Bayesian games for optimal cybersecurity investment with incomplete information on the attacker

Yunfei Zhao[a], Linan Huang[b], Quanyan Zhu[b], and Carol Smidts[a]

[a]Department of Mechanical and Aerospace Engineering, The Ohio State University

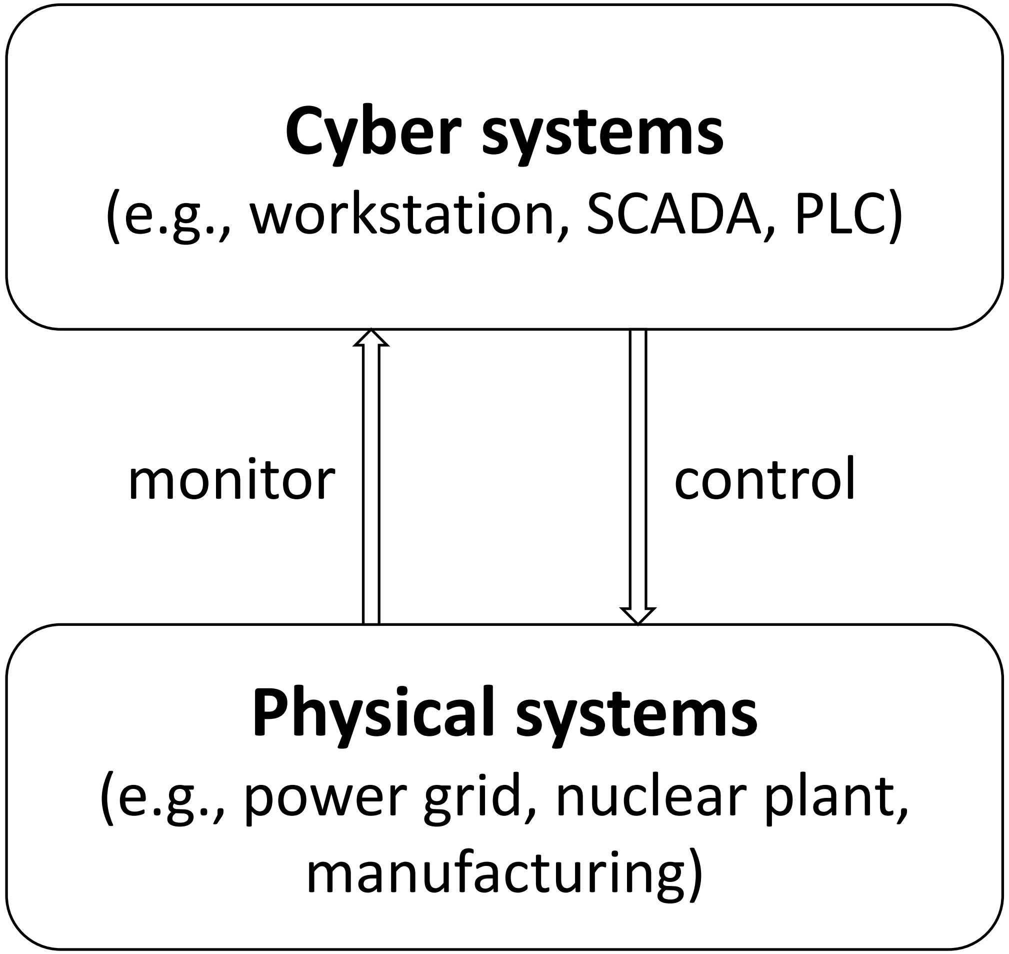
[b]Department of Electrical and Computer Engineering, New York University

