Evolution of strategic decision making: DOTA 2 as a proxy for cybersecurity environments

A. L. Sallaska [*], **D. Biro** [†], **S. Duran** [‡], **and M. Stuart** [§]

[*] The MITRE Corporation, [†] Albert Einstein College of Medicine, [‡] Pompeu Fabra University, and [§] University of California, Berkeley

Submitted to Proceedings of the National Academy of Sciences of the United States of America

Computer hackers use certain strategies to penetrate systems. These strategies evolve over time, usually in response to the defense mechanisms employed by the system administrators. Being able to identify the strategies and when they change is of paramount importance to ensure the safety of the systems. Because data to help this effort is scarce, this paper explores the possibility of using competitive, strategic video game data as a proxy to identify strategies and their change points.

Cybersecurity | Intrusion detection algorithms | adaptive strategies | video game data

Abbreviations: DOTA, Defense of the Ancients

Introduction

Existing performance metrics of cyber intrusion detection algorithms, such as false positive or negative rates, are unable to capture the level of granularity necessary to significantly improve the algorithms, especially when a single, definitive outcome is rarely the case for this domain. Traditional static cyber defense systems also require long lead times to install patch updates, and staving off damage in real time is unfeasible using these metrics. Therefore, metrics must evolve to provide real-time evaluations of adaptive adversaries whose strategies may change depending on the protective mechanisms they encounter, as well as characterizing sequences of detections.

Usable data from within the cyber domain that may help to strengthen detection algorithm scoring is nearly nonexistent. If actual attacks are documented in the real world, this data is rarely made available and may be network specific (hence, not generalizable). Thus, a proxy for the data is necessary. An online battle arena video game called Defense of the Ancients 2 (DOTA 2) is a rich data source of real-time adaptive adversaries. DOTA 2 is a strategic, competitive, multiplayer game where two teams of five individuals each compete against each other to complete objectives and to destroy the other team?s base in a time frame of $\sim$ 20 to $\sim$ 90 minutes. The players deploy various in-game and between-game tactics and procedures to achieve a specific measurable objective. Professional players vie for tens of millions of dollars in prize pools each year, and over 2 billion games have been played. The results in this paper are using data from a cache of 500 GB of aggregated game data ($\sim$ 2.5 million games played over one year) and from X GB of raw, event-by-event data. Our goal is to use this data to shed light on how we can 1) detect and 2) quantify the rate of change of strategies in co-evolutionary systems.

This is akin to the classic 'Red Queen hypothesis' in evolutionary biology, but in this case we are interested in human behaviors where a strategy can be considered most generally as a 'meme' of sorts. Our hypotheses include: 1) a mapping exists between game observables and a set of strategies, 2) a measurable signal can be extracted from which to ascertain the adoption, stabilization, and decay of specific strategy traits, 3) changes in strategies occur over time, and 4) strategy changes are driven (at least in part) from behaviors of the opposing team. We postulate that testing these hypotheses will require an understanding of the co-evolutionary dynamics of the overall environment. In particular, the human behavioral components underlying the adversary/defense team actions will need to be assessed. The use of data from a multiplayer online game for this purpose assumes there is a valid mapping between the 'game-space' to 'cyber-space' behaviors from which useful inferences can be made. Through this exercise we hope to understand what types of data (if any) are useful for this purpose and how one might develop proxies to characterize strategies. Ultimately, we hope that the analysis could be applied against realistic data specific to a cyber intrusion.

The Game: DOTA 2

An aerial view of the DOTA game board is shown in Fig. 1. The goal of the game is to destroy the opposing team's base, their Ancient, located either in the lower left or upper right corner of the figure.

