Математические вопросы кибернетики и вычислительной техники 18, 1997, 58-64.

О методе реализации защиты от несанкционированного доступа в АТМ-сетях

А. М. Айрапетян, И. Л. Арутюнов, А. Г. Тарханян

Институт проблем информатики и автоматизации
НАН РА и ЕрГУ

В работе рассматриваются проблемы управления АТМ сетей. Показана актуальность реализации защиты доступа в АТМ сетях. Наиболее приемлимым решением для данной проблемы является добавление аутентикационного механизма при установлении виртуальных соединений. Предлагается метод защиты доступа (firewall) с использованием аутентикации, который является составной частью системы управления АТМ сетью.

Введение

На сегодняшний день многие организации проявляют интерес к коммуникационным сетям как на уровне пользователей общедоступных (public) сетей, так и частных (private) сетей. Таким образом, управление коммуникационными сетями становится важным вопросом в технологии связи. Вследствии быстрых изменений в сетевых технологиях, а также появления высококвалифицированных сетевых пользователей, управление сетями приобретает особую актуальность. Под сетевым управлением понимается создание, управление и функционирование коммуникационных сетей. В [6][7] выделено два основных аспекта сетевого управления: функциональный и административный. Функциональный аспект - это маршрутизация, управление потоками и перегрузкой, обнаружение ошибок и восстановление, а также - производительность. Административный аспект относится к проектировнию и планированию, пользовательскому интерфейсу, вопросам обеспечения защиты, составлению отчетов и др. Невозможно переоценить важность проектировния и планирования. В известном смысле любая другая функция зависит от функций проектировния и планирования. В связи с появлением интегрированных сетей с архитектурами, в которых звук, данные, текст и изображение передаются по одной и той же сети, а также широким использованием INTERNET, на первый план выходит такакя функция управления как "защищенность" узлов сети от несанкционированного доступа. Т.е. администраторам сетей необходимо получить средство для управления доступом к узлам сети, как составной части всей системы управления сетью. Особенно актуаль- но все вышесказанное для сетей с архитектурой АТМ (Asynchronous Transfer Mode).

1 Управление в АТМ-сетях

На сегодняшний день управление сетью является в основном набором дискретных процедур направленных на решение определенных проблем. Методы и средства, используемые для мониторинга и управления трафика для локальных сетей, не являются достаточными, когда необходимо управлять ресурсами в глобальных сетях. Кроме того, трафик установления соединений, чувствителен к задержкам, требует специального внимания, которое не является необходимым для асинхронных приложений. Эта разновидность фрагментированного подхода к управлению сетью не подходит для АТМ, которая использует одну и ту же технологию для передачи различных видов трафика и запуска различных приложений через локальные и

глобальные сети. Администраторам сети необходимо сквозное наблюдение ряда условий - от пропускной способности до задержки ячеек для неустойчивых соединений. Они также должны иметь возможность мониторинга и управления физически коммутируемой инфраструктуры. Ни одна система основанная на SNMP (simple network management protocol) платформе не предлагает возможностей объемных протоколов, необходимых для управления широкомасштабными ATM сетями. В настоящее время рабочая группа сетевого управления форума ATM[3] разрабатывает сквозную модель управления[1], которая включает в себя сервис, предоставляемый частными и общедоступными сетями, и определяет стандарт коммуникации их друг с другом. Модель также определит взаимодействие между SNMP и CMIP (common management information protocol). Пять ключевых интерфейсов управления определены в этой работе M1-M5 (см рис.1). Все они актуальны для сквозного мониторинга и контроля. Для администраторов сетей предприятий важны в первую очередь M1 и M2, они определяют интерфейс между системой управления сетью на стороне пользователя и ATM-станцией или сетевым переключателем. Однако ожидается, что управление в ATM сетях пойдет по направлению использования так называемых ячеек функционирования, администрирования, управления - OAM (operational, administration and management), а не с использованием таких протоколов, как SNMP или CMIP. Например, появится возможность динамической реконфигурации в случае ошибок. Сетевые узлы и конечные станции получат возможность реконфигурировать друг друга. Эта архитектура будет распределенной, в том смысле, что управление, включающее мониторинг и конфигурационные способности, будет распределено по всей инфраструктуре сети. ATM-форум предлагает 53 байтные OAM ячейки. Они будут содержать специализированные поля, которые будут определять их функции: управление ошибками, управление производительностью, активизация - деактивизация (для запуска и прерывания предыдущих функций управления). Ячейки OAM дадут возможность устройствам ATM-сети собирать информацию о сквозных соеденениях, уменьшить необходимость распределения базы управляющей информации MIB (management information base) по сети и уменьшить трафик относящийся к управлению.

