XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V : С.192-193

УДК 004.056.55

А.П.Лубанец (асп., каф. Телематика), В.С.Заборовский, д.т.н., проф.

КЛАСТЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ВОПРОСЫ ОРГАНИЗАЦИИ ПАРАЛЛЕЛЬНЫХ ВЫЧИСЛЕНИЙ НА БАЗЕ КРИПТОАКСЕЛЕРАТОРОВ

Разработчики систем информационной безопасности (СИБ) сталкиваются со значительными трудностями при выполнении основополагающего требования: работа системы без значительных накладных расходов. Другими словами, СИБ должна быть построена таким образом, чтобы минимизировать потери производительности канала связи, что, ввиду многомерности сетевого пространства и методов обеспечения информационной безопасности в этом пространстве, является сложной научно-технической задачей.

Проводимые исследования и анализ информационных потоков в компьютерных сетях на пакетном уровне указывает на специфическую природу происходящих процессов, не укладывающуюся в традиционные рамки известных случайных моделей [1]. Дальнейшие исследования показали, что сетевой пакетный трафик при описании процессов передачи данных характеризуется свойствами самоподобия или масштабной инвариантности статистических характеристик, которые принято относить к фрактальным процессам [2].

Поэтому системы информационной безопасности необходимо проектировать в соответствии со структурой сетевых потоков: по принципам иерархии, самоподобия и масштабирования [3]. Такой подход получил наименование «кластер информационной безопасности» [4].

Акцент в функциональности кластера информационной безопасности делается на средствах криптографической обработки данных, ввиду того, что только использование данных средств позволяет:

- свести эквивалентность или сводимость угрозы к математической задаче, чтобы доказать безопасность информационной системы при условии, что указанная задача является сложной;
- иметь возможность прогнозирования безопасности информационной системы;
- сравнивать однотипные средств защиты информации, обеспечивающие защиту от одних и тех же угроз, и выбирать наилучший вариант [5].

В рамках данной работы рассматривается вариант решения проблемы высокопроизводительной криптографии в рамках концепции кластера информационной безопасности.

Основной проблемой применения криптографических технологий является большая вычислительная ресурсоемкость алгоритмов шифрования, среди которых выделяют три основных типа:

1) алгоритмы симметричного шифрования;
2) алгоритмы ассиметричного (двухключевого) шифрования;
3) алгоритмы получения хэш-функций.

Самыми ресурсоемкими являются последние два. И хотя симметричные алгоритмы значительно превосходят ассиметричные по скорости, для них стоит известная всем проблема конфиденциальной передачи ключа, что без использования ассиметричных алгоритмов в сложных инфокоммуникационных системах неактуально.

Если решать проблему ускорения криптографических алгоритмов исключительно программными средствами, то скорость будет невелика. К примеру, авторами была получена

скорость 35 Мбит/сек для KAME-реализации протокола IPSec в режиме туннелирования с использованием AH/MD5 и ESP/AES на криптошлюзах под управлением FreeBSD.

В настоящее время необходимо обрабатывать потоки в 100 Мбит/сек и уже чаще в 1000 Мбит/сек. Поэтому там, где есть большие вычислительные затраты целесообразно использование параллельных алгоритмов. Задача криптографической обработки информации в сетях, ввиду внутреннего параллелизма сетевого трафика, является естественным претендентом для ее решения на вычислительных системах построенных в соответствии с кластерной архитектурой. Задача параллельной криптографической обработки была решена ранее на вычислительном MPI-кластере [6]. На пяти узлах (10 процессоров) была получена производительность около 300% по сравнению с запуском задачи на одном узле. При этом остается альтернативный путь – создание аппаратных криптографических ускорителей. Учитывая, что в один корпус компьютера стандартной x86-архитектуры оптимальна (с точки зрения производительности шины PCI) установка трех интенсивно обменивающихся карт, а именно такой режим подразумевает криптографическая обработка, получаем то, что при наличии мультиплексирующего драйвера и операционной системы, хорошо работающей с прерываниями и механизмом DMA, можно получить значительное ускорение выполнения низкоуровневых криптографических функций «шифрование», «дешифрование», «подпись» и «проверка». Если производительности одного, полученного описанным способом, узла не хватает для обработки потока (к примеру, если это Gigabit Ethernet), то возможно объединение достаточного количества узлов в кластер с редиректором, реализующим оптимальную по времени реагирования на изменение характера потока дисциплину обслуживания, например, как это сделано в [6].

Стоит отметить, что макетные образцы криптоакселераторов, выполненные на базе ПЛИС Apex фирмы Altera в одиночном режиме, демонстрировали производительность 120 Мбит/сек и в мультиплексирующем (три акселератора) – 210 Мбит/сек (производительность указана для мультиплексирующего драйвера под ОС FreeBSD для криптоускорителя блочного алгоритма SPECTR-H64).

Приведенные исследования положены в основу масштабируемой по производительности криптографической подсистемы кластера информационной безопасности и должны обеспечить работоспособность данной подсистемы на скорости канала для современных технологий сетевого взаимодействия и различных вариантов ускоряемых криптографических алгоритмов.

ЛИТЕРАТУРА:

1. Leland W.E., Taggu M.S., Willinger and Wilson D.V. On the Self-Similar Nature of Ethernet Traffic. Proceedings of ACM SIGCOMM'93, San Francisco, 1993, v 23.

2. А.Я.Городецкий, В.С.Заборовский. Фрактальные процессы в компьютерных сетях. СПб, Из-во СПбГТУ, 2000.

3. Лубанец А. Вычислительные кластеры для создания систем информационной безопасности в высокоскоростных компьютерных сетях. // Конфидент. 2003. №2. С. 70-74.

4. Заборовский В., Лубанец А. Кластер информационной безопасности // Бди. 2003. №2. С. 32-35.

5. Ростовцев А.Г. Криптография и защита информации // Проблемы информационной безопасности. №2. 2002.

6. Концепция кластера информационной безопасности и реализация в соответствии с ней VPN-шлюза и анализатора сетевого трафика / Лубанец А.П., Заборовский В.С. // Материалы Второго Международного научно-практического семинара «Высокопроизводительные параллельные вычисления на кластерных системах», Нижний Новгород, издательство ННГУ, 2002.