Ensuring the Defense of Paths and Perimeters in Dynamic Defender-Attacker Blotto Games (dDAB) on Graphs

Bryce L. Ferguson, Daigo Shishika, and Jason R. Marden

2022 58th Annual Allerton Conference on Communication, Control, and Computing (Allerton) | 979-8-3503-9998-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/ALLERTON49937.2022.9929422

***Abstract*— When can we defend a region of space from being breached by an adversary? To answer this, we consider the Dynamic Defender-Attacker Blotto Game (dDAB) played on a graph, in which a fleet of defensive assets must be maneuvered through a network with the objective of defending a specified set of nodes from an adversarial fleet. In this framework, we seek to understand how the defender's objective (which nodes to defend in the graph) affects the amount of resources required to provide a safety guarantee. Particularly, we are interested in understanding how to defend paths-through and perimeters-of regions of space. Using the dDAB framework, we show the necessary and sufficient size of the defender's fleet needed to guarantee the defense of line graphs and cycle graphs, respectively. We find that more defender assets are needed for paths and perimeters that are less direct.**

I. Introduction

In large-scale setting prone to adversarial encounters (e.g., cyber-networks [1], interconnected enterprises [2], or large physical locations [3]), it can be difficult to guarantee a sufficient level of security with a single defense entity. As such, a large portion of research has been devoted to understanding the effectiveness of multi-agent or multi-robot teams of defensive assets to defend [4] or surveil [5] various objectives. When the defensive resources are allocated [6], [7] and assigned tasks [8], [9] appropriately, we can hope to achieve our defense objectives with fewer physical resources.

Autonomous and multi-agent security methods have been studied in many relevant settings, including patrols [4], network routing [10], [11], physical infrastructure [12], networks of subsystems [13], [14], and cyber-networks [1]. Within each of these settings, the defender's ability to offer security guarantees in the face of uncertain adversarial actions is hard [15] and depends on the specific defense objective we seek to guarantee. In this work, the types of objectives we are interested in understanding are defending regions of space from being breached by an adversary, particularly paths and perimeters, and answering: *how does the shape and size of a region we aim to protect affect or defense capabilities?*

Adversarial interactions can be modeled as zero-sum games, where two players (attacker and defender) have inversely aligned objectives (guard or breach an area, etc.). To capture the important features of these interactions, we consider the Colonel Blotto game [16], in which two opposing players assign 'troops' to 'battlefields' and win a reward for each battlefield to which they have assigned more assets than their opponent. Though described in terms of troops and battlefields, the Colonel Blotto game has been used to gain understandings in the defense of wildlife [17], security of airport terminals [18], and control over borders [19]. The Colonel Blotto framework has also been used to understand the capabilities of a opposing players with asymmetric strength and information [20], [21]. However, in this work we want to understand dynamic interactions between attackers and defenders who seek not just to maximize payoff (by securing valuable objectives more often than not), but guarantee a specific defense objective, i.e., a path or perimeter is never breached.

We consider the dynamic Defender-Attacker Blotto game, in which a defender and attacker each maneuver fleets of assets through nodes in a graph [22]. Each node is a battlefield in the sense of Colonel Blotto, and a node is 'breached' when the attacker assigns more assets to it than the defender, otherwise the defender has guarded it. Graph and network structures of similar forms have been used to investigate the security of cyber-attacks to networked computer infrastructures [1], [23], [24], connected enterprise systems [2], and in surveillance and tracking [3], [25]. In this work, we use the graph structure to gain insights into how to use multi-agent systems to defend spatial structures; specifically, we model paths as line graphs and perimeters as cycles within a larger network structure and find what defense policies can be used to guarantee no nodes in sets of this form are breached. Path and perimeter defense has been well studied in the literature [26]–[30] and even the use of multi-agent teams has been considered [31]–[35]. Here we want to understand how our objective (what type of graph to defend) affects our ability to guarantee the region is not breached. Specifically, we wish to know how many defending assets are needed to defend a path or perimeter, or what level of investment is needed to ensure the area is guarded.

Our results consider the graph-centric framework of the dDAB game and provide the necessary and sufficient number of defending assets needed to guarantee the defense of a line graph or a cycle graph along with the procedures for designing defense policies that provide this defense guarantee. We find that as a line graph becomes less direct (longer than the shortest path) and a cycle graph becomes less tightly closed (shorter paths through regions of the cycle) more defending assets are needed to guarantee the set is

B. L. Ferguson and J. R. Marden are with the department of Electrical and Computer engineering at the University of California, Santa Barbara {blferguson, jrmarden}@ece.ucsb.edu

D. Shishika is with the department of Mechanical Engineering at George Mason University {dshishika}@gmu.edu

We gratefully acknowledge the support from ARL grant ARL DCIST CRA W911NF-17-2-0181, ONR Grant #N00014-20-1-2359, AFOSR Grant #FA95550-20-1-0054, and NSF Grant #ECCS-2013779.

protected. Additionally, we show how these results can be combined to defend larger regions by looking at the union of paths and perimeters to construct sufficient strategies for any objective.