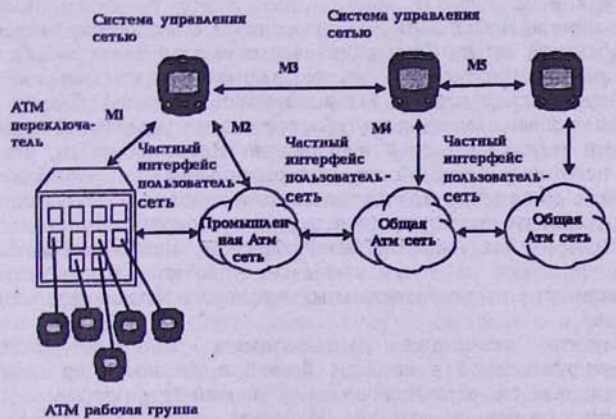

Рис. 1 Модель управления ATM.

2 Защита АТМ сетей

На сегодняшний день одной из самых распространенных систем защиты промЦышленных сетей от несанкционированного доступа являются так называемые firewalls [2]. Они являются одним из нерешенных вопросов АТМ-сетей. Firewall - это логические фильтры на мультипротокольных маршрутизаторах для управления и ограничения доступа к различным частям сети. Например, они могут разрешить доступ из общей сети в частную для протоколов FTP, но могут запретить тот же доступ для протокола Telnet. Используемые в настоящее время firewall являются надежным методом защиты сети. Наиболее распространенное место их установки это стык частной и общей сети. Firewall-ы реализованы сегодня на маршрутизаторах, которые могут работать не только на 3-ем уровне OSI передачи информации пакетов, но также просматривать и более высокие уровни, например номер порта TCP, для того чтобы выделить информацию необходимую для функционирования firewall.

Однако не совсем ясно, каким образом реализовать firewall в среде АТМ. Проблема в том, что как только устанавливается АТМ соединение, ни одно промежуточное устройство не в состоянии обработать поток данных посылаемый через это соединение. А это противоречит концепции firewall. Как только устанавливается связь между двумя узлами, любые данные могут посылатся без сетевого администрирования. Несмотря на то, что firewall или другие механизмы защиты могут быть реализованны в виде оконечных систем, это не является практичным решением.

Существует предложение, чтобы фильтрация в АТМ-сетях происходила во время установления связи, а не во время передачи данных. Специальные информативные элементы должны быть определены внутри сигнальных сообщений (это те сообщения, с помощью которых непосредственно устанавливается связь между двумя конечными узлами в АТМ сетях) для индикации протокола верхнего уровня, посредством которого необходимо установить соединение (например FTP или Telnet). Затем промежуточные переключатели могут отфильтровать соединения используя информацию полученную во время установления сообщения, такую как адрес отправителя и получателя, и т.д.

Фильтрация АТМ-адресов может быть использована на стыке между частной и общей сетью или глобальной сетью. Фильтрация адреса в этой точке может быть использована для разрешения соединения из доверенных адресов (например из удаленного узла, принадлежащего той же административной группе). Такого типа защита может быть использована вместе с другими средствами управления высокого уровня, использующими технику адресной фильтрации. Несмотря на то, что эти приемы могут иметь некоторые возможности, они ограничены тем, что конечной системе неизвестно какое соединение будет использовано, так как АТМ-соединения главным образом происходят на нижних уровнях внутри протокольного стека, а не в самом приложении. Поэтому как только установится связь, узел может посылать пакеты любого типа, и дойти до точки назначения любого поддерживаемого приложения, вне зависимости от опознавательных признаков задачи для, которой установлено соединение.

Необходимо отметить тенденцию использования многими сетевыми администраторами маршрутизаторов в качестве firewall в частности на границах частных сетей с общими, даже для соединения двух АТМ сетей друг с другом.

Одно из возможных решений данной проблемы видится в добавлении аутентикационного механизма, базирующегося на криптографии, в процедуру установления соединений АТМ.

3 Реализация firewall с использованием механизма аутентикации

Аутентикация - это идентификация плюс верификация. *Идентификация* - это процесс утверждения опознавательных признаков, а *верификация* - это процесс с помощью которого утверждение проверяется [11]. Поэтому, корректность аутентикации зависит в первую очередь от того на сколько серьезно проведена процедура верификации. Объекты в распределенных системах которые могут быть различным образом идентифицированны, определяются как *ведущие*. Существует три типа аутентикации в вычислительных системах:

(A1), аутентикация содержимого сообщения - определение, что содержимое полученного сообщения совпадает с отправленным;

(A2), аутентикация происхождения сообщения - определение того, что отправитель полученного сообщения тот же, кто записан в поле отправителя сообщения;

(A3), опознавательная аутентикация - верификация того, что опознавательные признаки *ведущих* такие же, как утверждены.

