U.S. DEPARTMENT OF ENERGY

PNNL-17868

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

# Annual Report for the TDMAA LDRD, FY08

GA Fink WM Maiden
JN Haack EW Fulp

September 2008

Pacific Northwest
NATIONAL LABORATORY

## DISCLAIMER



PACIFIC NORTHWEST NATIONAL LABORATORY
*operated by*
BATTELLE
*for the*
UNITED STATES DEPARTMENT OF ENERGY
*under Contract DE-AC05-76RL01830*

**Printed in the United States of America**

**Available to DOE and DOE contractors from the**
**Office of Scientific and Technical Information,**
**P.O. Box 62, Oak Ridge, TN 37831-0062;**
**ph: (865) 576-8401**
**fax: (865) 576-5728**
**email: reports@adonis.osti.gov**

**Available to the public from the National Technical Information Service,**
**U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161**
**ph: (800) 553-6847**
**fax: (703) 605-6900**
**email: orders@ntis.fedworld.gov**
**online ordering: http://www.ntis.gov/ordering.htm**

This document was printed on recycled paper.
(9/2003)

PNNL-17868

# Annual Report for the TDMAA LDRD, FY08

GA Fink WM Maiden
JN Haack EW Fulp

September 2008

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

## Project Title: Tactical Deployment and Management of Adaptive Agents (TDMAA)

**Investigators:** Glenn A. Fink (PI), Jereme Haack, Wendy Maiden, and Errin Fulp (Wake Forest University).

**Project Relevance Statement:** This research aims to develop a framework for diverse organizations within a critical infrastructure to cooperatively secure their cyber assets. TDMAA addresses critical needs of the DOE, DoD, DHS, and other federal agencies for resilient, self-defending networks, and to decrease time between attack onset and remediation.

**Introduction and Project Description:** The tremendous speed of attackers on today's networks and machines has driven defenders to rely on automation to separate misuse attempts from legitimate use of cyber resources. The ultimate cyber defense objective for many is a completely autonomous system that defends computer resources in the background, allowing normal business to proceed unobstructed. But in the final analysis, humans will always be responsible for the actions of their machines. Thus, it is critically important that humans be able to monitor and guide these systems, particularly when they are used to protect safety-critical systems and critical infrastructures.

TDMAA provides a framework for cooperative cyber defense for groups of interdependent enclaves via a society of humans and autonomous adaptive software agents. The enclaves in an infrastructure share common overarching operational goals and may share physical equipment, but generally they do not share policies, etc. Examples of this type of infrastructure include the computers and networks supporting our national electric power grid, the distributed, heterogeneous computing collaboratories used in open science, or the computer equipment used to support partner countries in coalition warfare. We seek to discover ways that humans can exert supervisory influence on the system while retaining the rapid, adaptive response of the system.

**Results and Accomplishments:** TDMAA has adapted ideas from social insect behavior models for cyber defense in a digital environment and developed heuristic models to discover the parameters that influence the behavior of these systems. We have conducted sensitivity testing to determine which parameters are the most influential to the overall, long-term system behavior. We have discovered two lever parameters that serve as goals for supervising the behavior of societies of agents: target activation level and target crowding level. By adjusting these parameters, human supervisors can change the behavior of all agents, system-wide.

Our accomplishments in FY 2008 include three publications in progress, external collaborations with Naval Postgraduate School, Wayne State University, and Wake Forest University. We have presented a poster at VizSEC '08, an invited talk on autonomic computing at USENIX LISA '07, and a talk on adaptive deception at Phoenix Challenge (Spring 2008). We plan to present a poster on our collaborative work with Wake Forest University at the USENIX LISA '08 conference.

In FY08, we more carefully defined the entire framework and each relationship contained in it. We analyzed system failure modes and inherent weaknesses in our algorithms in an effort to understand the ideal conditions and constraints for using this approach to cyber security and devised an initial approach for trust management to mitigate these failure modes.

We have made progress both in the mobility of sensors and their ability to classify data. We updated the mobility simulation to use ant colony algorithms and three kinds of indicators as opposed to the single indicator model used last year. The simulation led us to create an algorithm to translate the discontinuous geography of cyber space into a more continuous space that will work for ant colony algorithms. A screenshot of the revamped simulation is shown in Figure 1.

Finally, we have done some preliminary automated analysis work using using support vector machines (SVMs) to predict/detect failures at nodes. We took syslog data from PNNL's 1,100 node MPP2 cluster computer and used it to detect disk failures with 80% accuracy within a 48-hour window. This approach can use the same techniques train classifiers to predict or detect events of cyber security interest.

