УДК 004.67

МАЛЮКОВ П.Н.,
РАДЕР Р.И.

СИСТЕМА ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ АБОНЕНТОВ ТЕЛЕФОННОЙ СЕТИ

Предложен алгоритм и система для обнаружения аномального поведения абонентов с учётом групповых изменений в поведении. Написан прототип и имитатор поведения пользователей для анализа алгоритма. Проанализирована работа алгоритма в трех режимах: однопользовательском, многопользовательском без учета тренда и многопользовательском с учетом тренда.

Algorithm and anomaly behavior of end users detection system is proposed. Program for detecting anomalous behavior and user behavior simulator for analyzing algorithm is developed. Algorithm is analyzed in 3 modes: single user, multi user without considering trend, multi user with trend considering.

1. Введение

Операторы связи по всему миру испытывают значительные потери из-за мошенников. По данным исследования CFCA (международная организация для контроля мошенничества, обеспечения доходов и предотвращения потерь) в 2013 году, потери составляют 46.3 миллиардов долларов в год, что больше на 15% по сравнению с аналогичным исследованием в 2011 году. С увеличением потерь, 8% компаний переложило функции по борьбе с мошенничеством из финансовых отделов в отделы IT и безопасности (сейчас 38% от всех компаний) [1].

Игнорировать проблему мошенничества невозможно, так же как и прекратить, поэтому цель – обнаружить вредоносное вмешательство в каналы и средства связи, неправомерное использование услуг как можно раньше и предотвратить его.

2. Анализ проблемы

Системы мониторинга трафика распознают аномальный трафик, используя анализ и построение шаблона поведения отдельного пользователя [2]. Такие системы обычно являются частью системы безопасности и не являются самодостаточными — при обнаружении интервенции, в зависимости от политики безопасности, абонент сразу блокируется или подаётся сигнал сотруднику оператора для ручной обработки.

Проблемой такого подхода являются периодические и единоразовые массовые изменения поведения абонентов системы. Примером могут служить праздники, как Новый год, социально-политические события и многое другое. При этом такие события по-разному влияют на пользователей с разными шаблонами поведения, например корпоративных пользователей редко затронут семейные праздники, а такие дни как «черная пятница» повлияют на количество исходящих вызовов корпоративного сегмента, но не частных пользователей.

Учёт этих факторов позволит уменьшить процент ложных срабатываний системы, соответственно уменьшить количество ручной работы или недовольных абонентов из-за автоматической блокировки, что позволит уменьшить затраты на поддержание системы безопасности.

Целью работы является разработка системы мониторинга журналов CDR (Call Detail Record) для обнаружения аномального поведения абонентов с учётом массовых изменений шаблонов использования системы.

Как показало исследование телефонного оператора AT&T, достаточно эффективным способом составления шаблона поведения пользователей является построение вектора 24x7 элементов с количеством звонков за каждый час каждого дня недели [3].

3. Предлагаемый метод

Метод заключается в построении шаблона поведения пользователя на основе нескольких недель наблюдения, и впоследствии обнаружения звонков, которые выходят за рамки текущего шаблона. Соответственно, работа алгоритма делится на 2 этапа: режим обучения и рабочий режим.

Учитывая случайную природу совершения телефонного звонка по отношению к оператору, для анализа поведения можно исходить из предположения, что число звонков за определённый промежуток времени будет распределено по распределению Пуассона.

Также учтём, что поведение пользователя зависит от дня недели. Тогда запись поведения

пользователя можно определить как вектор длиной L=H*7, где H – число разбиений суток, а 7 – количество дней в недели. Для уменьшения случайной составляющей, составляется несколько записей поведения по неделям. Количество хранимых записей W влияет на точность конечного шаблона поведения P

$$P = \left(\overline{\lambda_1}, \overline{\lambda_2}, \ldots, \overline{\lambda_L}\right) \quad (1)$$

который можно определить как усреднённый вектор записей поведения за предыдущие W недель, где среднее значение считается как экспоненциально взвешенное скользящее среднее с окном в количество записей:

$$EMA_n = (1-\alpha)x_n + \alpha EMA_{n-1} \quad (2)$$

что можно привести к не рекурсивной формуле [5]:

$$EMA = \frac{x_n + \alpha x_{n-1} + \alpha^2 x_{n-2} + \ldots + \alpha^{n-1} x_1}{1 + \alpha + \alpha^2 + \ldots + \alpha^{n-1}} \quad (3)$$

Это позволяет уменьшить запаздывание, придавая большее значение последним значениям.

