АЛГОРИТМ ПО установления КВК-соединения на абонентском доступе сети ПД с учетом обеспечения ИБ

М.Басараб, д.ф.-м.н., зав.кафедрой "Информационная безопасность" МГТУ им. Н.Э.Баумана,
Р.Бельфер, к.т.н., доцент кафедры "Информационная безопасность" МГТУ им. Н.Э.Баумана / a.belfer@yandex.ru,
Е.Глинская, ст. преподаватель кафедры "Информационная безопасность" МГТУ им. Н.Э.Баумана,
А.Кравцов, с.н.с. НИИЦ ЦНИИ ВВКО

УДК 621.392, DOI: 10.22184/2070-8963.2017.69.8.64.69

Алгоритм программного обеспечения, выполняющего функцию установления соединения на участках абонентского доступа сети ПД, изложен на сети технологии виртуальных каналов гипотетической конфигурации по двум параллельным путям маршрутизации. ПО включает диспетчер программ и описание алгоритма 12 программ.

Введение

На кафедре "Информационная безопасность" МГТУ им. Н.Э.Баумана ведется работа по созданию учебного лабораторного стенда (УЛС) имитатора сети передачи данных. Цель этих работ – получение знаний и опыта для создания отечественных сетей ПД категории специального назначения, к которым предъявляются высокие требования по надежности, информационной безопасности и другим характеристикам. В работе по УЛС [1] приводятся технологии построения сетей ОгП: коммутация пакетов (КП) данных по физическим адресам; коммутация пакетов данных по логическим адресам; коммутация каналов. На данном этапе разработки имитатора сети ПД в УЛС принята коммутация пакетов данных по логическим адресам (на базе виртуальных каналов). Эта технология используется в сетях связи общего пользования X25, Frame Relay, ATM и в социальной сети MPLS [2, 3]. Показано, что параллельная передача одних и тех же сообщений по нескольким путям маршрутизации позволяет решать задачи по выполнению высоких требований по таким показателям, как надежность, задержка вероятности доставки сообщений. В [4] приводится укрупненный алгоритм установления/разъединения, передачи данных и сброса соединения на базе виртуальных каналов на примере гипотетической структуры сети с пучком маршрутов из четырех путей маршрутизации.

Настоящая работа посвящена описанию разработанного алгоритма программного обеспечения установления коммутируемого виртуального канала (КВК) на абонентском доступе имитатора сети ПД с учетом обеспечения информационной безопасности. Этот алгоритм используется при создании УЛС. В качестве имитатора сети ПД принята гипотетическая двухмаршрутная конфигурация. Рассматривается участок абонентского доступа на этапе установления соединения (КНК). ПО имитатора сети ПД разрабатывается на одном компьютере. Работа выполняется студентами на пятом и шестом курсах в плане создания учебного лабораторного стенда и проведения лабораторных работ.

Конфигурация имитатора сети ПД

Алгоритм ПО в настоящей статье изложен на примере установления соединения в конфигурации имитатора сети ПД с адресацией оконечных пунктов и центров коммутации пакетов (ЦКП), приведенной на рисунке. Здесь приняты следующие физические адреса: оконечных пунктов 101 (a), 102 (b), 103 (c); ЦКП абонентских доступов этих оконечных пунктов 11 (ЦКП 1.1), 21 (ЦКП 2.1); оконечных пунктов 601 (f), 602 (d), 603 (e); ЦКП абонентских доступов этих оконечных пунктов 31 (ЦКП 3.1), 32 (ЦКП 3.2).

Описание алгоритма ПО в статье приводится на примере установления КВК между оконечными пунктами a и f. Источником сообщения "Запрос вызова" (ЗВ) на установление соединения примем оконечный пункт a. Первый путь маршрутизации включает ЦКП 1.1 и ЦКП 3.1, второй путь – ЦКП 3.1 и ЦКП 3.2 абонентских доступов.

