An Embedding-based Framework for Detecting Similar Mobile Applications

Weizhuo Li[1,2], Buye Zhang[3], Liang Xu[1,2], Meng Wang[1,2(✉)], Anyuan Luo[3], and Yan Niu[4(✉)]

[1] School of Computer Science and Engineering, Southeast University, Nanjing, China.
liweizhuo@amss.ac.cn meng.wang@seu.edu.cn
[2] Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education, China.
[3] School of Cyber Science and Engineering, Southeast University, Nanjing, China.
[4] China Academy of Industrial Internet, Beijing, China. niuyan@pku.edu.cn

Abstract. With the popularity of smart phones and mobile devices, large amounts of mobile applications (a.k.a."app") have been developed and published. Detecting similar apps from a large pool of apps is a basic and important task because it has many benefits for various applications (e.g., app recommendation). There exist several works that try to combine different metadata of apps in application markets to measure the similarity between apps in a principled way and obtain encouraging results. However, few methods pay attention to the roles (e.g., normal users, cybersecurity analysts) of this service. One the other hand, existing methods do not distinguish the characters of contents in these metadata (e.g. structured labels, unstructured text). It is hard for them to capture higher-order correlations among apps and obtain their accurate semantic representations. In this paper, we propose a novel framework by knowledge graph (KG) and embedding techniques to fill these gaps. For the construction of KG, we further design a lightweight ontology tailored for the service of cybersecurity analysts. Benefited from a well-defined schema, more linkages can be shared among apps. To detect similar apps, we divide the transformed relations in KG into structured and unstructured ones according to their related contents. So the representations of apps can be accurately learned by suitable embedding techniques and optimized for improving the performance of similar apps detection. The preliminary result indicates the effectiveness of our framework comparing to several existing methods in terms of reciprocal ranking average and minimum ranking.

Key words: Similar App Detection, Knowledge Graph, Ontology, Embedding

1 Introduction

With the popularity of smart phones and mobile devices, the number of mobile applications (a.k.a. "app") has been growing rapidly, which provides great convenience to users for online shopping, education, entertainment, financial management etc [1]. According to a recent report[5], as of August 2018, there were over 9.8 and 4.5 million apps available on Google Play[6] and App Store[7], respectively, and global downloads of mo-

[5] https://www.appannie.com/cn/insights/market-data/the-state-of-mobile-2019/
[6] http://play.google.com/store/apps
[7] https://www.apple.com/ios/app-store/

bile apps have exceeded 194 billion. With large amounts of apps, if a specific app is given as a query, it is difficult to find all other apps that are similar to the query one.

Detecting semantically similar apps from a large pool of apps is a basic and important task because it has many benefits for different stakeholders in the mobile app ecosystem [2]. For example, it is helpful for app platforms to improve the performance of their app recommendation systems and enhance the user experience of app search engines. For app developers, detecting similar apps can be useful for various purposes such as identifying direct competing apps, assessing reusability (if open source) and so on. Meanwhile, lots of apps also become the hotbeds for cybercriminals such as thieving private data, propagating false news and pornography, online-scam. Therefore, it is essential for cybersecurity analysts to supervise apps and prevent potential cybercriminals related to them.

Detecting similar apps is a nontrivial and difficult problem. One of the key challenges is how to explore and combine different modalities of data in app markets to measure the similarity between apps in a principled way. Previous studies provided solutions based on bag of words [3] or topic models [4, 5] to calculate the similarity of apps, which depended on description texts, titles and user reviews of apps. Recently, Chen et al. [2] and Lin et al. [6] proposed hybrid frameworks to achieve this service. The authors defined kernel functions and decision trees to integrate different metadata for improving the performances of similar apps detection.

Although existing methods have obtained some encouraging results, they still suffer from two limitations. Firstly, different objects (e.g., users, developers) expect different results of this service [7]. Therefore, it may not be suitable to directly utilize their algorithms to provide the service of similar apps detection for cybersecurity analysts. Secondly, existing works focus on basic features of metadata, whereas do not distinguish the characters of contents in these metadata (e.g. structured labels, unstructured text). It is hard for them to capture higher-order correlations among apps and obtain their accurate semantic representations.

To fill above gaps, in this paper, we present a novel framework for detecting similar apps using knowledge graph and embedding techniques. We focus on one kind of apps, namely sensitive apps, that own more conditions or plausibility than normal apps that become the hotbeds for cybercriminals. We define a lightweight ontology including basic classes and properties from the view of cybersecurity analysts and construct the knowledge graph (KG) of sensitive apps. Benefited from a well-defined schema, more linkages can be shared among apps. To detect similar apps, the underlying idea of our framework is to divide the transformed relations in KG into structured and unstructured ones according to their contents. So the representation of apps can be accurately learned by the suitable embedding techniques and optimized for improving the performance of similar apps detection.

The main contributions of our work are summarized as follows.