$$\overline{\lambda_i} = \frac{\lambda_{iw} + \alpha\lambda_{i(w-1)} + \ldots + \alpha^{n-1}\lambda_{i1}}{1 + \alpha + \alpha^2 + \ldots + \alpha^{w-1}} \quad (4)$$

В режиме обучения система принимает записи о звонках, измеряет частоту звонков и фиксирует её в записях поведения. Когда нужное количество записей сохранено (в зависимости от выбранного критерия, или достигается заданная дисперсия, или задается необходимое количество записей), система переводится в рабочий режим для конкретного абонента. То есть в один момент времени часть абонентов может обрабатываться в режиме обучения, а часть — в рабочем режиме. Это необходимо, так как во время работы системы могут подключиться новые абоненты.

Подсчёт текущей частоты f_H делается на основе времени инициации последних K звонков для каждого абонента отдельно. Имея вектор $t_i^{phone}, i = \overline{1..K}$ отметок времени инициации звонков (в секундах) рассчитываем предполагаемую частоту за определённый промежуток времени T:

$$T = \frac{24 \cdot 60 \cdot 60}{H} \quad (5)$$

Предполагаемая частота за время одной ячейки шаблона:

$$f_H = T \cdot f \quad (6)$$

где f – текущая частота за секунду

$$f = \frac{1}{T_{avg}} \quad (7)$$

T_{avg} - среднее время между звонками. Для уменьшения эффекта запаздывания за изменением частоты, здесь также целесообразно использовать экспоненциально взвешенное среднее значение:

$$T_{avg} = EMA_n(t_n - t_{n-1}, t_{n-1} - t_{n-2}, \ldots, t_2 - t_1) \quad (8)$$

Тогда:

$$f_H = \frac{24 \cdot 60 \cdot 60}{H * EMA(t_n - t_{n-1}, \ldots, t_2 - t_1)} \quad (9)$$

В рабочем режиме система продолжает фиксировать записи поведения, то есть обучение не останавливается. В этом режиме начинает работать алгоритм кластеризации, который классифицирует шаблоны пользователей на k кластеров. Количество классов может быть варьировано с измерением для обеспечения точного разделения абонентов по характеру использования системы. Для кластеризации можно использовать алгоритм k-means, запускаемый периодически после записи очередной записи поведения (раз в неделю), но в виду его сложности для большого количества абонентов целесообразно использовать его потоковую модификацию [4], что позволит классифицировать шаблоны сразу после получения новых данных.

Помимо этого включается проверка каждого звонка на соответствие шаблону поведения. Проверка на соответствие может осуществляться как с использованием доверительных интервалов, так и проверкой с учетом дисперсии. Пусть предполагаемый доверительный интервал (f_{min}, f_{max}) с необходимой надёжностью, задаваемой оператором, а отклонение от предполагаемого значения для интенсивности рассматриваемого временного промежутка λ_i из шаблона поведения P:

$$d = \frac{f_H^i - \lambda_i}{f_{max} - f_{min}} \quad (10)$$

где i – номер ячейки шаблона. Тогда при $-1 \le d \le 1$ значение текущей частоты находится в пределах ожидаемой.

Для установившегося состояния системы, среднее значение отклонений:

$$trend_C = \frac{\sum d_i^C}{N^C} \quad (11)$$

где i – номера абонентов класса C, будет около нуля. Если же будет происходить сезонное изменение или некоторый иной фактор, который влияет на характер использования си-

стемы класса или нескольких классов пользователей, тренд покажет характер этих изменений.

Смыслом функции тренда является процент отклонения класса абонентов от предыдущего характера использования системы. Поэтому, для уменьшения ложных срабатываний системы обнаружения аномального поведения, необходимо расширить доверительный интервал на вычисленный тренд.

Таким образом, интервенция может быть обнаружена сравнением текущей частоты с границами доверительного интервала, который равен:

$$\begin{cases} trend > 0, (f_{min}, f_{max} + trend) \\ trend < 0, (f_{min} + trend, f_{max}) \end{cases} \quad (12)$$

Собирая все части воедино, получаем алгоритм:

```
1. for каждая новой записи CDR:
2.  if (шаблон абонента в рабочем режиме) и (CDR не соответствует шаблону) then
3.   подать сигнал об интервенции
4.  end if
5.  модифицировать запись поведения
6.  пересчитать текущую частоту
7.  пересчитать тренд
8.  if прошло время Tcluster then
9.   инициировать задачу кластеризации абонентов
10.  end if
11. end for
```

Где Tcluster – время с последней кластеризации.

