УДК 681.518

СЕГМЕНТИРОВАНИЕ РЕКОМЕНДАТЕЛЬНОЙ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ МЕТОДА ОРГАНИЗАЦИИ СОЕДИНЕНИЯ «КЛИЕНТ - СЕРВЕР», ОСНОВАННОГО НА ПРОГРАММНО-КОНФИГУРИРУЕМЫХ СЕТЯХ И ПРИМЕНЕНИИ ПРОТОКОЛА С БЫСТРЫМ ПЕРЕСКОКОМ IP-АДРЕСА

Бритвина Е.В.[1]

[1]ФГБОУ ВПО «Нижегородский государственный технический университет им. Р.Е. Алексеева», Нижний Новгород, Россия (603950, г. Нижний Новгород, ГСП-41, ул. Минина, д. 24), e-mail: ekbritv@heterarchica.com

Рекомендательная система, реализуемая в программном обеспечении SCSC, имеет кластерную архитектуру: кластер пользовательских данных, который принадлежит мобильному оператору, и кластер рекламных данных. Первый имеет очень важное значение в качестве объекта информационной безопасности, а второй должен быть открыт для нескольких рекламных агентств. В работе для решения задачи сегментирования рекомендательной системы предлагается использовать новейший метод организации соединения «клиент - сервер», основанный на программно-конфигурируемых сетях и применении протокола с быстрым перескоком IP-адреса. Технология прыгающего IP– адреса изолирует один сегмент от другого с помощью реализации SDN. Применение данной технологии радикально изменяет уровень безопасности системы в целом, несмотря на открытость одного из сегментов, в отличие от известных решений, использующих VPN.

Ключевые слова: рекомендательная система, графовая база данных, DDoS-атака, несанкционированный доступ.

RECOMMENDER SYSTEM SEGMENTATION USING FAST IP HOPPING PROTOCOL SDN IMPLEMENTATION

Britvina E.V.[1]

[1] "Nizhny Novgorod State Technical University n.a. R.E. Alekseev" Nizhny Novgorod, Russia (603950, Nizhny Novgorod, street Minin, 24), e-mail: ekbritv@heterarchica.com

Graph database based recommender system cluster architecture is described. The system is part of the VAS platform for smooth ads embedding to the mobile outgoing call progress phase. The software has to be deployed such way to has access to mobile operator central switching system. Two main hardware/software segments are defined: user data cluster owned by mobile operator and advertisement data cluster. The first one is very critical, as the information security object but the second segment has to be opened to multiple ads agencies. The problem is to support the platform necessary security level in this case. In the paper the new SDN based solution to interconnect two independent parts is proposed. Instead the particular VPN using the new method of permanent connection is described. The Fast IP Hopping protocol insulates the segments one from other using SDN implementation. The protocol based on the random IP address switching during every TCP session. The new quality of data access leads to high level of the system information security.

Keywords: Recommender System, LTE, graph database, DDoS attack.

Одним из приложений рекомендательных систем реального времени [1] вне традиционной области электронной торговли является их использование для встраивания рекламных или иных сообщений в сеанс исходящей связи абонентов мобильных (и фиксированных) телекоммуникационных сетей. Рассмотрим описанную в [2] систему, реализуемую в инфокоммуникационных сетях, использующих IMS (Internet Multimedia Subsystem [3]).

Рекомендательная система в этом случае реализуется в программном обеспечении SCSC, используя данные об абонентах и рекламные сообщения, хранящиеся в соответствующих базах данных. Как видно из функциональной схемы и в соответствии с общей структурой системы (рис. 1), рекомендательная система должна включать в себя как базу данных рекламных сообщений, которая создается и поддерживается рекламными агентствами и партнерами, так и базу данных пользователей, которая является охраняемым объектом оператора связи.

