

РОЗВ'ЯЗАННЯ ЗАДАЧІ КОМЕНТУВАННЯ З ІНТЕЛЕКТУАЛЬНОЮ ФІЛЬТРАЦІЄЮ СПАМУ

Вінницький національний технічний університет

Анотація

Розглянуто актуальність задачі коментування з інтелектуальною фільтрацією спаму. Для покращення точності розпізнавання спаму пропонується комбінувати методи, що використовують нейронні мережі і методи засновані на теоремі Байєса.

Ключові слова: спам, фільтрація спаму, нейронні мережі, коментування, соціальні мережі.

Abstract

We consider the relevance to intellectual tasks comment spam filtration. To improve the recognition accuracy is proposed to combine methods that use neural networks and methods based on Bayes' Theorem.

Keywords: Spam, spam filtering, neural networks, commenting, social networks.

Інтернет – це глобальна комп'ютерна мережа, що охоплює увесь світ. Сьогодні Інтернет має близько 3.2 млрд. абонентів понад у 150 країнах світу. Кількість інформації, доступної користувачам глобальної мережі Інтернет, з кожним роком стає все більше і більше. Постійно зростає кількість сайтів, збільшується число їх сторінок. За статистикою щомісяця розмір мережі збільшується на 7 – 10% [1]. Мережу в більшості випадків використовують як середовище для спілкування, наприклад, соціальні мережі, чати, форуми, електронна пошта тощо. Одним із видів спілкування та висловлення думок є коментування певних інформаційних матеріалів, але розвиток мережі Інтернет та засобів зв'язку привів до революції не тільки у сфері комунікацій, але і у сфері реклами і комерції, що, в свою чергу, породило проблему небажаної реклами та повідомлень (спаму) [2]. Спам – це рекламні повідомлення, які доставляються без згоди користувача, а також повідомлення, створені для шахрайських цілей [3]. Раніше спам-коментарі були лише у вигляді реклами (в основному ця реклама приводила до інших інтернет-ресурсів), але за декілька років почалося зростання кількості коментарів у вигляді політичного спаму, де коментарі пишуться з ціллю пропаганди і введення в оману. З такою проблемою особливо зараз стикнулася Україна.

З сучасними технологіями, для того, щоб створити сайт фактично не потрібні знання в царині програмування, а можна використати, зокрема, системи керування вмістом, як наприклад Joomla! Joomla! – це відкрита універсальна система керування вмістом для публікації інформації в Інтернеті. На поточний час у мережі доступно багато модулів, компонентів для коментування для CMS Joomla!, але вони або давно не оновлюються або просто малофункціональні. Найпопулярнішим є компонент Jcomments, але через величезну затримку виходу релізу виникла гостра необхідність в сучасних компонентах коментування [4].

Сучасний компонент коментування повинен мати такі основні функції як: можливість входу через соціальні мережі, такі як Facebook або Twitter; можливість зберігання коментарів, які були зроблені зі сторінок соціальних мереж на локальній БД; можливість виведення популярних коментарів; можливість виведення останніх коментарів; можливість коментування інших коментарів; наявність функції інтелектуальної фільтрації спаму.

Однією з перевагою майбутнього компонента коментування буде те, що в ньому буде вмонтований інтелектуальний модуль фільтрації спаму. Є різні методи фільтрації спаму, найпопулярніші з них: чорні списки, статистичні методи фільтрації спаму [5], використання CAPTCHA та методи на основі нейронних мереж, наприклад SOM [6, 7].

Метод чорні списки заносяться IP-адреси комп'ютерів, про які відомо, що з них ведеться розсилання спаму. Можна використовувати локальний список або список який підтримує хтось інший. Завдяки простоті реалізації, широке поширення одержали чорні списки, запит до яких здійснюється через службу DNS. Вони називаються DNSBL (DNS Black List). В даний час цей метод не дуже ефективний. Спамери знаходять нові комп'ютери для своїх цілей швидше, ніж їх встигають

заносити в чорні списки. Крім того, кілька комп'ютерів, що відправляють спам, можуть скомпрометувати весь поштовий домен і тисячі законслухняних користувачів на невизначений час будуть позбавлені можливості відправляти пошту серверам, що використовують такий чорний список[5].

Статистичні методи фільтрації спаму використовують статистичний аналіз змісту коментаря для прийняття рішення, чи є він спамом. Найбільшого успіху удалося досягти за допомогою алгоритмів, заснованих на теоремі Байєса [5]. Ці алгоритми працюють за таким принципом: кожному слову, що зустрічається у коментарі присвоюється два значення: ймовірність його присутності у спамі (Z) та ймовірність його присутності у звичайних повідомленнях. Величину Z називають спам-оцінкою слова. Для кожного нового листа за допомогою формули Байєса розраховується загальна спам-оцінка коментаря. Основним недоліком байєсовської фільтрації є висока ймовірність пропуску спаму, якщо у коментарі мало слів з високою спам-оцінкою [8].