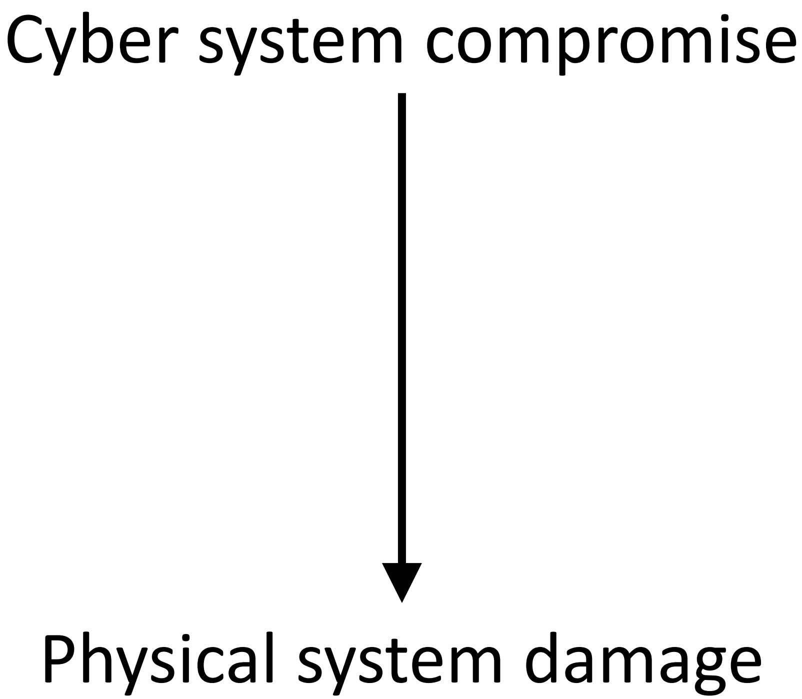
PSAM 16, Honolulu, HI

June 30, 2022

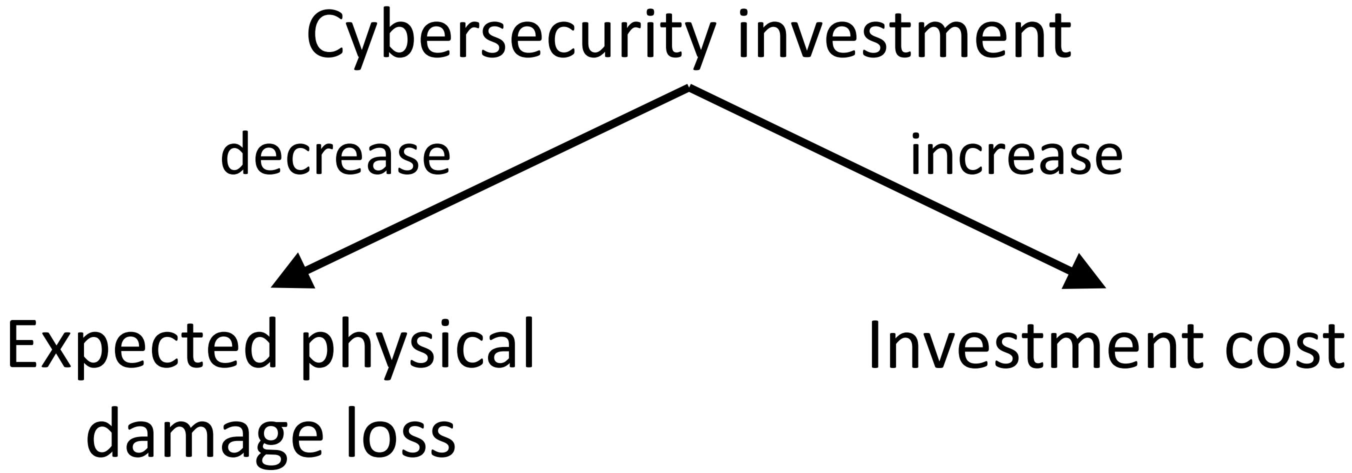
THE OHIO STATE UNIVERSITY

Background


Cyber systems
(e.g., workstation, SCADA, PLC)
monitor
control
Physical systems
(e.g., power grid, nuclear plant, manufacturing)

