Defensive Deception in a Hypergame

Gaurav Dixit, Jin-Hee Cho, Ing-Ray Chen
Department of Computer Science
Virginia Tech, Falls Church, VA
{gdixit, jicho, irchen}@vt.edu

Mu Zhu and Munindar P. Singh
Department of Computer Science,
NCSU, Raleigh, NC, USA
{mzhu5, mpsingh}@ncsu.edu

Charles Kamhoua
US Army Research Laboratory
Adelphi, MD, USA.
charles.a.kamhoua.civ@mail.mil

***Abstract*—To consider an uncertain, realistic attack-defense scenario, this work adopts hypergame theory to deal with uncertainty derived from the asymmetric information available to players who may have different perceptions of the given game. In particular, using hypergame theory, we model an attack-defense game where the defender uses multiple defense strategies, including defensive deception, whereas the attacker performs an advanced persistent threat attack. To investigate the performance of the strategies chosen by the attacker and defender based on their perceptions of a given situation, we develop a probabilistic model based on Stochastic Petri Nets. We evaluate the model in terms of the attacker and defender's expected utilities, attack success probability, and mean time to security failure.**

I. Introduction

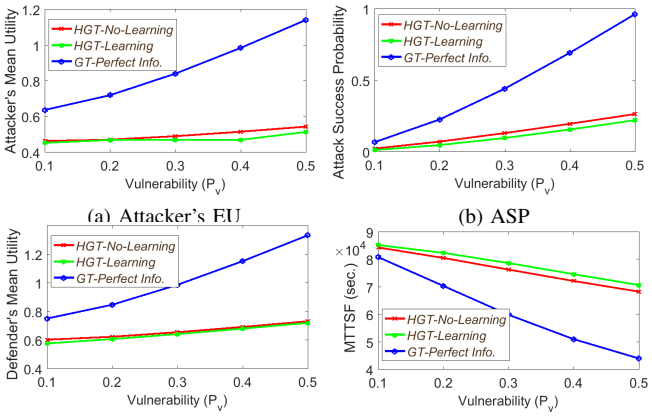
In real-life situations, decision making under uncertainty is nontrivial, particularly when the players may perceive a given situation differently. This work leverages hypergame theory to resolve conflicts of views of multiple players as a robust decision-making mechanism under uncertainty where the players may have different perceptions of the same game. Thus, it models players, such as attackers and defenders in cybersecurity, particularly to deal with advanced persistent threat (APT) attacks where they may have different views of the same game.

The key contributions of this work are as follows: (1) this work is the first that models an attack-defense game based on hypergame theory in order to deal with uncertainty in a given game; (2) we considered defensive deception techniques that can maximize uncertainty of an attacker with the aim of misleading an attacker's choice of strategy; (3) we investigated the effect of a player's (an attacker's or a defender's) learning towards an opponent's strategy on each player's expected utility, attack success probability, and mean time to security failure; and (4) we conducted a comparative performance study under three scenarios investigating the effect of players' learning and availability of perfect information in a given attack-defense game.

II. Attack-Defense Hypergame Framework

In a hypergame, players, either an attacker or a defender, form a different game based on its subjective perception. The different game is formed as a subgame where a full game consists of all available strategies of all players. We consider APT attacks following the cyber kill chain with four strategies including reconnaissance, delivery, stealthiness, and exploitation. To deal with the APT attacks, the defender employs four strategies, fake patch dissemination, real patch dissemination, moving target defense, and intrusion detection. Depending on the attacker's attack stage in the cyber kill chain, the defender takes an action to defend against the APT attack.

We considered three schemes when players play the attack-defense game using (i) hypergame theory without learning (HGT-No-Learning); (ii) hypergame theory with learning (HGT-Learning); and (iii) game theory with perfect information (GT-Perfect Info). The performance metrics used are: (i) each player's expected utility (EU) estimated by the netgain of a chosen strategy depending on an opponent's strategy; (ii) attack success probability (ASP) based on system failure conditions defined (e.g., confidential information is leaked out or too many nodes are compromised based on Byzantine failure); and (iii) mean time to security failure (i.e., MTTSF or system lifetime until the system fails).



(a) Attacker's EU (b) ASP

(c) Defender's EU (d) MTTSF

Fig. 1: Performance Comparison of HGT-No-Learning, HGT-Learning, and GT-Perfect Information.

III. Conclusions

The key findings from this research are: (1) the defender with learning capability takes more benefits than the attacker with learning capability as the defender's deception can increase uncertainty of the attacker leading to a suboptimal choice; (2) the accurate utility estimation is critical because players take actions based on the estimated expected utility values; (3) defensive deception techniques are more useful when there is higher uncertainty without learning, leading the attackers to perform highly resource consuming strategies without success.