**INTRODUCTION**

The key purpose of a defensive deception technique is to mislead an attacker’s view and make it choose a suboptimal or poor action for the attack failure [33]. When both the attacker and defender are constrained in their resources, strategic interactions can be the key to beat an opponent. In this sense, non-game-theoretic defense approaches have inherent limitations due to lack of efficient and effective strategic tactics. Forms of deception techniques have been discussed based on certain classifications, such as hiding the truth vs. providing false information or passive vs. active for increasing attackers’ ambiguity or confusion [3, 9].

Game theory has been substantially used for dynamic decision making under uncertainty, assuming that players have consistent views. However, this assumption fails as players may often subjectively process asymmetric information

available to them [22]. Hyper game theory [5] is a variant of game theory that provides a form of analysis considering each player’s subjective belief, misbelief, and perceived uncertainty and accordingly their effect on decision making in choosing a best strategy [22]. This paper leverages hyper game theory to resolve conflicts of views of multiple players as a robust decision making mechanism under uncertainty where the players may have different beliefs towards the same game. Hyper game theory models players, such as attackers and defenders in cyber security to deal with advanced persistent threat (APT) attacks. We dub this effort Foureye after the Foureye butterfly fish, demonstrating deceptive defense in nature [40].

To be specific, we identify the following nontrivial challenges in obtaining a solution. First of all, it is not trivial to derive realistic game scenarios and develop defensive deception techniques to deal with APT attacks beyond the

reconnaissance stage. This aspect has not been explored in the state-of-the-art. Second, quantifying the degree of uncertainty in the views of attackers and defenders is challenging, although they are critical because how each player frames a game significantly affects its strategies to take. Third, given a number of possible choices under dynamic situations, dealing with a large number of solution spaces is not trivial whereas the deployment and maintenance of defensive deception techniques is costly in contested environments. We partly addressed these challenges in our prior work in [12]; however, its contribution is very limited in considering a small-scale network and a small set of strategies with a highly simplified probability model developed using Stochastic Petri Network.

To be specific, this paper has the following **new key contributions**:

\_ We modeled an attack-defense game under uncertainty based on hypergame theory where an attacker and a defender have different views of the situation and are uncertain about strategies taken by their opponents.

\_ We reduced a player’s action space by using a sub game determined based on a set of strategies available where each sub game is formulated based on each stage of the cyber kill chain (CKC) based on a player’s belief under uncertainty.

\_ We considered multiple defense strategies, including defensive deception techniques whose performance can be significantly affected by an attacker’s belief and perceived uncertainty, which impacts its choice of a strategy.

\_ We modeled an attacker’s and a defender’s uncertainty towards its opponent (i.e., the defender and the attacker, respectively) based on how long each player has monitored the opponent and its chosen strategy. To the best of our knowledge, prior research on hyper game theory uses a predefined constant probability to represent a player’s uncertainty. In this work, we estimated the player’s uncertainty

based on the dynamic, strategic interactions between an attacker and a defender.

\_ We conducted comparative performance analysis with or without a defender using defensive deception (DD) strategies and with or without perfect knowledge available towards actions taken by the opponent. We measured the effectiveness and efficiency of DD techniques in terms of a system’s security and performance, such as perceived uncertainty, hyper game expected utility, action cost, mean time to security failure (MTTSF or system lifetime), and improved false positive rate (FPR) of an intrusion detection by the DD strategies taken by the defender.