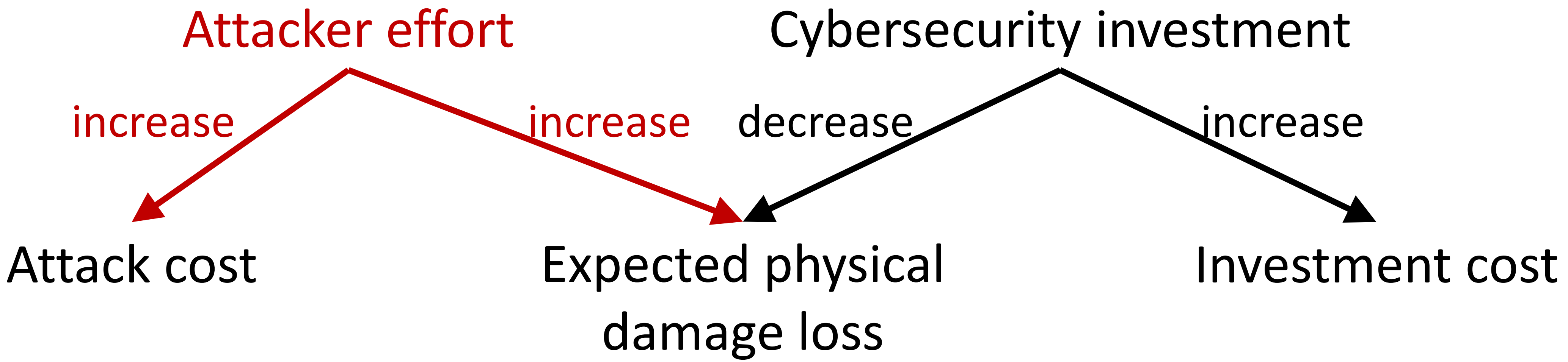

Cyber system compromise
Physical system damage

Single-agent decision-making



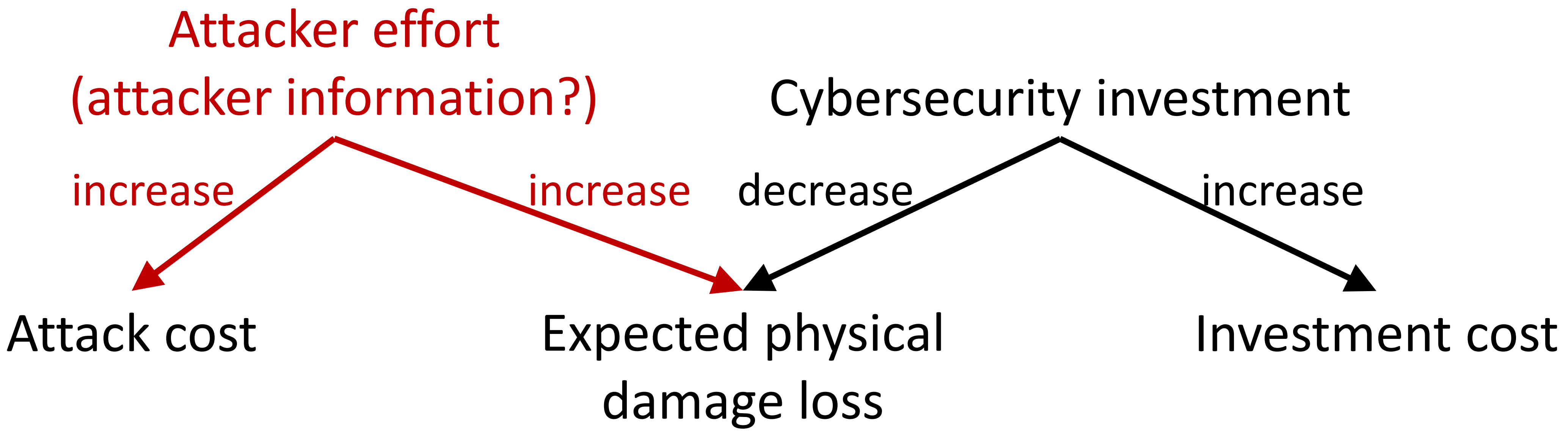
Optimal cybersecurity investment: the level of investment that achieves the **minimum sum** of **physical damage loss** and **investment cost**.

Multi-agent decision-making



Optimal cybersecurity investment: the level of investment that achieves the **minimum sum** of **physical damage loss** and **investment cost** considering **the effort of the attacker**.

Multi-agent decision-making with incomplete information



Optimal cybersecurity investment: the level of investment that achieves the **minimum sum** of **physical damage loss** and **investment cost** considering **the effort of the attacker** and with **incomplete information on the attacker**.

Problem formalization

- Problem
  - A piece of cyber equipment: if compromised, will incur physical loss of C
  - Players: defender – 1; attacker – 2
  - Defender cybersecurity investment: $a_1 \in [0, +\infty)$
  - Attacker type: $\theta_2 \in \Theta_2$
  - Attacker type distribution: $p(\theta_2)$
  - Attacker attack effort: $a_2 = \sigma_2(\theta_2) \in [0, +\infty)$
  - Cyber equipment vulnerability: $v(a_1, \sigma_2(\theta_2), \theta_2)$

Problem formalization (cont.)

