Математические структуры и моделирование
2002, вып. 10, с. 170–172

УДК 621.316.5

СИСТЕМА МУЛЬТИПЛЕКСИРОВАНИЯ РАЗНЕСЕННОГО TCP/IP ТРАФИКА

В.И. Ефимов, Р.Т. Файзуллин

Some special redirect points was added for security IP traffic construction.

Пусть необходимо передать информацию с одного компьютера на другой (далее демультиплексор и мультиплексор), обеспечивая при этом некоторую безопасность передачи данных. Предлагается осуществить разнесение передачи по нескольким физическим каналам отдельных частей передаваемого текста таким образом, чтобы с физической точки зрения перехват всех частей текста был затруднителен и сложность восстановления исходного текста без какой-либо его части была максимальной, или, иными словами, реализован аналог телефонного шифратора Д.Х.Роджерса [1] для WWW. Данная система в простейшей форме легко реализуется в стеке TCP/IP на сеансовом уровне модели ISO/OSI, благодаря использованию промежуточных передатчиков, рис 1.

Данные приложения на демультиплексоре разбиваются (демультиплексируются) на две части, в соответствии с алгоритмом работы программы, передавая каждую часть своему TCP-приложению. Каждое из TCP-приложений совместно с TCP-приложением на соответствующем передатчике заботится о надежной доставке передаваемых данных от демультиплексора к передатчику. После обработки данных на уровне TCP пакеты передаются уровню IP. В заголовке полученного IP - пакета в поле отправитель стоит IP-адрес демультиплексора, а в поле получатель IP адрес передатчика. Благодаря такой реализации происходит сокрытие «глобальных адресов», т.е. адреса конечного пункта назначения и адреса устройства, изначально отправившего данные. Т.е. при перехвате пакета на участке передатчик1 — мультиплексор, об адресе демультиплексора ни на каком уровне ничего сказать нельзя. Таким образом, передатчики выполняют двоякую функцию: выступают в роли посредников (proxy), позволяют задать траекторию прохождения трафика, выступая в качестве узловых точек (т.е. между двумя смежными точками образуется отдельное TCP/IP-соединение и передаются слагаемые адреса назначения). При работе на сеансовом уровне имеется возможность оперирования потоком данных и любыми его частями, не заботясь о его достоверности и надежности (в случае использования TCP в качестве транспортного протокола). Таким образом, возможны различные вариации самого модуля мультиплексирования. Один из его вариантов представлен на рис. 2.

© **2002 В.И. Ефимов, Р.Т. Файзуллин**

E-mail: rtf@univer.omsk.su

Омский государственный университет

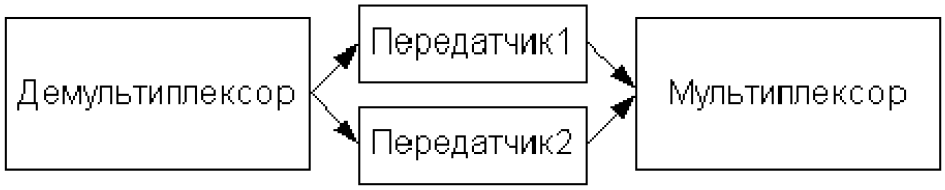

Рис. 1. Простейший случай системы мультиплексирования.

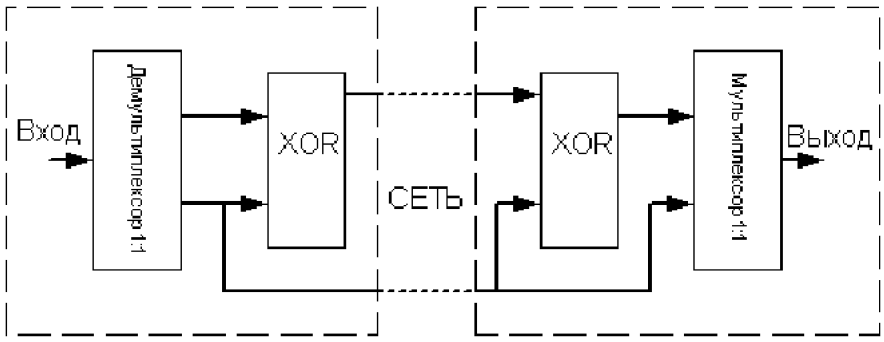

Рис. 2. Вариант работы мультиплексирующего модуля с маскированием каналов.