II. Problem Formulation

To understand our various defense objectives, we consider the dynamic Defender-Attacker Blotto (dDAB) game. Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be an undirected graph with nodes defining various locations and edges defining the possible travel between such locations. We assume $\mathcal{G}$ is connected and can be described by the adjacency matrix $A \in \mathbb{R}^{|\mathcal{V}|\times|\mathcal{V}|}$, where $A_{i,j} = 1$ if there exists an edge from node v_i to v_j (i.e., $(i,j) \in \mathcal{E}$) and $A_{i,j} = 0$ otherwise. For any two nodes $v, v' \in \mathcal{V}$, we let $d(v, v')$ denote the minimum number of edges needed to connect the two, i.e., the number of hops in a shortest path.

The defender and the attacker are each able to assign assets to nodes in the graph. Let $x(t) \in \mathbb{R}^{|\mathcal{V}|}_{\geq 0}$ denote an *allocation* for the defender, where $x_i(t) \geq 0$ denotes the amount of assets assigned to node v_i at time t. The total amount of assets that the defender is allotted is limited; as such, let $\sum_{v_i \in \mathcal{V}} x_i(t) = X \ \forall t \geq 0$, where X is the *defender's budget*. Similarly, the attacker is able to assign attacker assets corresponding to an allocation $y(t) \in \mathbb{R}^{|\mathcal{V}|}_{\geq 0}$ and is limited to a budget of Y.

At the initiation of the game, $t = 0$, the attacker assigns an allocation $y(0)$ then the defender assigns an allocation $x(0)$ in response in a Stackelberg style turn. In each subsequent time step $t > 0$, the defender and attacker sequentially take turns moving their assigned assets through the graph. To characterize this movement of assets, we say that at time $t > 0$ the defender picks $K^D_t \in \mathbb{R}^{|\mathcal{V}|\times|\mathcal{V}|}$ and the attacker picks $K^A_t \in \mathbb{R}^{|\mathcal{V}|\times|\mathcal{V}|}$ such that

$$x(t+1) = K^D_t x(t) \quad \text{and} \quad y(t+1) = K^A_t y(t).$$

In each turn $t > 0$ the defender goes first and chooses K^D_t in response to the allocations $x(t)$ and $y(t)$, and the attacker goes second and chooses K^A_t in response to the allocations $x(t+1)$ and $y(t)$. Each defender's movement decision K^D_t must satisfy

$$\begin{aligned} &\mathbb{1}^T K^D_t = \mathbb{1}^T \\ &[K^D_t]_{i,j} \geq 0 \ \forall v_i, v_j \in \mathcal{V} \\ &[K^D_t]_{i,j} = 0 \text{ if } A_{i,j} = 0, \end{aligned}$$

or that the budget constraint must remain satisfied (K^D_t column stochastic), and assets can only be moved between nodes that are connected by an edge in the graph. The attacker's movement decision K^A_t has similar requirements.

The defender's objective is to *guard* a predefined region, which we will characterize by a set of nodes $\mathcal{P} \subseteq \mathcal{V}$ referred to as the *protected set*. The attacker's objective is to *breach* this region by assigning more assets to a node in $\mathcal{P}$ than the defender. The attacker wins if $\exists v_i \in \mathcal{P}$ and $t \geq 0$ such that $x_i(t) < y_i(t)$. The defender wins if it can guarantee that the attacker does not breach indefinitely.

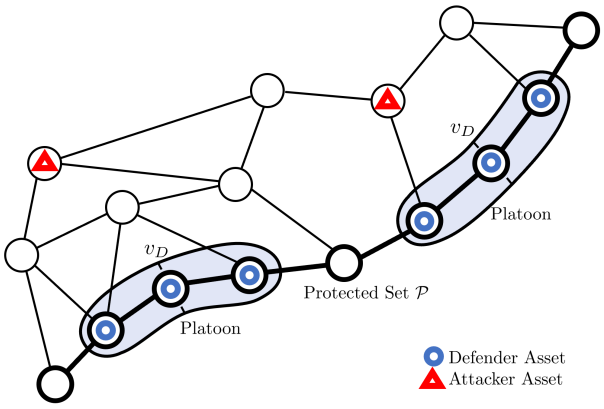

Fig. 1. Depiction of a platoon to deploy defending assets in the dynamic Defender-Attacker Blotto Game (dDAB). The center node of the platoon v_D serves as a reference for the position of the platoon as a whole. The objective of the defender is to ensure the attacker does not breach the protected set $\mathcal{P}$ (shown here as the nine bold nodes). The platoons can be used to respond to different attacker assets individually.

The main objective of this work is to identify the necessary and sufficient defender's budget needed to guarantee the protected set $\mathcal{P}$ is not breached. Certainly, the defender may choose to place a large number of assets on each node in $\mathcal{P}$ (i.e., $X = |\mathcal{P}| \cdot Y$), however this budget may become unreasonably large; thus we want to understand what are the fewest number of defender assets needed to guarantee the defense objective. We do this by providing a procedure to construct a defense policies that guarantees the protected set is guarded at all times and identifying situations where no fewer assets could provide the same guarantee. We will regularly use a specific type of defense policy where the defending assets are placed into *platoons*. We define a platoon as a structure of neighboring nodes, each with the same amount of defender assets, and a platoon leader with position v_D to reference the position of the structure overall. For example, if $\mathcal{G}$ is a grid network, a platoon may be a 3 by 3 set of nodes each with a unit defending asset, and the center node can be defined as the platoon leader to determine these 9 assets' locations.

