Applications of Colonel Blotto Games in Cyber-Physical System Security

Daniel Browne

Abstract

This report examines how game theory is used to enhance security in Cyber-Physical System (CPS) security games. CPSs are systems that merge physical processes, computing systems, and communication systems. These systems are vital in a range of applications, including critical infrastructure systems, medical devices, and transportation systems. Good communication between the physical and computing elements is necessary to ensure the smooth running of CPSs.

One game studied for its CPS security applications is the Colonel Blotto game, a two-player game that deals with resource allocation across multiple battlefields. The game has numerous applications in areas such as economics, political science, and computer science. Colonel Blotto can be used in CPS security games to protect critical infrastructure systems and create secure wireless sensor networks. Security managers can use strategic resource allocation to protect various sections of infrastructure from potential cyber threats.

The purpose of this project is to analyze the effects of varying resources in a simulated Colonel Blotto CPS security game. In this game, there is one attacker and one defender, and they each have a set number of resources. The resources are allocated across different cyber nodes simultaneously, determining whether the node is shut down, compromised, or successfully defended.

Cyber-Physical Systems

Cyber-Physical Systems (CPSs) have become crucial components in various applications such as transportation systems, critical infrastructure systems, and medical devices. CPSs consist of three primary components: physical processes, computing systems, and communication systems [2].

- **Physical processes** involve the components that interact with the physical world, such as sensors, actuators, and controllers.
- **Computing systems** are responsible for processing data, controlling physical processes, and making decisions based on the data collected from the physical processes.
- **Communication systems** provide the means for transmitting data between physical and computing systems.

Effective communication between the physical and computing components is vital to ensure that CPSs run smoothly. Communication protocols such as Wi-Fi and Bluetooth allow physical and computing components to exchange data and information such as sensor readings, control signals, and other critical information [2].

For example, a smart building's HVAC system is a CPS that integrates all three of the aforementioned primary components. The heating, ventilation, and air conditioning systems are physical processes while the controllers and software are computing systems. Communication systems for HVAC systems include Wi-Fi and other wireless protocols that allow the physical and computing components to communicate with each other.

Another example of a CPS is an autonomous vehicle. Physical processes in an autonomous vehicle involve sensors and actuators that interact with the physical world. The computing systems consist of an onboard computer and software that processes sensor data and makes decisions based on that data. The communication systems include cellular and wireless protocols that allow the vehicle to communicate with other vehicles and infrastructure.

Colonel Blotto

The Colonel Blotto game is a well-known two-player zero-sum game that involves resource allocation across multiple battlefields [3]. See Figure 2 for a diagram of the setup.

The game is played with a set of simple rules:

- There are n battlefields, and each player has m units of resources to allocate.
- The players distribute their resources across the n battlefields simultaneously, allocating integers between 0 and m on each battlefield.
- The player with the highest resource allocation on a given battlefield wins that battlefield.
- The player who wins the most battlefields wins the game.

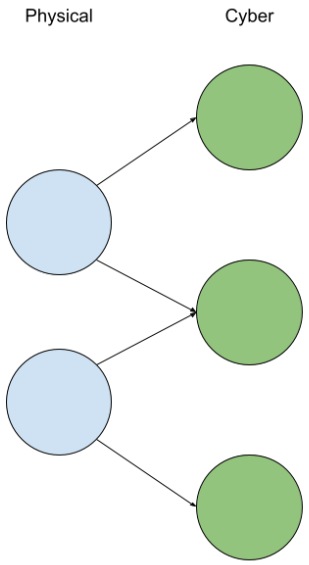


Figure 1: A diagram of a CPS with three cyber nodes and two physical nodes.

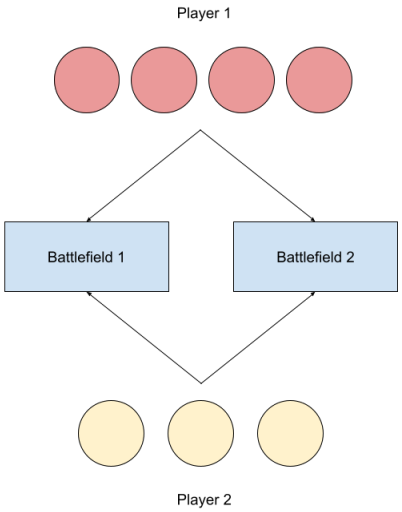


Figure 2: Example of a Colonel Blotto game.

