модели можно определить, выполнив следующие шаги вычислений.

1. Время кодирования запроса:

$$T_M(req(o,m,x,c)) \approx T_M(o+m+x+c) \approx K_M \times (|o| + |m| + |x| + |c|) \quad (9)$$

2. Время пересылки запроса:

$$T_S(req(o,m,x,c)) \approx K_S' \times (|o| + |m| + |x| + |c|) \quad (10)$$

3. Время поиска объекта, соответствующего метода, активации объекта и, собственно, вызова метода:

$$T_{FO}(o, N_O) + T_{Fm}(m, N_m(o)) + T_I(o,m) \quad (11)$$

Суммируя все временные затраты, получаем:

$$T_{y=o.m(x)|c} \approx (2K_M + K_S') \times (|o| + |m| + |x| + |y|) + (4K_M + 2K_S') \times |c| + T_{FO}(o, N_O) + T_{Fm}(m, N_M(o)) + T_I(o,m) \quad (12)$$

Переобозначая константу $K_{REL} = 2K_M + K_S'$, получаем:

$$T_{y=o.m(x)} \approx K_{REL} \times (|o| + |m| + |x| + |y|) + 2K_{REL} \times |c| + T_{FO}(o, N_O) + T_{FO}(o, N_O) + T_{Fm}(m, N_m(o)) + T_I(o,m)$$

Таким образом, мы получаем оценку времени вызова метода, основываясь на которой, можно получить критерии оценки эффективности реализаций механизмов вызова.

Исследуем теперь производительность системы в зависимости от типа используемых данных. Конфигурация тестовой системы – компьютер на базе процессора Duron 950 MHz, 256 Mb ОЗУ. Программа реализовывалась на Borland C++ Builder 5.0 с использованием брокера VisiBroker 4.0 (CORBA 2.4). В качестве операции была выбрана операция маршаллинга представления элементарной операции IAM (начального адресного сообщения).

IAM представлялось в виде 32 байтовой последовательности, содержащей код операции, адрес и дополнительные поля. Другими словами, исследовалась скорость маршаллинга/демаршаллинга 32 байт данных. Всего был произведен один миллион операций (рисунок 5).

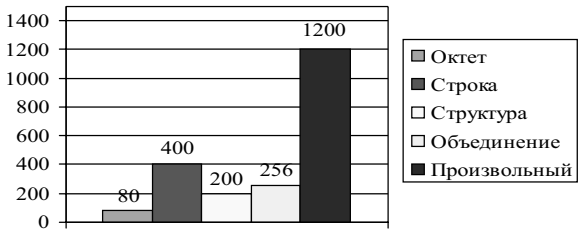

Рисунок 5. Скорость маршаллинга 1,000,000 32-байтовых IAM-представлений, секунд

Быстрее всего маршаллизуются данные, представленные октетами. Поэтому эффективнее всего для C++ использовать массивы данных типа CORBA::Long (конкатенация данных с типом CORBA::Long сохраняет линейной зависимость (3)). Использование произвольного типа вообще не позволит организовать анализ сигнальной линии при такой конфигурации.

Разработка интерфейсов для распределенных объектов требует более тщательного рассмотрения обеспечения производительности, нежели для объектов, принадлежащих одному адресному пространству. При реализации взаимодействия в распределенной среде следует внимательно рассмотреть возможные способы организации доступа к объектам. Основная работа по увеличению производительности подсистем должна касаться оптимальности описаний системного взаимодействия на языке IDL. Желательно использовать самые простые типы данных для передачи по сети. Также, необходимо держать в определенных рамках количество вызовов, чтобы обеспечить приемлемый уровень производительности (рекомендуется использовать конкатенацию сообщений).

Обмен данными должен происходить в асинхронном режиме, при отсутствии синхронизирующих задержек. При этом увеличивается скорость и производительность подсистем, ориентированных на потоковые данные.

Косвенной синхронизацией выступает время, за которое поступившее сообщение должно быть обработано и отправлено в поток. Если это время превышено, данные сообщения отбрасываются, а система сигнализирует, что не может справится с задачей анализа. Если же сообщение удачно обработано, то оно собирается по частям в буферной памяти анализатора и по достижению задержки в $T_ф$ передается в цифровой поток.

7. Экономическая целесообразность использования комплекса

При исследовании экономической целесообразности использования комплекса необходимо исходить из следующих соображений:

- стоимость защищаемой информации должна превышать стоимость комплекса;
- необходимо реализовывать только те функции, которые действительно необходимы в данной ситуации;
- по возможности необходимо использовать бесплатное ПО для реализации анализатора линий, однако следует помнить, что такое ПО, как правило, менее отлажено, обладает не всеми необходимыми функциями и, возможно, не обеспечивает приемлемый уровень производительности;
- всякое аппаратное и программное обеспечение морально устаревает. Однако ОКС7 является общепризнанным, повсеместно используемым стандартом и будет таковым еще в течение не менее 20 лет.

Данная разработка обладает рядом преимуществ перед ПРОТЕЙ-TFW:

- отсутствие в явном виде системы синхронизации, что увеличивает скорость реакции системы;
- работа в различных режимах – сквозном, обычном, с максимальной степенью анализа;
- использование бесплатных или условно-бесплатных программных средств;
- возможность объединения нескольких анализаторов.

Выводы

Необходимость в защите линий сигнализации очевидна, и решением проблемы является использование аппаратно-программных комплексов. В таких комплексах могут реализовываться дополнительные функции по сбору статистической информации о сети и организации виртуальных сетей. Скорость работы анализаторов зависит от их реализации, в меньшей степени аппаратной, чем программной. Поэтому необходимо рассматривать различные варианты реализации функций фильтрации, рациональных механизмов передачи данных.

Основным местом применения комплексов являются АТС, как частные, так и государственные. Возможность связывания анализаторов в единую сеть посредством магистрали CORBA, является неоспоримым преимуществом, поскольку возможен охват сети уровня города. Поскольку предлагается следовать рекомендациям ITU, возможна интеграция в другие системы.

Литература

1. ITU-T. Message transfer part (MTP). Recommendation Q.701-Q.707. – 1993. – Geneva.

2. Гольдштейн Б.С. Системный подход к реализации информационной безопасности узлов коммутации. Электросвязь, 2003. – №4. – С.28-32.

3. Слама Д., Гарбис Дж., Рассел П. Корпоративные системы на основе CORBA. М.: Издательский дом «Вильямс», 2000. – 368с.

4. Клейнрок Л. Теория массового обслуживания. М.: Машиностроение, 1979. – 432 с.