E-2 Unlimited Technologies

A Robust Algorithm for Detecting Rare Text in a Corpus with Limited Training Data©

An algorithm reducing cost, time, and increasing efficacy over current cybercrime detection systems and supporting GRC initiatives

Lead Inventors

- April Edwards, PhD, Vice President for Academic Affairs and Dean of the Faculty, Elmhurst College; former Professor, Mathematics and Computer Science, Ursinus College
- Lynne Edwards, PhD, Professor of Media and Communication Studies, Ursinus College; Distinguished Research Fellow, Annenberg Public Policy Center, University of Pennsylvania

Unmet Need

This invention originally was developed to address cyberbullying, but further study indicates the algorithm can address and mitigate an array of currently hard-to-detect **cybercrimes** as well as support **Governance, Risk, and Compliance (GRC) initiatives**.

Cyberbullying has many different shades and forms. Social media makes its users vulnerable to cybercrime, which is hard to track and impractical to detect manually across an increasing number of communication platforms. *Netspeak* can confuse many currently-used filters, though some syntactic commonalities can be identified and utilized during detection.

Even more difficult to detect than cyberbullying and perhaps costlier to society, are those situations where there are few instances of the feature being detected in a large volume of text. For example, content in **online communication and social media, online dating scams, terrorist activity,** and **financial fraud**.

Existing algorithms and detection systems based on them typically depend on manually developed dictionaries and / or require a large number of training instances rendering them unwieldy and requiring on-going labor-intensive efforts.

Opportunity

The inventors have developed a new algorithm for machine learning in short text (such as SMS messages or tweets). The algorithm is particularly tailored to identifying specific occurrences or types of instances within large volumes of text and they believe the algorithm is applicable to cyberbullying content in online communication, terrorist activity, and financial fraud.

Existing algorithms and systems based on them depend on manually developed dictionaries and / or require a large number of training instances. Latent Semantic Analysis (LSA) systems, for example, work by detecting term cooccurrence patterns in the entire corpus. LSA requires a large number of training instances, as well as significant run-time resources. As the corpus evolves, operators must re-train and re-optimize the system, which requires additional manual labeling and additional resources.

In contrast, the E-2 algorithm begins with a set of labeled training data and is refined by continuous learning on unlabeled data, reducing cost, time, and increasing efficacy.

Testing shows the initial algorithm is accurate with few false positives.

Continued on back

Unique Attributes

The distinguishing features of this algorithm, in comparison to other textual data mining techniques are:

- The keyword dictionary is built automatically. There is no need to manually develop and maintain a dictionary of keywords.
- The dictionary is built using an extremely small training set, when compared to the magnitude of the corpus that needs to be labeled. In this case, E-2 trained the algorithm on 1500 tweets, 94 of which contained cyberbullying content.
- The detection algorithm considers both the dictionary of keywords, as well as the word patterns in the text (as determined by part-of-speech tagging). The word pattern dictionary also is built dynamically from the small training set.
- The dynamic nature of the dictionary build allows operators to capture word and pattern changes as the language evolves over time. Additional labeling is not necessary but may improve the effectiveness of the algorithm.
- The algorithm is fast and effective. It does not require a lot of memory or processing time once the dictionary has been built.

Operational Applications

With further development, for rapid, cost effective detection and mitigation of cybercrime.

Stage of Development

Algorithm built, training sets available.

Intellectual Property

Protection in force.

Licensing Opportunity

Actively seeking licensee for commercialization.

References and Publications

- Kontostathis, K. Reynolds, A. Garron and L. Edwards (2013). Detecting cyberbullying: query terms and techniques. In Proceedings of the 5th annual ACM web science conference (pp. 195-204). ACM.

CONTACT

Merle Gilmore
L2C Partners
+1 610.662.0940
gilmore@l2cpartners.com

L2C PARTNERS™
Moving Inventions from Lab to Society