Последний пункт может быть модифицирован для потоковой кластеризации [5].

4. Модель для проверки метода

Для проверки метода были написаны система обнаружения аномального поведения пользователей, а также имитатор поведения пользователей.

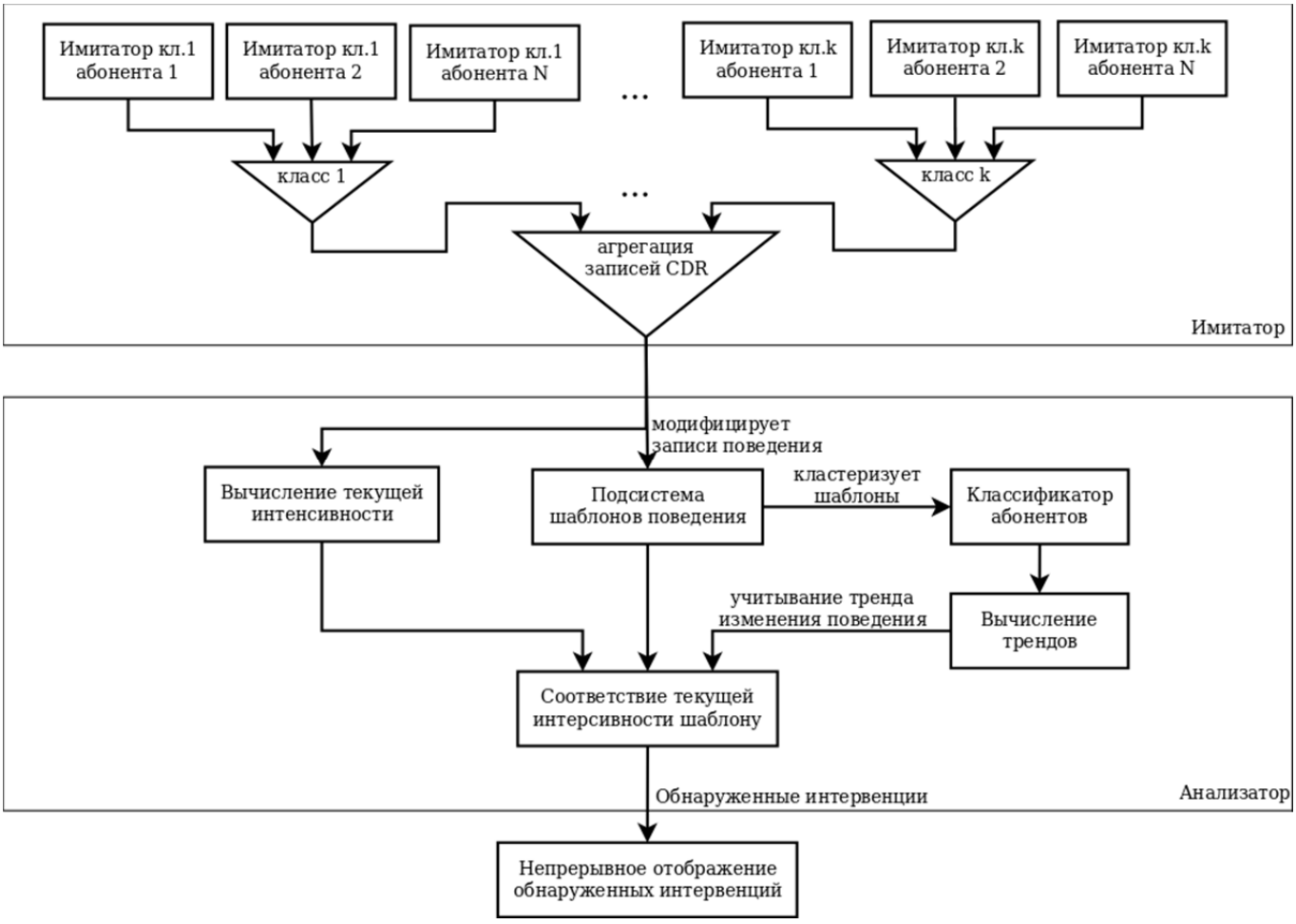

Рис. 1: Компоненты системы

Имитатор генерирует телефонные звонки, промежутки между которыми распределены по распределению Пуассона, с изменяемой интенсивностью по дням недели и временем суток.