- Objective
  - Defender:

Potential physical loss

Vulnerability

$$\max u_1(a_1, \sigma_2) = \sum_{\theta_2 \in \Theta_2} [-C \cdot p(\theta_2) \cdot v(a_1, \sigma_2(\theta_2), \theta_2)] - a_1$$

Defender utility

Attacker types

Attacker type probability

Cybersecurity investment

  - Attacker:

Potential physical loss

$$\max u_2(a_1, \sigma_2(\theta_2), \theta_2) = C \cdot v(a_1, \sigma_2(\theta_2), \theta_2) - \sigma_2(\theta_2)$$

Attacker utility

Vulnerability

Attack effort

Bayesian games for cybersecurity investment

- What we just described is actually a Bayesian game
  - The defender has incomplete information on the attacker
  - This incomplete information is described by the various types of attacker and the probability distribution over the types
- We can solve the game using the solution concept of Bayesian Nash equilibrium
  - i.e., obtain the Bayesian Nash equilibrium (a_1^*, σ_2^*) such that
  - For the defender:

$$u_1(a_1^*, \sigma_2^*) \geq u_1(a_1, \sigma_2^*), \forall a_1 \in [0, +\infty)$$

  - For the attacker of any type:

$$u_2(a_1^*, \sigma_2^*(\theta_2), \theta_2) \geq u_2(a_1^*, \sigma_2(\theta_2), \theta_2), \forall \theta_2 \in \Theta_2, \forall \sigma_2(\theta_2) \in [0, +\infty)$$

Obtain the Bayesian Nash equilibrium

- Obtain and solve the following system of partial differential equations

$$\frac{\partial u_1(a_1, \sigma_2)}{\partial a_1} = \frac{\partial\left[\sum_{\theta_2 \in \Theta_2}[-C \cdot p(\theta_2) \cdot v(a_1, \sigma_2(\theta_2), \theta_2)] - a_1\right]}{\partial a_1} = 0$$

$$\frac{\partial u_2(a_1, \sigma_2(\theta_2), \theta_2)}{\partial \sigma_2(\theta_2)} = \frac{\partial[C \cdot v(a_1, \sigma_2(\theta_2), \theta_2) - \sigma_2(\theta_2)]}{\partial \sigma_2(\theta_2)} = 0, \forall \theta_2 \in \Theta_2$$

THE OHIO STATE UNIVERSITY

Numerical case study

- Two types of attacker:
  - One with high capability ($\theta_2 = H$)
  - The other with low capability ($\theta_2 = L$)
- Cyber equipment vulnerability
  - For $\theta_2 = H$

$$v(a_1, \sigma_2(H), H) = \frac{\sigma_2(H)}{\alpha_H(a_1 + \sigma_2(H) + \beta)}$$

$\alpha_H \geq 1$ and $\beta > 0$

  - For $\theta_2 = L$

$$v(a_1, \sigma_2(L), L) = \frac{\sigma_2(L)}{\alpha_L(a_1 + \sigma_2(L) + \beta)}$$

$\alpha_L > 1$ and $\alpha_L > \alpha_H$

Numerical case study (cont.)

- Additional information about the problem:

Parameters (unit)	Parameter description	Nominal Value	Value Range
C (in USD)	Potential physical loss	1000	[0, 2000]
$p(H)$ (unitless)	Belief in $\theta_2 = H$	0.6	[0, 1]
α_H (unitless)	Parameter defining vulnerability for $\theta_2 = H$	5	[1, 10)
α_L (unitless)	Parameter defining vulnerability for $\theta_2 = L$	10	(5, 20]
β (in USD)	Parameter defining vulnerability	5	[1, 10]

- For each parameter setting, we can obtain the corresponding (a_1^*, σ_2^*)

Results for the setting with nominal parameter values

Parameters (unit)	Parameter description	Nominal Value	Value Range
C (in USD)	Potential physical loss	1000	[0, 2000]
$p(H)$ (unitless)	Belief in $\theta_2 = H$	0.6	[0, 1]
α_H (unitless)	Parameter defining vulnerability for $\theta_2 = H$	5	[1, 10)
α_L (unitless)	Parameter defining vulnerability for $\theta_2 = L$	10	(5, 20]
β (in USD)	Parameter defining vulnerability	5	[1, 10]