(A1) обычно поддерживается посредством вставки кода аутентикационного сообщения - MAC (message authentication code), в тело сообщения перед посылкой. Целостность сообщения может быть подтверждена по принятию сообщения посредством вычислением MAC-а и сравнением его с тем, что содержится в сообщении.

(A2) - это частный случай (A3). Успешная опознавательная аутентикация обычно проявляется в убеждении со стороны *ведущего* аутентикации (проверяющего), что аутентицированный *заявитель* владеет заявленными опознавательными признаками. Отсюда, последовательные действия со стороны заявителя являются качественными для заявленой идентификации; например (A3) необходима для случаев авторизации и функций учета.

Взаимная аутентикация это процесс, с помощью которого общающиеся друг с другом *ведущие* проверяют опознавательные признаки каждого из них, но не однонаправленная аутентикация, где только один *ведущий* проверяет признаки другого. В распределенной сети аутентикация осуществляется с помощью протокола, который использует обмен сообщениями. В дальнейшем мы будем называть эти протоколы протоколами аутентикации. Существующие системы используют очень примитивные аутентикационные методы, или они не используются вообще. Такого типа методы серьезным образом неадекватны, потому что понятие доверия в такого типа системах не понятно. Должна быть еще предложена удовлетворительная форма доверия. Во вторых, расширяющаяся распределенная система, содержащая в себе большое количество административных групп, порождает исключительно сложное взаимодействие доверия.

Аутентикация в сетевых системах осуществляется с помощью соответствующих протоколов. *Протокол* - это точно определенная последовательность вычислительных и коммуникационных действий. Коммуникационные действия передают сообщение от одного *ведущего* (отправителя) к другому (получателю), в то время как вычислительные действия изменяют внутреннее состояние *ведущего*. Два различных состояния могут быть идентифицированы по окончанию протокола, в одном случае приводя к успешной аутентикации, в другом случае - к ошибке.

Несмотря на то, что основная функция любой аутентикациии заключается в проверке заявленных признаков *ведущего*, специфичные успешные или ошибочные состояния очень протоколо-зависимы. Например, успех аутентикации во время установления связи коммуникационного протокола обычно осуществляется посредством распространения свежего сессионного ключа между двумя взаимно аутентицированными процессами. Другими словами, например, во время

аутентикации установления соединения успешность обычно проявляется в создании соединения от имени устанавливающего соединение. Протокол представляется в следующем формате. Коммуникационное действие, в котором P посылает сообщение M для Q представляется как P → Q: M, имея в виду что вычислительное действие записывается как P:..., где "..." - это спецификация вычислительного действия. Например типичный протокол установления соединения между H и U представлен ниже, (f - это однонаправленная функция, т.е по данному y вычислительно невозможно найти x так, что f(x)=y).

U → H: U
H → U: "Введите пароль"
U → H: p
H : вычисление y=f(p)
: получение записи (U, f(пароль$_U$)) из базы данных
: если y=f(пароль$_U$) тогда допустить, иначе отвергнуть.

Необходимо отметить, что концепция протоколов иллюстрирует только основные принципы разработки. Реальные протоколы могут использовать как симметричные, так и асиметричные криптосистемы [4, 5, 8, 10].

Наиболее важная часть аутентикации - это структура сертификатов с общим ключем. Каждый пользователь имеет уникальное имя. Доверенный сертификационный центр CA (certification authority) назначает уникальное имя каждому пользователю и генерирует подписанный сертификат, содержащий имя и пользовательский общий ключ. На рис. 2 представлен формат сертификата X.509.

Поле версии указывает на формат сертификата. Серийный номер уникален среди CA. Следующее поле идентифицирует алгоритм используемый для подписывания сертификата, вместе с другими необходимыми параметрами. Издатель - это имя CA. Срок действия - это пара дат; сертификат действителен, начиная с первой даты, по вторую включительно. Примечание - это имя пользователя. Параметры общего ключа включают в себя алгоритм, необходимые параметры, а также сам ключ. Последнее поле - это подпись CA.

Несанкционированный доступ к АТМ-узлам можно предотвратить посредством встроенного в переключатель комплекса программных средств, которые будут фильтровать соединения, используя адреса конечных узлов, и аутентицировать конечные узлы.

При этом вводится понятие так называемой административной группы. Административные группы определяют тип соединения (блокированный/ неблокированный) как для узлов внутри группы, так и для внешних по отношению к группе узлов.

