Stealthy Attacks on Pheromone Swarming

Janiece Kelly[1], Seth Richter[2] and Mina Guirguis[1]

Department of Computer Science, [1]Texas State University- San Marcos, [2]LeTourneau University

Introduction

In nature, pheromones are a chemical means of communication used by swarming insects to organize efficient movement among agents without relying on any centralized commands. Similarly, in a digital world, virtual pheromones can be used to control unmanned vehicles.

How:

- ★ Positive virtual pheromones emit from Areas of Interest
- ★ Agents move into areas with higher pheromone levels
- ★ Agents deposit negative pheromones to repel other agents

Advantages:

- ★ Robust against failures
- ★ Adaptive
- ★ Autonomous

Applications:

- ★ Target tracking
- ★ Search and rescue

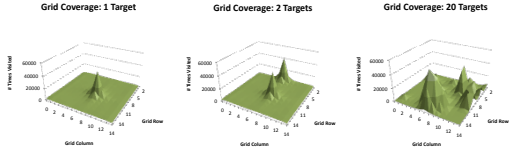
Problem: Agents communicate using wireless communications which are susceptible to jamming attacks.

Goals

Our goal is to identify vulnerabilities in digital pheromone swarming systems that capitalize on jamming wireless signals between the agents. Our ultimate goal is to protect these systems against stealthy attacks.

Methods: Characterization

We observed the typical characteristics of robot swarming behavior by measuring grid coverage under various pheromone strengths, evaporation rates and numbers of targets present.



Coverage over 100,000 Steps of a 15x15 Grid by 10 Robots: No Attack

After establishing a basis for a normal behavior, we implemented four types of attacks on the communication links between the agents and observed their effect. An attack's cost and effect is measured using the following:

$$\text{cost} = \#\text{ signals jammed}$$

$$\text{damage} = \#\text{ collisions caused}$$

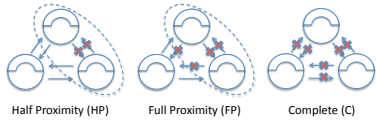
$$\text{potency (collisions)} = \frac{\#\text{ collisions caused}}{\text{cost}}$$

$$\text{potency (map difference)} = \frac{\sum \text{map differences caused}}{\text{cost}}$$

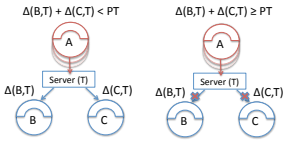
A collision occurs when multiple agents attempt to occupy the same grid cell.

Methods: Attacks

Attack Type	Description
Complete (C)	Jam all communication signals all the time
Half Proximity (HP)	Jam communication between robots within a specified radius
Full Proximity (FP)	Jam all outgoing communications for robots within a specified radius
Probability Threshold (PT)	Jam communication signals that will cause a map difference above a specified threshold

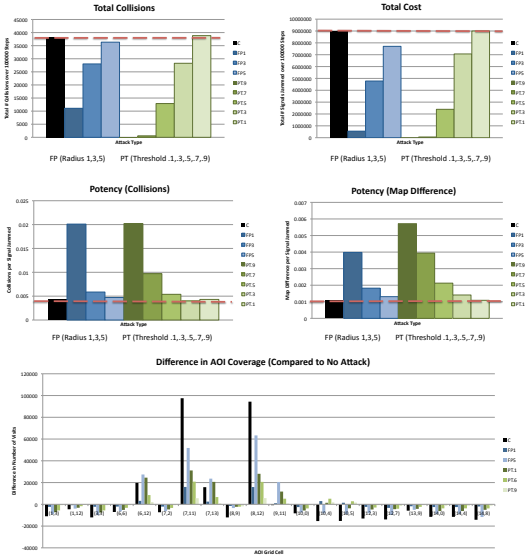


Simplified Representation of Proximity and Complete Attacks: The dotted line represents the attack radius and the red x represents a blocked or jammed communication.



Probability Threshold Attack Representation: Δ(C,T) represents the difference between a robot's local map (e.g., C) and the truth map (T). If resulting cumulative map differences from a jam are above a threshold PT, the signal will be jammed.

Results



Implementation

Robot responsibilities:

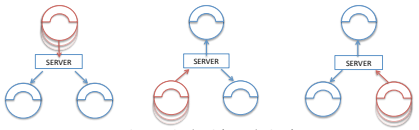
- ★Maintain a local map of pheromone locations
- ★Deposit negative pheromones onto the map after each movement
- ★Compute pheromone strengths for each grid cell

Robot communication:

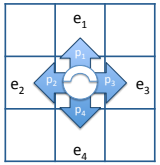
- ★Complete map of pheromone locations (but no pheromone strengths!)

Server (Aggregation Point) responsibilities:

- ★Receive copies of local maps
- ★Disseminate maps to every other active robot on the grid.



Map Communication Schematic: 3 Robots



Pheromone effect

$e_i = B^s$

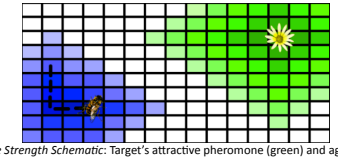
B is a scaling constant, s is the pheromone strength in the destination grid cell

Movement probability

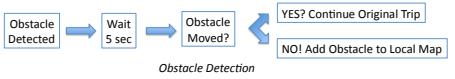
$p_i = e_i / E$

E is the sum of e_i values for all possible directions of movement

Grid Movement Schematic: Arrows represent possible directions of movement, e represents pheromone effect on a cell, p represents probability of moving to a cell.



Pheromone Strength Schematic: Target's attractive pheromone (green) and agent's trailing repulsive pheromones (blue)



Obstacle Detection

Conclusion

Pheromone swarming systems are vulnerable to Full Proximity (FP) and Probability Threshold (PT) attacks.

Collisions: FP and PT each have up to **4.7x** the potency of C
Map differences: FP has up to 3.6x the potency of C, PT has up to **5.5x** the potency

FP caused as many as 95% of the collisions of a complete attack, but by jamming only 86% as many signals. PT caused 101% of the collisions of a complete attack, by jamming roughly as many signals.

Future work: Securing swarming systems against these and other types of stealthy attacks.

This research is funded by NSF REU award #1156712 that is co-funded by the DoD and by NSF award #1149397.