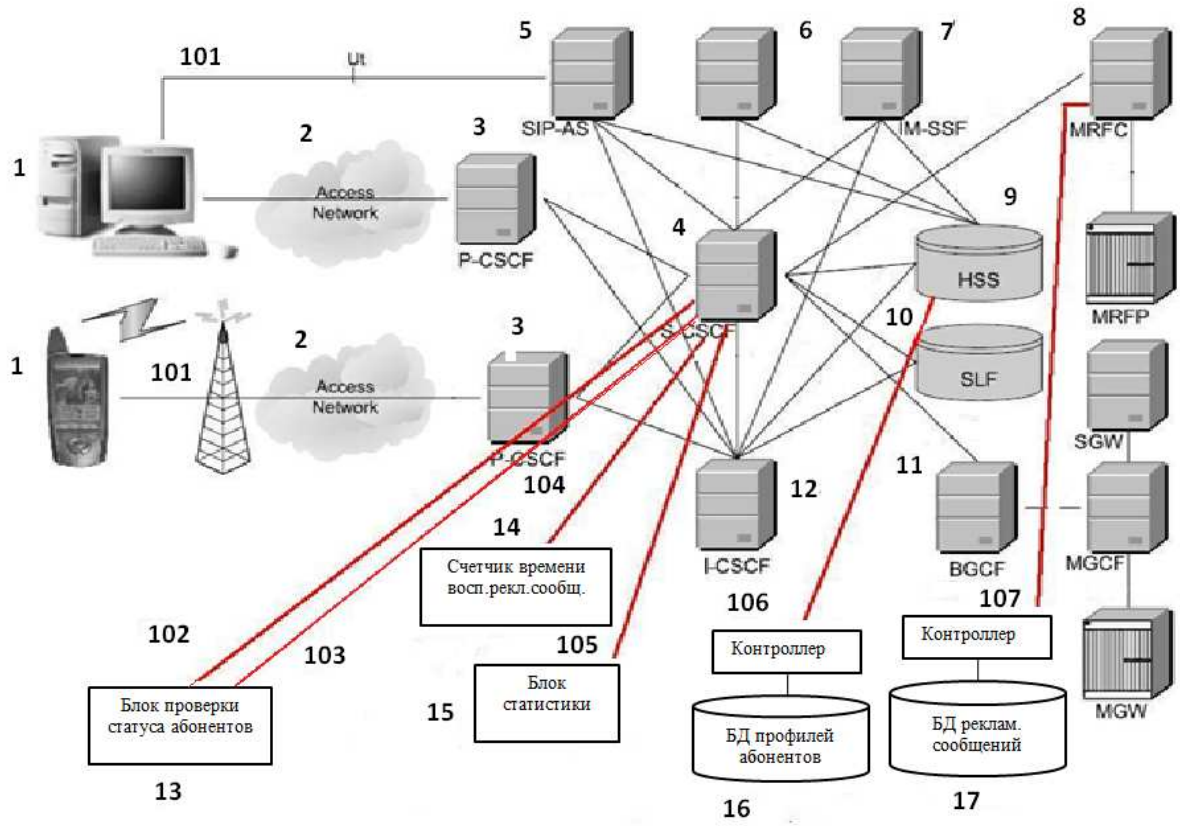

Рис. 1. Функциональная схема взаимодействия модулей системы встраивания рекламных сообщений с основными блоками UMTS сети с использованием IMS.

Размещение таких компонентов рекомендательной системы на одной площадке недопустимо и требует ее распределенного развертывания с объединением через каналы связи. Экономически выгодным здесь может быть только использование Интернета. Однако безопасность системы при сегментировании через Интернет потребует использования VPN для каждого из партнеров, что практически невыполнимо. В работе для решения задачи сегментирования рекомендательной системы предлагается использовать новейший метод организации соединения «клиент – сервер», основанный на программно-конфигурируемых сетях и применения и протокола с быстрым перескоком IP-адреса.

Рекомендательная система разбивается на два сегмента, один из которых представляет собой локальные сети партнеров, где создаются и хранятся в стандартных базах данных рекламные сообщения. Как правило, такие сети подключены к Интернету через шлюзы, оснащенные firewall.

Другой сегмент рекомендательной системы развертывается на площадках оператором мобильной связи и содержит весьма чувствительные персональные данные пользователей. Для этого сегмента такое решение в области безопасности не представляется приемлемым, поскольку стандартные средства firewall не защищают систему от атак, которые могут сделать невозможным наполнение базы данных сообщений, с другой стороны чувствительной к перехвату. Поэтому представляет большой интерес защита от несанкционированного доступа и DDoS–атак иными способами. В настоящей работе предлагается использовать технология прыгающего IP–адреса, а операторский сегмент рекомендательной системы разместить внутри программно-конфигурируемой сети.