В этом случае данные разносятся (мультиплексируются на два потока) побайтно. Затем первый поток маскирует второй, и уже эта последовательность посылается в один из каналов, являясь «как бы» более защищенной. Один из исходных потоков, представляя собой часть исходного текста, посылается в другой. На приемном конце данные первого канала снова маскируются потоком второго канала, образуя маскируемый поток и, мультиплексируясь с маскирующим потоком, образуют исходную последовательность. Этот вариант возможно использовать в сетях, где вероятность доступа злоумышленника к одному из каналов достаточно мала (по нему можно передавать немаскированный текст - «ключ»), а по другому, вероятность доступа к которому выше, данные передаются в «зашифрованном» виде. В конечном счете уязвимость системы тем ниже, чем выше плотность расположения в сети передатчиков (с их помощью мы точнее задаем маршрут прохождения пакетов). Вторым критическим параметром для описанного случая можно считать энтропию исходного сообщения. При ее большом значении, даже после мультиплексирования побайтно, по двум каналам, без маскирования, при условии перехвата сообщения не более чем одного канала, восстановление исходной последовательности представляет нетривиальную задачу. Простейшим способом повышения энтропии текста может служить его архивирование и/или предварительное шифрование методом двойной перестановки блоков данных.

Литература

1. Kahn D. *The story of secret writings.* Macmillan. N.Y. 1967.

Математические структуры и моделирование
2002, вып. 10, с. 172–191

УДК 519.876.5:681.518

ИМИТАЦИОННОЕ ИССЛЕДОВАНИЕ КОНЦЕПЦИЙ СБОРА ИНФОРМАЦИИ ДЛЯ ИНДЕКСОВ ПОИСКОВЫХ СИСТЕМ

И.А. Земсков

In the e article the description of web resources' information state monitoring system is presented. Then two simulation models of this system for two building concepts were built. Computer models were realized on Python with SimPy package. The result of our own experiment is considered.

Введение

Общий круг проблем, стоящих перед разработчиками подсистем сбора информации для поисковых систем, был обозначен в статье [1]. В этой же статье кратко были рассмотрены возможные подходы к решению поставленных проблем. Эти подходы формируют три основные концепции (роботов, сенсоров, мобильных роботов) реализации подсистем создания представления об информационном содержимом сети Интернет. В настоящее время наибольшее развитие получила концепция роботов. Фактически она является единственной концепцией, применяемой поисковыми системами сети Интернет. Так как поиск публикаций, проливающих свет на причины такого предпочтения, не дал никакого результата (утверждение о том, что концепцию роботов легко внедрить, за аргумент не принималось), то остаётся загадкой фактически нулевой интерес со стороны разработчиков и исследователей к альтернативным концепциям. Однако отсутствие интереса к альтернативным концепциям не означает отсутствие интереса к развитию различных стратегий в рамках концепции роботов. А вот здесь становится заметной практика предварительного имитационного моделирования для исследования вновь предлагаемых стратегий разработки роботов с целью нахождения наиболее оптимальных вариантов построения алгоритмов их функционирования [2]. Применение имитационного моделирования в исследованиях тесно связанно с термином «система». Пристальный взгляд на обозначенную проблемную область позволяет заметить, что мы действительно имеем дело с системой. Согласно Р.Шеннону [3], система определяется как группа, или совокупность объектов, объединённых некоторой формой регулярного взаимодействия или взаимозависимости для выполнения заданной функции. В нашем случае совокупностью объектов системы S можно назвать совокупность информационных ресурсов и узла поисковой системы, занимающегося мониторингом

© **2002 И.А. Земсков**

E-mail: zemskov@univer.omsk.su
Омский государственный университет