Итак, программное обеспечение включает диспетчер программ и описание алгоритма 12 программ. Рассмотрим эти компоненты.

Как работает ПО

Диспетчер программ DISP управляет последовательным выполнением программ $P_1, P_2 \ldots P_{12}$.

Программа P1 – установление адресов оконечных пунктов и ЦКП сети ПД.

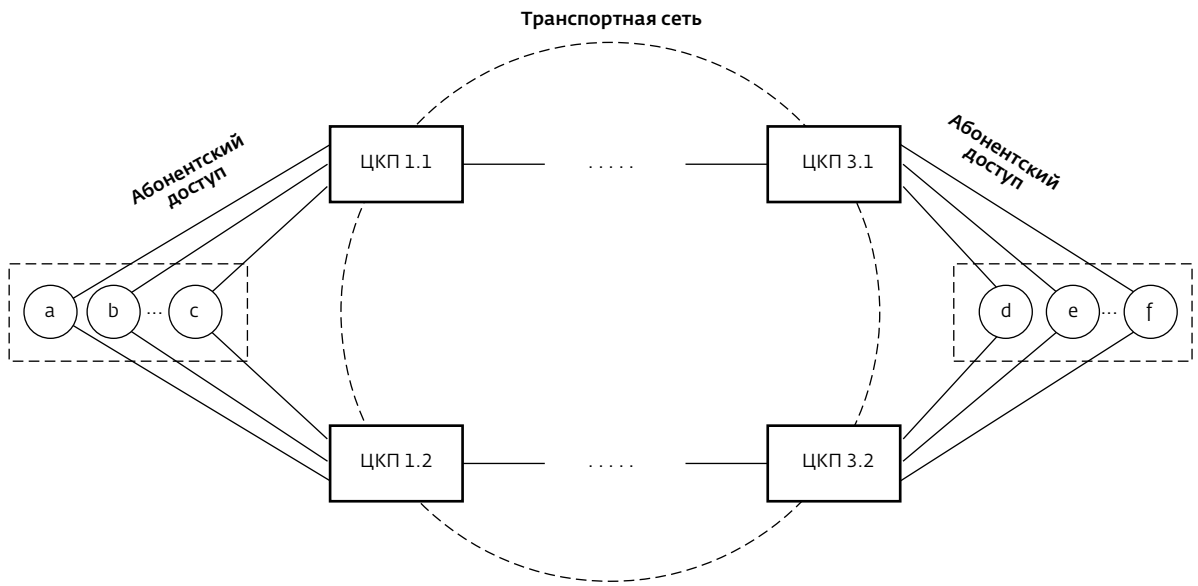
Программа P_2 – формирование очередей N1, N2 и N3 свободных блоков и очередей свободных номеров [3, 5]. Ее задачи: выделить память под N1 свободных блоков, создать очереди свободных блоков $O_{своб.}$ из N1 свободных блоков, создать очереди свободных номеров $O_{свн1112}$ и их характеристики $H_{свн1112}$ в ЦКП 1.1 и ЦКП 1.2 (примем $O_{свн1112}$=809; 802; 805; 814;815; 816); выделить память под N2 свободных блоков, создать очереди свободных блоков $O_{своб.}$ из N2 свободных блоков, создать очереди свободных номеров $O_{свн3132}$ и их характеристики $H_{свн3132}$ в ЦКП 3.1 и ЦКП 3.2 (примем $O_{свн3132}$=714; 722; 715; 720; 717; 719). Значения этих очередей используют уникальные логические адреса вместо физических адресов. Такие логические адреса называют логическими канальными номерами (LCN – Logical Channel Number). Они служат для создания таблиц маршрутизации коммутируемого виртуального канала.

