Информатика и вычислительная техника

УДК 621.39

Оценка времени установления сессии между пользователями при наличии межсетевого экрана

К. Е. Самуйлов, А. Ю. Ботвинко, Э. Р. Зарипова

Кафедра прикладной информатики и теории вероятностей
Российский университет дружбы народов
ул. Миклухо–Маклая, д. 6, Москва, Россия, 117198

Для эффективной разработки, дальнейшего внедрения и эксплуатации информационных систем связи необходимо предусмотреть своевременную защиту программ и баз данных, средств хранения, обработки и передачи информации. Для анализа производительности, надёжности и безопасности телекоммуникационных систем, а также для получения первичных оценок временных характеристик широко используются методы теории массового обслуживания. В статье для исследования метода оценки времени установления сессии при наличии межсетевого экрана выбрана процедура установления сессии между двумя конечными пользователями по протоколу установления сессий (Session Initiation Protocol, SIP) между двумя пользователями с одним межсетевым экраном по пути следования сигнальных сообщений. Под межсетевым экраном (firewall) подразумевается программный или аппаратный комплекс, реализующий функции фильтрации сетевого трафика между отправляющей и принимающей стороной по некоторому набору правил, определяемых политикой безопасности. Предложенный метод оценки основан на применении модели открытой экспоненциальной сети массового обслуживания. Приведён пример расчёта среднего времени установления сессии и средней задержки запроса сессии. Расчёт проведён для технических характеристик, соответствующих прокси-серверу CiscoASA 5500-Xc обслуживающим модулем SSP-10. Расчёт временных характеристик показывает приемлемость применения данного оборудования в сети связи и его малое влияние на временные характеристики даже при высокой нагрузке.

Ключевые слова: Session Initiation Protocol, межсетевой экран, время установления сессии, открытая сеть массового обслуживания, качество восприятия.

Введение

Для обеспечения надёжной информационной инфраструктуры необходимо своевременно разрабатывать и внедрять аппаратные или программные комплексы, обеспечивающие фильтрацию входящего потока по некоторым правилам. При внедрении таких комплексов, обеспечивающих контроль и безопасность, необходимо учитывать временные задержки для информационных потоков, проходящих проверку на безопасность. В данной работе исследуется время установления сессии между двумя пользователями, где информационные потоки проходят через межсетевой экран (МЭ) в прямом и обратном направлении.

В качестве примера выбрана одна из наиболее чувствительных к временным задержкам услуг — установление сессии между двумя абонентами при наличии двух прокси-серверов и одного межсетевого экрана по пути следования сигнальных сообщений. Время установления сессии включает время передачи сигнальных сообщений протокола установления сессий (Session Initiation Protocol, SIP) между двумя пользователями, время фильтрации сообщений в межсетевом экране, время ожидания и время обслуживания на каждом из прокси-серверов. Наличие МЭ увеличивает время установления сессии, однако обеспечивает контроль и фильтрацию проходящих через него сетевых сообщений. МЭ не избавляет от угроз утечки информации или от загрузки пользователями вредоносных программ, например, вирусов. Использование межсетевых экранов для защиты сетей вносит

Статья поступила в редакцию 27 ноября 2015 г.

Исследование выполнено при частичной финансовой поддержке РФФИ в рамках научных проектов № 15-07-03608, 15-07-03051.

задержку при передаче сообщений и, соответственно, вызывает необходимость учёта дополнительных задержек при установления сессии, что, в свою очередь, приводит к повышению требований к производительности межсетевых экранов по сравнению с фильтрацией не мультимедийного трафика. В статье ставится задача оценки времени установления сессии при внедрении в сеть МЭ.

Статья имеет следующую структуру. Первый раздел содержит описание процедуры установления сессии между двумя пользователями при наличии двух серверов SIP и одного МЭ. Приведён порядок обмена сигнальными сообщениями по протоколу установления сессий SIP, перечислены логические и функциональные блоки, принимающие участие в процедуре установления сессии. После детального изучения рекомендованных международными стандартами показателей качества восприятия было отмечено, что время установления сессии не может превышать 2 с [1].

