Mordashkin Vjacheslav Konstantinovich, NIKIRET; 1 Prospect Mira str., Zarechny, Penza region, 442965, Russian Federation; chief specialist; PhD in Technical Sciences. Tel.: +79603284509. E-mail: adrom@yandex.ru.

References

1. STO – 94160974 – P-119-03-05.2014. Standard NP «APC». Providing anti-terrorist protection of buildings and structures. Activities and solutions to ensure the antiterrorist protection of buildings and structures. General requirements. (In Russian).
2. SP 132. 13330.2011. Ensuring anti-terrorist protection of buildings and structures. General requirements for design. (In Russian).
3. RF Federal Law «About counteraction to terrorism» of March 06, 2006. №35-FZ (as amended on December 31, 2014). (In Russian).
4. RF Federal Law «On Countering Extremist Activity» of July 25, 2002, № 114-FZ (as amended on November 23, 2015). (In Russian).
5. GOST R 52551-2006. *Sistemy ohrany i bezopasnosti. Terminy i opredelenija.* [State Standart 52551-2006. Security and safety systems. Terms and Definitions].
6. Criminal Code of the Russian Federation of June 13, 1996, № 63-FZ (as amended on March 30, 2016), title X, Chapter 29, art. 281, part 1. (In Russian).
7. Technological terrorism. Russian Emergency Ministry term. Available at: http://www.mchs.gov.ru/dop/terms/item/88381/ (accessed 20.04.16) (In Russian).
8. Order Ministry of Transport of the Russian Federation, the Federal Security Service, Ministry of Internal Affairs «On approval of the list of potential threats of acts unlawful interference against objects of transport infrastructure and vehicles» of March 5, 2010, № 52/112/134. (In Russian).
9. Shepit'ko G.E. *Problemi oxrannoi bezopasnosti ob'ektov. Chast' 1* [Problems of protection in ensuring the safety of objects. Part 1]. Moscow, Russkoe slovo Publ., 1995. 352 p.
10. Abolmazov E. I., Abolmazova M.E. Operejaushie i blokirushie vozdeistvie [Anticipate and blocking counter]. *Sistemy bezopasnosti svjazi i telekommunikacij*, 1997, March-April, pp. 44-45.
11. Resolution of the Government of the Nizhny Novgorod Region «On approval of the state program «Ensuring public order and counteraction of criminality in the Nizhny Novgorod region in 2014-2016 years» of December 20, 2013, № 978 (as amended on February 27, 2014, № 128, and on April 10, 2014, № 233). Available at: http://government-nnov.ru/?id=158823 (accessed 05.08.15). (In Russian).
12. Informational and analytical note to the report of the Chief of Municipal Administration Russian Ministry of Internal Affairs for the city of Sarov in front of the City Duma of Sarov of February 27, 2014. Available at: http://www.52.mvd.ru›upload/site54…OR2ZsXzPjk.doc (accessed 05.08.15) (In Russian).
13. The public report of the Department of Education Administration of Sarov for the 2012-2013 academic year. Available at: http://www.do.sar.ru›docs /public_doc/2013/2.pdf (accessed 05.08.15) (In Russian).
14. Report of the Chief of the Russian Interior Ministry of Bor for The Board of Deputies of Bor, Nizhny Novgorod region, of January 28, 2014. Available at: http://www.52.mvd.ru (accessed 05.08.15). (In Russian).
15. Bor-statistika. Available at: http://bor-nn.ru/glavnaya/bor-statistika.html (accessed 21.04.16). (In Russian).

Received 20.05.2016

УДК 004.491.22

АДАПТАЦИЯ НАИВНОГО БАЙЕСОВСКОГО КЛАССИФИКАТОРА К МЕХАНИЗМУ КЛАССИФИКАЦИИ ЭЛЕКТРОННЫХ СООБЩЕНИЙ

Бурлаков М.Е., Голубых Д.А., Осипов М.Н.
Самарский национальный исследовательский университет им. С.П. Королева, Самара, РФ
E-mail: knownwhat@gmail.com

Рассматривается классификация электронных сообщений как адаптивными, так и неадаптивными алгоритмами. Особое внимание уделяется применению алгоритма наивного байесовского классификатора в решении задачи классификации блоков данных. Показана возможность реализации алгоритма при рассмотрении элементов в рамках электронного сообщения в качестве независимых событий с применением апостериорного правила принятия решений. Определен процесс обучения наивного байесовского классификатора как подсчет вероятности встречи того или иного слова в электронном сообщении.