- Bayesian Nash equilibrium

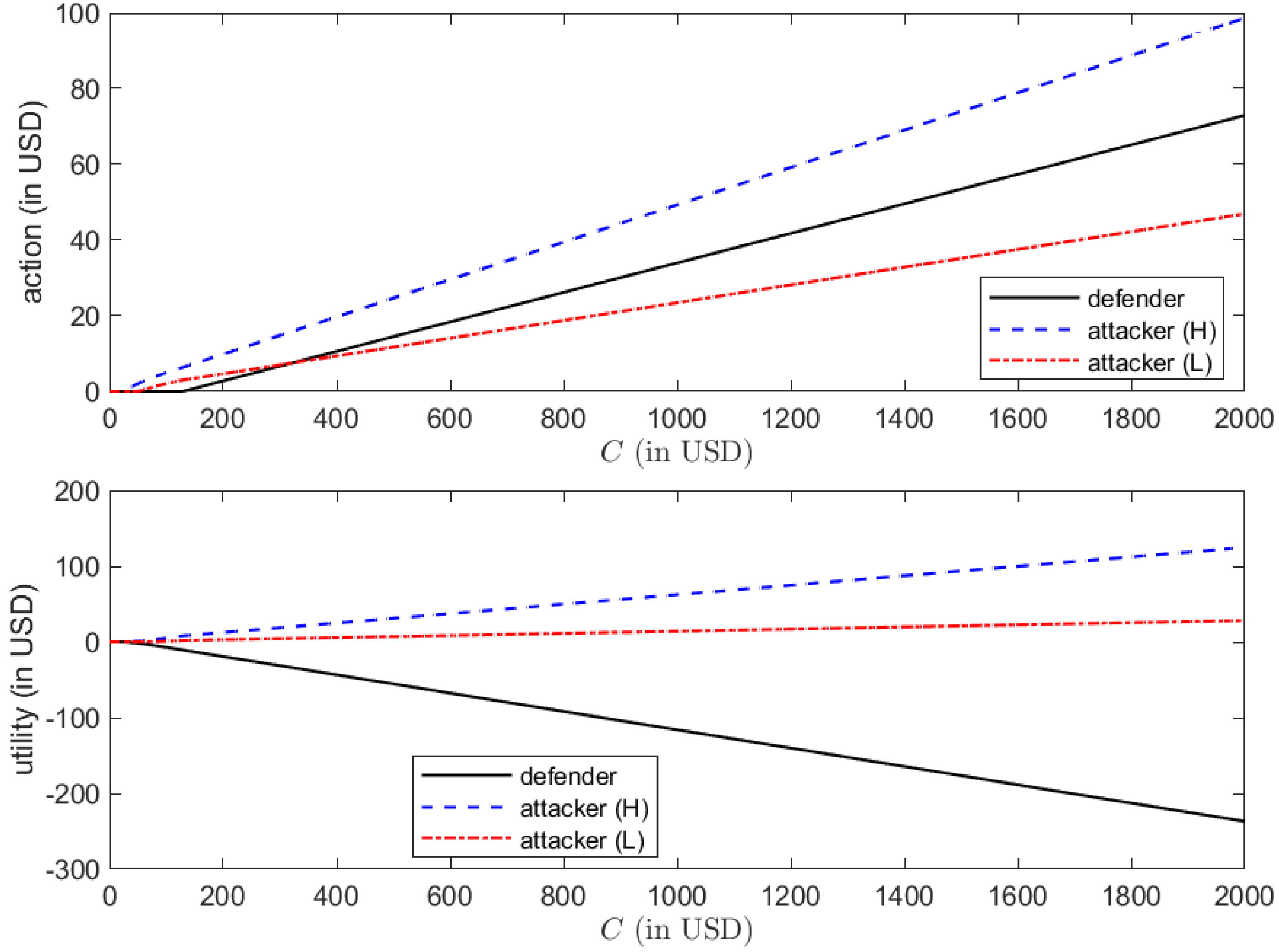
$$(a_1^* = 33.97\ USD, \sigma_2^*(H) = 49.31\ USD, \sigma_2^*(L) = 23.46\ USD)$$

- Utility
  - Defender: $u_1(a_1^*, \sigma_2^*) = -116.03\ USD$
  - Attacker of type H: $u_2(a_1^*, \sigma_2^*(H), H) = 62.40\ USD$
  - Attacker of type L: $u_2(a_1^*, \sigma_2^*(L), L) = 14.12\ USD$

