DOI: https://doi.org/10.15688/NBIT.jvolsu.2022.1.2

УДК 004.7
ББК 32.972.5

ИССЛЕДОВАНИЕ ПЕРЕДАЧИ SMS-ТРАФИКА В СЕТИ СВЯЗИ

Надежда Николаевна Ермакова

Аспирант, кафедра телекоммуникационных систем,
Волгоградский государственный университет
ermakova.nadezhda@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Александр Игоревич Трофимов

Студент, кафедра телекоммуникационных систем,
Волгоградский государственный университет
trofimov.ai@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Евгений Сергеевич Семенов

Кандидат технических наук, доцент,
заведующий кафедрой телекоммуникационных систем,
Волгоградский государственный университет
semenov.evgeniy@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В статье исследуются особенности и методы передачи SMS-трафика при помощи API-интерфейса, рассматриваются параметры и API-функции для передачи SMS-сообщений, также анализируются причины потери трафика и варианты последующего предотвращения потерь. Рассмотрена схема взаимодействия между SMS-центром и обычными абонентами. Проведен анализ захваченного трафика с помощью специального программного обеспечения – Wireshark. Рассматриваются различные виды потерь в телекоммуникационных сетях и устанавливается корреляция с факторами, воздействующими на канал связи.

Ключевые слова: сетевой трафик, SMS, анализ данных, СМС-сообщения, протоколы передачи данных, SMPP протокол, потеря пакетов данных.

© Ермакова Н.Н., Трофимов А.И., Семенов Е.С., 2022

Одним сообщением в SMS (Short Message Service – «служба коротких сообщений») передается 160 символов в 7-битной кодировке (арабские цифры и латинский алфавит), 140 символов в 8-битной кодировке (алфавит французского и немецкого языков) и 70 символов в 16-битной кодировке (кириллица и иероглифы). При отправке учитываются такие параметры, как:

– дата и время отправки SMS-сообщения;

– номер А (отправитель) и номер В (получатель);

– схема кодирования SMS-сообщения;

– идентификатор используемого протокола;
– статус доставки SMS-сообщения.

По данным параметрам определяется точная адресация абоненту и читабельность сообщения. Пример переданного сообщения представлен на рисунке 1.

На рисунке 2 представлена схема передачи сообщения от клиента до абонента. Пользователь отправляет данные SMS по удобному для него протоколу (http), а провайдер передает мобильным операторам по протоколу SMPP [3].

В настоящее время распространенным и недорогим методом является SMS-рассылка по API, которая позволяет передавать сообщения через Интернет. SMSC-операторы принимают данные (сообщения абонентов, рассылки, уведомления и т. д.) от SMS-провайдеров при использовании протокола SMPP [2]. SMPP (аббревиатура: Short Message Peer-to-peer Protocol) в переводе с английского означает «Короткое сообщение равноправных узлов», описывает взаимодействие между SMS-сервером и конечным клиентом, условиями его реализации являются бесперебойно работающий сервер и программное обеспечение, совместимое с SMS-шлюзом провайдера [5].

От клиента осуществляется рассылка сообщений, которые передаются посредством протоколов http или https (популярные протоколы, поддерживающие большинство языков программирования; также могут быть использованы протоколы SMTP, FTP, POP3, Telnet и DTN и т. д.), преобразовывают их в PDU-запрос и передают в SMS-центр методом GET или POST.

Использование API-функции обязывает использовать определенные параметры:

– основной адрес шлюза: https://sms.sms.ru/api/;
– название компонента;
– название функции.

Например:

https://sms.sms.ru/api/user/balance, где user – компонент, balance – функция;

https://sms.sms.ru/api/message/send, где message – компонент, send – функция.

Результат запроса возвращается в формате JSON, например:

{“balance”:417.71,”status”:”success”}

Для авторизации используется связка логин + api-ключ. Логином для основного аккаунта обычно является E-mail, который был указан при регистрации, api-ключ можно задать в разделе настроек ЛК «Настройки API».