Ключевые слова: классификация электронных сообщений, наивный байесовский классификатор, достоверный блок информации, недостоверный блок информации.

Введение

В современных системах передачи информации крайне актуально стоит задача, связанная с классификацией блоков данных и электронных сообщений, передающихся от отправителя к адресату через разного рода системы (mail, web, irq и т.д.). Для ее решения применяется множество как адаптивных (искусственные нейронные сети, искусственные иммунные алгоритмы, генетические алгоритмы), так и неадаптивных (методы графов сценариев атак, методы анализа систем состояний, экспертные системы, методы на спецификациях, сигнатурные методы) методов [1-11].

Задача классификации электронных сообщений в рамках информационной системы сводится к отнесению входящего потока данных к соответствующему классу (например, по релевантности, по отправителю, по объему и содержимому). Наиболее актуальным направлением в анализе и классификации сообщений считают классификацию по их содержимому, когда можно без знания об источнике сообщения с определенной долей вероятности определить, к какому классу она относится, и либо отправить сообщение дальше, либо остановить его движение по информационной системе.

Одна из основных задач классификации блоков данных и электронных сообщений заключается в их распределении по двум классам достоверности [11-16]: достоверной (актуальной, легитимной и т.д.) и, соответственно, информации недостоверной.

При этом под достоверной (легитимной) информацией понимается набор данных, который не представляет из себя угрозы для информационной системы, в которой происходит ее циркуляция, с точки зрения доступности, целостности и конфиденциальности. В противном случае информация называется недостоверной (нелегитимной). Примером подобной классификации является антиспам-система или программно-аппаратный комплекс антивирусной защиты, задача которых также сводится к определению достоверности входящего в информационную систему сообщения по его содержимому.

Как было отмечено, существует большое число адаптивных и неадаптивных алгоритмов, способных классифицировать блоки данных (электронные сообщения) по содержимому, одним из которых является классический наивный байесовский классификатор (НБК), который в изначальном своем определении не адаптирован для решения задачи классификации электронных сообщений на классы достоверной и недостоверной информации. Для решения задачи классификации электронных сообщений относительно их содержимого на обозначенные классы с применением НБК требуется проведение процесса адаптации алгоритма.

Задача адаптации

Рассмотрим процесс адаптации НБК к процессу классификации электронных сообщений по их содержимому на класс достоверной и недостоверной информации. Для этого рассмотрим базовый элемент – электронное сообщение, представленное в виде вектора $\vec{x}$, состоящее из конечного числа слов $X_1 \ldots X_n$:

$$\vec{x} = \langle X_1 \ldots X_n \rangle, \tag{1}$$

где $X_1 \ldots X_n$ – слова, входящие в данное сообщение. Пусть $C = \{C_1, C_2\}$ множество классов достоверных (C_1) и недостоверных сообщений (C_2). Тогда вероятность отнесения слова $\vec{x}$ в подмножество (класс) $C_i \in C$ есть вероятность попадания всех его слов в данный класс:

$$p(C_i \mid \vec{x}) = p(C_i \mid X_1,\ldots, X_n). \tag{2}$$

Исходя из теоремы Байеса [17]:

$$p(C_i \mid X_1,\ldots, X_n) = \frac{p(C_i)p(X_1,\ldots, X_n \mid C_i)}{p(X_1,\ldots, X_n)}. \tag{3}$$