1. We study the problem of detecting mobile application similarity serviced for cybersecurity analysts. To the best of our knowledge, this is the first work that focuses on this problem;
2. We present a novel framework to tackle this problem, in which we construct knowledge graph based on defined ontology and employ suitable embedding techniques to optimize the representations of apps;
3. We construct a new dataset based on the constructed knowledge graph for evaluation. Compared with several existing methods, the preliminary result indicates that

our approach for detecting similar apps of a new one can obtain better performances in terms of reciprocal ranking average and minimum ranking.

The rest of this paper is organized as follows. Related work is introduced in Section 2. Section 3 presents the implementation details of our framework for detecting similar apps. The evaluation is reported in Section 4, followed by a conclusion in Section 5.

2 Related work

In this section, we mainly review the research efforts on detecting similar apps and building knowledge bases of apps. For embedding techniques, we refer readers to [8,9] for a recent overview on this topic.

2.1 Detecting Similar Mobile Applications

Detecting semantically similar apps from a large pool of apps is a basic and important problem, as it is beneficial for various applications, such as app classification and app recommendation, app search, etc.

Bhandari et al. [3] linked the title, description and user reviews of an app as one document, and then built the vector using the TD-IDF weighting scheme. They also used cosine similarity to calculate the pairwise similarity.

Yin et al. [4] treated the description of an app as a document and applied LDA to learn its latent topic distribution. In this way, each app was represented as a fixed length vector. Then, the similarity between two apps was computed as the cosine similarity of their vectors.

Chen et al. [2] proposed a framework called SimApp that detected similar apps by constructing kernel functions based on multi-modal heterogeneous data of each app (e.g., description texts, images, user reviews) and learned optimal weights for the kernels.

Park et al. [5] exclusively leveraged text information such as reviews and descriptions (written by users and developers, respectively) and designed a topic model that could bridge the vocabulary gap between them to improve app retrieval.

Lin et al. [6] developed a hybrid framework that integrated a variety of app-related features and recommendation techniques, and then identified the most important indicators for detecting similar app. The authors employed gradient tree boosting model as the core to integrate the scores by using user features and app metadata as additional features for the decision tree.

Although existing methods have obtained some encouraging results, it may not be suitable for these algorithms to provide the same service for cybersecurity analysts. Because different objects (e.g., users, developers) expect different results of this service [7]. On other hand, existing methods do not distinguish the characters of contents in these metadata (e.g. structured labels, unstructured text). It is hard for them to capture higher-order correlations among apps and obtain their accurate semantic representations. Relatively, we define an ontology in view of cybersecurity analysts, and utilize existing metadata of apps to construct a knowledge graph to achieve this goal. Moreover, we employ suitable embedding techniques to optimize the representation of apps.

2.2 Knowledge Bases for Mobile Applications

Many interesting insights can be learned from data on application markets and aggregations of that data, which gain a remarkable attraction from academia and industry [10]. For example, Google Play is one of the largest markets that contain millions of apps for the Android platform.

Drebin [11] provides a considerate number (5,560) of malware to the public with detailed malicious behaviors inside, which were identified and classified by a machine learning method. These samples were categorized into 149 families in terms of contained malicious behaviors.

Commercial databases have mirror metadata from Google Play and other app markets and sell access to this information (e.g. appannie.com, appbrain.com and appszoom.com [12]). Most of these commercial databases contain comprehensive metadata of millions of apps but they lack links to other resources.

AndroZoo++ [13] is an ongoing effort to gather executable Android applications from as many sources as possible and make them available for analysts. In addition, the authors figured out 20 types of app metadata to share with the research community for relevant research works.

AndroVault [14] is a knowledge graph of information on over five million Android apps. It has been crawled from diverse sources including Google Play and F-Droid since 2013. AndroVault computes several attributes for each app based on downloaded android application package, in which entities can be heuristically clustered and correlated by attributes.

Commercial databases and AndroZoo++ mainly focus on the scale of apps. The goal of their collecting apps is to sell their access and share them with the research community. Relatively, Drebin and AndroVault dedicate to provide abundance apps for malware detection. All of these knowledge bases pay little attention to similar apps detection serviced for cybersecurity analysts, which is essential for them to supervise apps and prevent potential cybercriminals. To the best of our knowledge, our work is the first step towards employing knowledge graph and embedding techniques to tackle this problem.

3 Detecting Similar Mobile Applications

At the beginning of presenting our framework, we give a formalized definition that models the similarity of apps.