In this work, we largely focus on two types of objectives: defending paths and defending perimeters. These regions can be identified as protected sets $\mathcal{P}$ that are line graphs or cycles. In these settings, our platoon will be a sequence of nodes in $\mathcal{P}$, see Fig. 1. In Section III, we prove the necessary and sufficient number of defender assets needed to defend paths and perimeters and provide insights into how to defend more general regions.

III. Defense Objectives

A. Defending a Path

The first defense objective we focus on is that of guarding a path. In this setting, an attacker may aim to breach the protected path to break the connection from the origin to the destination. To view this objective in the dDAB framework, we let $\mathcal{P}$ be a line graph within some larger graph structure $\mathcal{G}$. To understand the number of defender assets needed to make sure the path is not breached (i.e., X such that we

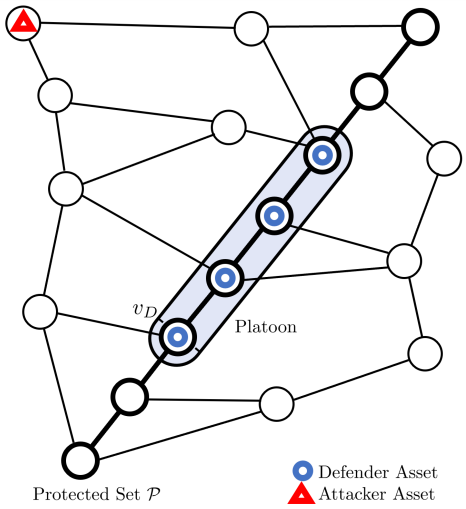

Fig. 2. Line graph as the protected set $\mathcal{P}$ (bold nodes) to understand the defense of a path. From Theorem 1, the size of the platoon needed to guarantee the defense of the path is increasing with the difference between the length of the path and the graph distance from the origin and destination, i.e., a non-direct path requires more assets to defend.

can guarantee $x_i(t) \geq y_i(t)$ for all $v_i \in \mathcal{P}$ and $t \geq 0$), we must understand the attacker's capabilities. Therefore, we introduce the following definition on the graph structure to describe how the attacker is able to move through the network.

Definition 1. *In a graph $\mathcal{G}$, a protected set $\mathcal{P} = \{v_1, \ldots, v_{|\mathcal{P}|}\}$ that is a line graph (i.e., $(v_i, v_{i+1}) \in \mathcal{E}$ $\forall i \in \{1, \ldots, |\mathcal{P}| - 1\}$) is said to be α-*hops longer than shortest *for an integer α if*

$$d(v_1, v_{|\mathcal{P}|}) = (|\mathcal{P}| - 1) - \alpha.$$

Essentially, Definition 1 asserts that an attacker asset is not able to travel from the origin to the destination of the $\mathcal{P}$ in α less hops than the length of $\mathcal{P}$. Naturally, we assume $|\mathcal{P}| > \alpha$ and also that $|\mathcal{P}| \geq 3$ as otherwise, trivially, $X = |\mathcal{P}|$. Further, note that when Definition 1 is satisfied with $\alpha = 0$, $\mathcal{P}$ is a shortest path from v_1 to $v_{|\mathcal{P}|}$.

Now, we seek to understand how many defender assets are needed to defend a path. In Theorem 1, we find the necessary and sufficient amount of defender assets needed to defend the path in the dDAB game.

Theorem 1. *To guarantee the defense of a line graph $\mathcal{P} \subseteq \mathcal{G}$ that is α-hops longer than shortest,*

$$X \geq (3 + \alpha)Y \tag{1}$$

defender assets are sufficient in any such $(\mathcal{P}, \mathcal{G})$ and necessary to guarantee every such $(\mathcal{P}, \mathcal{G})$ can be defended[1].

This result shows us that (i) the defender can guarantee their defense objective with a reasonable budget, and (ii) the budget grows as the attacker's capabilities grow, or the path becomes less direct. To show that (1) is sufficient to defend a path that is α-hops longer than shortest, we will provide the procedure for constructing a defender policy that guarantees no node in $\mathcal{P}$ is breached (as illustrated in Fig. 2). To show that (1) is necessary to guarantee any path that is α-hops longer than shortest can be defended, we provide an example where no fewer will do.

Before proving the theorem, we highlight an important corollary that emerges.

Corollary 1. *To guarantee there exists a path $\mathcal{P} \subseteq \mathcal{G}$ that connects some v_o and v_d that can be defended,*

$$X \geq 3Y \tag{2}$$

defender assets are necessary and sufficient.

If the defender's objective is to merely guarantee that there is *some* path from an origin to the destination that can be defended, they need only $X = 3Y$ assets. This corollary emerges from Theorem 1 by considering the shortest path that connects v_o and v_d and observing that $\alpha = 0$ for a shortest path.

Proof of Theorem 1: We start by assuming that the attacker possesses a single, unsplittable asset that they move through the network and later show that these results can be generalized to the full setting. Let $v_A \in \mathcal{V}$ denote the position of the attacker asset. Let $\mathcal{P} = \{v_1, \ldots, v_{|\mathcal{P}|}\}$ be a line graph indexed value $i \in \{1, \ldots, |\mathcal{P}|\}$. Now, we consider a defense policy of a single platoon, where z defender assets are aligned concurrently along the line graph $\mathcal{P}$. To refer to the position of the platoon, we define v_D as the lowest index of the platoon, i.e., nodes $\{v_D, \ldots, v_{D+z-1}\} \subseteq \mathcal{P}$ are utilized by a single defender asset each.