Программа P_3 – установление ассоциации безопасности на абонентском доступе оконечного пункта источника. Ее задачи: сформировать в оконечном пункте источника (в примере – a) установления КВК сообщение, включающее следующую последовательность параметров: тип сообщения (примем M=1), конфигурация сети (Z1), протокол аутентификации (Z2), шифрования (Z3), хэширования (Z4), алгоритма контроля целостности (Z5), причем в каждом из параметров устанавливается один или несколько вариантов – например, параметр Z1 выбирается из нескольких гипотетических конфигураций сети ПД (в УЛС предусмотрены две такие конфигурации – двухмаршрутная и четырехмаршрутная; в настоящей работе примем двухмаршрутную конфигурацию Z1=1 (стандарты Z3, Z4, Z5, выбираются с использованием библиотеки по адресу https://www.cryptopp.com)); сформировать в ЦКП 1.1 , ЦКП 1.2 сообщения, включающие выбранные параметры, и отправить это сообщение в оконечный пункт a.

Программа P_4 – создание имитаторов сертификатов на абонентском доступе оконечного пункта источника (алгоритм настоящей и следующей программы будет приведен в статье, которую планируется опубликовать в следующем номере журнала "ПЕРВАЯ МИЛЯ").

Программа P_5 – взаимная аутентификация оконечной станции источника виртуального соединения и ЦКП абонентского доступа, создание головного ключа. Один из результатов работы программы – создание общего головного ключа $K_и$ на участке абонентского доступа оконечного пункта источника установления соединения (коммутируемого виртуального канала).

Программа P_6 – формирование общего канального и сквозных ключей на участке абонентского доступа оконечного пункта источника установления соединения. Ее задачи – создать одинаковый для всех путей маршрутизации КВК общий канальный ключ шифрования/дешифрации $K_{аби.}$ $K_{аби}$=hash ($K_и$, Аоп), где $K_и$ – головной секретный ключ, созданный при взаимной аутентификации, Аоп – адрес оконечного пункта источника установления соединения (в примере – 101), запомнить в памяти ключ $K_{аби}$ для использования на других фазах КВК (передача данных и др.); создать сквозной ключ $K_{инф}$ шифрования/дешифрации информационной части передаваемого пакета данных по установленному соединению (примем одинаковым ключ шифрования информационной части передаваемого пакета данных по установленному соединению для всех путей маршрутизации, для шифрования информационной части пакета данных в направлении передачи сообщения ЗВ и в обратном направлении эти ключи примем одинаковыми для всех путей маршрутизации $K_{инф}$=hash ($K_и$, Аоп, Аопн), где Аоп – адрес оконечного пункта источника установления соединения (в примере – 101),



Конфигурация имитатора сети ПД

адрес Аопн – адрес оконечного пункта назначения установления соединения (в примере – 601)); создать сквозной ключ $K_{Цинф}$ контроля целостности информационной части передаваемого пакета данных по установленному соединению (для информационной части пакета данных в направлении передачи "Запроса вызова" и в обратном направлении эти ключи примем одинаковыми для всех путей маршрутизации $K_{Цинф}$=hash($K_и$, Аопн, Аоп)).

Программа P_7 – определение уникального LCN и передача его в оконечный пункт источника установления соединения. Ее задачи: на основании данных характеристики очереди $O_{свн1112}$ определить адрес стоящего первым свободного номера, который назначается LCN=809 (см. программа P_2), произвести коррекцию очереди $O_{свн1112}$ и ее характеристик [3] (в результате очередь $O_{свн1112}$: 802; 805; 814; 815; 816); произвести ключом $K_{аби}$ шифрование LCN=809 по согласованному алгоритму при выполнении программы P_3, отправить из ЦКП 1.1 и ЦКП 1.2 зашифрованный LCN=809 в оконечный пункт источника установления соединения (в примере а); отправить в ЦКП 1.1 и ЦКП 1.2 из оконечного пункта источника по двум путям маршрутизации зашифрованный ключом $K_{аби}$ физический адрес исходящего оконечного пункта – в контрольном примере – 101, физический адрес оконечного пункта назначения, в примере – 601 (по первому пути маршрутизации – в ЦКП 1.1, по второму – в ЦКП 1.2), произвести дешифрацию на приеме в ЦКП 1.1 и ЦКП 1.2.

