Using Hidden Markov Models and Feature Tracking to Detect Anomalous Behavior

Daniel Seita CS 281a Final Project
University of California, Berkeley

Problem Statement

We have a series of observations and are interested in **detecting anomalous behavior**. As an example, we may wish to monitor the nuclear weapons development of other countries. We can observe events, such as whether nuclear power plants are being built or the actions of countries in political conferences, but these are all observed and we do not know the true "state sequence" of the other countries. We can model the actions of those countries developing nuclear weapons using Hidden Markov Models (HMMs). The goal, then, is given a series of observations, to **determine with high probability when anomalous events occur**, which here would be the progression of a nuclear weapons development program in another country.

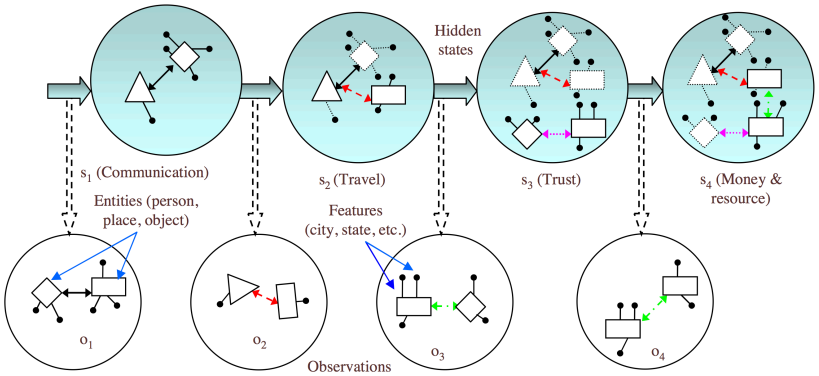
Overview of HMMs

HMMs consist of a state space along with a sequence of observations. The power of HMMs is that we can do inference to determine the optimal state sequence (which is hidden) while only given the observations.

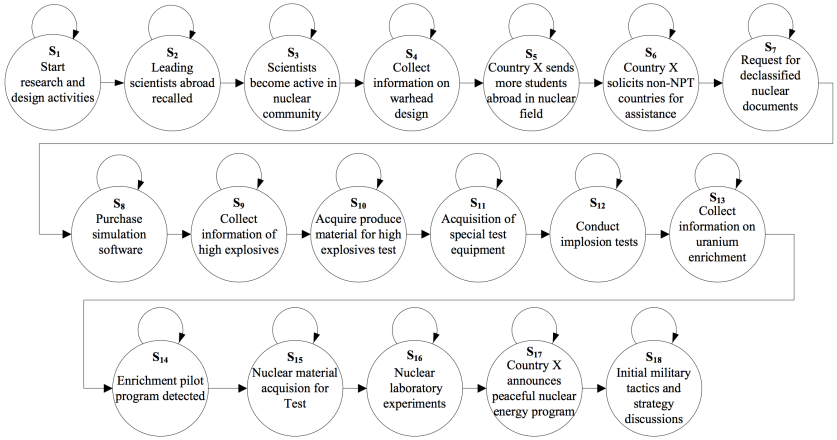
Our task here is a little different because we have transitions/arcs between nodes as our actual "states" which requires a modification of the algorithm.

TODO Describe our task a little more and explain why HMMs are important.

Determine State Sequence Given Observations of Transactions



HMM Example for Research & Development



This example outlines a sequence of states that we wish to detect.

Current Progress and Results

What I've done so far: (1) Implemented a HMM generation sequence and (2) Implemented HMM class to determine forward-backward probabilities, (3) Ran some trials. (TODO: Put a figure somewhere here … this looks lame as it is)

What I plan to do: (1) Determine what happens when we miss some data, (2) Determine additional ways an adversary could "confound" our results, (3) Deeper comparisons of this method versus maximum likelihood.

References

1. Satnam Singh, Haiying Tu, William Donat, Krishna Pattipati, and Peter Willett. *Anomaly Detection via Feature-Aided Tracking and Hidden Markov Model*. IEEE Transactions on Systems, Man, and Cybernetics, 2009.
2. Need to add a second reference soon!