PNNL-17094

Pacific Northwest
National Laboratory
Operated by Battelle for the
U.S. Department of Energy

Tactical Deployment and Management of Autonomous Agents, LDRD Final Report

GA Fink

November 2007

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

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)

FY07 LDRD Annual Report

Project Title Tactical Deployment and Management of Adaptive Agents

Investigators Glenn Fink

Project Relevance Statement

The goal of this project is to enable system defenders within organizations that are members of a larger infrastructure to cooperatively and adaptively defend their computer systems against dynamical cyber attackers. At a high level, the expected outcome of this research is to design a hierarchical framework for software agents to defend an organization autonomously while remaining responsive to human-provided policy guidance and human-initiated behavioral incentives.

Introduction and Project Description

Our approach makes humans an intrinsic part of the solution, engaging humans without requiring their direct control. Most other approaches concentrate on the intelligence of the technology while ignoring the need for human supervision. Our approach also concentrates on the difficult problem of enabling diverse organizations within an infrastructure to cooperate in an adaptive cyber defense. All other known approaches are targeted at single organizations or enterprises.

We defined a four-level hierarchy of humans and intelligent software agents called the Cooperative Infrastructure Defense (CID) that can be used to defend an organization that participates in an infrastructure. The resulting symbiotic hierarchy has a few human *supervisors* at the top level and at least three levels of agents beneath them. At the top, each human is responsible for a small number of *organizational units* (a set of computer resources on the same local network owned by the same organization). The lowest level variety of intelligent agents, called *Sensors*, are very simple, diverse, cooperating agents that roam randomly around the computers of an organizational unit looking for symptoms of problems that they are programmed to find.

Results and Accomplishments

The emphasis in FY 2007 was on exploring adaptive agent technologies to identify appropriate ways that a human tactician can interact with agents to defend cyber systems. The outcome significantly advanced our understanding of the scientific and technology challenges needed to integrate adaptive systems with predictive defense within infrastructures. Additionally, we have advanced solutions that address some of these challenges.

For the underlying intelligent software agent technology, we selected the Holland Classifier, a program that learns to perform a certain task by interacting with a partially unknown environment that provides feedback in the form of numerical reward. The agents use temporal difference learning to estimate the goodness of candidate behaviors in terms of expected reward. The goal is to define boundaries for the agents and design reward systems that can be manipulated more naturally by human supervisors.

During FY07, we built four prototypes of this system: two for the purpose of understanding the dynamical behavior of Sensors, and two to investigate alternative models of Sensor behavior based on social insect communication (e.g., ants and bees). We produced a study of the behavior of the Ant Model that showed how Sensors can control invading attackers via emergent, self-organizing behavior that arises from simple rules. Our single most important finding was the discovery of two factors that control Sensor population levels without external control. We published a paper on autonomic computing related to this work and gave several public presentations. Also, this work gained the interest of DARPA as a potential program.

In the coming fiscal year, FY08, we plan to survey other biological and economic models and construct a simulation with greater mathematical rigor and higher simulation fidelity. We will use this model to examine the underlying complex behaviors of the system and their interactions with one another. Our goal is to more directly address the concerns of the nation's critical power infrastructure and determine the potential impacts and pitfalls of actually fielding such a technology.

Figure Caption: **CID demonstration testbed for the Ant Model**