Во втором разделе статьи исследованы временные характеристики, которые необходимо учитывать при установлении сессии: время установления сессии и задержка запроса установления сессии (англ, Session Request Delay, SRD), эту характеристику в дальнейшем будем называть задержкой запроса сессии. Время установления сессии является характеристикой качества восприятия (англ., Quality of Equipment, QoE). В разделе предложен метод оценки временных характеристик.

В третьем разделе предложенный метод используется для расчета времени установления сессии для оборудования Cisco. Оценено влияние времени фильтрации трафика в межсетевом экране на среднее время установления сессии и среднюю задержку запроса сессии. Заключение содержит основные выводы исследования.

1. Процедура установления сессии при наличии межсетевого экрана

В спецификациях протокола SIP, разработанных группой MMUSIC (Multiparty Multimedia Session Control) комитета IETF (Internet Engineering Task Force) [2,3], предусмотрены 3 основных сценария установления соединения: простое взаимодействие между двумя клиентами пользователей, соединение двух пользователей с участием сервера переадресации и соединение двух пользователей с использованием прокси-сервера.

Данные сценарии отличаются способом поиска адреса и приглашения вызываемого пользователя. При простом взаимодействии клиентов вызывающему пользователю для установления соединения необходимо знать текущий адрес вызываемого пользователя. При использовании сервера переадресации вызывающий пользователь передаёт серверу переадресации сообщение с известным ему адресом вызываемого пользователя, а сервер переадресации обеспечивает переадресацию вызова на текущий адрес этого пользователя. В этом случае сервер переадресации определяет текущий адрес вызываемого пользователя у сервера определения местоположения. В сценарии с использованием прокси-сервера функции поиска и приглашения вызываемого пользователя возлагаются на прокси-сервер.

На практике сценарии установления соединения могут состоять из более сложных цепочек – например, вызов может пройти сервер переадресации и несколько прокси-серверов. Более того, запросы могут быть размножены и переданы по разным маршрутам и т. п. В статье исследован один из возможных простых сценариев – установление сессии между двумя пользователями с участием цепочки из двух прокси-серверов и одного межсетевого экрана. Прокси-сервер Proxy-1 выполняет посреднические функции для первого пользователя, а прокси-сервер Proxy-2 – для второго пользователя. Предположим, что оборудование первого пользователя расположено внутри сети, защищённой межсетевым экраном, обеспечивающим контроль проходящих сетевых пакетов с целью выявления и предотвращения попыток несанкционированного доступа или злоупотребления сетевыми ресурсами. В этих условиях при фильтрации межсетевым экраном исходящих пакетов от

первого пользователя и входящих пакетов от второго пользователя появляется дополнительная задержка. Схематичное расположение пользователей и функциональных элементов сети представлены на рис. 1.

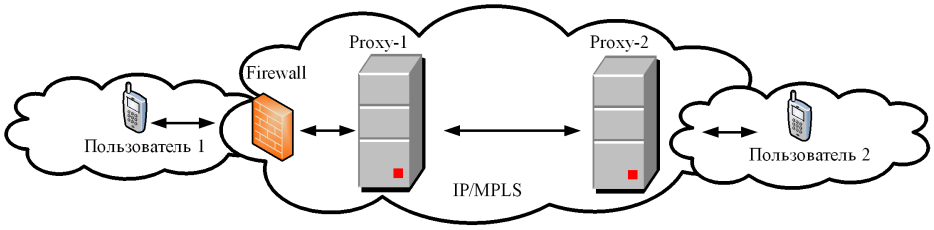

Рис. 1. Взаимодействие функциональных элементов при установлении сессии при наличии межсетевого экрана

Функциональными элементами, принимающими участие в процедуре установления сессии, являются прокси-серверы (Proxy-1 и Proxy-2), межсетевой экран (Firewall), магистральная сеть IP/MPLS и оборудование пользователей. Заметим, что некоторые из этих элементов могут быть реализованы на практике совместно, например, межсетевой экран может быть объединён с прокси-сервером в одном оборудовании. Для предварительной оценки времени установления сессии выбрана процедура, где каждый функциональный элемент реализован отдельно.

