Eric Downing

Bryan Ford

11/4/2016

Initial Setup

Installed

Python

R

Github

Cygwin

SSH into [eric@68.36.180.156](mailto:eric@68.36.180.156)

First Steps

1. Began by focusing and learning about the aspect of what we want to do in regards to the log data that we have.
2. Read paper: <https://users.cs.fiu.edu/~taoli/pub/Li-sigkddExp.pdf> to get a better understanding of the challenge presented before us.
3. After reading the article, there are a few relevant things that could be deduced from understanding all log information.
   1. With a good classification of each of the log items, if one were to properly categorize them, they could all be grouped and introduced into different states
   2. With each of them into a new state, we could begin to get probabilities of the occurrence of future states given the present state.
   3. Once all this has been accomplished we can then narrow it down to probabilities of generating an error state.
      1. From here we could then begin to reduce that probability by examining the current state, or the one that would lead to an error.
4. Different Algorithms that are useful:
   1. Naïve Bayes
   2. Forward
   3. Baum-Welch
   4. Viterbi
5. (Hidden) Markov Models
   1. Markov Chain (being the simplest) would give probabilities of a transition to the next states.
6. Mapping Certain Keywords together could help in creating a more generalized system
   1. In the article, it was explained that between Linux and Windows machines there was a different context that necessarily didn’t mean different things but would add difficulty to the categorization process.
      1. It may not be a bad idea to have a map of certain keywords so that categorization is improved.
7. Given the temporal information, we could come up with a way to deduce the possibilities of errors in a given time frame and may be able to correlate that to a different event.
8. Possibility of writing a parser that would go through a log file and insert all relevant information into a database
   1. Here we could use our categorizer and implement it this way
   2. Having the info in a data store would allow us to access information faster than would reading it every time from a text file.
      1. One and done
   3. With the ability to create other tables and what not from the store we could build some bridging tables and further develop our understanding of the data being given from the logs
   4. If written correctly, this could be a general program which could be used for any other necessary items in the future
9. Possible Visual representations of data
   1. This is not necessary, however, being able to present info is never bad
   2. Given all the information and displaying everything with its given timestamp we could potentially see a point that errors occur and make preparations for when they are about to occur