Definition 1 *(Mobile App Similarity Modeling) [2]. Given a collection of mobile apps $\mathcal{A}$, the objective of mobile app similarity modeling problem is to learn a function $f : \mathcal{A} \times \mathcal{A} \rightarrow R^+$, such that $f(a_i, a_j)$ can measure the semantic similarity for any two apps $a_i, a_j \in \mathcal{A}$.*

Fig. 1 presents the framework for detecting similar apps. After we extracted the metadata of apps from application markets and external resources, we further construct a knowledge graph tailored for the service of cybersecurity analysts, in which a lightweight ontology is defined to formalize the basic classes and properties. Benefited from a well-defined schema, more linkages can be shared among apps. To detect similar apps, the underlying idea is to divide the transformed relations in KG into structured and unstructured ones according to their related contents. So the representations of apps can be learned from suitable embedding techniques and optimized for improving the performance of similar apps detection. Next, we will illustrate each part in detail.

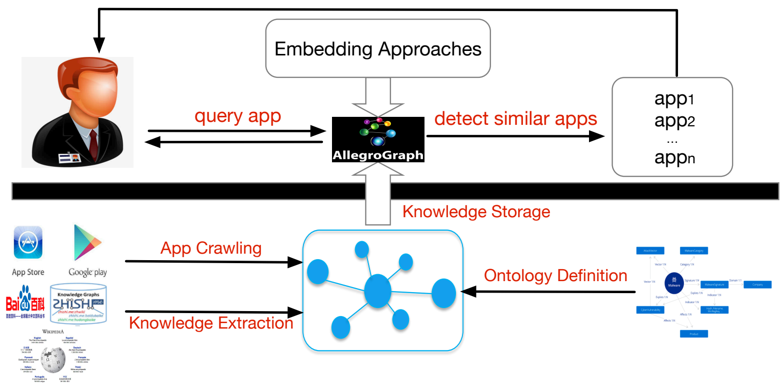

Fig. 1: The framework of detecting similar mobile applications

3.1 The Construction of Mobile Application Knowledge Graph

Ontology definition To model a well-defined schema of apps according to their sensitivity, we frequently discuss with analysts worked on the China Academy of Industrial Internet, and discover that the vast majority of conceptualizations (e.g., function point, interaction mode) described for sensitive apps are not available online. Therefore, we choose appropriate terms based on the survey of existing conceptualizations in view of sensitivity, and define a set of properties by protégé[8] to cover the sensitivity of mobile.

Fig. 2 shows the overview of our light-weight ontology, Note that red edges and blue ones represent *subclassof* and *rdfs:type* relations, respectively, which are two basic relations. The green ones represent the object properties, and violet ones represent data properties. Overall, we define 30 basic concepts and properties in ontology. Benefited from a well-defined schema, it not only can make apps to present more comprehensive properties to analysts, but also can generate more shared linkages among apps.

App crawling With the help of scrapy framework[9], we crawl the descriptive information of apps published from Google Play and App Store. Note that we do not download application packages of them because we focus on supervising the sensitive apps rather than detecting malicious codes of them. To achieve this goal, we design several heuristic conditions to guide sensitive apps crawling. The main conditions are listed as follows.

- If the state of one app is not available (e.g., off the shelf), it may be a sensitive app.
- If download times of one app are more than one thousand, it may be a sensitive app.
- If the description of one app contains sensitive tokens (e.g., belle, lottery), it may be a sensitive app.
- If one app shares the same companies or developers with sensitive apps, it may be a sensitive app.

Knowledge extraction Crawling the data of apps from application markets is the most direct way to build KG. However, the known labels often inadequately cover the value

[8] https://protege.stanford.edu/
[9] https://scrapy.org/

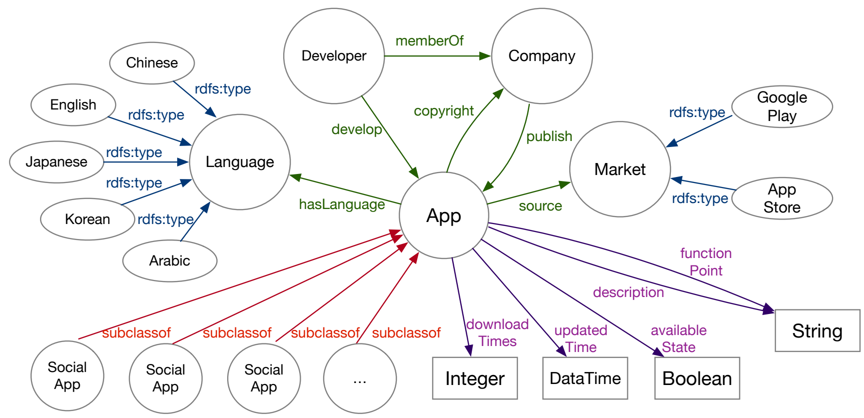

Fig. 2: The overview of lightweight ontology

of properties in our designed ontology, which impedes the discovery of the shared linkage among apps. Therefore, we try to extract related web pages from external resources (e.g., Baidu Baike[10] and Wikipedia[11]) to fill the lacked value of these properties. We mainly consider the following strategies to parse the web pages of sensitive apps and populate their property value.