- If both players allocate the same resources on a given battlefield, it is considered a tie.

- The Colonel Blotto game can be played with any number of battlefields and resources, and players can use different allocation strategies, such as concentrating their resources on one battlefield or spreading them evenly across multiple battlefields.

The game is named after Colonel Blotto, a fictional military officer who must distribute troops among different battlefields. Although initially formulated as a military strategy problem, the game has been applied to various fields, including economics, political science, and computer science.

The Colonel Blotto game has several applications in security games for CPSs. These systems are crucial in critical infrastructure systems, smart transportation systems, and industrial control systems.

One application for security games in CPSs is protecting critical infrastructure systems. Cyber attacks pose a significant threat to these systems, which are essential for the functioning of society. Therefore, by using the Colonel Blotto game, security managers can strategically allocate their security resources across various parts of the infrastructure to defend against potential cyber attacks [1].

Another application is in developing secure wireless sensor networks used in various applications, including environmental monitoring, smart grids, and smart buildings. Security managers can effectively allocate their resources across different parts of the wireless sensor network to prevent potential attacks and ensure network security [1].

Security Game Simulation

This project serves to explore a simulated Colonel Blotto CPS security game in which there is one attacker and one defender, each with a specific amount of resources to use (defender resources $\rightarrow$ D, attacker resources $\rightarrow$ A). The resources are distributed between each of the cyber nodes simultaneously, which will determine if the node is either successfully defended (D > A), shut down (D = A), or compromised (D < A). See Figure 1 for the system configuration that was used.

In this game each communication pathway between the cyber and physical layers is valued equally, meaning that the center physical node (payoff = 2) is worth twice as much as each external physical nodes (payoff = 1). This is essentially a version of the Colonel Blotto game where there are three battlefields with differing payoff values. The following is the list of payoffs depending on the status of each node:

- **Defended Node (D>A or A=0):** The attacker is denied access from the cyber node; therefore, only the defender gains points because the attacker did not necessarily lose anything.

- **Shut Down Node (D=A):** The attacker is able to shut down the cyber node, denying the system access to the node but the attacker does not gain any information to use for their own gain. Neither player gains points.

- **Compromised Node (D<A):** The attacker successfully takes control over the cyber node, using the information retrieved for their own gain. In this case, the defender loses points and the attacker gains points.

Throughout the course of this simulation, each player was given resources ranging from 1-10, with each combination of attacker and defender resources being tested in its own trial to provide insight as to how each player values the resources they have access to. Listed below is a step-by-step process on how each trial was conducted:

1. A list of possible strategies is generated for the resources available to each player. For example, if the defender has 3 resources, then the list of possible strategies for allocation between the three nodes would be:
   - *0, 0, 3*
   - *0, 1, 2*
   - *1, 0, 2*
   - *0, 2, 1*
   - *1, 1, 1*
   - *2, 0, 1*
   - *0, 3, 0*
   - *1, 2, 0*
   - *2, 1, 0*
   - *3, 0, 0*
2. The strategies for both the attacker and defender are compared with each other and payoffs are calculated based on the rules listed above.
3. To reduce computational complexity, dominated strategies are removed because if both players are playing logically, there would be no reason to choose these strategies. A dominated strategy is a strategy that is always worse than another available strategy, no matter what the other player does.
4. Fictitious play is used to simulate multiple games and calculate the average payoff for each player. Fictitious play is a learning algorithm in game theory that models how rational players adjust their strategies based on the observed actions of other players. Players assume that their opponents' strategies are fixed and update their own strategy based on the frequency distribution of observed actions. The goal is to converge to a Nash equilibrium, where no player can improve their payoff by changing their strategy.

Data and Results

The data gathered from this project shows a direct correlation between resources available and expected payoff. If a player is given more resources they are expected to get a greater payoff; if their opponent is given more resources they can expect a lesser payoff. In addition to this, some patterns did occur with the strategies that each player converged to throughout the simulations.