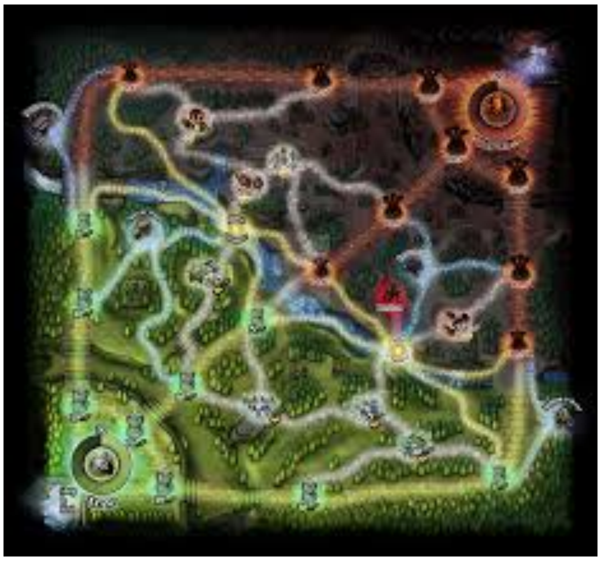

Fig. 1. Game board of DOTA 2.

Reserved for Publication Footnotes

Ten human players are divided into two teams of five (the Dire and the Radiant teams), each controlling a ‘hero’ character, which is chosen via a drafting process in professional games (discussed in more detail in the following section). Each hero has its own set of unique abilities and is generally divided into one of three categories: intelligence, strength, or agility. Throughout the game, the heroes amass 1) experience (XP) in order to become more powerful and unlock special abilities and 2) gold in order to buy items which also increase power.

There are three main ‘lanes’ to reach each Ancient, along the outer edges and down the diagonal. There is also a jungle landscape between the lanes. Various computer-controlled characters called ‘creeps’ are deployed throughout the game which allow heroes to gain experience. Defensive towers also line the lanes and protect the Ancient against enemy heroes.

The Draft. Heroes are chosen from a pool of ∼ 120 characters. In professional games, there are twenty choices for ten human players, five hero picks and five hero bans for each team, chosen in the following order:

B1 B2 B1 B2 P1 P2 P2 P1 B1 B2 B1 B2 P2 P1 P2 P1 B2 B1 P2 P1

where B indicates a ban, P indicates a pick, and the number refers to the team.

Analysis and Results

Draft.

Salva

Dan

Within Game (Anne). Data from throughout each game was extracted and analyzed in order to determine underlying strategies. A hidden Markov model was used and is discussed below after an overview of the data processing.

Data

The raw game data was initially downloaded from a DOTA 2 repository in a binary form. A java parser was written to convert the data into a JSON format, with each event occurring in the game generating an output. An example for a hero movement event is shown below:

{“tick”:24516,“time”:825,“type”:“DT_DOTA_Unit_Hero_X”, “team”:3,“x”:99,“y”:171}

where ‘tick’ is a subunit of ‘time’, and team indicates 2 or 3 (which must be connected with Dire or Radiant, see below). The type of event includes position, items, abilities, gold, XP, damage, healing, and death, with each type triggering different tags following the type. This event-by-event data, which can include multiple events per time step, was transformed into a single time step which keeps track of all events occurring at that step for each hero on each team. Aggregated statistics for the game a whole, such as which team won and draft order, was folded in with this event data. The draft order from the aggregated statistics allows the hero names and team number (2 or 3) to be correlated with each team, Dire or Radiant, as the Radiant are denoted as team 0 in the draft. This is important as the win is denoted as a boolean value for if the Radiant team won or lost, not if team 2 or 3 won or lost.

Figure 2 shows an example of the time evolution of one game metric, XP. This was a fairly unbalanced, fast game in which the Dire team won.

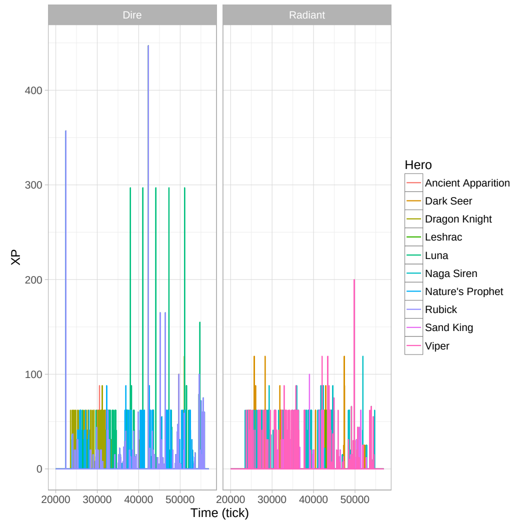

Fig. 2. Evolution of experience points, XP, throughout a sample game for each team and hero.

