كشف الهجوم الأمني الناشئ باستخدام شبكة الكبسولة العصبية

الطالبة/ سحر جبير الطلحي

اسم المشرف على الرسالة
د/ ميسون أبو الخير
د/ انتصار الكيال

المستخلص

في مجال الأمن السيبراني، أصبح تحليل بيانات الشبكة الاجتماعية مجالًا بحثيًا أساسيًا نظرًا لخصائصه المتمثلة في توفير تحديثات في الوقت الفعلي حول الأحداث الواقعية. أظهرت الدراسات أن تويتر يمكن أن يحتوي على معلومات حول التهديدات الأمنية قبل بعض المواقع المتخصصة. وبالتالي، يمكن أن يساعد تصنيف التغريدات على أنها متعلقة بالأمان أو غير متعلقة بالأمان في التحذيرات المبكرة لمثل هذه الهجمات.

تم استخدام العديد من التقنيات لتصنيف النص باستخدام خوارزميات تعلُم الآلة والشبكات العصبية وخوارزميات التعلم العميق التي تمت تجربتها والتحقق من أداءها على نطاق واسع للكشف عن الهجمات السيبرانية باستخدام بيانات تويتر. تعد الشبكة العصبية التلافيفية والشبكة العصبية المتكررة من أحدث التقنيات وأحدثها. ومع ذلك، تعاني الشبكة العصبية التلافيفية والشبكة العصبية المتكررة من قيود تتعلق ببنيتها مما أدى إلى اقتراح شبكة الكبسولة.

في هذه الدراسة، قمنا بالتحقيق في استخدام شبكة الكبسولة، خوارزمية التعلم العميق الجديدة، لأول مرة في مجال الكشف عن الهجمات الأمنية باستخدام تويتر. نحن نهدف إلى زيادة دقة تصنيف التغريدات باستخدام شبكة الكبسولة بدلاً من الشبكة العصبية التلافيفية والشبكة العصبية المتكررة. لتحقيق الهدف البحثي، قمنا بتكييف التمثيل الأساسي لشبكة الكبسولة ليكون متوافقًا مع مجموعة بيانات التغريدات. تم استخدام تقنية بحث عشوائي لضبط متغيرات النموذج. تم إجراء سلسلة من التجارب والمقارنات لتقييم كفاءة المساهمة البحثية. حقق النموذج المقترح في هذه الدراسة دقة ٩٢,٢١٪ متفوقا على نماذج الشبكة العصبية التلافيفية التي تم بناؤها لغرض المقارنة، وأحدث نماذج الدراسات السابقة التي تستخدم الشبكة العصبية التلافيفية والشبكة العصبية المتكررة.

Emerging Security Attack Detection using Capsule Neural Network

Sahar Jubair Altalhi

Supervised By
Dr. Maysoon Abulkhair
Dr. Entisar Alkayal

ABSTRACT

In cybersecurity, analyzing social network data has become an essential research area due to its property of providing real-time updates about real-world events. Studies have shown that Twitter can contain information about security threats before some specialized sites. Thus, the classification of tweets into security-related and not security-related can help with early warnings for such attacks.

Many techniques for text classification using different traditional machine learning (ML), neural network (NN), and deep learning (DL) algorithms have been widely investigated for detecting cyber-attacks using Twitter data. Convolutional
neural network (CNN) and recurrent neural network (RNN) are two of the most recent and advanced techniques. However, CNN and RNN suffer from limitations related to its architectures which lead to proposing the capsule network (CapsNet).

In this study, we investigated the use of the CapsNet, the new DL algorithm, for the first time in the field of security attack detection using Twitter. We aim to increase the accuracy of tweet classification by using CapsNet rather than CNN or RNN. To achieve the research objective, we adapted the original implementation of CapsNet to be compatible with the tweet dataset. A random search technique was used to tune the model's hyperparameters. A series of experiments and comparisons were conducted to evaluate the research contribution efficiency. The experimental results showed that CapsNet exceeded the baseline CNN, and CNN and RNN previous works on the same dataset, with accuracy of 92.21% and a 92.2% F1-score using word2vec embedding. Besides, in all experiments, the word2vec embedding performed better than a random initialization.