# CONCLUSION

From this study, we obtained the following **key findings**:

\_ An attacker’s and defender’s perceived uncertainty can be reduced when defensive deception (DD) is used. This is because the attacker perceives more knowledge about the system as it performs attacks as an inside attacker. On the other hand, the defender’s uncertainty can be reduced by collecting more attack intelligence by using DD while allowing the attacker to be in the system.

\_ Attack cost and defense cost are two critical factors in determining HEUs (hyper game expected utilities). Therefore, high DHEU (defender’s HEU) is not necessarily related to high system performance in MTTSF (mean time to security failure) or TPR (true positive rate) which can also be a key indicator of system security. Therefore, using DD under imperfect information (IPI) yields the best performance in MTTSF (i.e., the longest system lifetime) while it gives the minimum DHEU among all schemes.

\_ DD can effectively increase TPR of the NIDS in the system based on the attack intelligence collected through the DD strategies.

This work bring up some important directions for future research by: (1) considering multiple attackers arriving in a system simultaneously in order to consider more realistic scenarios; (2) estimating each player’s belief based on machine learning in order to more correctly predict a next move of its opponent; (3) dynamically adjusting a risk threshold, i.e., Eq. (6), depending on a system’s security state; (4) introducing a recovery mechanism to restore a compromised node to a healthy node allowing the recovery delay; (5) developing an intrusion response system that can reassess a detected intrusion in order to minimize false positives while identifying an optimal response strategy to deal with intrusions with high urgency; and (6) considering another intrusion prevention mechanism, such as moving target defense, as one of the defense strategies.