В силу того, что вероятность появления того или иного слова $X_1 \ldots X_n$ в сообщении x есть события равновероятные, то соотношение (3) можно переписать следующим образом:

$$p(C_i \mid X_1 \ldots X_n) = p(C_i)p(X_1 \ldots X_n \mid C_i). \tag{4}$$

С другой стороны, в силу независимости появления слов $X_1 \ldots X_n$ в сообщении x, значение $p(X_1 \ldots X_n)$ есть величина постоянная (константа), которая равна:

$$Q = p(X_1 \ldots X_n). \tag{5}$$

В нашем случае каждое слово из сообщения X_k условно независимо от любого другого слова X_j при $k \neq j$, то есть

$$p(X_k \mid C_i, X_j) = p(X_k \mid C_i). \quad (6)$$

С другой стороны, числитель эквивалентен совместной вероятности:

$$p(C_i, X_1 \ldots X_n), \quad (7)$$

которая, по определению условной вероятности, будет иметь значение

$$\begin{gathered} p(C_i, X_1, \ldots, X_n) = \\ p(C_i)p(X_1 \mid C_i)\ldots p(X_n \mid C_i) = \\ = p(C_i)\prod_{j=1}^{n} p(X_j \mid C_i). \end{gathered} \quad (8)$$

Из той же независимости $X_1 \ldots X_n$ условное распределение по подмножеству (классу) C_i может быть выражено как

$$p(C_i \mid X_1 \ldots X_n) = \frac{1}{Q} p(C_i)\prod_{j=1}^{n} p(X_j \mid C_i), \quad (9)$$

где Q равно значению, полученному в (5).

Таким образом, НБК объединяет исследуемую модель (в нашем случае это модель электронных сообщений с непустым содержимым) с правилом решения (возможностью проведения процесса классификации электронных сообщений на классы достоверных и недостоверных сообщений). Для определения соответствующего класса в процессе классификации в НБК выделяют такое понятие, как апостериорное правило принятия решения – под которым понимают правило, позволяющее определить наиболее вероятную гипотезу (решение относительно определения класса) [18].

Для процесса классификации в соответствии с НБК определим функцию-классификатор classify(•), которая для множества слов $X_1 \ldots X_n$ электронного сообщения x из класса электронных сообщений C имеет вид

$$classify(\vec{x}) = \arg\max_c p(C_i)\prod_{j=1}^{n} p(X_j \mid C_i). \quad (10)$$

Определим процесс обучения наивного байесовского классификатора как подсчет вероятности встречи того или иного слова в сообщении $X_j \in x$. Стоит заметить, что наивный байесовский классификатор при классификации сообщения делает предположение, что разные слова в тексте на одну и ту же тему появляются независимо друг от друга.

Проецируя (10) на задачу классификации электронных сообщений по классам достоверных и недостоверных сообщений, получаем

$$classify(\vec{x}) = \arg\max_{v_j \in V} P(v_j)\prod_i P(a_i \mid v_j), \quad (11)$$

где множество V = {достоверные сообщения, недостоверные сообщения}; $P(v_j)$ – вероятность принадлежности электронного сообщения классу v_j из множества достоверных и недостоверных сообщений, v_j рассчитывается как частота вхождения класса V_j во множество обучающих выборок; a_i – i-ое слово в электронном сообщении; $P(a_i \mid v_j)$ – вероятность содержания слова a_i в электронном сообщении принадлежащем классу v_j, рассчитывается исходя из частоты анализируемого слова, находящегося в обучающем массиве данных.

Таким образом, процесс обучения НБК построен по принципу постоянного (по мере поступления новых электронных сообщений с непустым содержимым в классификаторе от информационной системы или от пользователя) обновления частоты слов. Алгоритм классифицирует только те слова либо набор слов, которые ранее при анализе не встречались.

Заключение

Таким образом, НБК работает в рамках решения задачи классификации электронных сообщений по классам достоверности множества V, то есть алгоритм анализирует сообщение по словам, изменение количества которых влияет на механизм классификации через вероятностную составляющую, и этим решается основная задача классификации блоков данных и электронных сообщений, их распределение по соответствующим классам достоверности.

