УДК 004.93

Показатели качества систем распознавания пользователей по динамике подписи на основе наивного классификатора Байеса и нейронной сети

Гураков М.А.*, Кривоносов Е.О., Костюченко Е.Ю.*****

Томский государственный университет систем управления и радиоэлектроники, ТУСУР, проспект Ленина, 40, Томск, 634050, Россия

**e-mail: g.mishell@gmail.com*

***e-mail: egor-yrga@mail.ru*

****e-mail: key@keva.tusur.ru*

Аннотация

Исследовано поведение параметров систем распознавания пользователей по динамике подписи на основе модифицированного наивного классификатора Байеса и нейронной сети в зависимости от значения порогов в соответствующих системах. Получены оценки качества системы аутентификации в виде вероятностей ошибок 1-го и 2-го рода. Были проведены исследования по определению возможности объединения классификатора на основе нейронной сети и классификатора Байеса путем линейного комбинирования выходов для снижения суммарной вероятности ошибки классификации без учета рода ошибки.

Ключевые слова: идентификация, подпись, классификатор Байеса, нейронная сеть, интеграция, линейная зависимость, ошибки первого и второго рода.

Аутентификация пользователя по динамике подписи на основе классификатора Байеса

Одна из актуальных задач защиты информации – реализация быстрой, удобной для пользователя идентификации, при которой количество несанкционированных доступов стремится к нулю, а отказы в доступе не доставляют пользователям заметных проблем. Одним из средств повышения показателей защищённости систем является использование многофакторной биометрической аутентификации. Цель настоящего исследования – создать систему идентификации на основе дополнения традиционной парольной защиты дополнительным фактором – подписью на графическом планшете, позволяющую поднять показатель защищенности по сравнению с исходной версией [1].

Создаваемая система основана на алгоритмах наивного модифицированного классификатора Байеса и нейронной сети. Наивный классификатор Байеса служит для распознавания принадлежности объекта некоторому классу, в данном случае классу подписей отдельного пользователя. Применение классификатора состоит из двух частей – обучения и распознавания.

При подготовке параметров, участвующих в проведении процедуры аутентификации, выполнялись следующие действия:

1) съем зависимостей положения пера на планшете $x(t)$ и $y(t)$, высоты $z(t)$, давления на планшет $p(t)$, угла наклона пера к планшету $\varphi(t)$ и угла между пером и плоскостью, образованной осями y и z и пером $\theta(t)$, от времени t (итого 6 характеристик);

2) приведение нормировки подписи к фиксированному размеру, ограниченному максимальными значениями характеристик, путем линейного преобразования, а также перерасчет зависимостей шага 1 с учетом нормировки;

3) расчет зависимостей скоростей и ускорений изменения характеристик от времени (итого вместе с исходными 18 характеристик);

4) применение преобразования Фурье и выделение амплитуд постоянной составляющей и первых семи гармоник временных зависимостей из шага 1 – итого 8 амплитуд – получаем на выходе $n = 8 \times 18 = 144$ параметра, записываемых в БД и используемых классификаторами при анализе.

Далее осуществлялось построение классификатора:

1) рассматриваются все значения одного из параметров и делятся квантильными значениями на интервалы, содержащие одинаковое значение реализаций этого параметра, если таких интервалов *m*, то есть *m*-1 значений квантилей – границ между этими интервалами;

2) определяются условные относительные частоты попадания значений в каждый из таких интервалов для каждого из пользователей. Эти частоты являются оценками условных вероятностей $P(A_i \mid B_j)$. Здесь событие A_i - попадание *i*-го параметра в текущий интервал, B_j - принадлежность подписи *j*-му пользователю. Также рассчитывается условная относительная частота попадания в интервал для всех пользователей, кроме того, оценивалась условная вероятность попадания в интервал для остальных пользователей кроме текущего $P(A_i \mid \neg B_j)$. По сути,

определенные на предыдущем шаге границы интервалов вместе с полученными оценками условных вероятностей полностью описывают классификатор Байеса.

После построения классификатора можно проводить классификацию подписей на предмет принадлежности тому или иному пользователю.