Table 1: Attacker Payoffs

D/A	1	2	3	4	5	6	7	8	9	10
1	0.80	2.00	2.66	3.19	3.59	3.99	3.99	3.99	3.99	3.99
2	0.79	1.59	2.00	2.70	3.19	3.19	3.59	3.59	3.99	3.99
3	0.40	0.81	1.40	2.00	2.36	2.69	3.04	3.19	3.40	3.59
4	0.39	0.79	1.33	1.66	2.00	2.38	2.85	2.87	3.12	3.19
5	0.00	0.41	0.85	1.23	1.59	2.00	2.27	2.52	2.76	2.92
6	0.00	0.01	0.77	1.15	1.48	1.67	2.00	2.29	2.65	2.65
7	0.00	0.39	0.57	0.83	1.14	1.43	1.67	2.00	2.22	2.41
8	0.00	0.00	0.43	0.78	1.04	1.27	1.62	1.71	2.00	2.19
9	0.00	0.00	0.40	0.54	0.83	1.09	1.31	1.57	1.73	2.00
10	0.00	0.00	0.39	0.41	0.77	1.02	1.21	1.39	1.65	1.76

Table 2: Defender Payoffs

D/A	1	2	3	4	5	6	7	8	9	10
1	1.98	0.00	-2.00	-3.19	-3.59	-3.99	-3.99	-3.99	-3.99	-3.99
2	2.40	0.80	0.00	-1.64	-2.40	-2.80	-3.19	-3.59	-3.99	-3.99
3	2.79	1.74	0.55	0.00	-1.20	-2.03	-2.40	-2.68	-3.06	-3.19
4	3.19	2.39	1.29	0.57	0.00	-0.91	-1.71	-2.11	-2.39	-2.58
5	3.66	2.64	1.90	1.02	0.36	0.00	-0.94	-1.49	-1.85	-2.19
6	3.99	3.91	2.24	1.58	0.93	0.31	0.00	-0.79	-1.33	-1.64
7	3.99	3.19	2.52	1.94	1.38	0.75	0.25	0.00	-0.74	-1.19
8	3.99	3.82	2.83	2.36	1.72	1.20	0.66	0.24	0.00	-0.65
9	3.99	3.99	3.19	2.53	2.03	1.48	1.00	0.57	0.20	0.00
10	3.99	3.99	3.19	2.98	2.31	1.83	1.34	0.92	0.53	0.18

The only resource combination that did not follow the direct correlation was when the defender had 7 resources to allocate and the attacker had 2. In this scenario, the defender is able to guarantee one defended node with the possibility of defending more if they adopt a *3,3,1* strategy. This gives the attacker a chance at a non-zero payoff if the 2 attacking resources are allocated to the node that is only defended by 1 resource. The strategies used contrast the 6 defending and 2 attacking resources scenario because here the defender converges to always using a strategy of *2,2,2* to never have a compromised node.

Another strategy pattern arises in any scenario in which the attacker has 1 more resource than the defender. In these scenarios, the two players reach an equilibrium in which the attacker puts all of the resources on the middle node to guarantee that the node will be compromised, while the defending resources are allocated to the other two nodes. This will always provide a net 0 payoff to the defender and a payoff of 2 for the attacker.

Future Work

This project details the patterns that arise from one specific Colonel Blotto CPS security game. More work can be done exploring the effect that using different network configurations or varying the number of players has on the outcome of the simulation.