Технологическая идея подобна тому, как она описана в [4].

В рассматриваемой работе предлагается способ защиты от распределенных атак типа «отказ в обслуживании», основанный на механизмах защиты на уровне протоколов и предложенный в рамках изобретения [5]. Здесь для обеспечения снижения нагрузки на сервер от производящих атаку «ботов» и исключения блокировки пакетов от легитимного клиента используется смена адреса сервера по расписанию, известному только авторизованному пользователю. Боты не получают достоверной информации о расписании смены адресов и не могут посылать запросы на адрес сервера, таким образом теряя возможность создать значительную нагрузку, нарушающую нормальное функционирование ресурса.

Предлагаемое решение аналогично тому, как делается это в радиотехнических системах с перескоком частоты (Frequency Hopping). Приемник и передатчик в течение интервала передачи одного сообщения переходят с одной частоты на другую синхронно, тем самым обеспечивая непрерывный процесс передачи информации. Передатчик злоумышленника, пытающийся поставить помеху приемнику или прослушать канал, не знает расписания смены частот и потому не может создать значительного ущерба работе защищенной с помощью перескока частоты радиолинии.

В нашем случае роль частоты играет IP-адрес, и клиент должен знать, по какому расписанию он изменяется у сервера. При этом расписание не должно быть открытым для внешних наблюдателей.