При проведении классификации по классической схеме классификатора Байеса нам нужны условные вероятности или их оценки для следующих событий $A_1A_2...A_n$ - попадание каждого из 144 рассматриваемых параметров одновременно именно в те интервалы, которые присутствуют в классифицируемом примере.

$$P^*(B_j) = P(B_j \mid A_1A_2...A_n) = \frac{P(A_1A_2...A_n \mid B_j)P(B_j)}{\sum_{k=1}^{m} P(A_1A_2...A_n \mid B_k)P(B_k)} \text{ [5]} \qquad (1)$$

Однако, получить эту оценку не представляется возможным, поскольку даже для двух интервалов существует 2^{144} вариантов распределения всех параметров по интервалам, что приводит к незначительным (в реальности – единичным) значениям частот получения каждой из реализаций и невозможности получить значимую оценку условных вероятностей.

Для проведения классификации сделаны следующие модификации классического классификатора Байеса:

1. Сделано предположение о независимости вероятностей попадания в интервалы для различных параметров. Предположение, очевидно, верным не является, но позволяет перейти к произведению вероятностей и получить хоть какие-то оценки. Кроме того, сделано предположение о равенстве безусловных

вероятностей для всех пользователей. Рассматриваются только 2 вероятности – вероятность принадлежности *j*-му пользователю

$$P^{**}(B_j) = \prod_{i=1}^{n} P(B_j \mid A_i) = \prod_{i=1}^{n} \frac{P(A_i \mid B_j)P(B_j)}{P(A_i \mid B_j)P(B_j) + P(A_i \mid \neg B_j)P(\neg B_j)} =$$
$$= \prod_{i=1}^{n} \frac{P(A_i \mid B_j) \cdot \frac{1}{r}}{P(A_i \mid B_j)\frac{1}{r} + P(A_i \mid \neg B_j)\frac{r-1}{r}} \quad (2)$$

и вероятность непринадлежности *j*-му пользователю

$$P^{**}(\neg B_j) = \prod_{i=1}^{n} P(\neg B_j \mid A_i) = \prod_{i=1}^{n} \frac{P(A_i \mid \neg B_j)P(\neg B_j)}{P(A_i \mid B_j)P(B_j) + P(A_i \mid \neg B_j)P(\neg B_j)} =$$
$$= \prod_{i=1}^{n} \frac{P(A_i \mid \neg B_j) \cdot \frac{r-1}{r}}{P(A_i \mid B_j)\frac{1}{r} + P(A_i \mid \neg B_j)\frac{r-1}{r}} \quad (3)$$

где r – общее количество пользователей.

Строго говоря, получаемые величины не являются вероятностями в строгом их понимании из-за некорректности предположения о независимости, однако они могут быть использованы в качестве меры принадлежности подписи тому или иному пользователю [3].

2. Т.к. значения отдельных оценок вероятностей, входящих в произведения (2) и (3) меньше (1), то получаемое после перемножения для 144 параметров значение меры очень мало и удобнее использовать в качестве меры логарифм отношения правдоподобия:

$$W(B_j) = \ln\left(\frac{P^{**}(B_j)}{P^{**}(\neg B_j)}\right) = -n\ln(r-1) + \sum_{i=1}^{n}(\ln P(A_i \mid B_j) - \ln P(A_i \mid \neg B_j)) \quad (4)$$

3. Диапазон изменения меры, описанной в пункте 2, в отличии от вероятности, не определён, и при проведении классификации при превышении некоторого порога w пример считается принадлежащим пользователю j. Пороги могут определяться как одинаковыми w для всех пользователей, так и различными w_j для каждого, что может позволить повысить точность классификации (в данной работе этот механизм не рассматривается и оставляется для дальнейшего исследования). Значения порогов определяются экспериментально.

Краткое описание предыдущих этапов

На предыдущем этапе исследования были достигнуты следующие результаты:

1. На основе [3] и [4] был реализован наивный классификатор Байеса.

Реализация модифицированного наивного классификатора Байеса принимала решение на основе соотношения (4). Однако, в первом приближении решение о принадлежности подписи пользователю принималось не на основе превышения порога, а на основе нахождения максимального значения меры среди пользователей.