Consider the attacker and platoon leader's distance to any node on the graph, $d(v_A, v_i)$ and $d_{\mathcal{P}}(v_D, v_i)$ respectively, where $d_{\mathcal{P}}(\cdot, \cdot)$ is the distance between two nodes in $\mathcal{P}$ while only using nodes in $\mathcal{P}$ as we limit the defender to this region. The defender's ability to guard a node can be expressed by the difference between these two numbers, which we will call the *advantage number*,

$$a_i = d(v_A, v_i) - d_{\mathcal{P}}(v_D, v_i). \tag{3}$$

The defender's aim is to stay closer to nodes in $\mathcal{P}$ than the adversary, and thus wants a_i to be larger. The objective of the defender can now be rewritten; at each time step, the defender must satisfy

$$\begin{aligned} &a_i > 0 \ \forall v_i \in \{v_1, \ldots, v_{D-1}\} \subset S \quad \text{and,} \\ &a_i > -z + 1 \ \forall v_i \in \{v_{D+1}, \ldots, v_{|\mathcal{P}|}\} \subset S, \end{aligned} \tag{4}$$

to guarantee that a defender asset is always closer to a node in the protected set than the adversary is.

First, we show there is a valid starting position that satisfies (4). Try $v_D = v_1$, and the first condition in (4) is satisfied. If $\exists i > D$ such that $a_i \leq -z + 1$ then try $v_D = v_2$ and check again. Continue increasing D until $a_i \geq -z + 2$ for all $i > D$. Now, we solve for a value of z such that no preceding node can dissatisfy (4). If for some $j < D$, $a_j \leq 0$ then this implies $d(v_A, v_j) - d_{\mathcal{P}}(v_D, v_j) \leq 0$.

[1]In the special case where $\alpha = |\mathcal{P}| - 2$, (i.e., the origin and destination of the path are directly connected), still only $X = |\mathcal{P}|Y$ defender assets are needed as this will always guarantee every node in $\mathcal{P}$ cannot be breached.

From before, because D was increased precisely until (4) was satisfied for all $i > D$, there exists an $i > D$ such that $d(v_A, v_i) - d_{\mathcal{P}}(v_D, v_i) = -z + 2$. Combining these two observations we see

$$d(v_A, v_j) + d(v_A, v_i) \leq d_{\mathcal{P}}(v_D, v_j) + d_{\mathcal{P}}(v_D, v_i) - z + 2. \quad (5)$$

If we select $z = 3 + \alpha$, then (5) implies

$$d(v_A, v_j) + d(v_A, v_i) \leq (|\{v_j, \ldots, v_i\}| - 1) - \alpha - 1. \quad (6)$$

Observing that $d(v_i, v_j) \leq d(v_A, v_j) + d(v_A, v_i)$, then concatenating the rest of $\mathcal{P}$ breaks the assumption that $\mathcal{P}$ is α-hops longer than shortest.

Now, from this valid starting position, the attacker is only able to increase or decrease each advantage number by one each turn. The attacker cannot move to a position that makes the v_i and v_j dissatisfy (4) for some $i > D$ and $j < D$ at the same time (following the arguments from above). As such, the defender simply increases or decreases D depending on which side has a node with advantage breaking (4), if any. Again, by following the same logic as before, moving to this new position cannot make a negative advantage occur on the other side of v_D, so this approach will always guarantee that (4) is satisfied for all $v \in \mathcal{P}$ and thus the defense objective is guaranteed.

To see how this method generalizes to an attacker that can distribute their assets over multiple nodes, consider that a platoon of the above form is defined for each mass of attacker assets in the graph, where the amount of defender assets in each platoon is scaled proportionally to the associated amount of attacker assets. By letting these platoons run in parallel, the defense objective can be guaranteed against any number of attackers such that $X = (3 + \alpha)Y$.

To show $(3 + \alpha)Y$ defender assets are necessary to guarantee defense in every $(\mathcal{P}, \mathcal{G})$ that is α-hops longer than shortest (as this was the number used in the sufficient platoon), consider a line graph $\mathcal{P}$ where $3 + m$ consecutive nodes connect to a single node $v' \notin \mathcal{P}$. The attacker can place all their assets at v' and in one turn move to any of the $3 + m$ consecutive nodes, thus all must be assigned Y defender assets at the end of the defender's turn. □

B. Defending a Perimeter

The second defense objective we consider is that of preventing the attacker from breaching some connected region of space, as such, we look to gain insights into problems defending the perimeter of said region. We can use the dDAB framework to model a perimeter as a cycle within a graph, i.e., the protected set $\mathcal{P} = \{v_1, \ldots, v_{|\mathcal{P}|}\}$ where $(v_{|\mathcal{P}|}, v_1) \in \mathcal{E}$, and $|\mathcal{P}| \geq 3$. In defending a perimeter, the attacker can only attempt to breach the region from outside; the shape of the region (and perimeter) ultimately affects the attacker's capability to circle and breach the perimeter. With this in mind, we introduce the following definition in relation to the cycle graph $\mathcal{P}$.