Model

A hidden Markov model (HMM) was used to explore the latent strategies with DOTA games. The observed signals were assumed to be observables from the game itself, and the hidden signal was assumed to be the desired strategy. One of the most relevant and revealing observables in the game are the positions of the players. Fighting is highly correlated with distance, as if two opposing heroes are nearby each other, the probability they will fight is high in order to win the game. Experience is also accumulated through fighting, and hence, is correlated with distance.

One method to convert absolute distances of each player into observable states is to coarse grain by relative distance among heroes on a given team. The states were defined as follows, where the number indicates the number of heroes that are considered “close” together in a cluster:

- 1-1-1-1-1
- 1-1-1-2
- 1-1-3
- 1-2-2
- 2-3
- 1-4
- 5

For example, the state “1-1-1-1-1” indicates all heroes are far apart, whereas “5” denotes heroes are clustered closely together. “Closeness” is defined by a relative distance threshold: if the relative distance between hero A and hero B is below the set threshold, then A and B are considered “close”. This threshold was set to be 5 units, with the range of the game board being ∼ 100 units × ∼ 100 units. Sensitivity on the hidden states on this threshold was tested and found to be XXXXX.

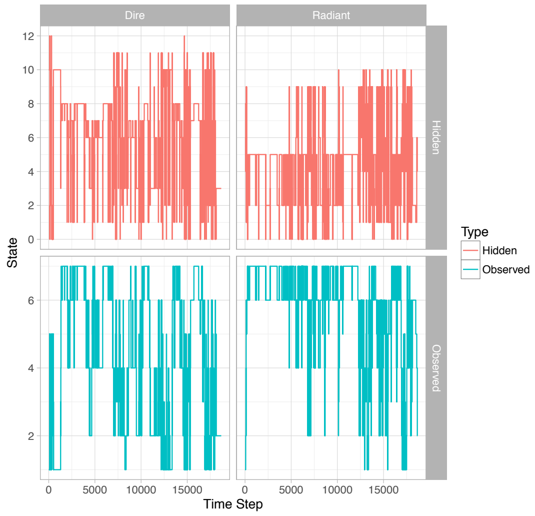

Fig. 3. Evolution of hidden and observed states for a sample game. Note, the hidden state X may not correspond directly to the observed state X. These numerical labels are arbitrary and used only for plotting purposes.

The time series of states for a sample game is shown in Fig. 3. For each time step in the game, an observed state was assigned to each team. This sequence served as an input to the HMM. The code to estimate the model parameters and the most likely hidden state sequence was provided by Simon DeDeo (http://tuvalu.santafe.edu/∼simon/styled-8/). The code uses the Akaike information criterion (AIC) in order to estimate the number of hidden states in the model. For the example game above, the number of hidden states for the Dire team was 13 and 11 for the Radiant, as compared to seven observable states.

The model that produces the hidden states for the Radiant is shown in Fig. 4.

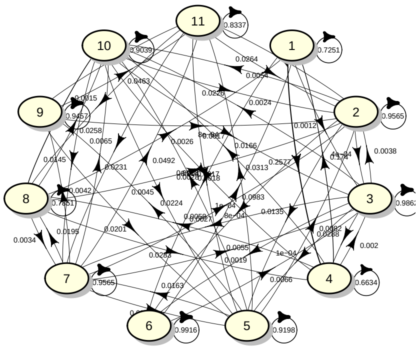

Fig. 4. Hidden Markov model for one team of the sample game.

Future work will involve unsupervised learning in order to extract the states, using distances within each team (as is done deterministically above), distances among all players, and adding additional features in addition to distances such as XP or gold.

Between Games (Marla).

Conclusions

X

Appendix

An appendix without a title.

Appendix: Appendix title

An appendix with a title.

ACKNOWLEDGMENTS. x