2. Был произведён комплекс расчётов для определения количества интервалов, при котором обеспечивается минимальное среднее количество ошибок в процессе аутентификации пользователей на основе модифицированного наивного классификатор Байеса. По результатам расчётов было найдено уравнение регрессии вида

$$f(m) = 0,08253 \cdot m^2 - 2,699 \cdot m + 4,42 \quad (5)$$

В рамках этого уравнения отражено изменение вероятности ошибки классификации $f(m)$ в зависимости от количества интервалов m, на которые делится набор наблюдаемых значений каждого из параметров, при вычислении оценок условных вероятностей в рамках формул (1-4). Уравнение строилось для диапазона целых $m \in [2; 25]$.

Из уравнения (5) следует, что оптимальным режимом классификации для данного вида классификатора Байеса является деление всех наблюдаемых значений параметров на 2 интервала, содержащие одинаковое количество значений [2].

3. Было проведено тестирование программы из 100 циклов обучения классификатора, в процессе которого были получены следующие характеристики, описывающие качество полученной системы: средняя вероятность ошибки классификации по итогам всех циклов – 4,78%, минимальная вероятность ошибки классификации в рамках одного построения классификатора – 1,62%, среднее квадратичное отклонение вероятности ошибки – 1,43%. По результатам тестирования сделано заключение о возможности применения модифицированного наивного классификатора Байеса для идентификации.

4. Была создана программа [2], реализующая алгоритм аутентификации на базе нейронной сети и начаты работы по согласованию работы наивного классификатора Байеса и нейронной сети для их совместного применения для классификации. В качестве нейронной сети используется персептрон с одним скрытым слоем, количество нейронов в промежуточном слое подобрано с целью минимизации итоговой вероятности ошибки классификации и выбрано равным 30.

Входы нейронной сети – те же 144 параметра подписи, что и для классификатора Байеса, выходы – количество совпадает с количеством пользователей, выход, отвечающий принадлежности пользователю на этапе обучения равен 1. Нейронная сеть обучается также на 80 процентах базы подписей. Данная выборка извлекается и используется для обучения модифицированного наивного классификатора Байеса, что обеспечивает равенство условий его обучения с обучением нейронной сети, затем каждый из способов аутентификации применяется на оставшиеся 20 процентов подписей, и результаты сравниваются.

Расчёт ошибок первого и второго рода

В качестве шага исследования был введен порог, который определял достаточность результирующего значения выхода наивного классификатора Байеса и нейронной сети для принятия решения об аутентификации пользователя, в отличии от простого определения по максимальному выходу. Введение порога позволило провести исследования поведения ошибок первого и второго рода в обоих алгоритмах аутентификации.

Алгоритм расчёта ошибок первого рода:

- считалось количество отторжений системой санкционированных пользователей,
- полученное значение делилось на сумму всех попыток санкционированных пользователей идентифицироваться.

Алгоритм расчёта ошибок второго рода:

- считалось количество принятий системой несанкционированных пользователей,

- полученное значение делилось на разность произведения количества всех подписей и пользователей и количество легальных пользователей.

Результат исследования параметров модифицированного классификатора Байеса (рис.1) и нейронной сети (рис.2) представлены ниже:

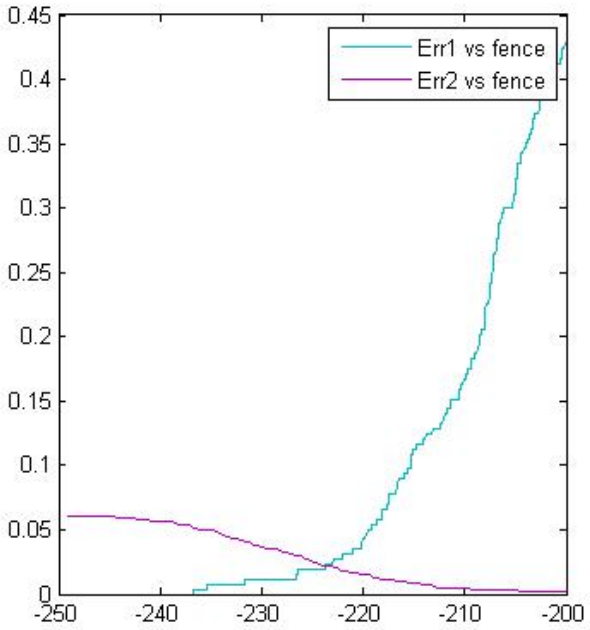

Рисунок 1 - Графики зависимостей ошибок первого и второго рода модифицированного классификатора Байеса от порога принятия решения *w*