Литература

1. Васильев В.И. Интеллектуальные системы защиты информации. М.: Машиностроение, 2012. – 172 с.
2. Vacca J.R. Computer and Information Security Handbook // Newnes, 2012. – 1200 p.
3. Nunes L., Timmis J. Artificial Immune Systems: A New Computational Intelligence Approach // Springer Science & Business Media, 2002. – 380 p.
4. Хайкин С. Нейронные сети. М.: ИД «Вильямс», 2008. – 1103 p.
5. Abe S. Support Vector Machines for Pattern Classification // Springer Science & Business Media. 2005. – 473 p.
6. Kollias S. Artificial Neural Networks // Springer Science & Business Media. 2006. – 1008 p.
7. Дасгупта Д. Искусственные иммунные системы и их применение. Пер. с англ. М.: ФИЗМАТЛИТ, 2006. – 344 с.

8. Tarakanov A.O. Immunocomputing: principles and applications // Springer Verlag, New York, 2003 – 193 p.
9. Borger E. The Abstract State Machines Method for High-Level System Design and Analysis // Dipartimento di Informatica, Universita di Pisa. 2007. – P. 30-35.
10. Shim J.K. Information Systems and Technology for the Noninformation Systems Executive // CRC Press. 2000. – 672 p.
11. Lunt T.F., Tamaru A., Gilham F. A real-time intrusion-detection expert system (IDES) // Final Technical Report. 1992. – P. 10-13.
12. Бурлаков М.Е. Метод фильтрации входящего трафика на основе двухслойной рекуррентной нейронной сети // Ползуновский вестник. АлтГТУ им. И.И. Ползунова, №3/2, 2012. – С. 215-219.
13. Бурлаков М.Е., Осипов М.Н. Аудит безопасности локальной вычислительной сети с помощью динамической системы на нейронах с реакцией на последовательности. // Информационное противодействие угрозам терроризма. № 20, 2013. – С. 166-170.
14. Delvin D., O'Sullivan B. Satisfiability as a Classification Problem // University College Cork. URL: http://www.cs.ucc.ie/~osullb/pubs/classification.pdf (д.о. 03.01.2016).
15. Fernandez-Delgado M., Cernadas E., Barro S. Do we Need Hundreds of Classifiers to Solve Real World Classification Problems // University of Santiago de Compostela. URL: http://jmlr.csail.mit.edu/papers/volume15/delgado14a/delgado14a.pdf.
16. Schapire R. Machine Learning Algorithms for Classification // Princeton University. URL: http://www.cs.princeton.edu/~schapire/talks/picasso-minicourse.pdf.
17. Гмурман В.Е. Теория вероятностей и математическая статистика. М.: Высшее образование, 2005. – 400 с.
18. Боровиков В. STATISTICA. Искусство анализа данных на компьютере: Для профессионалов. СПб.: Питер, 2003. – 688 с.

Получено 20.03.2016

Бурлаков Михаил Евгеньевич, лаборант Кафедры безопасности информационных систем (БИС) Самарского национальный исследовательский университета (СНИУ) им. акад. С.П. Королева. Тел. 8-929-703-33-38. E-mail: knownwhat@gmail.com

Голубых Денис Алексеевич, студент СНИУ им. акад. С.П. Королева. Тел. 8-927-604-39-09. E-mail: den1008@bk.ru

Осипов Михаил Николаевич, к.ф.-м.н., доцент, зав. Кафедрой БИС СНИУ им. акад. С.П. Королева. Тел. 8-927-263-57-77. E-mail: osipov7@yandex.ru

NAIVE BAYESIAN CLASSIFIER ADAPTATION FOR E-MAIL CLASSIFICATION MECHANISM

Burlakov M.E., Golubyh D.A., Osipov M.N.
Samara University, Samara, Russian Fedeartion
E-mail: osipov7@yandex.ru

Actually there are many difficulties for solutions of email classification problems. One is the problem of content analysis for two classification groups containing reliable and unreliable data. There are known a number of adaptive and non-adaptive algorithms that should help to solve described problem. Nowadays naive Bayesian classifier algorithm is one of the most popular tool in the field of data classification problem solution. This work is concerned on how to adapt naive Bayesian classifier mechanism for e-mail classification, where e-mails are classified as reliable and unreliable information blocks. We determine naive Bayesian classifier learning process as calculation the probability of one or another word meeting into e-mails.

Keywords: e-mail classification, naïve Bayesian classifier, reliable information block, unreliable information block.