**Path Forward:** The TDMAA project has five major goals for FY 2009:

1. To field a prototype CID system on a cluster or grid computer and study its aptitude for

discovering and resolving specific types of cyber attack.

2. To better define the hierarchy of agents and their interactions with humans.
3. To incorporate trust management into the agent hierarchy.
4. To publish papers to capture the bulk of the work done on TDMAA over its three-year life span.
5. To engage clients that would benefit from our research so that the work may continue as a funded project in out years.

Accomplishment of these goals is critical to the success of this research and will also help to ensure that cyber defenders are equipped with tools to match the growing threat from network-based attacks.

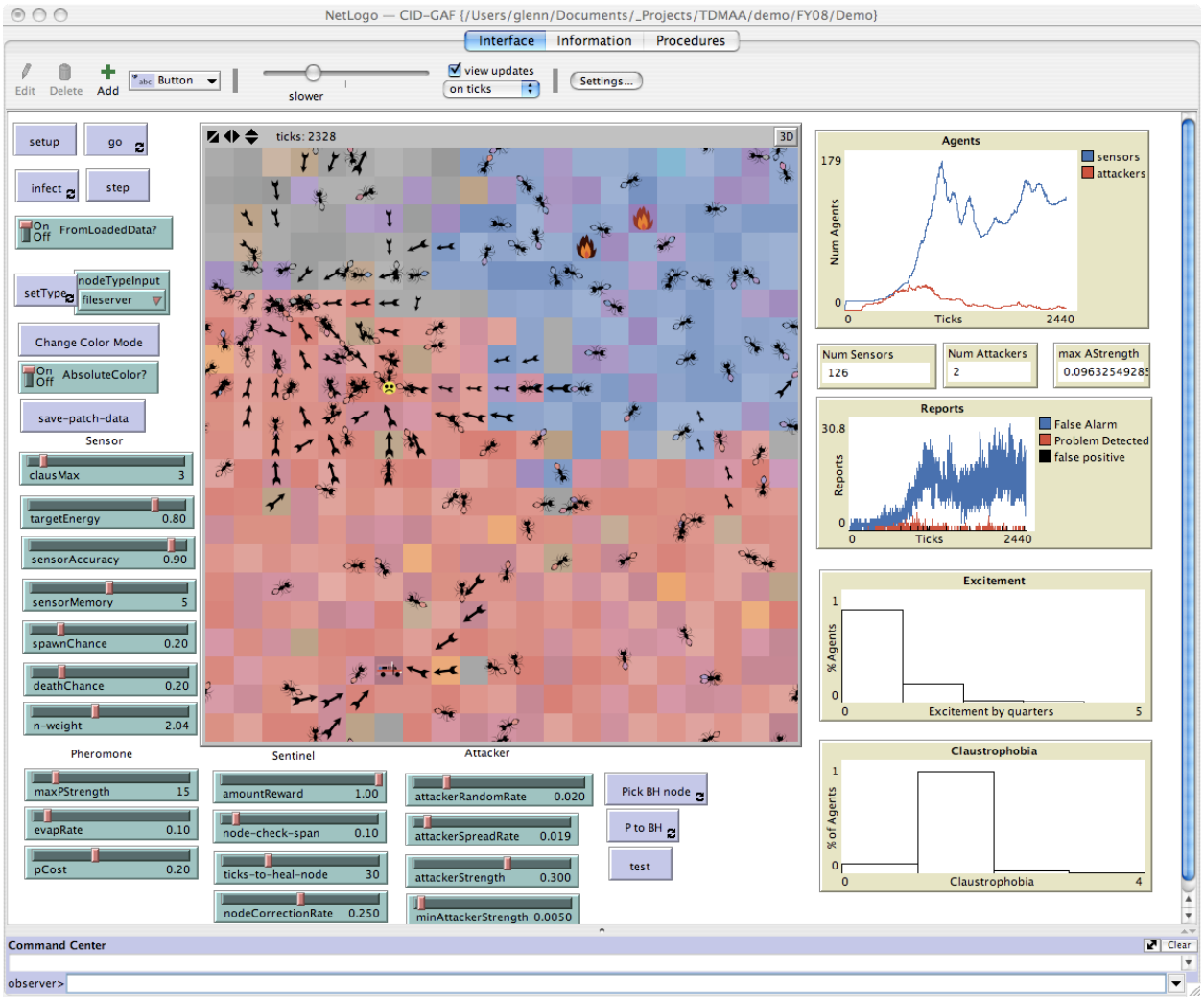


**Figure 1: TDMAA simulation model using ant-colony algorithms and multiple data sources.**