- **String matching method**. It is a mainstream method of knowledge extraction. With the defined mappings between properties (e.g., *Market*) in ontology and attributes (e.g., *Platform*) in inforbox, we can complete the value of several properties.
- **Template-based method**. For one property such as *function point*, we design several templates tailored for textual descriptions in web-pages to obtain the lacked functions of apps.
- **Named entity recognition**. For the concepts *Developer* and *Company*, we utilize the parsed pos of named entity recognition [15](e.g., LSTM+CRF) to capture the related value.

In addition, we make use of the triples asserted in zhishi.me [16] to further complete our KG as many as possible. It is one of the largest knowledge bases that cover three Chinese encyclopedias.

Knowledge storage After we utilized the crawled data to instantiate the properties in our designed ontology and finishing knowledge extraction, we transform them to RDF triples $\{(s, p, t)\}$ by Jena[12]. For knowledge storage, we employ AllegroGraph[13] to store the transformed triples, which is one of the efficient graph bases for storing the RDF triples and supporting SPARQL query[14] seamlessly. Benefited from SPARQL query

[10] https://baike.baidu.com
[11] http://en.wikipedia.org/wiki/Wiki
[12] http://jena.apache.org/
[13] https://allegrograph.com/
[14] https://www.w3.org/2001/sw/wiki/SPARQL

and inference rules implied in ontology, it can present comprehensive information of apps for analysts.

To keep the knowledge graph in sync with the evolving apps, we will periodically update the descriptive information of apps by crawling above sources and record the updated logs.

3.2 Similar Apps Detection based on Embedding

To better supervise apps and prevent cybercriminals related to them, we develop the service of similar apps detection based on embedding models. As shown in Fig. 3, given the descriptive information of an app, we divide various relations stored in KG into structured and unstructured ones according to their contents. Then, we try to employ suitable embedding models to learn the representations of apps.

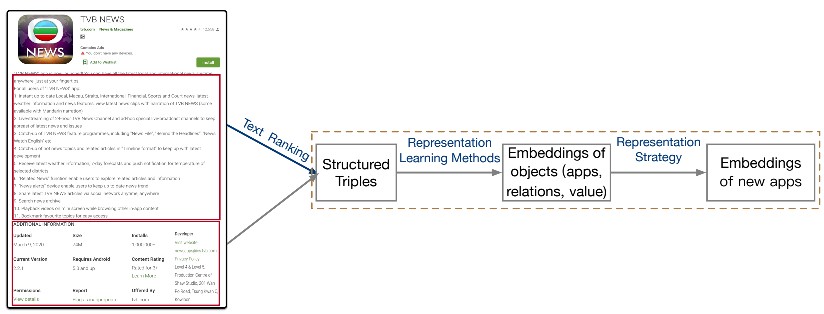

Fig. 3: The workflow of similar apps detection based on embedding approaches

Embedding based on structured triples For structured triples, we try to employ KG embedding [8] and network embedding (NE) models [9] to learn the representations of apps. KG embedding aims to effectively encode a relational knowledge graph into a low dimensional continuous vector space and achieves success on relational learning tasks like link prediction and triple classification. Network embedding can effectively preserve the network structure and capture higher-order similarities among entities. Although they are suitable to model the structured triples, the merits of them are different. KG embedding can learn the representations of entities and relations in KG simultaneously. Relatively, network embedding sacrifices the semantics of edges for capturing higher-order semantic similarities among entities.

Embedding based on unstructured texts Note that, KG embedding and NE models can not make use of the description texts of apps to enhance the potential correlations of apps. To address this problem, we extract the important tokens of app description texts by TextRank algorithm [17], which is a graph-based ranking model for text processing. The corresponding formula is defined as follows.

$$Sim(S_i, S_j) = \frac{|\{t_k | t_k \in S_i \cap t_k \in S_j\}|}{log(N_i) + log(N_j)}, \quad (1)$$

where $S_i = t_i^1, t_i^2, ..., t_i^{N_i}$ and $S_j = t_j^1, t_j^2, ..., t_j^{N_j}$ are two sentences in the description text of one app, N_i and N_j are the number of tokens in S_i and S_j, t_k is one shared token between two sentences. After iteratively calculated the text-rank value of each token, we can obtain several important tokens by a threshold θ to represent the description text of this app. Then, we introduce a new relation *relatedTo* tailored for these tokens and generate new triples to feed into KG embedding models. For NE models, we only treat app and each token as two nodes in the network, and add one edge to connect them.

The representations of new apps With helpful of embedding techniques, the similarities between apps can be calculated based on cosine measure. However, it is still challenging for KG embedding and NE models to obtain accurate embeddings for new apps because these apps are not fed into the training process.