Definition 2. *In a graph $\mathcal{G}$, a protected set $\mathcal{P} = \{v_1, \ldots, v_{|\mathcal{P}|}\}$ that is a cycle graph (i.e., $(v_i, v_{i+1}) \in \mathcal{E}$ $\forall i \in \{1, \ldots, |\mathcal{P}| - 1\}$ and $(v_{|\mathcal{P}|}, v_1) \in \mathcal{E}$) is said to be* Graph Convex *if for each $v \in \mathcal{V}$, when $|\mathcal{P}|$ is even,*

$$\exists \hat{v} \in \mathcal{P} \text{ s.t. } d(v, \hat{v}) \geq \frac{|\mathcal{P}|}{2},$$

and when $|\mathcal{P}|$ is odd,

$$\exists \hat{v}, \hat{v}' \in \mathcal{P} \text{ s.t. } d(v, \hat{v}') \geq d(v, \hat{v}) \geq \frac{|\mathcal{P}| - 1}{2}.$$

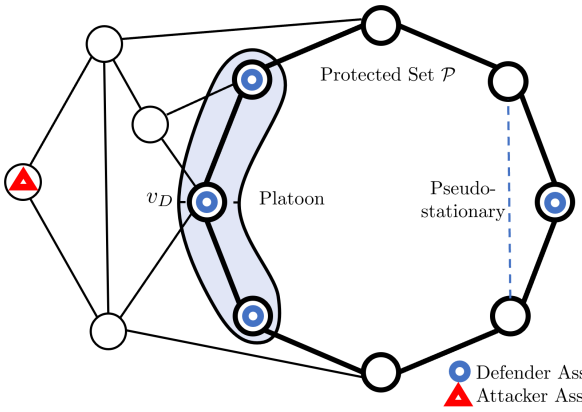

Fig. 3. Cycle graph as a protected set $\mathcal{P}$ (bold nodes) to understand the defense of 2-D areas. From Theorem 2, more assets are needed as the attacker posses greater ability to traverse the outside of the cycle. The use of pseudo-stationary defender assets essentially allow the defender to remove nodes from the protected set (bold nodes) and form a new, smaller cycle that can be defended by a platoon of three (note the allocation in this picture is not optimal but is done for illustrative purposes).

Though Definition 2 may initially be counter-intuitive, it most accurately captures our notion of defending a region; it does not imply that $\mathcal{P}$ is the shortest cycle at any root node, rather that the graph distance *around* the cycle is no shorter than following the cycle. The different definitions between even and odd cardinality cycles is to handle the case that two nodes may be equal distance around the cycle when $|\mathcal{P}|$ is odd. Note that this definition also directly implies that the graph distance between two nodes in the cycle is no less than the shortest path between them along the cycle, i.e., $d(v_i, v_j) \geq d_{\mathcal{P}}(v_i, v_j)$.

We now seek to understand how many defender assets are needed to defend the perimeter of a region. In Proposition 1, we provide the necessary and sufficient number of defender assets to guarantee the defense of a cycle in the dDAB game.

Proposition 1. *To guarantee the defense of a cycle graph $\mathcal{P} \subseteq \mathcal{G}$ that is Graph Convex,*

$$X \geq 3Y \quad (7)$$

defender assets are necessary and sufficient to guarantee the defense of $\mathcal{P}$ in $\mathcal{G}$.

This proposition offers a similar insights as Corollary 1: the defender requires three times the amount of attacker assets to guarantee the defense of a region that has some notion of 'directness'. As before, we wish to understand how the shape of this region being less direct can cause the required number of assets to grow. As such, we extend the definition of Graph Convex.

Definition 3. *In a graph $\mathcal{G}$, a protected set $\mathcal{P} = \{v_1, \ldots, v_{|\mathcal{P}|}\}$ that is a cycle graph (i.e., $(v_i, v_{i+1}) \in \mathcal{E}\ \forall i \in \{1, \ldots, |\mathcal{P}| - 1\}$ and $(v_{|\mathcal{P}|}, v_1) \in \mathcal{E}$) is said to be* β Graph Convex *if there exists $\mathcal{Q} \subseteq \mathcal{P}$ that is the largest subset of nodes that becomes a Graph Convex cycle with the addition of any edges consecutive edges $v_i, v_{i+k} \in \mathcal{Q}$ that makes $\mathcal{Q}$ a cycle that maintains the same ordering as $\mathcal{P}$, and $|\mathcal{P} \setminus \mathcal{Q}| = \beta$.*

This definition allows us to consider perimeters that, on their own, are not Graph Convex, but can still represent a defensible perimeter.

Theorem 2. *To guarantee the defense of a cycle graph $\mathcal{P} \subseteq \mathcal{G}$ that is β Graph Convex,*

$$X \geq (3 + \beta)Y \tag{8}$$

defender assets are sufficient to guarantee the defense of $\mathcal{P}$ in $\mathcal{G}$ and necessary to guarantee the defense of every such $(\mathcal{P}, \mathcal{G})$.

This theorem offers similar insights as Theorem 1: the defender can achieve their defense objective with a reasonable amount of assets, and as the perimeter becomes less direct, the number of required defender assets increases. As with Theorem 1, we will prove the sufficiency of (8) by considering a specific type of defender policy where a platoon of 3 defender assets travel around the cycle and β are placed as pseudo-stationary assets that essentially remove the node from the protected set. When $\beta = 0$, we recover only 3 assets are needed, i.e., the attacker can not get around the outside faster than the perimeter length.