Телефон	Сообщение	Дата поступления	Дата отправки	Дата доставки или последнего изменения статуса	Статус (Помощь)	Имя отправителя	IP
– 79655555555	АКЦИЯ!-80%! ТРИ ДНЯ!	2022-02-26 11:17:26	2022-02-26 11:17:26	2022-02-26 11:17:00	Доставлено	WO_WO_WO	89.89.896.890

Рис. 1. Детализация успешно переданного SMS-сообщения

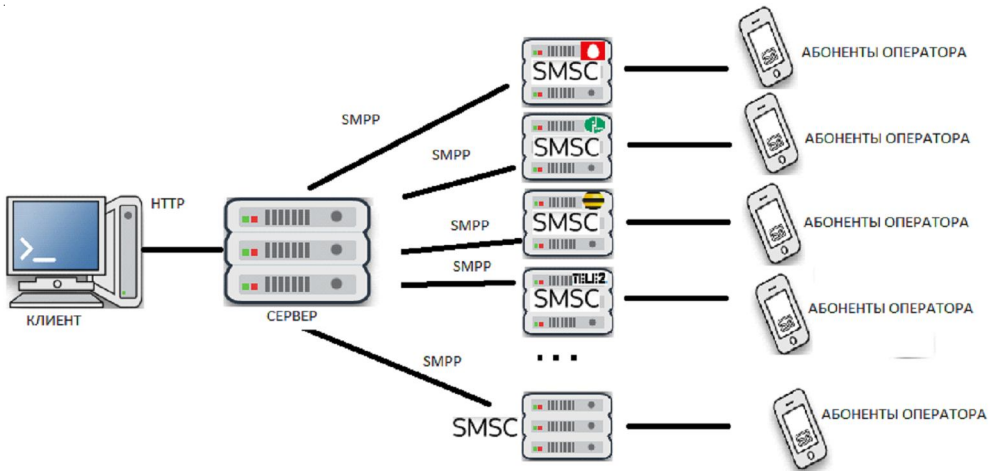

Рис. 2. Схема рассылки SMS-сообщений по API

Пример:

https://sms.sms.ru/api/user/balance?user=some@email.com&apikey=ABC123.

Параметры user и apikey необходимо указывать для всех функций.

Визуально get-запрос очень похож на строку в привычном браузере, чем представляет простоту своего применения http-протокола. Также get-запросы используются для получения статусов о доставке, информации о балансе.

Если происходит потеря пакетов, это означает, что сетевое соединение теряет информацию во время передачи. Соответственно, снижается надежность сетевого взаимодействия как с локальными, так и с удаленными устройствами.

Информация по сети передается пакетами данных, которые могут быть доставлены неполными, поврежденными или с иными дефектами, что делает их бесполезными. Можно использовать повторную переотправку сообщений, но если объем данных большой, но необходимо продиагностировать сеть передачи данных. Если фиксируются большие потери данных, то анализируются и учитываются следующие причины:

– перегрузка сети (возникает в пик пропускной способности, в час наибольшей нагрузки, когда пакеты, формируя очередь, игнорируются или отбрасываются и из-за долгого ожидания). При этом необходимо проверить пропускную способность канала передачи данных (например, с помощью веб-приложения speedtest, а также коммерческие условия договора с поставщиком интернета) [4];

– неправильная коммутация оборудования (маршрутизаторы, коммутаторы, брандмауэры и другие аппаратные устройства могут быть недостаточно мощными, тем самым являясь наиболее уязвимыми);

– повреждения на физическом уровне (повреждение кабеля Ethernet);

– программные ошибки: ни одно программное обеспечение не является безупречным. Микропрограмма сетевого оборудования или программного обеспечения компьютера может содержать ошибки, которые могут привести к потере пакетов. В этом случае потребителю необходимо обратиться к поставщику оборудования.

Для обнаружения потери пакетов используются программные приложения, среди них популярные: ping устройств, утилита tcpdump.

Утилита tcpdump запускается с параметрами: -i eth0 для захвата основного сетевого интерфейса или с параметром: -c 10 для захвата только десяти пакетов (пример представлен на рис. 3).