Additionally, fictitious play is not the only way to find each player's strategies and generate the average payoffs. There are other methods that would require further code optimizations to be able to run in a reasonable amount of time when given large sets of possible strategies. The reason why some strategies that are expected to provide a payoff of 4.00 have a payoff of 3.99 when fictitious play is used is because

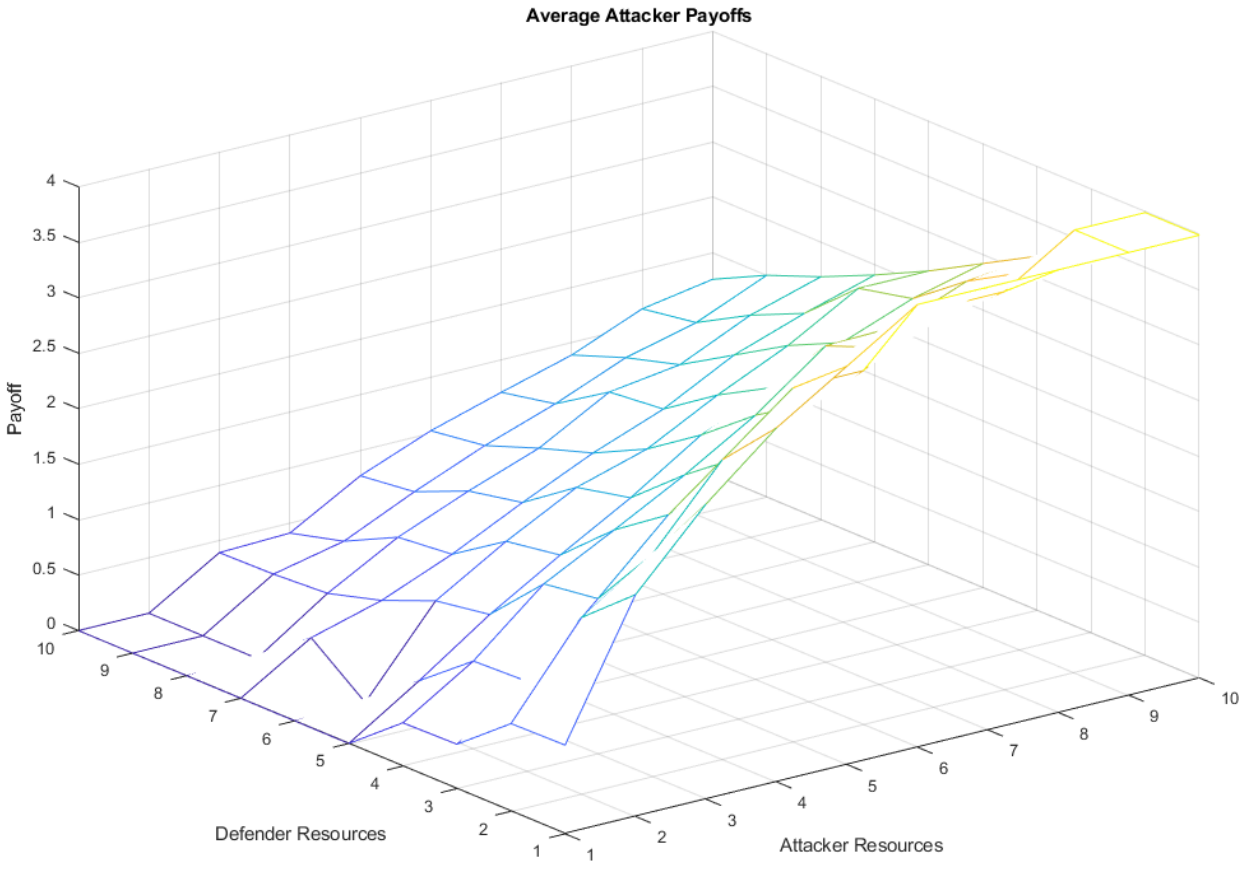
it takes a few rounds for the players to discover a Nash equilibrium. For the first few rounds, it is possible that one or both players choose sub-optimal strategies before the equilibrium is found. In future work, one could explore applying methods used in linear algebra to calculate expected payoffs more precisely with the drawback of increasing the computation complexity.

