МЕТОДЫ БОРЬБЫ СО СПАМОМ В VOIP ТЕЛЕФОНИИ

Полудворянин С. М., Нестеренков С. Н.
Кафедра программного обеспечения информационных технологий, Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: siarheipoludvaranin@gmail.com, nsn@bsuir.by

Стремительное развитие сервисов VoIP телефонии в последние годы привело к появлению нового вида спама: навязчивых телефонных звонков рекламного характера. В англоязычной литературе это явление известно под термином SPIT - spam over Internet telephony. Каждый год операторы связи и правоохранительные органы получают огромное количество жалоб на эти нежелательные звонки. Данный вид спама не только приносит финансовые потери пользователям телефонии, но также раздражает их нежелательными оповещениями. По этой причине операторам связи важно блокировать спамеров телефонии на уровне сети, чтобы завоевать доверие своих клиентов. В этой статье мы рассмотрим некоторые подходы для борьбы с нежелательными звонками на уровне сети.

Введение

На данный момент существует множество подходов для борьбы с телефонным спамом. Эти подходы могут быть сгруппированы в несколько категорий. К первой категории можно отнести подходы, основанные на контентном анализе. Они обрабатывает речевой поток между участниками звонка и блокирует абонентов, если обнаруживается, что поток содержит нежелательные сообщения. Ко второй категории относятся подходы, основанные на списках. Они составляют и поддерживают базу данных черных, белых и находящихся под наблюдением пользователей. Третья категория - подходы, основанные на IVR (Interactive Voice Response - система предварительно записанных голосовых сообщений), которые требуют от вызывающего абонента решить какую-либо задачу. Наконец, к четвертой категории относятся подходы, основанные на репутации системы, которые вычисляют репутацию вызывающего абонента путем получения обратной связи от вызываемого абонента или используют данные предыдущих вызовов.

I. Списочные подходы

Подходы на основе списков доступа авторизуют личность вызывающего с помощью локальной и глобальной базы данных. Вариант черного списка содержит базу абонентов, звонки от которых будут заблокированы. Абоненты вне списка могут совершать звонки без ограничений. Как и в случае с E-Mail спамом, черные списки для интернет-телефонии мало эффективны из-за простоты подмены идентификаторов звонящего в большинстве протоколов сигнализации, применяемых в VoIP. Вариант белого списка - обратный черному. Он содержит доверенных абонентов, вызовы от которых могут быть авторизованы. В отличие от черных списков, спамер не может изменить идентификатор аккаунта, чтобы обойти белый список. Тем не менее, белые списки не являются полноценным решением проблемы, так как они будут запрещать звонки от абонентов, ранее не звонивших пользователю, т. е. тех, кто не был явно включен в белый список. В результате белые списки требуют решения проблемы представления - каким образом авторизовать кого-то в первый раз и решить, должен ли он быть помещен в белый список. Серые списки содержат абонентов, которые находится под наблюдением из-за подозрительного поведения. Основанные на списке подходы обычно реализуются в сочетании с другими подходами, которые отвечают за принятие решения о том, помещать ли вызывающего абонента в белый, серый или черный список [1].

II. Аутентификации абонента

Подходы, основанные на аутентификации, реализуют механизм проверки звонящего перед тем, как авторизовать звонок. Для фильтрации спам-звонков, распространяемых с помощью ботов, был предложен механизм обеспечения доверия, который позволяет вызывающему абоненту посредством IVR решать сложные головоломки. Тесты такого типа известны под термином CAPTCHA - Completely Automated Public Turing test to tell Computers and Humans Apart — полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей. Такой подход может быть успешным при блокировании вызовов, генерируемых компьютером, но для обработки большого количества одновременных вызовов потребуются сетевые ресурсы. Кроме того, решение головоломок может увеличить время установления вызова и создать дополнительные трудности для легитимного абонента, вынужденного решать головоломки при каждой попытке вызова. Другим примером аутентификации может служить голос звонящего абонента. Система хранит в базе данных известные голоса спам-ботов, анализирует входящий звуковой поток и блокирует звонок при обнаружении совпадений.