Программа P_8 – формирование сообщения "Запрос вызова", определение уникального LCN и передача его в оконечный пункт источника установления соединения. В табл.1 приведены форматы сообщений "Запрос вызова" на установление КВК по каждому из двух путей маршрутизации.

Первая строка относится к первому пути маршрутизации, вторая – ко второму. Формат сообщения "Запрос вызова" на установление КВК состоит из следующих полей для каждого сообщения ЗВ – состояние КВК – установление соединения "1": номер пути маршрута, физический адрес исходящего оконечного пункта (в примере – 601), физический адрес оконечного пункта назначения (в примере – 601), цепочка физических адресов ЦКП каждого пути принудительной маршрутизации (указаны физические адреса только ЦКП абонентского доступа), LCN, тип сообщения, конфигурация сети "1". Каждое сообщение содержит открывающий и закрывающий флаги 01111110.

Программа P_9 – формирование части строки таблиц маршрутизации по логическим адресам входных сообщений в ЦКП абонентского доступа оконечного пункта источника установления соединения. Таблица маршрутизации в ЦКП

Таблица 1. Формат сообщения ЗВ по каждому пути маршрутизации абонентского доступа источника соединения

Состояние КВК	Номер пути маршрутизации	Физический адрес оконечного пункта исходящего	Физический адрес оконечного пункта назначения	Цепочка физических адресов ЦКП маршрута	LCN	Тип сообщения	Конфигурация сети
1	1	101	601	11...31	809	1	1
1	2	101	601	12...32	809	1	1

абонентского доступа конкретного КВК для каждого пути маршрутизации состоит из двух строк. Одна строка таблицы маршрутизации относится ко всем сообщениям (включая и сообщение ЗВ), передаваемым от оконечного пункта в ЦКП, другая строка – от ЦКП в оконечный пункт. Каждая строка состоит из двух групп параметров (характеристик): относящихся к входящему сообщению в ЦКП абонентского доступа; относящихся к исходящему сообщению из ЦКП абонентского доступа в смежный с ним ЦКП транспортной части сети ПД. Будем считать адрес 21 ЦКП, смежного с ЦКП 1.1, и адрес 22 ЦКП, смежного с ЦКП 1.2.

Настоящая программа формирует часть строки таблиц маршрутизации по логическим адресам в ЦКП 1.1 и ЦКП 1.2 абонентского доступа, относящуюся к входящим от оконечного пункта (в примере а с адресом 101) в эти ЦКП сообщениям ЗВ. В ЦКП 1.1 ЗВ поступают по первому пути маршрутизации, в ЦКП 1.2 – по второму пути маршрутизации. В табл.2 приведены строки таблицы для первого пути маршрутизации, в табл.3 – строки таблицы ЦКП 1.2 для второго пути.

Как видно из этих таблиц, в строке маршрутизации приведены следующие параметры (характеристики): адрес источника сообщения, поступившего в ЦКП 1.1 или ЦКП 1.2 (в данном случае – оконечный пункт с адресом 101); LCN этого сообщения (в данном случае – 809); производилось ли назначение этого LCN в данном ЦКП (в данном случае – да). Это необходимо учесть в алгоритме разъединения КВК. В том случае, если это имело место, то необходимо это значение LCN установить в очередь свободных номеров.

