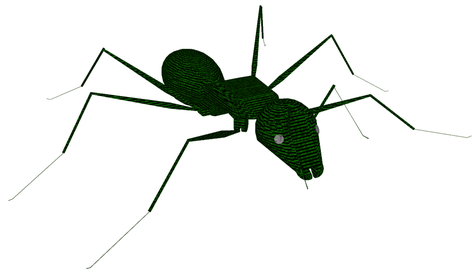
The Hive Mind: Applying a Distributed Security Sensor Network to GENI

http://hivemind.cs.ucdavis.edu/

University of California, Davis: Matt Bishop, Sean Peisert (PI), Steven Templeton
Battelle: Glenn Fink, Deborah Frincke (CoPI)
CA Labs: Carrie Gates (CoPI)
Wake Forest University: Michael Crouse, Errin Fulp



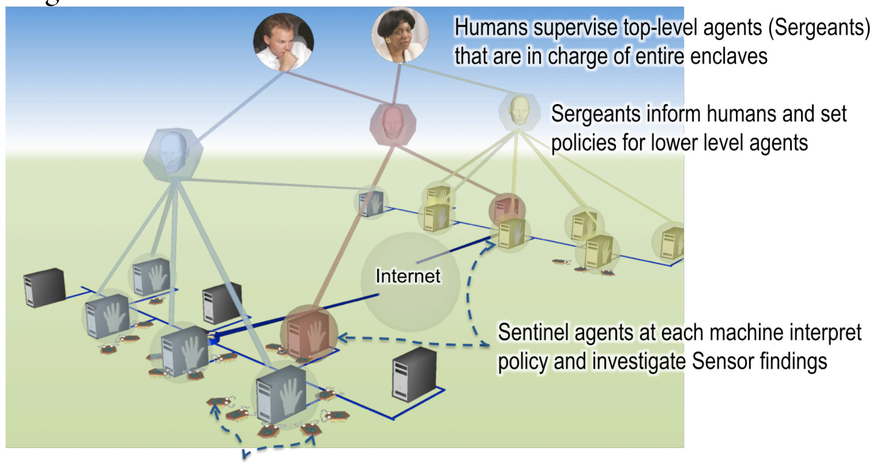
Project goals: define and prototype a security layer underlying GENI to allow providers of the system to collaboratively defend against attacks and misuse of GENI resources. Investigate reporting requirements that GENI needs to provide to support certain networking and security experiments.

Method: use decentralized security algorithms (*agents, sentinels,* and *supervisors*) that communicate between sensors, simulating the function of an ant hive.

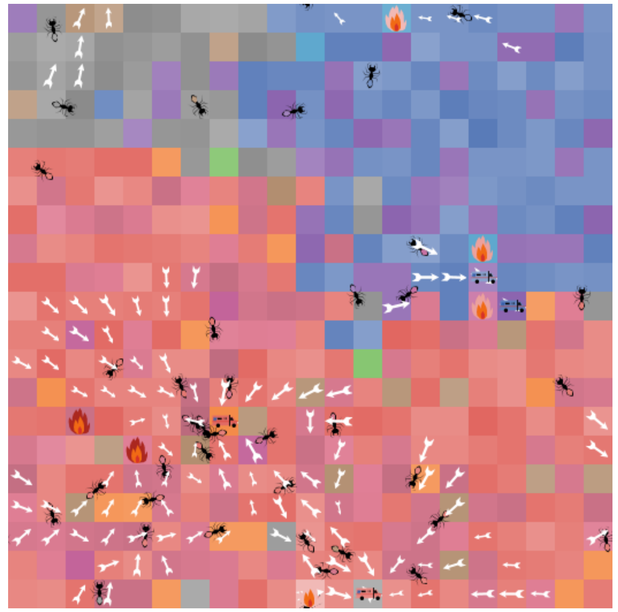
Impact:

- enable GENI to support experiments where there is communication between internal nodes (sensors or routers).
- enhance networking experiments by providing improved communication of capacity and usage information between routers.
- enhance security experiments to test the tradeoffs among different approaches to exchanging security information between sensors.

Digital Ants:



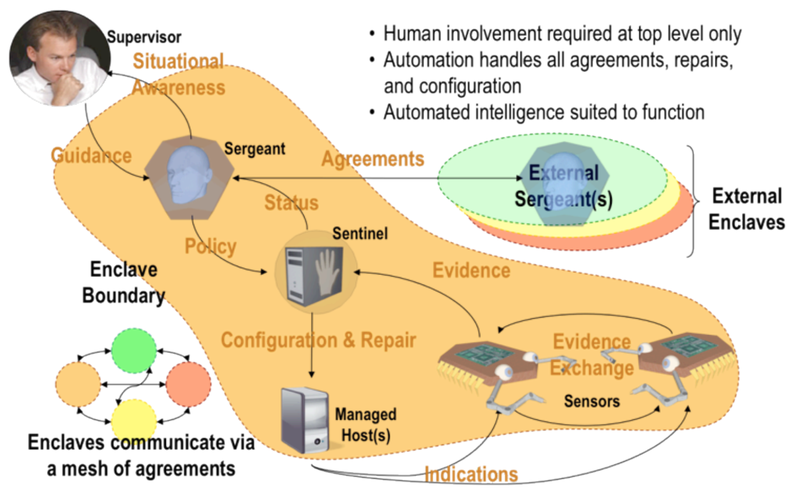
Mobile Sensor agents identify potential problems on machines and communicate via "pheromone"

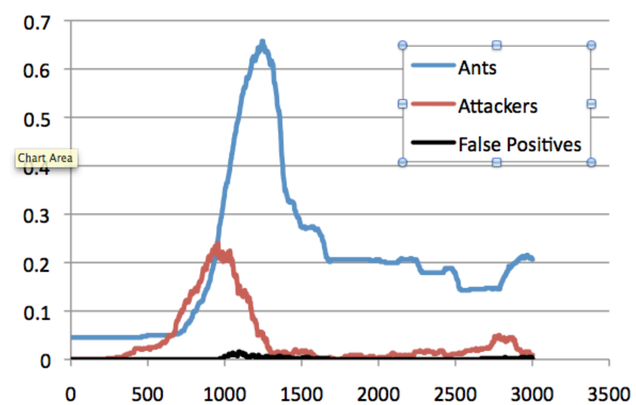


Ants are sensor agents.
Patches represent machines.
Flames are attackers.
White arrow indicate pheromone.
Ambulances indicate a patch being repaired.

Mapping to GENI Slices:

- "create_secure_slice.py" runs rspec augmented with a *Sentinel* on each GENI node and adds a *Sergeant* node to the slice, and initializes the process.
- Sentinels are told at initialization where their neighbors are.
- Sentinels have zero or more ants (sensors) active at initialization.
- *Ants* can forage, drop pheromone, linger, loose activation, and die.
- Ants move between Sentinels by message passing.
- Sentinels accept incoming ants, determine ants' state, execute their sensor function or drop pheromone, then send to next sentinel along path. No explicit state is maintained.
- New ants are created by sentinel by stochastic process.
- If a sentinel detects a significant problem, it sends a message to the sergeant.
- *Supervisors* (humans) interact with Sergeants for system status and to direct action.





This work was supported in part by the National Science Foundation and the GENI Project Office under Grant Number CNS-0940805.