Далее анализируются выходные данные с помощью специального программного обеспечения Wireshark [1; 6]:

1. Выбирается необходимый сетевой интерфейс, через который будет проводиться захват и анализ трафика (в нашем случае это интерфейс eth0).

2. При необходимости вводятся фильтры для корректного захвата трафика (чтобы не путаться в протоколах захваченного трафика, необходимо выбрать нужный протокол, в нашем случае это SMPP).

3. Указывается количество/размер дампа трафика, необходимого для анализа.

4. Наблюдается в режиме реального времени движение пакетов от источника к получателю, на основании чего можно осуществлять мониторинг сети с последующим обнаружением проблемных узлов.

Более наглядно это показано на рисунке 4.

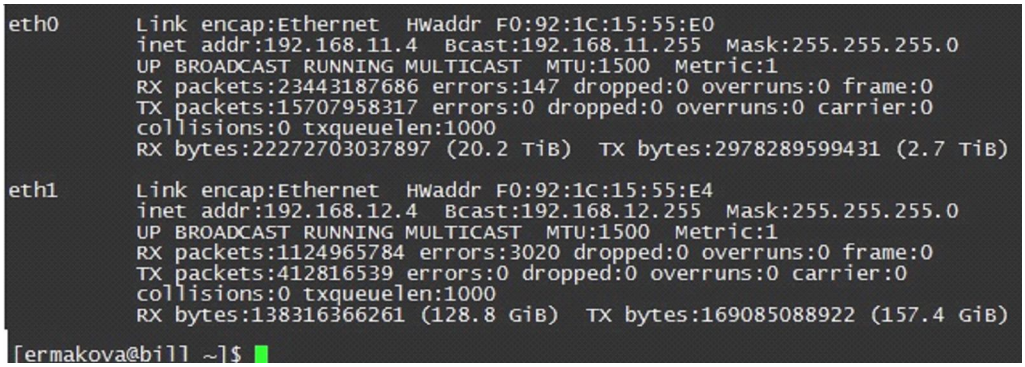

Рис. 3. Отображение интерфейсов сети с помощью команды tcpdump

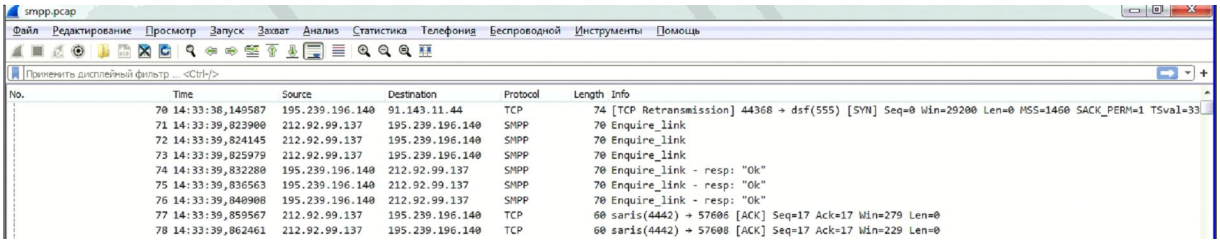

Рис. 4. Анализ захваченного трафика

Для устранения неполадок, связанных с потерей пакетов, можно использовать встроенные утилиты в ОС Windows и ОС Linux. Зачастую при наличии подробной карты сети стандартных приложений оказывается достаточно, чтобы понять, на каком из узлов сети наблюдаются неполадки. Системному администратору следует предпринять следующие шаги для устранения неисправности:

– проверить соединение Ethernet между устройствами;

– проверить действующее оборудование (маршрутизаторы, коммутаторы), возможно, устаревшее или неисправное, заменить;

– при программной ошибке – исправить в коде программы, возможна перезагрузка, обновление или переустановка ПО;

– при перегрузке сети – увеличить пропускную способность канала.

СПИСОК ЛИТЕРАТУРЫ

1. Гетьман, А. И. Анализ сетевого трафика в режиме реального времени: обзор прикладных задач, подходов и решений / А. И. Гетьман, Е. Ф. Евстропов, Ю. В. Маркин / Препринт ИСП РАН. – Электрон. дан. – 28, 2015 г. – 52 с. – Режим доступа: https://www.ispras.ru/preprints/archives/prep_28_2015.php.