Proof of Proposition 1: We start by assuming the attacker only deploys a unit asset at a single node $v_A \in \mathcal{V}$ which they move to try to breach the protected set. Let the protected set be a cycle $\mathcal{P} = \{v_1, \ldots, v_{|\mathcal{P}|}\}$. Consider the deployment of a platoon of three consecutive nodes along the cycle where v_D is used to reference the position of the center of the node, i.e., $\{v_{D-1}, v_D, v_{D+1}\} \subset \mathcal{P}$ with appropriate wrapping around the index set. Using the framework of the advantage number in (3), the defender must guarantee that

$$a_i \geq 0\ \forall v_i \in \mathcal{P}. \tag{9}$$

First, we show that there exists a valid starting position for the defender that satisfies (9). Given the attacker's starting position v_A, let $\hat{V} = \operatorname{argmax}_{v \in \mathcal{P}} d(v_A, v)$ denote the nodes in $\mathcal{P}$ that are farthest from v_A. If $|\hat{V}| = 1$ (or $|\mathcal{P}|$ is even) then pick $v_D \in \operatorname{argmax}_{v \in \mathcal{P}} d_{\mathcal{P}}(\hat{v}, v_D)$ as the opposite side of the cycle as $\hat{v} \in \hat{V}$. If $|\hat{V}| = 2$ (or $|\mathcal{P}|$ is odd) then pick $v_D \in \cap_{\hat{v} \in \hat{V}} \operatorname{argmax}_{v \in \mathcal{P}} d_{\mathcal{P}}(\hat{v}, v_D)$, or the node equally far from each in $\hat{V}$. Note that in either case, $d_{\mathcal{P}}(\hat{v}, v_D) = \lfloor |\mathcal{P}|/2 \rfloor$. Now, if there exists a $v_i \in \mathcal{P}$ such that $a_i < 0$, then

$$\begin{aligned} d(v_A, \hat{v}) &\leq d(v_A, v_i) + d(v_i, \hat{v}) \\ &< d_{\mathcal{P}}(v_D, v_i) + d_{\mathcal{P}}(v_i, \hat{v}) \\ &= \lfloor |\mathcal{P}|/2 \rfloor, \end{aligned}$$

or the cycle does not satisfy Graph Convex.

From this starting position, we show that the attacker can not move to make the advantage number negative on both sides of the platoon. Let $\mathcal{P}^{\text{cw}}(v_D)$ denote the set of nodes in $\mathcal{P}$ on the clockwise half of v_D and $\mathcal{P}^{\text{ccw}}(v_D)$ the set of those on the counter-clockwise half. If there exists a $v_i \in \mathcal{P}^{\text{cw}}(v_D)$ and a $v_j \in \mathcal{P}^{\text{ccw}}(v_D)$ such that $a_i, a_j < 0$ and v_D on the shorter path between them in $\mathcal{P}$, then $d(v_A, v_i) + d(v_A, v_j) < d_{\mathcal{P}}(v_D, v_i) + d_{\mathcal{P}}(v_D, v_j)$ implies there is a shorter path around than the cycle and $\beta = 0$ is contradicted. If there exists a $v_i \in \mathcal{P}^{\text{cw}}(v_D)$ and a $v_j \in \mathcal{P}^{\text{ccw}}(v_D)$ such that $a_i, a_j < 0$ and v_D on the longer path between them in $\mathcal{P}$, then v_A can reach any node in the cycle in less than $\lfloor |\mathcal{P}|/2 \rfloor$ and Graph Convexis again contradicted.

Finally, we show that the defender can always move to maintain a non-negative advantage number at every node. The attacker may only move one space per turn and thus may only increase or decrease an advantage number by one. From before, a negative advantage can only occur in the clockwise or counter-clockwise half of the cycle from v_D respectively. If there exists $v_i \in \mathcal{P}^{\text{cw}}(v_D)$ such that $a_i = -1$ moving v_D clockwise will make it zero. Note that this movement cannot make a node $v_j \in \mathcal{P}^{\text{ccw}}(v_D)$ become $a_j = -1$ else $d(v_A, v_i) = d_{\mathcal{P}}(v_D, v_i)$ and $d(v_A, v_j) < d_{\mathcal{P}}(v_D, v_j)$, implying

$$d(v_i, v_j) \leq d(v_A, v_i) + d(v_A, v_j) < d_{\mathcal{P}}(v_D, v_i) + d_{\mathcal{P}}(v_D, v_j),$$

contradicting the Graph Convexassumption again. □

Proof of Theorem 2: To guarantee the defense of perimeters that are β Graph Convex with $\beta > 0$, we consider the use of *pseudo-stationary* assets, where when such an asset is placed at a node, it does not move unless the platoon is adjacent to it. When the platoon would move through the node the pseudo-stationary asset was assigned to, the asset instead moves with the platoon, in front of it. When the (now length 4) platoon would move to no longer cover the original node with a pseudo-stationary asset, it leaves an asset behind at the original position (returning to a platoon of 3). This approach essentially removes the node to which a pseudo-stationary asset is assigned from the protected set $\mathcal{P}$, as the movement of the defending assets is now equivalent to skipping this node and leaving an asset on it at all times (see Fig. 3).