Сессия инициируется первым пользователем сигнальным сообщением Invite в момент нажатия клавиши на своём оборудовании. Процедура установления сессии учитывает запросы и ответы, пересылаемые от одного функционального блока к другому. Запрос Invite содержит информацию об адресате, ответом на запрос Invite является сообщение 100 Trying, которое высылается на предыдущий функциональный блок при успешной обработке сообщения Invite [1, 3]. Заметим, что в рамках данной работы исследуется случай успешного установления сессии без ретрансляций сообщений. С помощью данного сценария можно оценить среднее время установления сессии T_S от отправления инициирующего сообщения до начала предоставления данных и среднюю задержку запроса сессии T_{SRD} от момента инициации сессии до получения первым абонентом ответа 180 Ringing, которое указывает, что все функциональные блоки готовы к обслуживанию абонентов [3]. Процедура установления сессии учитывает время обслуживания в сети, магистральная сеть IP/MPLS представлена в виде отдельного функционального блока, время обслуживания в сети при движении в одну сторону от одного абонента к другому будет равно половине времени передачи в петле связи (англ., Round Trip Time, RTT). Сигнальное сообщение протокола установления сессий 180 Ringing передаётся от вызываемого абонента к вызывающему абоненту при успешном получении инициирующего сообщения Invite. Далее в процедуре установления сессии предусмотрен обмен сообщениями 200 Ok и Ack, что подтверждает приём ответа на запрос Invite. После обмена этими сигнальными сообщениями сессия считается установленной, начинается обмен данными между двумя абонентами.

Последовательность сигнальных сообщений в виде процедуры установления сессии при наличии одного межсетевого экрана представлена на рис. 2. Необходимо заметить, что внедрение межсетевого экрана в процедуру установления сессии увеличивает время установления сессии, т.к. происходит фильтрация трафика, в том числе сигнального, проходящего через межсетевой экран [4].

2. Расчёт времени установления сессии при наличии межсетевого экрана

Для оценки влияния времени фильтрации в межсетевом экране на время установления сессии между двумя абонентами предлагается математическая модель