Existing NE methods try to utilize the related information (or entities) of these apps to calculate their similarity. Arithmetic mean [18] and property concatenation [19] are two common strategies to represent the embeddings of new apps. Nevertheless, these two strategies ignore the semantics of properties in triples, which assume related information and entities of new apps have the same contributions. Hence, it may not reflect the reality embedding representations for new apps. To address this problem, we further optimized the property concatenation strategy based on entropy. Intuitively, this strategy can utilize the value or entities in each property to measure the importance of itself. Given one new app v_{n+1} and its related information (or entities) denoted by $\{(v_{n+1}, r_k, v_k)\}$, we formalize our strategy by Eqs. 2.

$$\mathbf{v_{n+1}} = w_1\mathbf{v_1} \oplus w_2\mathbf{v_2} \oplus ... \oplus w_m\mathbf{v_m}, \text{ s.t. } v_1, v_2, ..., v_m \in V \tag{2}$$

$$w_i = \frac{H(p_i)}{\sum_1^l H(p_t)}, \tag{3}$$

where $\mathbf{v_{n+1}}$ is the embedding representation of new app. $\mathbf{v_1}, \mathbf{v_2}..., \mathbf{v_m} \in \mathbb{R}^d$ are embedding representations of related information (or entities) $v_1, v_2, ..., v_m$, which belong to a set of nodes V in the network. $\oplus$ is a concatenate operation $\mathbb{R}^{a\times d} \oplus \mathbb{R}^{b\times d} \rightarrow \mathbb{R}^{(a+b)\times d}$, w_i is a weight calculated by all the entropy of app properties, $H(p_i)$ is an entropy of all the value and entities of property p_i, l is the number of them.

Inspired of the work in [20], for KG embedding methods, we can directly utilize the score function $f(v_{n+1}, r_k, v_k)$ of KG embedding methods to predict the different embeddings of v_{n+1} according to r_k and v_k. Then, we average the these predicted embeddings together to obtain the final representation of new app. The corresponding formula is defined as follows.

$$\mathbf{v_{n+1}} = \frac{1}{m}\sum_1^m (f(\cdot, r_1, v_1) + f(\cdot, r_2, v_2) +, ..., f(\cdot, r_m, m)), \tag{4}$$

where $\mathbf{v_{n+1}}$ is the embedding representation of new app, m is a number of related triples transformed from the new app and their entities are also contained in the train set. $f(\cdot, r_k, v_k)$ is a score function that can predict a virtual embedding of new app by r_k andv_k. For example, according to the score function $||h + r - t||_2$ defined in TransE [21], we can obtain a virtual embedding of $\mathbf{v_{n+1}} = \mathbf{v_k} - \mathbf{r_k}$, where $\mathbf{r_k}$ and $\mathbf{v_k}$ are embeddings of relation r_k and related value v_k.

4 Evaluation

In this section, we report the statistic of constructed knowledge graph for mobile applications, called MAKG, and verify the effectiveness of our proposed framework for detecting similar apps. Source codes of our implemented algorithms are available at https://github.com/zbyzby11/MAKG4Embedding, including datasets and results. A technical report with more details of evaluation can also be downloaded in the same address.

4.1 Statistics of the constructed knowledge graph

Statistics of MAKG are listed in Table 1. We have collected more than 241 thousand apps, which are divided into four categories including Tools, Social, News and Newspaper&Magazine. The last column lists the whole number of apps, entities, relations in MAKG. Due to the defined schema of apps, the number of relations in each category is the same. Besides, MAKG is a multilingual knowledge graph because of the language of their names and descriptions including Chinese, English, Japanese, Korean and Arabic.

Table 1: The detailed statistics of MAKG

Category	Tools	Social	News	Newspaper&Magazine	Total
♯Apps	129,730	70,948	36,325	4,422	241,425
♯Relations	30	30	30	30	30
♯Entities	235,333	146,598	70,386	4,369	445,028

In particular, cybersecurity analysts can query apps or certain facts from MAKG by SPARQL language, and MAKG can quickly return a list of corresponding apps as well as their comprehensive information by traversing knowledge base and implied inference rules. The average response time for retrieving one specified mobile app is 347ms.

4.2 Evaluation of Similar Apps Detection

Datasets and metrics To evaluate the effectiveness of our proposed strategies for similar app search, we select some apps with Chinese and English in MAKG and build a benchmark dataset named MAKG-E, as listed in Table 2. For each app in the test set, we invite several experienced analysts to select 20 most similar apps as a standard set from the candidate apps generated by TF-IDF algorithm based on their textual descriptions. MAKG-E^+ is an enhanced one that has integrated important tokens and corresponding relationships of apps based on TextRank algorithm, in which the threshold θ for selecting important tokens is set to 0.5.

