SAND2018-7808D

Operational Technology (OT) Text Analysis

Ryan Swanson
Bachelor of Science in Electrical Engineering - University of Colorado at Boulder - Graduating May 2020
Manager: Michael Haass – Mentor: Eric Goodman – MARTIANS
Sandia National Laboratories/NM, U.S. Department of Energy
July 31st 2018

Abstract

Our project extracts important words and their interrelationships from Operational Technology (OT) documents. In doing so, we can mitigate security risks from documentation. For example, if our program is given the sentence, "The Microcontroller has a built-in low-power Bluetooth module," it will recognize that this device is unsafe in a classified area. With Word2Vec, we created high-quality word embeddings that were used to create a dataset to train a neural network classifier. The latter finds word relationships in any text document.

What Is Word Embedding?

Word embedding is a tool for taking words that are inherently meaningless to computers and quantify semantic similarities. By embedding words as vectors, they are given geometric interpretation. Vectors have closer proximity for words with similar definitions, but are farther apart for unrelated words. Figure 1 below shows a plot of word vectors.

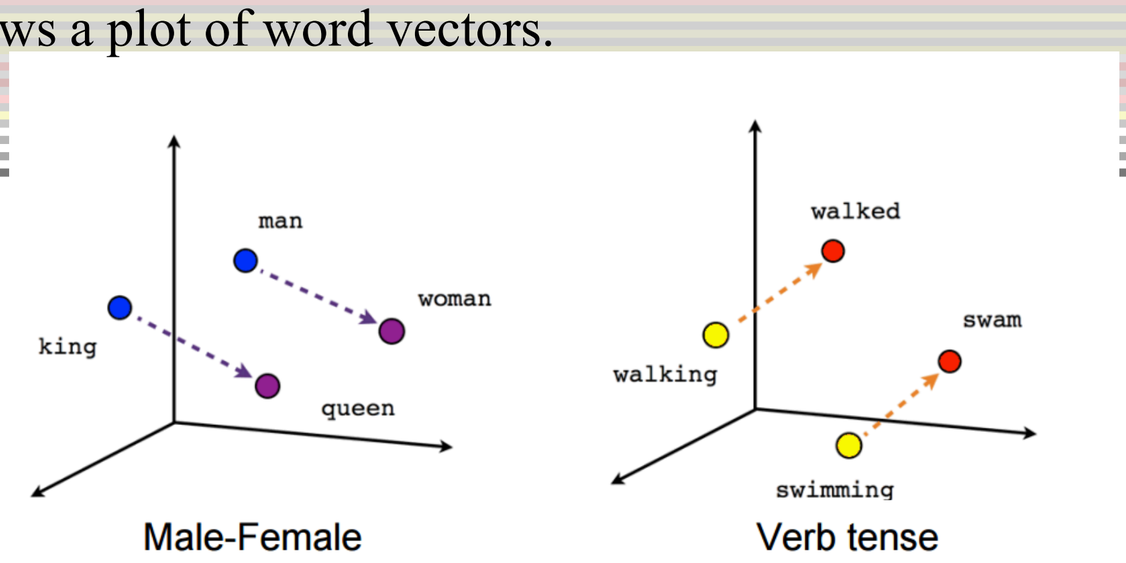

Figure 1: Plotted word vectors

Named Entity Extraction

Named Entity Extraction is a method for a computer to find "objects" in a sentence. We specifically searched for organization, people, and location names. Once organizations, people, and locations are extracted from a sentence, we perform a SPARQL query to the semantic database, Dbpedia, to find existing relationships between entities. Once we create a training set of sentences and the entity relationships in each sentence, we can train a neural network.

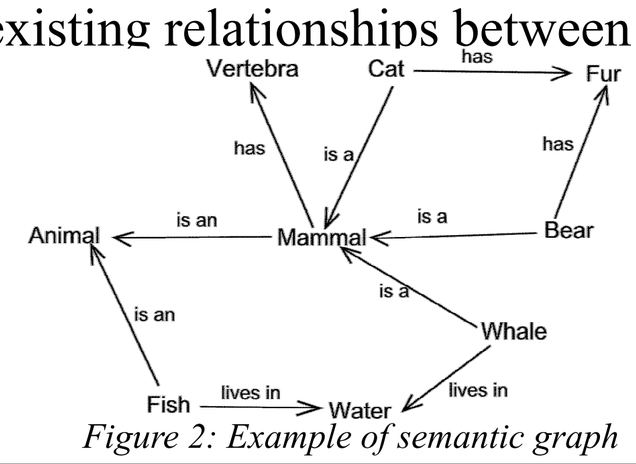

Figure 2: Example of semantic graph

Methods

- Create Word2Vec word embeddings with gensim
- Design a training set for a neural network with millions of sentences (using the entire Wikipedia)
  - Learn how to examine features of a sentence
  - Stanford's Named Entity Recognizer finds desired words
  - Perform SPARQL queries to DBpedia for pairs of entities
- Design and train a neural network
  - Input the extracted entities in vector representation
  - Output predicted relationship between the entities

Another Method

- Use Open Information Extraction created by Stanford to extract relationship triples
  - Learn relationships from relationship triples
  - Compare accuracy of Stanford Open Information Extraction to previous method

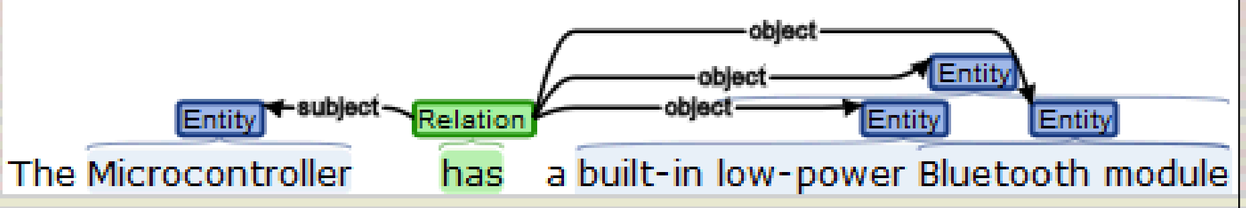

Figure 3: Visual example of relationship extraction

Results

- Created high quality word vectors with Word2Vec
  - $vec(King) - vec(Man) + vec(Woman) = vec(Queen)$
- Can accurately, extract entities from sentences using the Stanford NLP package
- Designed the architecture for Neural Network
- Open Information Extraction is severely inaccurate
  - First method will likely be more accurate

Future Work

- Finish collecting data to train our Neural Network
  - Query DBpedia for all relationships within Wikipedia
- Train the Neural Network on relationship pairs
  - Network will be an Long Short-Term Memory (LSTM) architecture
  - This will greatly increase accuracy
- Add threat assessment which detects if hardware and software is a threat
  - We currently only detect key words and the relationships between them
  - Automatically detecting threats from key words will save even more Sandian time!

U.S. DEPARTMENT OF ENERGY
National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. SAND #