Hidden Markov Models:
Applications for Cyber Intrusion Detection and Beyond

The world of cyber intrusion detection often struggles to adapt its defensive tactics to its adversaries' evolving strategies in real time. Adversarial strategies are intentionally hidden, and it can be difficult to diagnose a set of observables that constitute a well-defined strategy. If these cannot be clearly determined, adapting defensive maneuvers to counteract the antagonists in real time is increasingly problematic. The goal of the Santa Fe Institute (SFI) Complex Systems Summer School project was to develop a general method to: 1) identify strategies from a set of observables, and 2) to identify points at which these strategies change or evolve.

Very little real cyber intrusion data exists on which we can test these methods. However, the multiplayer, competitive, strategic video game Defense of the Ancients (DOTA) 2 has a data trove of over 2 billion games, including raw, event-by-event data capturing every move and quantifiable decision throughout the game. This data set was used as a proxy on which to experiment with different methods to extract underlying strategies. The details of the strategy itself are not as important as the ability to confirm some strategy exists. This general identification framework can then be potentially ported to the MITRE cyber security realm or other co-evolutionary domains.

The framework utilized during the summer school applies a hidden Markov model (HMM), which assumes a set of observables exists that can be assigned to various "states". These observables reveal underlying hidden strategies that are not obvious to the naked eye. The model assumes a certain number of hidden states and calculates the probabilities of transitions among these hidden states, as well as the emission probabilities of the observables from each hidden state (i.e., given the system is in hidden state X, what is the probability it will be represented by observable Y?). This process is repeated for different numbers of hidden states, and the optimal number of states is chosen using the respective model with the maximum likelihood (offset by the total number of hidden states, using a model-selection criterion known as the Akaike Information Criterion). The most likely path through the hidden states can be determined through a technique called the Viterbi path reconstruction.

SFI professor Simon DeDeo has implemented the HMM framework in a publicly-available code [1], and several MITRE employees are working closely with him to understand. This framework has been applied not only to the cyber security/DOTA use case but also several others models of dynamics of: 1) USDA facilities in an attempt to correlate observables to food-related outbreaks, and 2) fluctuations in the stock market.

Using the DOTA project as an example, the most revealing observable of strategy is most likely the player positions, though there are a myriad of other observables that could be analyzed as well. Using an unsupervised machine learning technique, states were assigned to each time step based on the relative distances of all ten players (e.g., all players in close proximity on the game board could represent one state, whereas all players spread far apart could represent another state). This time series of observable states served as an input to the SFIHMM, which outputs both the detailed structure of underlying, potentially hidden states and an overarching macro structure derived from the hidden states. For this example, sequences of relative player positions for ~ 50 games were concatenated together, and the positions were aggregated and averaged over a 60 second time interval.

Our preliminary results are shown in Fig. 1. The sequence of observables is on the bottom panel for 25 different states of relative player positions. The middle panel shows the most likely path through the hidden

system given the determined hidden states, with the model calculating 15 hidden states as the optimal number for this data set. The top panel is a meta-analyses of the hidden state structure, constraining the hidden system to two macro states. The dashed lines indicate the beginning of a new game.