According to the built benchmarks, we introduce two metrics from the field of information retrieval to evaluate ranking methods that formally are defined as follows.

$$RR = \sum_{i=1}^{n} \sum_{j=1}^{m} \frac{1}{Rank_{ij}} \qquad Rank_{min} = \frac{1}{n} \sum_{i=1}^{n} \arg\min_{l} Rank_{il}.$$

The first metric is reciprocal rank, written RR, which is defined as the sum of the reciprocal of $Rank_{ij}$. $Rank_{ij}$ indicates the jth similar apps in descending order for

Table 2: Statistics of datasets for evaluation

Dataset	Train			Test
	♯ Apps	♯ Nodes	♯ Edges	♯ Apps
MAKG-E	61771	126817	432411	100
MAKG-E^+	61771	165838	628458	100

the ith tested app. If the jth similar app belongs to the standard set, then $Rank_{ij} = j$. Otherwise, the rank value is 0. The second metric, written Rank$_{min}$, is defined as the minimum rank of similar apps in descending order for each given app. The larger RR is, the closer of the similar search list is to the ideal one. Relatively, the smaller Rank$_{min}$ is, the earlier people can see similar apps. Notice that, as similar apps in the standard set are not unique, we do not employ AUC (Area Under Curve) as a metric, which is one of the important indicators to evaluate the effectiveness of classification models.

Implementation details We utilize several state-of-the-art embedding techniques to implement our framework. For structured triples, we employ TransE [21], TransH [22], TransD [23] by OpenKE platform[15] to train them and obtain the representations of new apps. These KG embedding models try to exploit distance-based scoring functions and measure the plausibility of triples as the distance between two entities. The network embedding models are implemented based on DeepWalk [24], LINE [25], Node2Vec [26] by OpenNE platform[16].

In addition, we employ feature matching method (abbreviated as FM) and the pre-training model BERT [27] as baselines to verify the effectiveness of our framework. FM is implemented by calculating the overlapping entities related to apps based on Jaccard similarity[17]. Relatively, we transform all the triples into textual descriptions and feed them into BERT[18] for detecting similar apps of new ones.

To ensure a fair comparison, we fine-tune the hyperparameters (e.g., dimension, mini-batch size, learning rate, negative sampling number) of all the embedding models to obtain the best results.

The evaluation results Table 3 reports comparison results of each embedding technique for detecting similar apps in terms of RR and Rank$_{min}$. From the table, we can observe that:

- Benefited from TextRank algorithm applied in MAKG-E^+, FM and NE models can gain significant improvements compared with the original MAKG-E. Because these important tokens and relations can enrich the contexts of apps. It is helpful to capture semantic similarities among apps.
- LINE and Node2Vec outperform FM, BERT and translated-based models in both two datasets. It indicates that NE models can capture higher-order similarities between apps. Nevertheless, the results of DeepWalk are not well, the main reason is that DeepWalk is not expressive enough to capture the diversity of connectivity patterns in the constructed network.

[15] https://github.com/thunlp/OpenKE
[16] https://github.com/thunlp/OpenNE
[17] https://wiki2.org/en/Jaccard_index
[18] https://github.com/hanxiao/bert-as-service

– The performances of translated-based models and BERT are bad. We analyze that the inherent characters (e.g., multilingual textual descriptions, insufficient triples) of constructed datasets may affect them to capture accurate representations of apps. It is worth exploring the improved techniques and jointly optimized the performances of similar apps detection, we leave this issue for future work.

Table 3: Comparison results in terms of RR and Rank_{min}

Methods	MAKG-E		MAKG-E^+	
	RR	Rank_{min}	RR	Rank_{min}
FM	93.60	5.14	165.10	2.37
BERT	9.17	19.47	30.28	19.00
TransE	22.83	17.30	12.10	18.44
TransH	22.86	17.38	11.90	18.51
TransD	23.15	17.31	11.35	18.86
DeepWalk	83.55	9.07	117.68	4.18
Line	**100.53**	**4.56**	188.93	2.17
Node2vec	98.28	6.24	**206.34**	**1.35**

In terms of time consumption during the training process, we observe that Node2Vec takes a much longer time (20 hours) than the other systems because it needs to spend lots of time in the generation of random walk. Relatively, other embedding approaches only cost less than 1 hour. For example, LINE only costs 18 minutes for training the MAKG-E^+. Considering the real scenario of app similar detection, LINE with our optimized strategy can achieve a balance between performances and time consumption.

The results of different representation strategies of new apps Table 4 and Table 5 show the results of different representation strategies of new apps. We observe that LINE and Node2Vec with the suitable strategy outperform FM, BERT, TransE in both two datasets. Note that the performances of NE models with the concatenation strategy based on entropy are better than the original one and arithmetic mean in most cases. It indicates that our optimized strategy can solve the representation problem of new apps to some extent. Nevertheless, Node2Vec equipped with our strategy does not perform satisfactorily in MAKG-E^+. We discover that the test apps corresponding to good results equipped with arithmetic mean are different from the ones with our strategy. It makes sense to combine these two strategies for detecting similar apps, we leave this issue for future work.