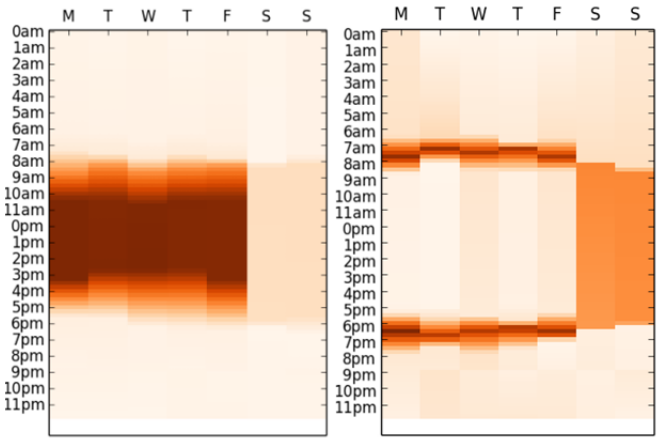

Рис. 2: Два класса имитируемых абонентов

Визуализация шаблонов двух классов пользователей на ***Рис. 2***. Первый класс – абоненты, производящие звонки в начале и в конце рабочего дня, а также активные в выходные дни. Второй класс – типично корпоративные пользователи, производящие звонки в бизнес-часы. Как видно, вносится случайная составляющая по дням недели, и для каждого абонента она своя.

В имитаторе есть возможность произвести интервенцию одной группы пользователей, либо нескольких, переводя из одного установившегося состояния в другое. Тем самым есть возможность протестировать работу системы обнаружения аномального поведения.

В анализаторе H=24, это значит что каждая ячейка шаблона отображает один час использования, коэффициент EMA $\alpha_1 = \alpha_2 = 0.8$.

Для подсчёта текущей интенсивности звонков для конкретного абонента всегда хранится K=10 последних записей времени инициации звонка, производится по формуле (9).

Подсистема шаблонов поведения каждый час сохраняет текущую частоту в запись поведения.

Классификатор абонентов запускается раз в неделю и запускает алгоритм кластеризации k-means++, основанный на расстоянии Евклида. Вычисление тренда делается на основе формулы (11).

Проверка соответствия текущей интенсивности шаблону происходит используя расширенный доверительный интервал с надёжностью p=0.997, расширенный по формулам (12) по рассчитанному тренду.

Перед началом работы системы, оператор задаёт параметры системы: α_1 для вычисления экспоненциально взвешенного скользящего среднего (EMA) для шаблона поведения, H — количество разбиений суток, W — количество недель работы системы в режиме обучения для конкретного абонента, α_2 для вычисления EMA текущей частоты, K — ширина окна для вычисления текущей частоты, p - надёжность доверительного интервала, C — количество кластеров абонентов. При внедрении данной системы, последний параметр может быть опущен и добавлен этап подбора параметра для большей точности работы системы.

Проанализирована работа алгоритма в трех случаях:

1) Интервенция в работу только одного абонента (***Рис. 3***)

2) Интервенция в работу одного класса абонентов, работа без учёта тренда (***Рис. 4***)

3) Интервенция в работу одного класса абонентов, работа с учётом тренда (***Рис. 5***)

На верхних графиках показана зависимость количества звонков, максимально допустимое количество звонков и точками обозначены обнаруженные интервенции. На нижних графиках показан тренд.

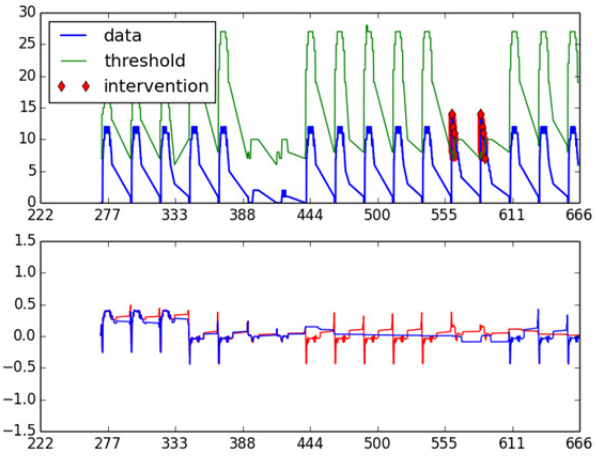

Рис. 3: Единичная интервенция одного телефонного номера в выходные дни

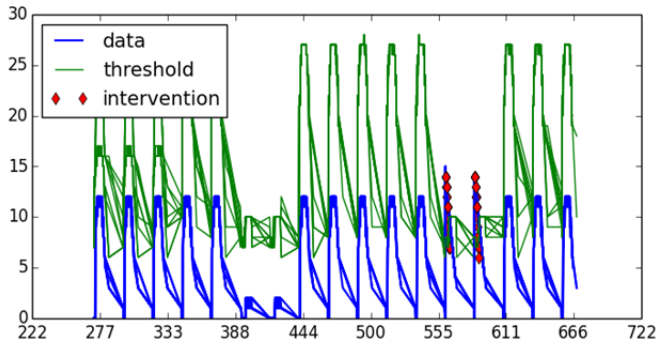

Рис. 4: Интервенция в работу одного класса абонентов без учета тренда. По оси абсцисс – время в часах (в модели) с начала

работы системы, по оси ординат – количество звонков.