To devise a sufficient policy, consider placing a pseudo-stationary asset at each $v \in \mathcal{P} \setminus \mathcal{Q}$, of which there are β. The nodes in $\mathcal{Q}$ can now be defended as a cycle, as the pseudo-stationary assets essentially act as edge for the platoon of 3 to travel only on nodes in $\mathcal{Q}$. The result of Proposition 1 shows the platoon of 3 can defend $\mathcal{Q}$

To see that this is necessary, consider a cycle where $3+\beta$ consecutive nodes in $\mathcal{P}$ are connected to a node $v \notin \mathcal{P}$. Then each of those $3 + \beta$ nodes must posses a defender asset when $v_A = v$; additionally, the furthest node from v in $\mathcal{P}$ is $\lfloor |\mathcal{P}|/2 \rfloor - \beta$ hops away so the cycle is Graph Convex.

To extend this result to a general adversary, consider assigning the pseudo-stationary nodes with Y assets at each then fractionalizing the remaining $3Y$ assets into platoons in

response to how the attacker fractionalize its own assets, as was done in Theorem 1. □

C. Insights on General Defense Objectives

In the previous subsections, we have gained insights into how defense policies can be designed to defend paths and perimeters, however, we may also be tasked with defending more general structures. In Remark 1, we address this by letting $\mathcal{P}$ be an arbitrary subset of the vertex set and use our previous results to gain an understanding of how to devise defense strategies in this setting.

Remark 1. *Let $\mathcal{P} \subseteq \{\cup_{i=1}^{A} L_i\} \cup \{\cup_{j=1}^{B} C_j\}$ be a protected set formed by a union of line graphs $\cup_{i=1}^{A} L_i$ and cycles $\cup_{j=1}^{B} C_j$, where each line graph L_i is α_i-hops longer than short and each cycle is β_j-hops longer around. Then*

$$X \geq \left(\sum_{i=1}^{A} (3 + \alpha_i) + \sum_{j=1}^{B} (3 + 2\beta_j) \right) Y, \qquad (10)$$

defender assets are sufficient in any such $(\mathcal{P}, \mathcal{G})$ and necessary to guarantee every such $(\mathcal{P}, \mathcal{G})$ can be defended.

Essentially, for any protected set $\mathcal{P}$, if we can define a union of line graphs and cycles that cover $\mathcal{P}$, then we can come up with a defense policy and number of assets that is guaranteed to guard the protected set using results from Theorem 1 and Theorem 2. In some contexts, this can be intuitive and potentially describe the necessary number of defender assets, e.g., a line graph connecting two cycles. In general, it can become context dependent on how well this approach does relative the minimum number of assets needed to defend the arbitrary protected set $\mathcal{P}$.

IV. Conclusion

In this work, we used the model of dynamic Defender-Attacker Blotto games to understand the level of investment in defensive assets needed to guarantee the protection of a path or perimeter. By considering the graph-centric approach, we found the necessary and sufficient number of assets needed to defend line and cycle graphs respectively, and extended these results to a spatial interpretation to gain insights about paths and perimeters in 2-Dimensional space. Future work will investigate defending more general types of regions and consider how uncertainty about an attacker's capabilities can affect our defense guarantees.

References

[1] K. Ingols, R. Lippmann, and K. Piwowarski, "Practical attack graph generation for network defense," in *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*, 2006, pp. 121–130.

[2] R. P. Lippmann, K. W. Ingols, C. Scott, K. Piwowarski, K. J. Kratkiewicz, M. Artz, and R. Cunningham, "Evaluating and strengthening enterprise network security using attack graphs," 2005.

[3] G. Ferri*, A. Munafò*, A. Tesei, P. Braca, F. Meyer, K. Pelekanakis, R. Petroccia, J. Alves, C. Strode, and K. LePage, "Cooperative robotic networks for underwater surveillance: an overview," *IET Radar, Sonar & Navigation*, vol. 11, no. 12, pp. 1740–1761, 2017. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-rsn.2017.0074

[4] N. Agmon, S. Kraus, and G. A. Kaminka, "Multi-robot perimeter patrol in adversarial settings," in *2008 IEEE International Conference on Robotics and Automation*. IEEE, 2008, pp. 2339–2345.

[5] A. Renzaglia, L. Doitsidis, A. Martinelli, and E. B. Kosmatopoulos, "Multi-robot three-dimensional coverage of unknown areas," *The International Journal of Robotics Research*, vol. 31, no. 6, pp. 738–752, 2012.

[6] B. L. Ferguson and J. R. Marden, "Robust Utility Design in Distributed Resource Allocation Problems with Defective Agents," *Dynamic Games and Applications*, pp. 1–23, aug 2022. [Online]. Available: https://link.springer.com/article/10.1007/s13235-022-00470-y

[7] J. R. Marden, "The Role of Information in Distributed Resource Allocation," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 3, pp. 654–664, 2017.

[8] G. A. Korsah, A. Stentz, and M. B. Dias, "A comprehensive taxonomy for multi-robot task allocation," *The International Journal of Robotics Research*, vol. 32, no. 12, pp. 1495–1512, 2013.

[9] A. Khamis, A. Hussein, and A. Elmogy, "Multi-robot task allocation: A review of the state-of-the-art," *Cooperative robots and sensor networks 2015*, pp. 31–51, 2015.

[10] M. S. Kang, S. B. Lee, and V. D. Gligor, "The Crossfire Attack," in *2013 IEEE Symposium on Security and Privacy*, 2013, pp. 127–141.