Table 4: Comparison results of different representation strategies in terms of RR

Dataset	FM	BERT	TransE	Arithmetic Mean ($*$)			Concatenation ($\star$)			Concatenation based on Entropy ($\diamond$)		
				DeepWalk	LINE	Node2Vec	DeepWalk	LINE	Node2Vec	DeepWalk	LINE	Node2Vec
MAKG-E	93.6	9.2	22.8	83.2	71.0	93.7	68.0	49.0	51.2	83.6	**100.5**	98.3
MAKG-E^+	165.1	30.3	12.1	106.4	170.0	**206.3**	88.6	73.9	94.7	117.7	188.9	118.9

Table 5: Comparison results of different representation strategies in terms of Rank$_{min}$

Dataset	FM	BERT	TransE	Arithmetic Mean ($*$)			Concatenation ($\star$)			Concatenation based on Entropy ($\diamond$)		
				DeepWalk	LINE	Node2Vec	DeepWalk	LINE	Node2Vec	DeepWalk	LINE	Node2Vec
MAKG-E	5.14	19.47	17.30	9.41	7.28	6.08	8.38	10.29	9.90	9.07	**4.56**	6.24
MAKG-E^+	2.37	19.00	18.44	5.28	2.89	**1.35**	6.92	8.85	5.71	4.18	2.17	4.53

Case study In this subsection, we present three real-world cases in MAKG-E$^+$ to illustrate the effectiveness of our proposed framework for detecting similar apps.

Table 6 indicates that optimized NE models outperform FM and other embedding techniques significantly in most cases. For *17 LIVE* and *9CHAT*, the minimum ranks of them in FM are beyond the 12th and 8th, respectively. Relatively, these value in LINE and Node2Vec has been significantly improved, which obtain the ideal ranking. In terms of RR, the performances of NE models are better than the ones of FM and other embedding techniques. It indicates that more apps in the standard set can be detected.

Table 6: Three real cases of similar apps detection tested on MAKG-E$^+$

Name of app	Fast News		17 LIVE		9CHAT	
	RR	Rank$_{min}$	RR	Rank$_{min}$	RR	Rank$_{min}$
FM	1.42	1	0.08	12	0.125	8
TransE	0.43	8	0.00	20+	0.00	20+
TransH	0.36	13	0.00	20+	0.00	20+
TransD	0.67	3	0.00	20+	0.00	20+
DeepWalk$^\diamond$	1.27	1	1.00	1	0.10	10
Line$^\diamond$	2.54	1	0.31	4	3.00	1
Node2vec*	1.83	1	0.33	3	2.56	1

5 Conclusion and Future Work

In this paper, we presented a novel framework by knowledge graph and embedding techniques, which is suitable for cybersecurity analysts to find similar apps. We further designed a light-weight ontology for the construction of knowledge graph, which can present more comprehensive information of apps to analysts and generate more shared linkages among apps. To obtain accurate representations of new apps, we employed TextRank algorithm to enhance the structured information and optimized the concatenation strategy for network embedding models. The preliminary result indicated the effectiveness of our framework comparing to several existing methods in terms of reciprocal ranking average and minimum ranking.

In future work, we will explore the following research directions: (1) As the constructed knowledge graph of mobile applications is multilingual, it is essential to achieve knowledge alignment of their names and descriptions, which is helpful to improve the performances of similar apps detection. (2) KG embedding and NE models in our framework are utilized independently, we will consider to combine them for optimizing the representation of apps together. (3) MAKG a continuous work that provides the service for cybersecurity analysts, we will collect more apps and explore other worthy services.

Acknowledgements

This work was partially supported by the National Key Research and Development Program of China under grant (2017YFB1002801,2018YFC0830200), the Natural Science Foundation of China grant (U1736204, 61906037), the National 242 Information Security Plan grants (6909001165).