THE OHIO STATE UNIVERSITY

Sensitivity of results to certain parameter values

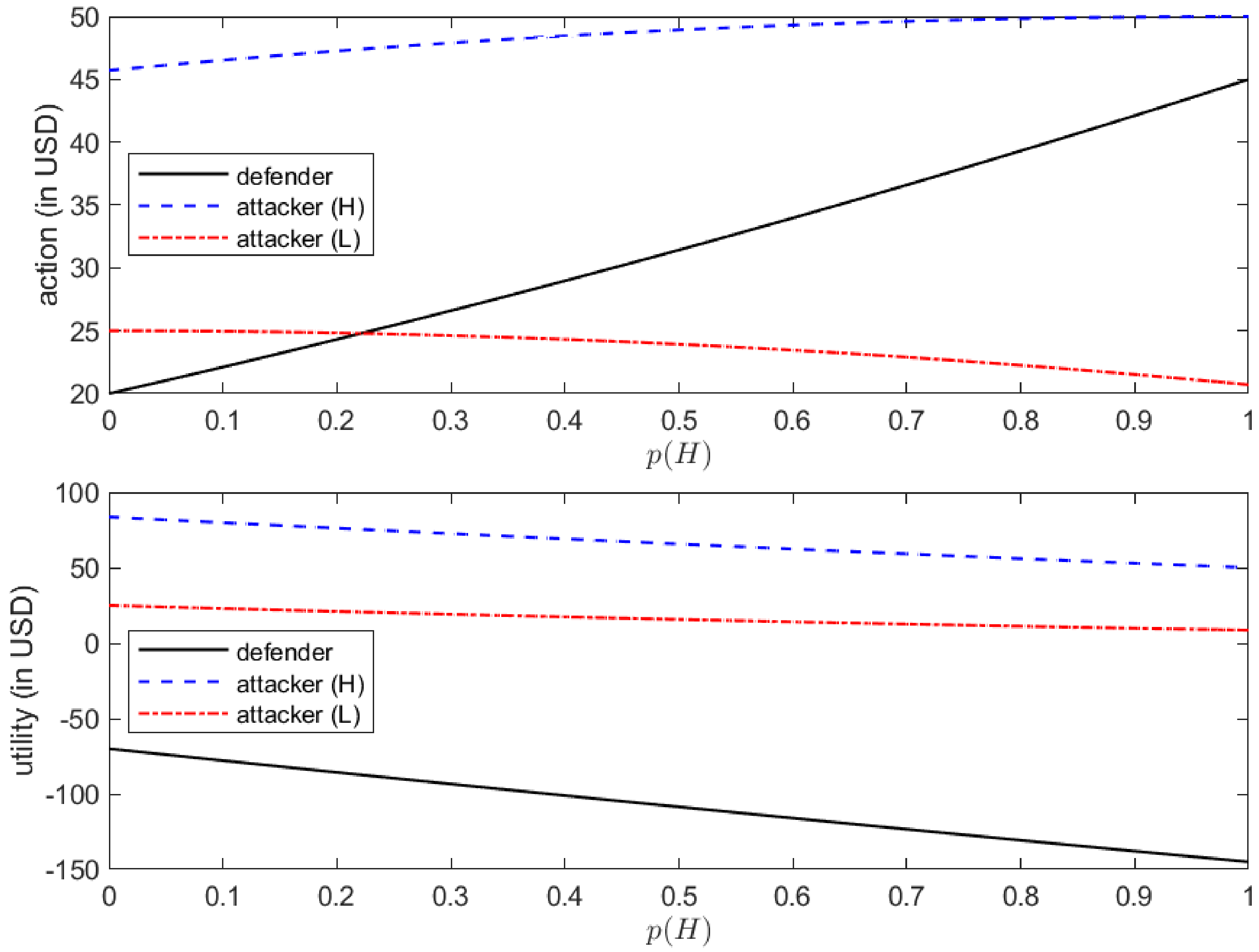
- The effect of C on the outcome



THE OHIO STATE UNIVERSITY

Sensitivity of results to certain parameter values (cont.)