III. Репутация абонента

Подходы, основанные на репутации, используют социальные отношения между участниками звонка для оценки репутации звонящего. Прямое доверие между абонентами обеспечивает доверие вызывающего абонента к взаимодействию с вызываемым абонентом. Глобальный рейтинг репутации играет важную роль, когда вызываемый абонент получает вызов от неизвестного контакта, и опирается на совокупный рейтинг с другими абонентами, которые уже взаимодействовали со звонящим. В VoIP телефонии доверие между конкретными абонентами и глобальная репутация могут быть вычислены двумя способами: с использованием обратной связи вызываемого абонента и с помощью информации из CDR (Call Detail Record - подробная запись о вызове). Во втором подходе репутация вызывающего абонента может быть вычислена из средней продолжительности звонка, количества коротких и длинных звонков, таких свойств социальных сетей, как количество контактов пользователя, коэффициент локальной кластеризации, индекс сплоченности, количество входящих и исходящих звонков пользователя (алгоритм SymRank - адаптация алгоритма Google PageRank) [2].

Существуют исследования, где глобальная репутация вычисляется с использованием алгоритма репутации Eigentrust. Это алгоритм, позволяющий вычислить репутацию каждого узла в сети на основе истории взаимодействия между узлами сети. Историю взаимодействия можно представить как матрицу связности между узлами, в каждой ячейке которой хранится оценка доверия к узлу, представленная как разность между количеством успешных и неуспешных попыток передачи данных.

Для расчета репутации также часто применяются алгоритмы машинного обучения, в частности, обучение с частичным привлечением учителя - способ машинного обучения, разновидность обучения с учителем, которое также использует неразмеченные данные для тренировки — обычно небольшое количество размеченных данных и большое количество неразмеченных данных. Примером имплементации может служить система на основе алгоритма MPCK–Means. Система кластеризует спам-звонки и легитимные звонки по некоторых свойствам, после чего «учитель» отмечает какой из кластеров является спамом. Свойством звонка в данном случае может быть как информация, полученная из сигнального трафика, такая как номер звонящего, направление звонка, длительность звонка, а также данные, полученные из медиа траффика, такие как длина пауз между словами. Однако такой подход требует обратной связи с пользователем, а также дополнительной настройки клиентских устройств [3].

Данту Р. и Колан П. в своих исследованиях представили многоступенчатую систему обнаружения спама, основанную на трех модулях: модуль доверия и репутации, модуль агрегирования обратной связи и модуль черного и белого списков. Доверие вычисляется путем получения прямой обратной связи от вызываемого абонента, а репутация вызывающего абонента вычисляется с использованием функции байесовского вывода.

Еще один подход, основанный на репутации, разработали Мохаммед Азад и Риккардо Морла. Для вычисления прямого доверия между абонентами он использует количество партнеров абонента для исходящих звонков, количество повторяющихся исходящих звонков и их длительность, количество входящих звонков и их длительность. Для подсчета глобальной репутации используется метод степенных итераций. Входными данными алгоритма является матрица нормализованных значений прямого доверия между каждой парой пользователей. Вызывающий получает высокую репутацию в сети, если ему удается иметь хорошие оценки прямого доверия с большим количеством вызываемых абонентов. Репутация снижается, если у него небольшие оценки доверия с большим количеством вызываемых [4].

Методы, основанные на репутации, также могут применяться в сочетании с другими подходами обнаружения спама, которые являются многоступенчатыми и взаимодействуют с другими этапами для принятия окончательного решения о вызывающем абоненте.

Заключение

В данной статье мы рассмотрели основные подходы борьбы с спамом в VoIP телефонии. Более детально описали подходы основанные на вычислении репутации абонентов сети. К сожалению, нет никакого универсального способа для предотвращения спама в VoIP телефонии так же, как не существует такого решения для борьбы со спамом в электронной почте. Тем не менее, сочетание нескольких методов может обеспечить основу для борьбы со спамом в VoIP сетях.

Список литературы

1. The Session Initiation Protocol (SIP) and Spam (RFC 5039) [Electronic resource] / Internet Engineering Task Force. – Mode of access: http://tools.ietf.org/html/rfc5039 – Date of access: 20.09.2019.
2. Bokharaei, H. K. You can SPIT, but you can't hide: Spammer identification in telephony networks / H. K. Bokharaei, A. Sahraei [etc.] // 2011 Proceedings IEEE INFOCOM – 2011. – P. 41–45.
3. Wu, Y. S. Spam detection in voice-over-IP calls through semi-supervised clustering / Y. S. Wu, S. Bagchi [etc.] // IEEE/IFIP International Conference on Dependable Systems Networks – 2009. – P. 307–316.
4. Azad, A. M. Caller-REP:Detecting unwanted calls with caller social strength / A. M. Azad, R. Morlla // Computers & Security – 2013. – Vol. 39 – P. 219–236.