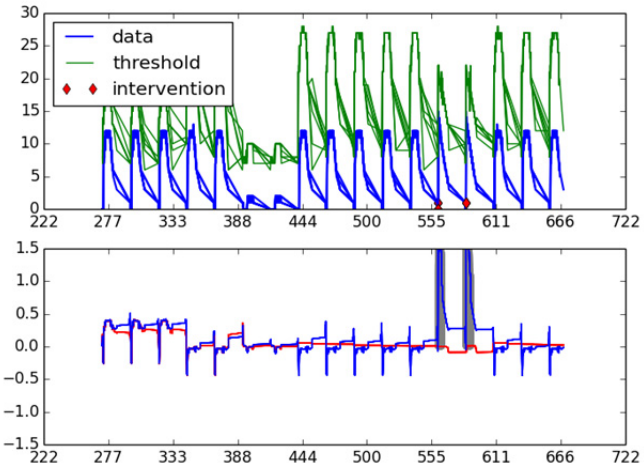

Рис. 5: Интервенция в работу класса абонентов с учетом тренда

Как видно, при интервенции в работу одного абонента (***Рис. 3***) тренд не изменяется и интервенция обнаруживается легко (количество подозрительных звонков практически совпадает с фактическим).

При групповом изменении поведения (***Рис. 5***) видно два пика линии тренда, приходящиеся на выходные дни (в данном опыте пользователи, которые никогда не звонили по выходным меняют это поведение). На верхнем графике видно, что уровень интервенций очень низкий, что означает правильную работу алгоритма – групповое изменение поведение не считается подозрительным.

Для проверки, второй опыт был проведён с теми же исходными данными, но без учёта тренда (***Рис. 4***). На графике видно, что уровень интервенций практически совпадает с количеством фактических звонков в рассматриваемом участке, что значит высокую вероятность мошенничества. Таким образом, способ учёта групповых изменений действительно уменьшает количество ложных срабатываний.

5. Выводы

Алгоритм потоковый, не требует накопления данных, все хранимые данные можно записывать в циклический список, тем самым потребляя стабильное количество памяти и имея небольшой отпечаток памяти (footprint).

Проанализирована работа алгоритма в многопользовательском режиме с учетом тренда, а также проведено сравнение с однопользовательским режимом и многопользовательским режимом без учета тренда режимах для оценки эффективности метода.

Метод применим к многим алгоритмам и легко модифицируется под конкретные задачи и требования, такие как способ определения интервенции или список отслеживаемых параметров.

Список литературы

1. Communications Fraud Control Association (CFCA) 2013 Global Fraud Loss Survey [Электронный ресурс] // Communications Fraud Control Association: [сайт]. [2013]. URL: http://www.cfca.org/pdf/survey/Global%20Fraud_Loss_Survey2013.pdf
2. Rosas É.., Analide C. Telecommunications Fraud: Problem Analysis - an Agent-based KDD Perspective [Электронный ресурс] // Fourteenth Portuguese Conference on Artificial Intelligence: [сайт]. [2009]. URL: http://epia2009.web.ua.pt/onlineEdition/402.pdf
3. Becker R.A., Cáceres R., Hanson K., Loh J.M., Urbanek S. Clustering Anonymized Mobile Call Detail Records to Find Usage Groups [Электронный ресурс] // AT&T Researchers — Inventing the Science Behind the Service: [сайт]. URL: http://www.research.att.com/techdocs/TD_100397.pdf
4. Cargal J.M. Discrete Mathematics for Neophytes: Number Theory, Probability, Algorithms, and Other Stuff - Chapter 32 out of 37 // Books in the Mathematical Sciences. 1988. URL: http://www.cargalmathbooks.com/32%20Averages%20.pdf
5. Lecture 6 — Online and streaming algorithms for clustering Sanjoy Dasgupta [Электронный ресурс] // Department of Computer Science and Engineering, University of California, San Diego: [сайт]. URL: http://cseweb.ucsd.edu/~dasgupta/291/lec6.pdf