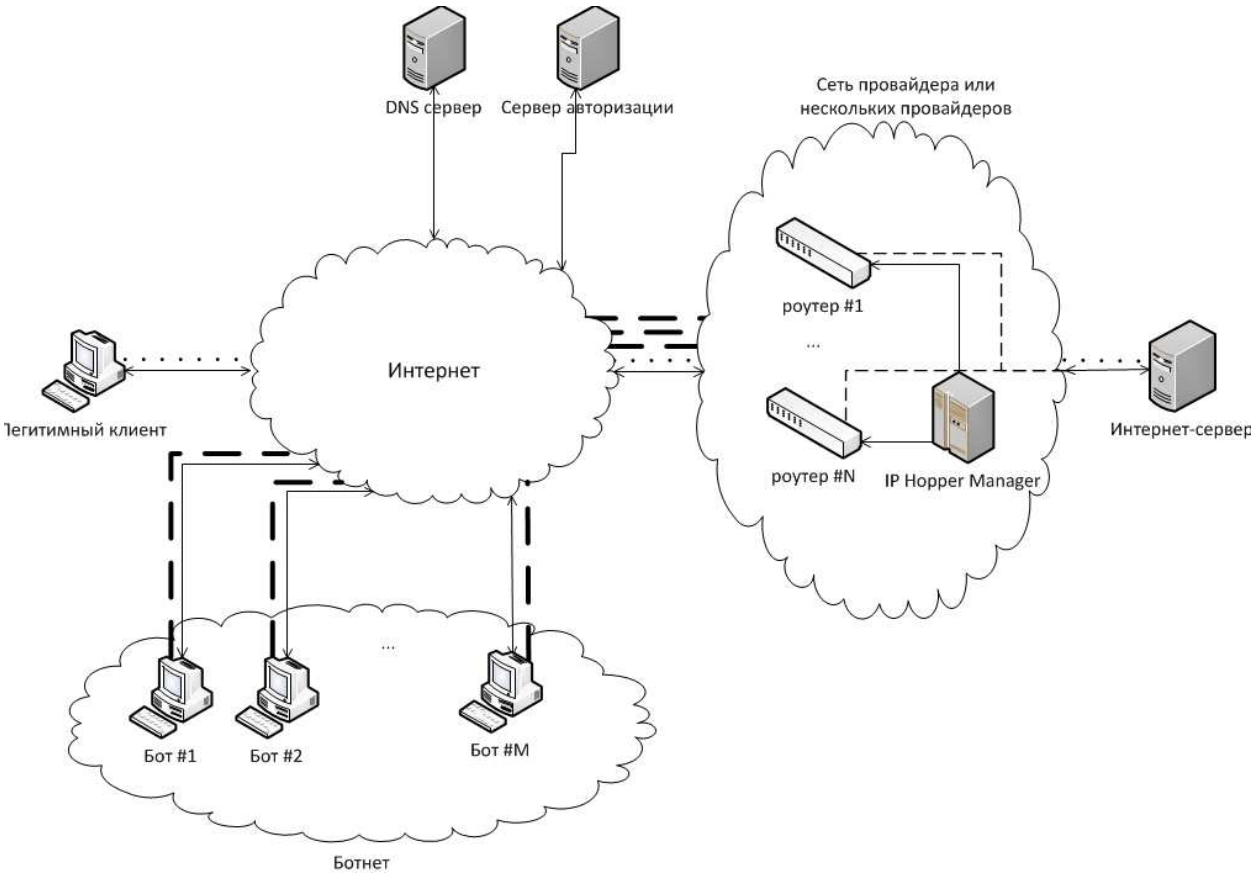

Рис. 2. ПКС защиты операторского сегмента рекомендательной системы

За основу была взята ПКС, образованная контроллером ПКС и двумя программируемыми роутерами. Контроллер осуществляет управление сетью и выполняет функции HopperManager для осуществления протокола быстрого перескока сетевых адресов, что делает соединение этого сегмента с любым легитимным клиентом партнерской сети безопасным как к перехвату, так и к атакам типа «отказ в обслуживании». На рисунке 2 представлена общая схема развертывания многосегментной рекомендательной системы с использованием защиты операторских сегментов с помощью протокола быстрого перескока сетевых адресов и реализацией в виде ПКС.

Таким образом, дается решение для развертывания масштабируемой рекомендательной системы на распределенном кластере с двумя сегментами, разделенными территориально и объединенными как IP-подсети через Интернет. Однако в отличие от известных решений, использующих VPN, нами предложено применить на границе сегментов механизм быстрого перескока сетевых адресов, что радикально изменяет уровень безопасности системы в целом, несмотря на открытость одного из сегментов. Отметим также, что для реализации ПО системы в целом используются технологии больших данных [6]: распределенная файловая система HDFS, фреймворк Hadoop и приложение GraphLab.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ (Соглашение о предоставлении субсидии № 14.574.21.0034 от 17.06.2014).

Список литературы

1. Крылов В.В. Алгоритм поиска максимально релевантных элементов на основе метризованного графа тесного мира / В.В. Крылов, Е.В. Бритвина // Вестник ННГУ. – 2014. - № 2 (2). - С. 178-181.
2. Способ доставки целевой рекламы и/или информации абоненту посредством инфокоммуникативных сетей и система для его осуществления / Е.В. Бритвина, В.В. Крылов, Д.М. Пономарев : Патент 2461879 РФ, МПК G06Q30/02; 2011117023/08; Заявл. 29.04.2011, Опубл. 20.09.2012.
3. Гольдштейн Б.С. Сети NGN. Оборудование IMS : учебное пособие / Б.С. Гольдштейн, В.Ю. Гойхман, Ю.В. Столповская. – СПб. : Теледом ГОУ ВПО «СПбГУТ», 2010.
4. Крылов В.В. Защита IP-подсетей от DDoS-атак и несанкционированного доступа методом псевдослучайной смены сетевых адресов, вопросы защиты информации / В.В. Крылов, К.Н. Кравцов // 2014. - № 3. - С. 24-31.
5. Способ взаимодействия терминального устройства клиента с сервером по сети Интернет с повышенным уровнем защиты от DDoS-атак и система для реализации способа / В.В. Крылов, Д.М. Пономарев; Общество с ограниченной ответственностью «МераЛабс» : Патент 2496136 РФ, МПК G06F11/07, G06F15/173, H04L12/24. № 2496136; Заявл. 14.05.12, Опубл. 20.10.13.
6. Крылов В.В. Большие данные и их приложения в электроэнергетике / В.В. Крылов, С.В. Крылов. - М. : Lennex Corp., Нобель Пресс, 2014. – 168 с.

Рецензенты:

Соколова Э.П., д.т.н., зав. кафедрой «Информатика и системы управления» НГТУ им. Р.Е. Алексеева, г. Нижний Новгород;

Хранилов В.П., профессор, заместитель директора ИРИТ по научной работе НГТУ им. Р.Е. Алексеева, г. Нижний Новгород.