[11] D. Grimsman, J. P. Hespanha, and J. R. Marden, "Stackelberg equilibria for two-player network routing games on parallel networks," in *2020 American Control Conference (ACC)*. IEEE, 2020, pp. 5364–5369.

[12] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530–544, 2006.

[13] M. Abdallah, T. Cason, S. Bagchi, and S. Sundaram, "The Effect of Behavioral Probability Weighting in a Simultaneous Multi-Target Attacker-Defender Game," in *2021 European Control Conference (ECC)*, 2021, pp. 933–938.

[14] D. Kovenock and B. Roberson, "The optimal defense of networks of targets," *Economic Inquiry*, vol. 56, no. 4, pp. 2195–2211, 2018.

[15] F. Duvallet and A. Stentz, "Imitation learning for task allocation," in *2010 IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2010, pp. 3568–3573.

[16] B. Roberson, "The colonel blotto game," *Economic Theory*, vol. 29, no. 1, pp. 1–24, 2006.

[17] L. Xu, S. Gholami, S. McCarthy, B. Dilkina, A. Plumptre, M. Tambe, R. Singh, M. Nsubuga, J. Mabonga, M. Driciru, and Others, "Stay ahead of Poachers: Illegal wildlife poaching prediction and patrol planning under uncertainty with field test evaluations (Short Version)," in *2020 IEEE 36th International Conference on Data Engineering (ICDE)*. IEEE, 2020, pp. 1898–1901.

[18] M. Tambe, *Security and game theory: algorithms, deployed systems, lessons learned*. Cambridge university press, 2011.

[19] J. Pita, M. Jain, J. Marecki, F. Ordóñez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus, "Deployed armor protection: the application of a game theoretic model for security at the los angeles international airport," in *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track*, 2008, pp. 125–132.

[20] K. Paarporn, R. Chandan, M. Alizadeh, and J. R. Marden, "A General Lotto game with asymmetric budget uncertainty," *arXiv preprint arXiv:2106.12133*, 2021.

[21] ——, "Characterizing the interplay between information and strength in Blotto games," in *2019 IEEE 58th Conference on Decision and Control (CDC)*, 2019, pp. 5977–5982.

[22] D. Shishika, Y. Guan, M. Dorothy, and V. Kumar, "Dynamic Defender-Attacker Blotto Game," *arXiv preprint arXiv:2112.09890*, 2021.

[23] S. Jajodia, S. Noel, and B. O'berry, "Topological analysis of network attack vulnerability," in *Managing cyber threats*. Springer, 2005, pp. 247–266.

[24] P. Ning and D. Xu, "Learning attack strategies from intrusion alerts," in *Proceedings of the 10th ACM conference on Computer and communications security*, 2003, pp. 200–209.

[25] N. Alon and A. Mehrabian, "Chasing a fast robber on planar graphs and random graphs," *Journal of Graph Theory*, vol. 78, no. 2, pp. 81–96, 2015. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/jgt.21791

[26] D. Shishika and V. Kumar, "Perimeter-defense game on arbitrary convex shapes," 2019. [Online]. Available: https://arxiv.org/abs/1909.03989

[27] ——, "A review of multi agent perimeter defense games," in *International Conference on Decision and Game Theory for Security*. Springer, 2020, pp. 472–485.

[28] E. Garcia, A. Von Moll, D. W. Casbeer, and M. Pachter, "Strategies for defending a coastline against multiple attackers," in *2019 IEEE 58th Conference on Decision and Control (CDC)*. IEEE, 2019, pp. 7319–7324.

[29] E. S. Lee, D. Shishika, and V. Kumar, "Perimeter-defense game between aerial defender and ground intruder," in *2020 59th IEEE Conference on Decision and Control (CDC)*, 2020, pp. 1530–1536.

[30] L. Zhang, Q. Wei, K. Gu, and H. Yuwen, "Path hopping based sdn network defense technology," in *2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD)*, 2016, pp. 2058–2063.

[31] D. G. Macharet, A. K. Chen, D. Shishika, G. J. Pappas, and V. Kumar, "Adaptive partitioning for coordinated multi-agent perimeter defense," in *2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2020, pp. 7971–7977.

[32] A. K. Chen, D. G. Macharet, D. Shishika, G. J. Pappas, and V. Kumar, "Optimal multi-robot perimeter defense using flow networks," in *Distributed Autonomous Robotic Systems*, F. Matsuno, S.-i. Azuma, and M. Yamamoto, Eds. Cham: Springer International Publishing, 2022, pp. 282–293.

[33] D. Shishika, D. Maity, and M. Dorothy, "Partial information target defense game," in *2021 IEEE International Conference on Robotics and Automation (ICRA)*, 2021, pp. 8111–8117.

[34] M. Chen, Z. Zhou, and C. J. Tomlin, "A path defense approach to the multiplayer reach-avoid game," in *53rd IEEE conference on decision and control*. IEEE, 2014, pp. 2420–2426.

[35] A. K. Chen, B. L. Ferguson, D. Shishika, M. Dorothy, J. R. Marden, G. J. Pappas, and V. Kumar, "Path defense in dynamic defender-attacker blotto games (ddab) with limited information," 2022. [Online]. Available: https://arxiv.org/abs/2204.04176