DOI: 10.18469/ikt.2016.14.2.15

Burlakov Michael Evgenyevich, Samara University, 1 Akademika Pavlova str., Samara, 443011, Russian Federation, Laboratory Assistant of the Department of Information Systems Security. Tel.: +79297033338. E-mail: knownwhat@gmail.com.

Golubyh Denis Alekseevich, Samara University, 1 Akademika Pavlova str., Samara, 443011, Russian Federation, student. Tel.: +79276043909. E-mail: den1008@bk.ru.

Osipov Michael Nikolaevich, Samara University, 1 Akademika Pavlova str., Samara, 443011, Russian Federation, the Head of Department of Information Systems Security. Tel.: +792726035777. E-mail: osipov7@yandex.ru

References

1. Vasylyev V.I. *Intellektualnie sistemi zaschity informacii* [Intelligent Information Security Systems]. Moscow, Mashinostroenie Publ., 2012. 172 p.
2. Vacca J.R. *Computer and Information Security Handbook*. Newnes, 2012. 1200 p.
3. Nunes L., Timmis J. *Artificial Immune Systems: A New Computational Intelligence Approach*. Springer Science & Business Media. 2002. 380 p.
4. Haikin S. *Neironnie seti* [Neural networks]. Moscow, Vilyams Publ., 2008. 1103 p.
5. Abe S. *Support Vector Machines for Pattern Classification*. Springer Science & Business Media, 2005. 473 p.
6. Kollias S. *Artificial Neural Networks*. Springer Science & Business Media, 2006. 1008 p.
7. Dasgupty D. *Isskustvennie immunye sistemi i ih primemenie* [Artificial Immune Systems and their Applications]. Moscow, FIZMATLIT Publ., 2006. 344 p.
8. Tarakanov A.O. *Immunocomputing: principles and applications*. Springer Verlag, New York, 2003. 193 p.
9. Borger E. *The Abstract State Machines Method for High-Level System Design and Analysis*. Dipartimento di Informatica, Universita di Pisa. 2007. doi: 10.1007/978-1-84882-736-3_3
10. Shim J.K. *Information Systems and Technology for the Noninformation Systems Executive*. CRC Press, 2000. 672 p.
11. Lunt T.F., Tamaru A., Gilham F. A real-time intrusion-detection expert system (IDES). *Final Technical Report,* 1992, pp. 10-13.
12. Burlakov M.E. Method filtracii vhodyashego trafika na osnove dvuhsloinoi rekurrentnoi neironnoi seti [Method of filtering incoming traffic based on a two-layer recurrent neural network]. *Polzunovsky vestnik*, 2012, no. 3-2, pp. 215-219.
13. Burlakov M.E., Osipov M.N. Audit bezopasnosti lokalynoy vychislitelnoy sistemy na neyronahs reakciey na posledovatelnosti [Security audit of LAN by using dynamic system neurons reacting to the sequence.]. *Informacionnoe protivodeystvie ugrozam terrorizma*, 2013. № 20. – pp. 166-170.
14. Delvin D., O'Sullivan B. *Satisfiability as a Classification Problem*. University College Cork. Available at: http://www.cs.ucc.ie/~osullb/pubs/classification.pdf (accessed 03.01.2016).
15. Fernandez-Delgado M., Cernadas E., Barro S. *Do we Need Hundreds of Classifiers to Solve Real World Classification Problems*. University of Santiago de Compostela. Available at: http://jmlr.csail.mit.edu/papers/volume15/delgado14a/delgado14a.pdf (accessed 03.01.2016).
16. Schapire R. *Machine Learning Algorithms for Classification*. Princeton University. Available at: http://www.cs.princeton.edu/~schapire/talks/picasso-minicourse.pdf (accessed 03.01.2016).
17. Gmurman V.E. *Teoriy veroiytnostey i matematicheskaya statistika* [Theory of Probability and Mathematical Statistics]. Moscow, Vishie obrazovanie Publ., 2005. 400 p.
18. Borovikov D. STATISTICA. *Iskusstvo analiza dannih na kompyutere: dlya proffesionalov* [STATISTICA. The art of data analysis on a computer: for proffesionals]. St. Petersburg, Piter Publ., 2003. 688 p.

Received 20.03.2016