Программа P_{10} – формирование части строки таблиц маршрутизации по логическим адресам исходящих сообщений из ЦКП абонентского доступа оконечного пункта источника установления соединения. Для подготовки к передаче сообщения ЗВ от ЦКП абонентских доступов (в примере ЦКП 1.1 и ЦКП 1.2) в ЦКП транспортной сети ПД (в соответствии с цепочкой ЦКП маршрута, указанной в сообщении ЗВ) необходимо LCN, стоящий первым в $О_{свн1112}$ (т.е. LCN=802), снять с $О_{свн1112;}$ заменить в сообщении ЗВ (табл.1) LCN=809 на LCN=802 для всех путей маршрутизации. В результате $О_{свн1112}$: 805; 814; 815; 816. Настоящая программа формирует часть строки маршрутизации по логическим адресам в ЦКП 1.1 и ЦКП 1.2 абонентского доступа (табл.2 и табл.3), относящуюся к исходящим сообщениям от этих ЦКП в смежные с ними ЦКП транспортной части сети. Как видно из этих таблиц, в строке маршрутизации приведены следующие параметры (характеристики): адрес поступления сообщений из ЦКП 1.1 и ЦКП 1.2 в смежные ЦКП с адресами соответственно 21 и 22; LCN этого сообщения (в данном

Таблица 2. Таблица маршрутизации по логическим адресам в ЦКП 1.1

Номер КВК	Номер пути маршрутизации	Входящее сообщение в ЦКП 1.1			Исходящее сообщение из ЦКП 1.1		
		Адрес источника сообщения в ЦКП 1.1	LCN	$О_{свн}$	Адрес поступления сообщения из ЦКП 1.1	LCN	$О_{свн}$
1	1	101	809	Да	21	802	Да
	1	21	802	Да	101	809	Да

Таблица 3. Таблица маршрутизации по логическим адресам в ЦКП 1.2

Номер КВК	Номер пути маршрутизации	Входящее сообщение в ЦКП 1.2			Исходящее сообщение из ЦКП 1.2		
		Адрес источника сообщения в ЦКП 1.2	LCN	$О_{свн}$	Адрес поступления сообщения из ЦКП 1.2	LCN	$О_{свн}$
1	2	101	809	Да	22	802	Да
	2	22	802	Да	101	809	Да

случае – 802); производилось ли назначение этого LCN в данном ЦКП (в данном случае – да).

Программа $Р_{11}$ – алгоритм установления соединения на абонентском доступе оконечного пункта назначения. При разработке этого алгоритма необходимо учесть, что таблицы маршрутизации по логическим адресам в ЦКП 3.1 и ЦКП 3.2 сформированы в той части, которая относится к входящему в них сообщению ЗВ. Это реализуется при прохождении ЗВ на транспортном участке сети ПД. В табл.4 и 5 приведены эти части таблиц. Необходимо составить алгоритм программы формирования части строки маршрутизации по логическим адресам в ЦКП 3.1 и ЦКП 3.2 абонентского доступа, относящейся к исходящим сообщениям от этих ЦКП в оконечный пункт назначения (в примере f с адресом 601). Примем адрес 21 ЦКП, смежного с ЦКП 3.1; адрес 22 ЦКП, смежного с ЦКП 3.2.

Значение LCN = 714 получено из очереди свободных номеров в ЦКП 3.1 и ЦКП 3.2 (программа $Р_2$).

Кроме того, потребуется выполнить программы, аналогичные программам $Р_4$ и $Р_5$, создать одинаковый для всех путей маршрутизации КВК общий канальный ключ шифрования/дешифрации $К_{абн}$ = hash ($К_н$, Аоп), где $К_н$ – головной секретный ключ, созданный при взаимной аутентификации, Аоп – адрес оконечного пункта источника установления соединения (в примере 601); запомнить в памяти ключ $К_{абн}$ для использования на других фазах КВК (передача данных и др.); зашифровать LCN оконечного пункта назначения (в примере LCN = 714) и отправить в оконечный пункт (в примере по адресу 601).