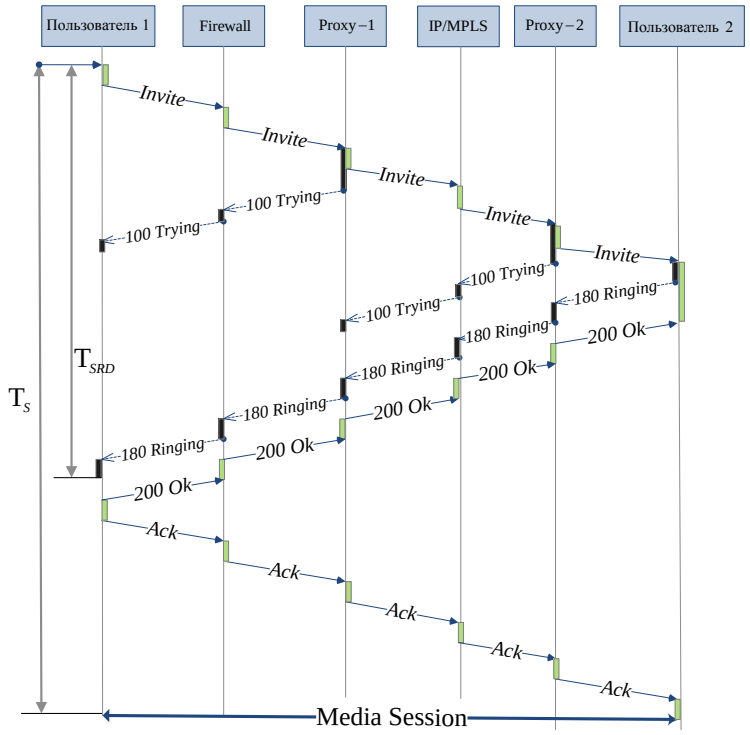

Рис. 2. Процедура установления сессии при наличии межсетевого экрана

в виде открытой сети массового обслуживания (CeMO), в которой время пребывания в сети соответствует времени установления сессии. Подобный подход исследовался в работах [5,6]. При данном подходе необходимо оценить время ожидания и время обслуживания последовательно по каждому функциональному блоку, затем, просуммировав все интервалы времени, получить время установления сессии. Таким образом, CeMO будет состоять из шести узлов в виде систем массового обслуживания (СМО), каждая СМО будет представлять отдельный функциональный блок, соответствующий процедуре установления сессии. Блоки, соответствующие оборудованию обоих пользователей и сети IP/MPLS, будут представлены с помощью СМО $M|M|\infty$, остальные блоки — в виде СМО $M|M|1|\infty$.

Обозначив интенсивность входящих сообщений λ_0, определим условие существования стационарного режима в виде (1), где μ_i^{-1} — время обслуживания сообщений прибором в СМО, соответствующей i-му блоку в процедуре установления сессии [6]

$$\lambda_0 < \min\left(\frac{\mu_2}{5}; \frac{\mu_3}{5}; \frac{\mu_5}{4}\right). \tag{1}$$

Данное неравенство (1) следует из того, что в узлах 2, 3 и 5 могут возникать очереди, что нарушает стационарный режим.

Учитывая подход, предложенный в работах [5, 6], средняя задержка запроса сессии T_{SRD} и среднее время установления сессии T_S определяется в виде (2) и (3) соответственно.

$$T_{SRD} = 2\mu_1^{-1} + \frac{2}{\mu_2 - 5\lambda_0} + \frac{2}{\mu_3 - 5\lambda_0} + 2\mu_4^{-1} + \frac{2}{\mu_5 - 4\lambda_0} + \mu_6^{-1}; \tag{2}$$

$$T_S = 2\mu_1^{-1} + \frac{3}{\mu_2 - 5\lambda_0} + \frac{3}{\mu_3 - 5\lambda_0} + 3\mu_4^{-1} + \frac{3}{\mu_5 - 4\lambda_0} + 2\mu_6^{-1}. \tag{3}$$

Время фильтрации межсетевым экраном сигнального сообщения равно времени пребывания сигнального сообщения во втором функциональном блоке (Firewall). Время фильтрации одного сообщения при установлении сессии представлено формулой (4)

$$T_F = \frac{1}{\mu_2 - 5\lambda_0}. \tag{4}$$

Проведём расчёт показателей влияния наличия межсетевого экрана на среднюю задержку запроса сессии и на среднее время установления сессии. Эти показатели отражены в формулах (5) и (6) соответственно.

$$N_{T_F\_T_{SRD}} = \frac{2T_F}{T_{SRD}}; \tag{5}$$

$$N_{T_F\_T_S} = \frac{3T_F}{T_S}. \tag{6}$$

3. Пример расчета времени установления сессии

Для предварительной оценки временных характеристик были выбраны исходные данные, характерные для оборудования Cisco. Технические характеристики прокси-сервера соответствуют прокси-серверу Cisco на платформе Sun Fire V120. Для характеристик межсетевого экрана выбран Cisco ASA 5500-X с обслуживающим модулем (Security Service Processor - SSP) SSP-10. В таблице 1 перечислены исходные данные и их соответствие введённым в статье обозначениям.

Таблица 1

Исходные данные

Функциональный элемент	Пользователь-1	Firewall	Proxy-1	IP/MPLS	Proxy-2	Пользователь-2
Обозначение	μ_1^{-1}	μ_2^{-1}	μ_3^{-1}	μ_4^{-1}	μ_5^{-1}	μ_6^{-1}
Время обслуживания, мс	0,1	0,5	0,4	50	0,4	0,1

Результаты расчета средней задержки запроса сессии T_{SRD} и среднего времени установления сессии T_S приведены в виде графиков зависимости от интенсивности поступающих запросов (рис. 3).