References

1. Guozhu Meng, Matthew Patrick, Yinxing Xue, Yang Liu, and Jie Zhang. Securing Android App Markets via Modeling and Predicting Malware Spread Between Markets. *IEEE Trans. Information Forensics and Security*, 14(7):1944–1959, 2019.
2. Ning Chen, Steven C. H. Hoi, Shaohua Li, and Xiaokui Xiao. SimApp: A Framework for Detecting Similar Mobile Applications by Online Kernel Learning. In *WSDM*, pages 305–314, 2015.
3. Upasna Bhandari, Kazunari Sugiyama, Anindya Datta, and Rajni Jindal. Serendipitous Recommendation for Mobile Apps Using Item-Item Similarity Graph. In *AIRS*, pages 440–451, 2013.
4. Peifeng Yin, Ping Luo, Wang-Chien Lee, and Min Wang. App recommendation: a contest between satisfaction and temptation. In *WSDM*, pages 395–404, 2013.
5. Dae Hoon Park, Mengwen Liu, ChengXiang Zhai, and Haohong Wang. Leveraging User Reviews to Improve Accuracy for Mobile App Retrieval. In *SIGIR*, pages 533–542, 2015.
6. Jovian Lin, Kazunari Sugiyama, Min-Yen Kan, and Tat-Seng Chua. Scrutinizing mobile app recommendation: Identifying important app-related indicators. In *AIRS*, pages 197–211, 2016.
7. Afnan A. Al-Subaihin, Federica Sarro, Sue Black, and Licia Capra. Empirical comparison of text-based mobile apps similarity measurement techniques. *Empirical Software Engineering*, 24(6):3290–3315, 2019.
8. Quan Wang, Zhendong Mao, Bin Wang, and Li Guo. Knowledge Graph Embedding: A Survey of Approaches and Applications. *IEEE Trans. Knowl. Data Eng*, 29(12):2724–2743, 2017.
9. Peng Cui, Xiao Wang, Jian Pei, and Wenwu Zhu. A Survey on Network Embedding. *IEEE Trans. Knowl. Data Eng*, 31(5):833–852, 2019.
10. Franz-Xaver Geiger and Ivano Malavolta. Datasets of Android Applications: a Literature Review. *CoRR*, abs/1809.10069, 2018.
11. Daniel Arp, Michael Spreitzenbarth, Malte Hubner, Hugo Gascon, and Konrad Rieck. DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket. In *NDSS*, 2014.
12. Daniel E. Krutz, Mehdi Mirakhorli, Samuel A. Malachowsky, Andres Ruiz, Jacob Peterson, Andrew Filipski, and Jared Smith. A dataset of open-source android applications. In *MSR*, pages 522–525, 2015.
13. Li Li, Jun Gao, Médéric Hurier, Pingfan Kong, Tegawendé F. Bissyandé, Alexandre Bartel, Jacques Klein, and Yves Le Traon. AndroZoo++: Collecting Millions of Android Apps and Their Metadata for the Research Community. *CoRR*, abs/1709.05281, 2017.
14. Guozhu Meng, Yinxing Xue, Jing Kai Siow, Ting Su, Annamalai Narayanan, and Yang Liu. AndroVault: Constructing Knowledge Graph from Millions of Android Apps for Automated Analysis. *CoRR*, abs/1711.07451, 2017.
15. Jing Li, Aixin Sun, Jianglei Han, and Chenliang Li. A survey on deep learning for named entity recognition. *CoRR*, abs/1812.09449, 2018.
16. Xing Niu, Xinruo Sun, Haofen Wang, Shu Rong, Guilin Qi, and Yong Yu. Zhishi.me - weaving chinese linking open data. In *ISWC*, pages 205–220, 2011.
17. Rada Mihalcea and Paul Tarau. TextRank: Bringing Order into Text. In *EMNLP*, pages 404–411, 2004.

18. Jian Tang, Meng Qu, and Qiaozhu Mei. PTE: Predictive Text Embedding through Large-scale Heterogeneous Text Networks. In *SIGKDD*, pages 1165–1174, 2015.
19. Jizhe Wang, Pipei Huang, Huan Zhao, Zhibo Zhang, Binqiang Zhao, and Dik Lun Lee. Billion-scale Commodity Embedding for E-commerce Recommendation in Alibaba. In *SIGKDD*, pages 839–848, 2018.
20. Meng Wang, Ruijie Wang, Jun Liu, Yihe Chen, Lei Zhang, and Guilin Qi. Towards empty answers in sparql: Approximating querying with rdf embedding. In *ISWC*, pages 513–529, 2018.
21. Antoine Bordes, Nicolas Usunier, Alberto Garcia-Duran, Jason Weston, and Oksana Yakhnenko. Translating embeddings for modeling multi-relational data. In *NIPS*, pages 2787–2795, 2013.
22. Zhen Wang, Jianwen Zhang, Jianlin Feng, and Zheng Chen. Knowledge Graph Embedding by Translating on Hyperplanes. In *AAAI*, pages 1112–1119, 2014.
23. Guoliang Ji, Shizhu He, Liheng Xu, Kang Liu, and Jun Zhao. Knowledge Graph Embedding via Dynamic Mapping Matrix. In *ACL*, pages 687–696, 2015.
24. Bryan Perozzi, Rami Al-Rfou, and Steven Skiena. DeepWalk: Online Learning of Social Representations. In *SIGKDD*, pages 701–710, 2014.
25. Jian Tang, Meng Qu, Mingzhe Wang, Ming Zhang, Jun Yan, and Qiaozhu Mei. LINE: Large-scale Information Network Embedding. In *WWW*, pages 1067–1077, 2015.
26. Aditya Grover and Jure Leskovec. node2vec: Scalable Feature Learning for Networks. In *SIGKDD*, pages 855–864, 2016.
27. Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In *NAACL*, pages 4171–4186, 2019.