Ще одним часто використовуваним шляхом захисту від саму є САРТНА (комп'ютерний тест, який використовується для того, щоб визначити, хто використовує систему – людина чи комп'ютер). У найпоширенішому варіанті САРТСНА від користувача потрібно ввести символи, зображені, як правило, у спотвореному вигляді на пропонованому малюнку, іноді з додаванням шуму або напівпрозорості. Проблема використання САРТНА полягає в тому, що вона часто не зручна для користувача, а особливо для людей з обмеженими можливостями.

Метод на основі нейронного алгоритма SOM, у своєму основному варіанті створює графподібності вхідних даних, створюючи, таким чином, абстракції (узагальнення) деякого виду, виконуючи кластеризацію усіх вхідних векторів. Стосовно задачі фільтрації спаму, SOM буде використаний для того, щоб розподіляти усі вхідні коментарі, на основі обраних ознак за кластерами. Кожен кластер буде комплексною характеристикою повідомлення, при цьому відмінність одного кластера від іншого виражається швидше якісно, ніж кількісно. При цьому одні кластери будуть містити в основному тільки спам-коментарі, повідомлення, які не відносяться до спаму будуть міститися у другому кластері, а інші кластери будуть містити коментарі, які можуть потенційно відноситися до спаму. Для оцінки коментарів можна використовувати ймовірнісний підхід: чим ближче кластер до «сірої» зони, тобто до кластеру спам-повідомлень, тим вище ймовірність того, що прийняте повідомлення є спамом. Для обчислення відстані між кластерами можна використовувати евклідову відстань між центральними вузлами нейронної решітки кластерів. Для прийняття рішень в даному методі використовується алгоритм LVQ. Оскільки алгоритм LVQ орієнтується виключно на рішення задач статистичної класифікації або розпізнавання, даний метод добре підходить і для завдання фільтрації спаму [6].

Перевага нейромережевого підходу перед статистичними методами фільтрації спаму полягає в тому, що не робиться ніяких попередніх припущень про характер небажаних повідомлень, а семантичні зв'язки враховуються автоматично.

В роботі пропонується використовувати декілька методів розпізнавання спаму, тобто нейронні мережі будуть використовуватися як перший рівень захисту, вони будуть аналізувати поведінку користувача на сайті, а якщо цей користувач увійшов з соціальних мереж, то і ще активність в соціальних мережах, після цього буде проаналізовано відправлений ним коментар. А результати, отримані за допомогою нейронних мереж будуть корегуватися методами на основі теореми Байєса [9], що дозволить, в кінцевому підсумку, підвищити точність розпізнавання спаму.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Охотник Ю. В. В цифрах: количество пользователей интернета 15 лет назад и сегодня [Електронний ресурс] / Ю. В. Охотник. – Режим доступу <http://bit.ua/2015/05/internet-changes/>
2. Шарапов Р. В. Обнаружение ссылочного спама [Електронний ресурс] / Р. В. Шарапов – Режим доступу: http://rcdl2008.jinr.ru/pdf/191_196_paper22.pdf
3. Абдуллаев В. Г. Защита от спама в интернет пространстве. / Абдуллаев В. Г. // Радиоэлектроника и информатика . 2014. № 2 (65). С. 35 – 38.
4. Хорошевский А. В. Обзор JComments [Електронний ресурс] / А. В. Хорошевский – Режим доступу: <http://aleksius.com/joomla/rasshireniya/komponent-jcomments>
5. Кузьма Т. Н. Аналіз методів фільтрації СПАМу/ Т. Н. Кузьма // Матеріали Міжнародної науково-технічної конференції молодих учених та студентів «Актуальні задачі сучасних технологій». – Тернопіль, 11 – 12 грудня 2013 р. – С. 194 – 195.

6. Тарелина А. В. Метод фильтрации спама на основе нейросетевых алгоритмов som и LVQ // Современная наука: актуальные проблемы и пути их решения./ Тарелина А. В., Хорев П. Б. 2014. № 9. С. 21 – 25.
7. Бардаченко В. Ф. Таймерні нейронні елементи та структури. Монографія / В. Ф. Бардаченко, О. К. Колесницький, С. А. Василецький. – Вінниця : УНІВЕРСУМ-Вінниця, 2005, 126 с.
8. Ажмухамедов И. М. Усовершенствованный метод фильтрации нежелательного трафика./ И. М. Ажмухамедов, К. В. Запорожец // Вестник АГТУ. Серия: Управление, вычислительная техника и информатика. 2014. №1. С.98 – 104.
9. Айдаров Ю. Р., Создание интеллектуального спам-фильтра [Электронный ресурс] / Ю. Р. Айдаров, Л. М. Ермакова – Режим доступа: <http://www.permai.ru/files/projects/P19.pdf>

Коханський Максим Русланович – студент групи 2КН-126, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: maim.kohanskij@outlook.com;

Науковий керівник: **Арсенюк Ігор Ростиславович** – к. т. н., доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця.

Maksym R. Kokhanskyi – Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: maim.kohanskij@outlook.com;

Supervisor: **Arseniuk R. Ihor** – Cand Sc., Assistant Professor of the Chair of Computer Science, Vinnytsia National Technical University, Vinnytsia.