Условие существования стационарного режима (1) позволяет провести расчёт для значений интенсивности входящего потока вплоть до 400 запросов в секунду. Технические характеристики соответствуют прокси-серверу Cisco на платформе Sun Fire V120 и межсетевому экрану Cisco ASA 5500-X с обслуживающим модулем SSP-10. Предварительная оценка временных характеристик при наличии одного межсетевого экрана показывает приемлемые результаты, которые удовлетворяют рекомендованным международным стандартам показателей качества восприятия, среднее время установления сессии гораздо меньше 2 с и даже при интенсивности 380 запросов/с достигает значения 0,2 с. Средняя задержка запроса сессии SRD всегда меньше среднего времени установления сессии и при интенсивности входящего потока 380 запросов/с достигает 0,15 с.

Интересна оценка доли времени фильтрации сигнальных сообщений в межсетевом экране при расчёте временных характеристик. На рис. 4 изображены

показатели влияния времени фильтрации в межсетевом экране на время установления сессии. Отмечено, что время пребывания сигнальных сообщений в межсетевом экране не превосходит 10 процентов при интенсивности входящих сообщений для значений равных 370 запросов/с.

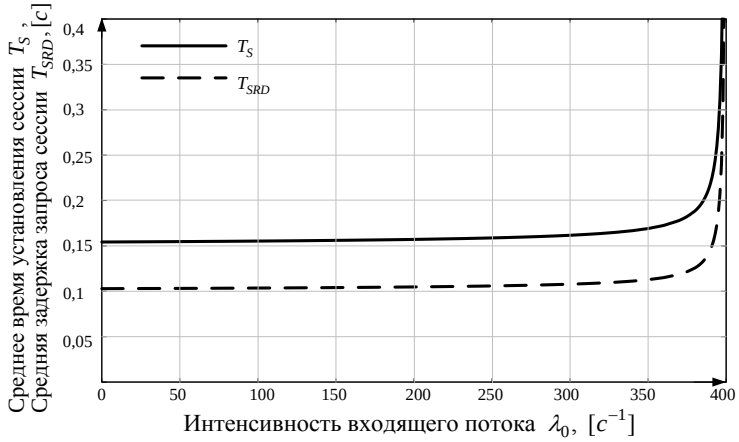

Рис. 3. Временные характеристики при установлении сессии с одним межсетевым экраном

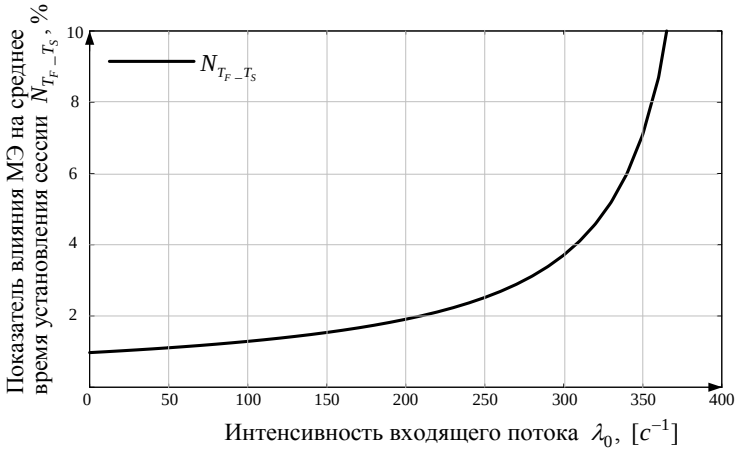

Рис. 4. Оценка доли времени фильтрации в межсетевом экране при установлении сессии

Заключение

В статье предложена математическая модель установления сессии между двумя пользователями с участием двух прокси-серверов и одного межсетевого экрана. Проведена оценка среднего времени установления сессии и средней задержки запроса сессии. Расчёт временных характеристик показал приемлемость использования оборудования Cisco ASA 5500-X с обслуживающим модулем SSP-10, использование межсетевого экрана необходимо в целях обеспечения информационной безопасности.