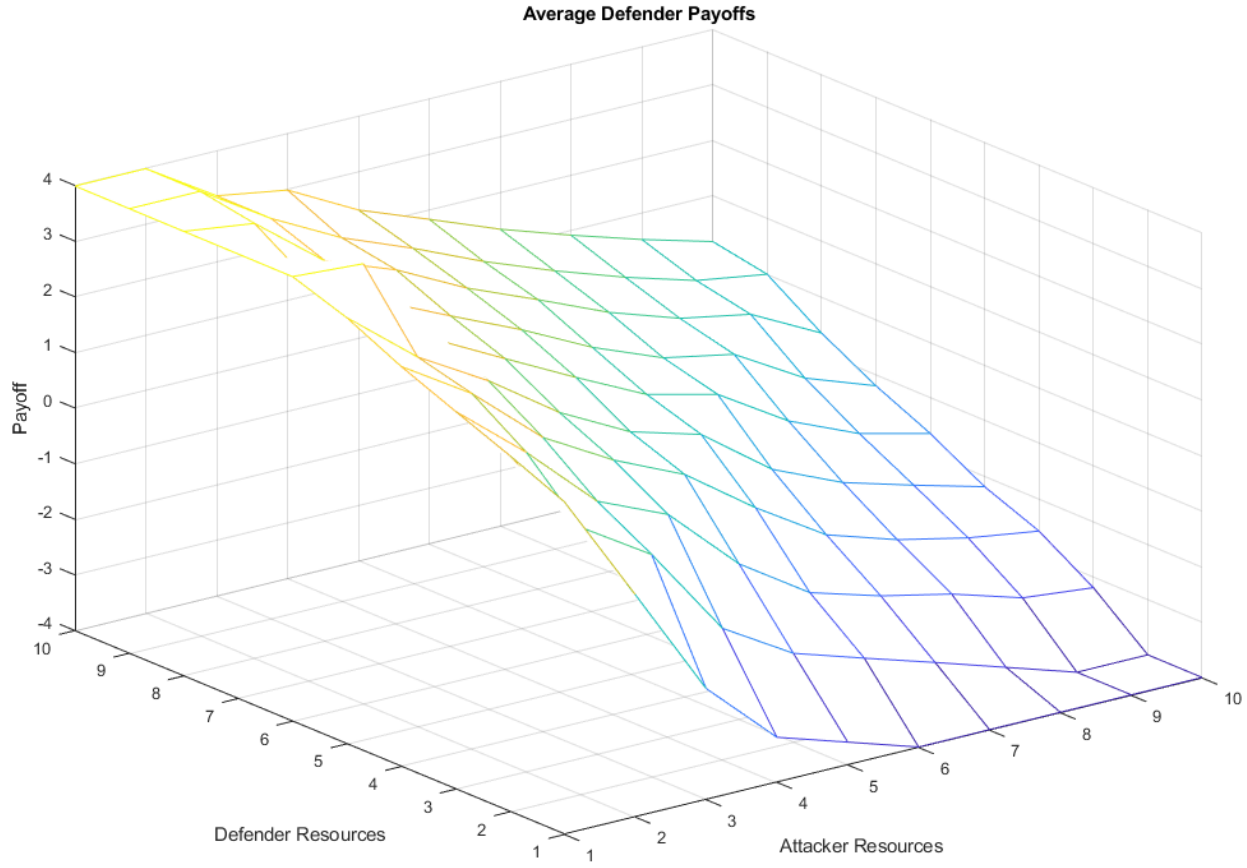
References

Bloc: A game-theoretic approach to orchestrate cps against cyber attacks. *IEEE Xplore*, August 2018.

Sathyan Munirathinam. Chapter six - industry 4.0: Industrial internet of things (iiot). In Pethuru Raj and Preetha Evangeline, editors, *The Digital Twin Paradigm for Smarter Systems and Environments: The Industry Use Cases*, volume 117 of *Advances in Computers*, pages 129–164. Elsevier, 2020.

Brian Robertson. The colonel blotto game. *Economic Theory*, 29:1–24, January 2006.


Average Attacker Payoffs
Payoff
4
3.5
3
2.5
2
1.5
1
0.5
0
Defender Resources
10
9
8
7
6
5
4
3
2
1
Attacker Resources
1
2
3
4
5
6
7
8
9
10


Average Defender Payoffs
Payoff
4
3
2
1
0
-1
-2
-3
-4
Defender Resources
10
9
8
7
6
5
4
3
2
1
Attacker Resources
1
2
3
4
5
6
7
8
9
10