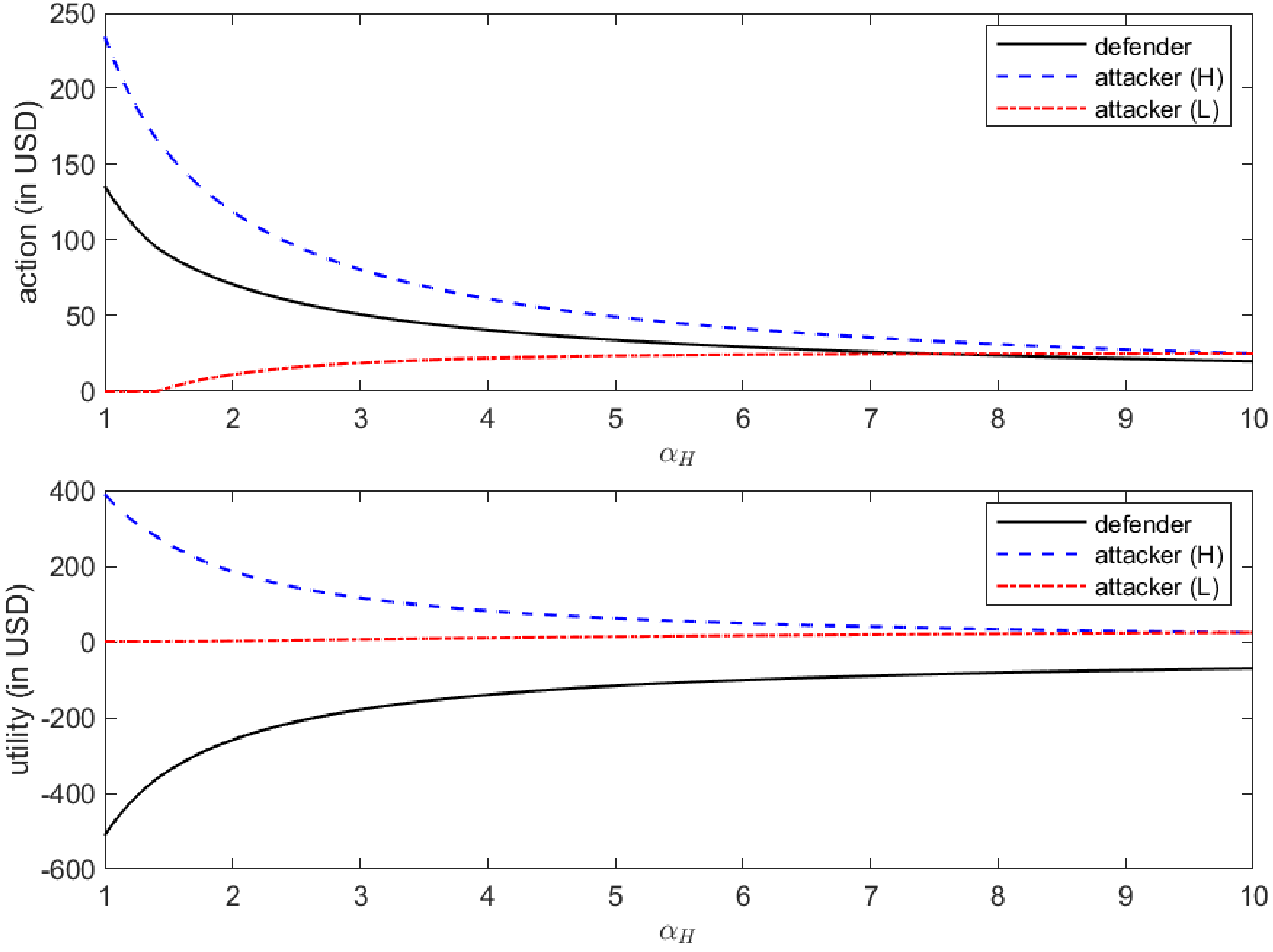
- The effect of $p(H)$ on the outcome



The Ohio State University

Sensitivity of results to certain parameter values (cont.)

- The effect of α_H on the outcome



Summary and future work

- Cybersecurity investment
  - Defender decision-making while considering the level of attacker effort
  - Incomplete information on the attacker
  - Bayesian games for modeling and solving the cybersecurity investment problem
- Numerical example
  - The outcome for a setting with nominal parameter values
  - Sensitivity of the outcome to various model parameters
- Future work
  - Multiple defenders, multiple attackers
  - Determination of model parameters

Acknowledgement

- This research is being performed using funding received from the DOE Office of Nuclear Energy's Nuclear Energy University Programs.

Thank you!