Программа $Р_{12}$ – подтверждение установления коммутируемого виртуального канала. Функция подтверждения установления КВК выполняется передачей по сети ПД сообщения "Вызов принят" (ВП) от оконечного пункта назначения в оконечный пункт источника сообщения ЗВ на установление соединения КВК. Коммутация этого сообщения в ЦКП производится по таблице маршрутизации по логическим номерам. Формат сообщения ВП состоит из двух полей: тип сообщения М = 2, LCN. На каждом абонентском доступе производится шифрование/дешифрация канальным ключом сообщения ВП. Поэтому для выполнения коммутации сообщений ВП на основе строк маршрутизации, полученных при передаче сообщения ЗВ, необходимо составить еще одну строку. Обе эти строки таблиц маршрутизации (в примере табл.2–5) служат для маршрутизации сообщений не только ВП, но и сообщений передачи данных.

Таблица 4. Таблица маршрутизации по логическим адресам в ЦКП 3.1

Номер КВК	Номер пути маршрутизации	Входящее сообщение в ЦКП 3.1			Исходящее сообщение из ЦКП 3.1		
		Адрес источника сообщения в ЦКП 3.1	LCN	$O_{свн}$	Адрес поступления сообщения из ЦКП 3.1	LCN	$O_{свн}$
1	1	21	924	Нет	601	714	Да
	1	601	714	Да	21	924	Нет

Таблица 5. Таблица маршрутизации по логическим адресам в ЦКП 3.2

Номер КВК	Номер пути маршрутизации	Входящее сообщение в ЦКП 3.2			Исходящее сообщение из ЦКП 3.2		
		Адрес источника сообщения в ЦКП 3.2	LCN	$O_{свн}$	Адрес поступления сообщения из ЦКП 3.2	LCN	$O_{свн}$
1	2	22	924	Нет	601	714	Да
	2	601	714	Да	22	924	Нет

Покажем использование дополнительных строк при передаче ВП для подтверждения установления КВК: сообщения ВП с LCN = 714 передаются от оконечного пункта (в примере с адресом 601) в ЦКП 3.1 по адресу 31 (путь маршрутизации 1 табл.4) и в ЦКП 3.2 по адресу 32 (путь маршрутизации 2, табл.5); в соответствии с таблицами маршрутизации в ЦКП 3.1 и ЦКП 3.2 производится замена в ВП с LCN = 714 на ВП с LCN = 924; ВП с новыми LCN направляются в зависимости от пути маршрутизации в транзитные ЦКП. От ЦКП 3.1 адреса 31 (табл.4) по первому пути в ЦКП 2.1 по адресу 21, от ЦКП 3.2 адреса 32 (табл.5) по второму – от пути в ЦКП 2.2 по адресу 22.

Выводы

Разработанный вариант алгоритма программного обеспечения может быть использован для проведения студентами научно-практических работ в рамках учебного лабораторного стенда. Целью создания этого стенда является подготовка кадров для создания отечественных сетей ПД категории специального назначения с высокими требованиями по надежности, информационной безопасности и другим характеристикам.

ЛИТЕРАТУРА

1. **Матвеев В.А., Бельфер Р.А., Кравцов А.В.** Анализ технологий построения сети передачи данных с высокими требованиями по информационной безопасности, надежности и задержке // Электросвязь. 2017. № 5. С. 46–49.
2. **Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г.** Сети связи. Учебник для ВУЗов. – СПб.: БХВ-Санкт-Петербург. 2011. 400 с.
3. **Бельфер Р.А.** Сети и системы связи (технологии, безопасность) / Учеб. пособие по дисциплине "Сети и системы связи", электронное учеб. изд. – М.: МГТУ им. Н.Э.Баумана. 2012. 723 с.
4. **Матвеев В.А., Басараб М.А., Бельфер Р.А., Кравцов А.В., Мерзляков Д.И.** Алгоритм функционирования УЛС защищенной сети ПД на базе виртуальных каналов с высокими требованиями к качеству обслуживания // Электросвязь. 2017. № 8. С. 57–62.
5. **Бельфер Р.А.** Разработка и отладка программного обеспечения устройств сетей передачи данных: методические указания к лабораторным работам по дисциплине "Системы и сети передачи данных". – М.: ФГБОУ ВПО "МГТУ им. Н.Э.Баумана", 2014. 134 с.