Допустим, узел A пытается установить соединение с узлом B. Эти два узла входят в административную группу G, элементы которой могут общаться друг с другом. По сигнальному сообщению узла A переключатель α определяет группу, в которую входит данный узел, и посылает сертификат данного узла конечному переключателю β,
который хранит информацию о узле B. Конечным переключателем производится аутентикация узла A, желающего установить соединение, т.е. проверяется целостность сертификата, производится верификация подписи. На основе этой информации и делается вывод о том, можно ли устанавливать соединение, или нет.

Как было рассмотрено выше, OAM-ячейки содержат в себе поля управления и администрирования. Для посылки сертификатов могут быть использованы административные поля OAM-ячеек.

Такой механизм предполагает наличие главного аутентикационного-управляющего центра, который проводит начальную конфигурацию переключателей

т.е. определет состав группы, тип внутреннего и внешнего соединения для нее, а также аутентикацию самих переключателей.

В целом комплекс защиты ATM-сетей можно представить с использованием классической схеммы: УПРАВЛЯЮЩАЯ СИСТЕМА - УСТРОЙСТВО. Управляющая система представляет собой комплекс програмного и аппаратного обеспечения, с помощью которого производится конфигурирование промежуточного переключателя, а именно, создание административных групп, добавления в них конечных узлов, установка атрибутов, изменение состояния, сбор статистики. Наличие таких виртуальных групп для определения типа межузлового соединения позволит расширить возможности firewall, добавив возможности шифровки потоков между узлами, кроме обычного блокирования соединений.

Программа управления может быть реализована как с использованием традиционных языков: C, C++, так и используя объектно-ориентированные языки, например JAVA. В последнем случае решается одна из важнейших проблем - проблема переносимости программных средств. На сегодняшний день JAVA является достаточно гибким и универсальным языком, позволяющим использовать наиболее перспективные направления межсетевого управления и администрирования, а также объектно-ориентированную архитектуру приложений. Кроме того, данная методика позволяет построить управлющую систему на основе WEB.

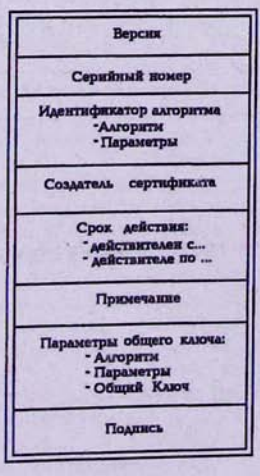

Рис. 2. Формат сертификата X.509

Литература

1. P.Alexander, K.Carpenter, "ATM Net Management: A Status Report", Data Communication, Sep. 1995.
2. A.Alles, "ATM Internertworking", Enginnering InterOp, Las Veghas,1995.
3. ATM Forum/95-0013R8.
4. Data Encryption Standard, FIPS Pub. 46, National Bureau of Standards, Washington , D.C., Jan. 1977.

5. W. Diffie and M.E. Helman, "Privacy and Authentication: An Introduction to Cryptography," Proc. *IEEE*, Vol. 67, No.3, Mar. 1979, pp.397-427.
6. J.L.Filmer, J.M. Mellichamp, S. Narayanan "An expert system for whide area network component configuration",Expert Systems, February 1992, Vol. 9, No.1, p.3-9.
7. Musgrave L., (1986) "Sorting out the solutions: network management is the eyes of the beholder", Datamation 15,98.
8. R.L.Riwest, A.Shamir, and L. Adelman, "A Method for Obtaining Digital Signatutes and Public-Key Cryptosystems, "Comm.ACM, Vol.21, No.2, Feb. 1978, pp.120-126.
9.B. Schneier, "Applied Cryptography Second Edition:protocols, algorithms, and source code in C", John Wiely & Sons, Inc, 1996
10. G.J. Simmons, "Symmetric and Assymetric Encryption", ACM Computing Syrveys, Vol. 11, No.4, Dec.1979. pp.305-330.
11. T.Y.C.Woo, S.S.Lam "Authentication for Distributed Systems", COMPUTER, January 1992, p. 39-50.

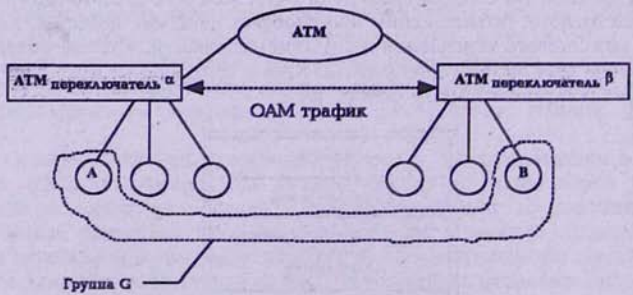

Рис.3 Пример аутентицированного соединения в АТМ сети