Полученные результаты могут найти применение при решении задач оценивания влияния МЭ на качество установления соединения протокола SIP. При дальнейших исследованиях производительности систем связи область применения построенной математической модели и предложенного метода может быть расширена на случай оценки показателей качества других услуг связи, чувствительных к длительности задержки передачи данных.

Литература

1. Triple-play Services Quality of Experience (QoE) Requirements Cluster: Techrep Technical Report-126 / DSL Forum. — 2006.
2. *Rosenberg J., Schulzrinne H., Camarillo G. et al.* RFC 3261, SIP: Session Initiation Protocol. — 2002. — `http://www.ietf.org/rfc/rfc3261.txt`.
3. *Malas D., Morton A.* RFC 6076, Basic Telephony SIP End-to-End Performance Metrics. — 2011. — `http://www.ietf.org/rfc/rfc6076.txt`.
4. *Иванов К. В., Тутубалин П. И.* Марковские модели защиты автоматизированных систем управления специального назначения. — Казань: ГБУ «Республиканский центр мониторинга качества образования», 2012. — С. 216.
5. *Самуйлов К. Е., Лузгачев М. В., Плаксина О. Н.* Разработка вероятностной модели для анализа показателей качества протокола инициирования сеансов связи. — Вестник РУДН. Серия: «Математика. Информатика. Физика», 2007. — С. 53–63.
6. *Gaidamaka Y., Zaripova E.* Session Setup Delay Estimation Methods for IMS-Based IPTV Services / Ed. by S. Balandin, S. Andreev, Y. Koucheryavy. — Springer International Publishing Switzerland, 2014. — Vol. 8638. — Pp. 408–418.

UDC 621.39

Session Setup Time Estimation in the Network with a Firewall

K. E. Samouylov, A. Yu. Botvinko, E. R. Zaripova

Department of Applied Probability and Informatics
Peoples' Friendship University of Russia
6, Miklukho-Maklaya str., Moscow, Russian Federation, 117198

In modern telecommunication networks is implemented information transmitting security for protection programs and databases. We propose the approach of signaling messages processing estimation in case when the network includes one firewall and two proxy servers. Firewall is based on security rules and define security police. We choose a session setup procedure between two users using the Session Initiation Protocol as an illustration of the method. Signaling messages are moving from the first user to the second through IP/MPLS network, proxy servers and firewall. The chain of signaling messages must successfully service before media traffic starts. We get preliminary estimation of performance measures for modern firewall Cisco ASA 5500-X with Security Service Processor SSP-10. Numerical example shows, that firewall Cisco ASA 5500-X serves signaling messages can be implemented. Mean waiting time and mean service time in this firewall has little effect on the session setup time and the session request delay.

Key words and phrases: Session Initiation Protocol, firewall, session setup time, open queuing network, Quality of Experience.

References

1. Triple-Play Services Quality of Experience (QoE) Requirements Cluster, Tech. Rep. Technical Report-126, DSL Forum (2006).

2. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, RFC 3261, SIP: Session Initiation Protocol (June 2002). URL `http://www.ietf.org/rfc/rfc3261.txt`
3. D. Malas, A. Morton, RFC 6076, Basic Telephony SIP End-to-End Performance Metrics (Jan. 2011).
URL `http://www.ietf.org/rfc/rfc6076.txt`
4. K. V. Ivanov, P. I. Tutubalin, Markov Models of Protection of Automated Control Systems for Special Purposes, Kazan: "Republican Center of Education Quality Monitoring", 2012, in Russian.
5. K. E. Samouylov, M. V. Luzgachev, O. N. Plaksina, Modelling SIP Connections with Open Multiclass Queueing Networks, Bulletin of Peoples' Friendship University of Russia. Series "Mathematics. Information Sciences. Physics", 2007, in Russian.
6. Y. Gaidamaka, E. Zaripova, Session Setup Delay Estimation Methods for IMS-based IPTV Services, Vol. 8638, Springer International Publishing Switzerland, 2014, pp. 408–418.