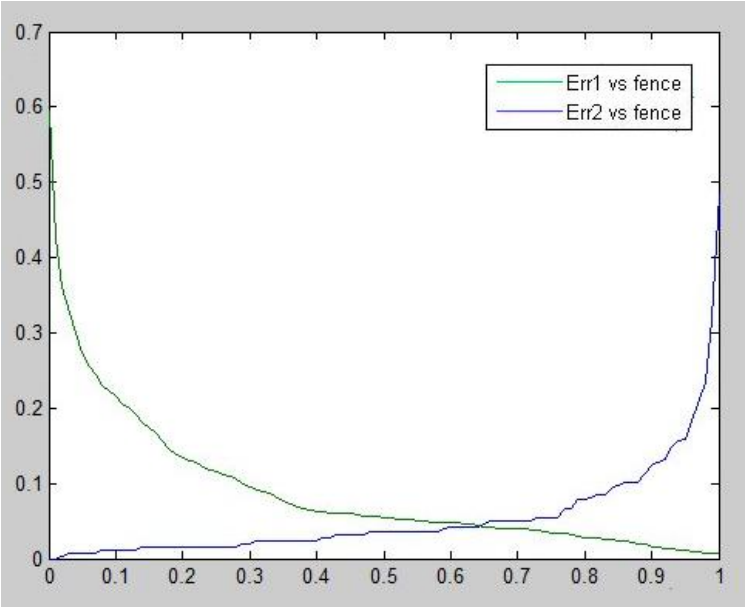

Рисунок 2 – Графики зависимостей ошибок первого и второго рода нейронной сети от порога принятия решения *w*

Разница в масштабах и порядках значения *w* объясняется использованием логарифмической меры при работе с классификатором Байеса: при проведении величины, проставленной на данном графике к вероятности масштаб осей будет одинаков, результат работы не изменится (или ухудшится за счет потери точности при преобразовании) однако смысл графика будет не понятен – переход от 0 к 1 будет происходить слишком быстро. По итогам данного исследования получены кривые, позволяющие определять ошибки 2 рода в зависимости от ошибок первого рода и наоборот. Кроме того, реализован модуль для подсчета этих ошибок, который может быть использован в дальнейшем при исследовании объединения классификаторов.

Проверка возможности интеграции систем на основе линейной комбинации выходов классификаторов

Следующим шагом была проверка возможности интеграции классификаторов на основе линейной комбинации их выходов. Критерий оптимизации может быть представлен как:

$$V = \sum_{i}\sum_{j}\left|\alpha \cdot a_1 + \beta \cdot a_2 - \delta - b\right| \to \min, \quad (6)$$

где a_1 – логарифмические выходы наивного классификатора Байеса;

a_2 – выходы нейронной сети;

b – эталонное значение классификатора;

α, β, δ – параметры системы объединения классификаторов;

V – наблюдаемое значение объединенного критерия.

Результат оптимизации показал, что ведущее значение при работе интеграции имеет нейронная сеть (табл. 1) ввиду сходства результатов их работы. Для проверки данного предположения было предпринято сравнение математических ожиданий результатов работ систем. Равенство дисперсий результатов нейронной сети и линейной интеграции было доказано через критерий Фишера – Снедекора, значения дисперсий были признаны равными при уровне значимости 0,05. Было проведено сравнение выборок вероятностей ошибок с целью проверки математических ожиданий на равенство, либо на то, что математическое ожидание вероятностей ошибок работы нейронной сети больше, чем математическое ожидание вероятностей ошибок работы линейной интеграции. Было рассчитано наблюдаемое

значение Фишера – Снедикора $Z_{набл}$ = 0,495, из таблиц критических точек распределения Фишера – Снедикора в [5] было найдено критическое значение критерия $Z_{крит}$ = 1,96 при значимости α = 0,05. $Z_{набл} < Z_{крит}$, из чего следует, что математические ожидания, а следовательно и результаты работы нейронной сети и линейной интеграции, следует считать одинаковыми.