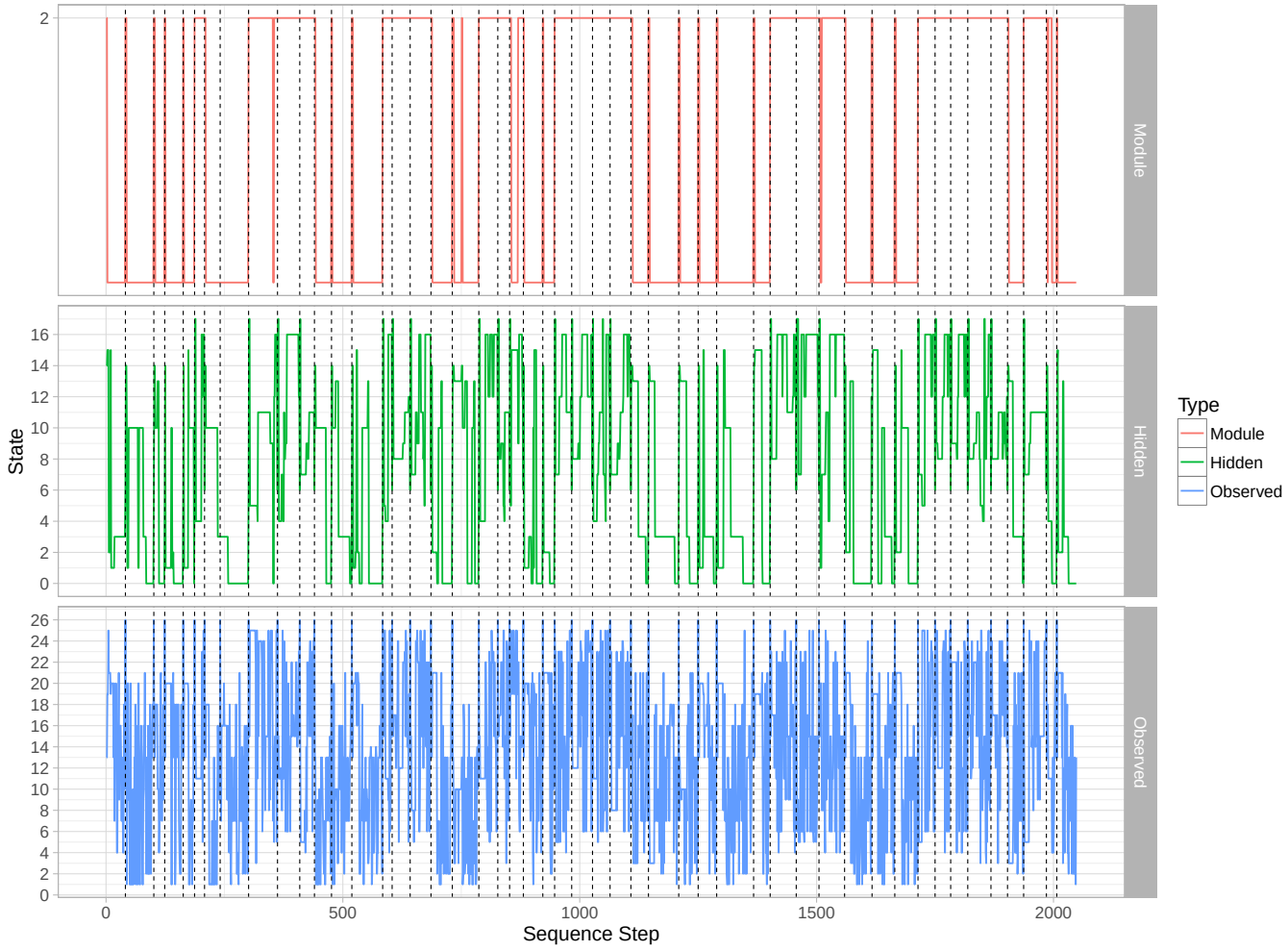

Figure 1: Sample of concatenated games from a single DOTA 2 tournament. The bottom panel shows the observed state sequences, and the other panels show the output of the HMM (see text). Dashed lines indicate the start of new games.

The top panel seems to indicate that a macro structure exists across games: a game is either in one macro state or another, with very little oscillation between these macro states within a given game. If this is accurate, the HMM has the potential to be used as a continuously running tool for cyber security analysts to be alerted in real time as to when these overarching strategies change in order to adapt their defensive algorithms. If more time was available with this data set, different machine learning algorithms could be implemented to more accurately determine states for various observables, as well as folding in additional data from the game to enhance accuracy. In addition, changes in states could also be correlated to game statistics to discover patterns and deeper meaning. Because this framework is general and simply extracts hidden structure from sequences of observables, it is widely applicable to many dynamic domains.

References

[1] DeDeo, S., SFIHMM, `http://bit.ly/sfihmm`, 2016.