2. Дэвис, Д. Microsoft Windows Server 2003: протоколы и службы TCP/IP: техническое руководство / Д. Дэвис, Т. Ли. – М. : БИНОМ. Лаборатория знаний, 2005. – 749 с.

3. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – 5-е изд. – СПб. : Питер, 2016. – 992 с.

4. Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – 5-е изд. – СПб. : Питер, 2012. – 960 с.

5. Short Message Peer to Peer Protocol Specification v3.4 // SMPP Developers Forum. – Electronic data. – Document Version: 12-Oct-1999 Issue 1.2. – Mode of access: https://smpp.org/SMPP_v3_4_Issue1_2.pdf (date of access: 28.02.2022).

6. Wireshark: site. – 2022. – Mode of access: https://www.wireshark.org/ (date of access: 28.02.2022).

REFERENCES

1. Get'man A.I., Evstropov E.F., Markin Yu.V. Analiz setevogo trafika v rezhime real'nogo vremeni: obzor prikladnyh zadach, podhodov i reshenij [Real-Time Analysis of Network Traffic: An Overview of Applications, Approaches and Solutions]. *Preprint ISP RAN*, 2015, 28. 52 p. URL: https://www.ispras.ru/preprints/archives/prep_28_2015.php.

2. Davis D., Lee T. *Microsoft Windows Server 2003: protokoly i sluzhby TCP/IP: tehnicheskoe rukovodstvo* [Microsoft Windows Server 2003: TCP/IP Protocols and Services. Technical Guide]. Moscow, BINOM. Laboratoriya znaniy Publ., 2005. 749 p.

3. Olifer V.G., Olifer N.A. *Komp'juternye seti. Principy, tehnologii, protokoly* [Computer Networks. Principles, Technologies, Protocols]. Saint Petersburg, Piter Publ., 2016. 992 p.

4. Tanenbaum E., Weatherall D. *Komp'juternye seti* [Computer Networks]. Saint Petersburg, Piter Publ., 2012. 960 p.

5. Short Message Peer to Peer Protocol Specification v3.4. *SMPP Developers Forum*. URL: https://smpp.org/SMPP_v3_4_Issue1_2.pdf (accessed 28 February 2022).

6. *Wireshark*: *site*, 2022. URL: https://www.wireshark.org (accessed 28 February 2022).

INVESTIGATION OF SMS TRAFFIC TRANSMISSION IN COMMUNICATION NETWORK

Nadezhda N. Ermakova

Postgraduate Student, Department of Telecommunications Systems,
Volgograd State University
ermakova.nadezhda@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Aleksandr I. Trofimov

Student, Department of Telecommunications Systems,
Volgograd State University
trofimov.ai@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Evgeniy S. Semenov

Candidate of Sciences (Engineering), Associate Professor,
Head of the Department of Telecommunications Systems,
Volgograd State University
semenov.evgeniy@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The article explores the features and methods of sending SMS traffic using the API (Application Programming Interface), discusses the parameters and API functions for sending Short Message Service (SMS) messages, also analyzes of causes of the loss of the traffic and the options for subsequent prevention of this loss. The scheme of the interaction between the Short Message Service Center (SMSC) and ordinary subscribers is considered. The popular protocol Short Message Peer-to-Peer (SMPP) was used as the protocol under study, capable of transmitting any type of messages, and is an open protocol in the telecommunications industry, which is designed specifically to provide a flexible interface for exchanging SMS messages between SMS applications, platforms, routers and short message service centers. The analysis of the captured traffic was carried out using special software – Wireshark, that allows to apply filters to track the protocols that are used for SMS transmission. Various types of losses in telecommunication networks are considered and a correlation is established with the factors which affect the communication channel. The results obtained can be used to develop an algorithm for searching for lost packets that occur when traffic passes through switching nodes. This model is able to improve the quality of service for telecom operators.

Key words: network traffic, SMS, data analysis, SMS messages, data transfer protocols, SMPP protocol, data packet loss.