Таблица 1

Сводная таблица результатов работы интеграции и интегрируемых систем

Классификатор Байеса, вероятность ошибки, %	Нейронная сеть, вероятность ошибки, %	Линейная интеграция, вероятность ошибки, %
6,048387	2,016129	2,016129
6,048387	2,419355	2,822581
6,048387	3,629032	4,435484
5,645161	4,032258	4,032258
6,048387	2,419355	1,612903
6,451613	4,435484	3,629032
3,225806	2,822581	2,016129
4,83871	2,016129	1,612903
6,048387	3,629032	4,032258
7,258065	4,032258	3,629032
4,435484	2,419355	4,032258
3,629032	3,225806	2,822581
4,83871	4,032258	2,822581
3,629032	2,822581	1,612903
6,048387	4,435484	4,83871
5,241935	3,225806	4,032258
7,258065	5,241935	4,032258
5,241935	3,225806	2,419355
6,048387	5,241935	5,241935
4,435484	2,419355	2,822581

Из этого следует, что интеграция на основе линейной зависимости без учета раздельного учета ошибок первого и второго рода не приносит результатов, качественно превосходящих работу интегрируемых систем. По этому этапу сделано заключение о необходимости проведения исследования по объединению подходов с использованием не только линейного критерия оптимизации, а также необходимости раздельного учета ошибок первого и второго рода в рамках критерия, описанного в [6, 7].

Заключение

На данном этапе исследования были достигнуты следующие результаты:

1. Реализована аутентификация пользователя по динамике подписи на основе нейронной сети и модифицированного наивного классификатора Байеса.

2. Осуществлена попытка нахождения линейного критерия объединения классификаторов, показавшая неприменимость линейного объединения модифицированного наивного классификатора Байеса и нейронной сети в рассматриваемом виде для значимого снижения итогового суммарного уровня ошибки без разделения на ошибки 1 и 2 рода.

3. Были рассчитаны ошибки первого и второго рода для наивного классификатора Байеса и нейронной сети в зависимости от порога классификации.

4. Следующим этапом исследования поставлено сравнение классического и модифицированного классификаторов Байеса, а также выбор критерия оптимизации для объединения классификаторов с учетом специфики ошибок 1 и 2 рода [8].

Работа выполнена при поддержке Министерства образования и науки

Российской Федерации в рамках базовой части государственного задания ТУСУР на 2015 г. (проект № 3657).

Библиографический список

1. Ходашинский И.А., Савчук М.В., Горбунов И.В., Мещеряков Р.В. Технология усиленной аутентификации пользователей информационных процессов. // Доклады Томского государственного университета систем управления и радиоэлектроники. 2011. № 2 (24). С. 236-248.

2. Гураков М.А., Кривоносов Е.О. Аутентификация пользователя по динамике подписи на основе наивного классификатора Байеса. // Конференция участников группового проектного обучения ТУСУР, 2014: https://storage.tusur.ru/files/10909/KIBEVS-1005_Autentifikatsia_polzovatelya_po_dina.pdf (доступ 1.06.2015).

3. Субботин С.В., Большаков Д.Ю. Применение байесовского классификатора для распознавания классов целей // Журнал Радиоэлектроники, 2006, № 4: http://jre.cplire.ru/jre/oct06/2/text.html.

4. McCallum, A. and Nigam K. «A Comparison of Event Models for Naive Bayes Text Classification». In AAAI/ICML-98 Workshop on Learning for Text Categorization, pp. 41-48. Technical Report WS-98-05. AAAI Press. 1998.

5. Гмурман В.Е. Теория вероятностей и математическая статистика. – М.: Высшая школа, 2003. – 479 с.

6. Дорошенко Т.Ю., Костюченко Е.Ю. Система аутентификации на основе

динамики рукописной подписи // Доклады ТУСУР. 2014. № 2(32). С. 219-223.

7. Костюченко Е.Ю. Идентификация непрерывных биометрических сигналов на основе нейронных сетей: Дисс. канд. техн. наук, - Томск, 2010, 171 с.

8. Костюченко Е.Ю., Мещеряков Р.В., Крайнов А.Ю. Критерии информативности при обработке биометрических сигналов при помощи нейронных сетей // Доклады Томского государственного университета систем управления и радиоэлектроники. 2010. № 1(21). С. 118-220.