REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
24-08-2021	Final Report	1-Apr-2021 - 31-Aug-2021

4. TITLE AND SUBTITLE
Final Report: Verification and Synthesis of Assured Dynamic Cyber Defense with Deception and Counter Deception

5a. CONTRACT NUMBER
W911NF-21-1-0114

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Worcester Polytechnic Institute
100 Institute Rd.

Worcester, MA 01609 -2280

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
78495-CS.5

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Jie Fu
UU	UU	UU	UU		19b. TELEPHONE NUMBER 352-392-0912

RPPR Final Report
as of 19-Oct-2021

Agency Code: 21XD

Proposal Number: 78495CS **Agreement Number: W911NF-21-1-0114**
INVESTIGATOR(S):

Name: Jie Fu
Email: fujie@ufl.edu
Phone Number: 3523920912
Principal: Y

Organization: **Worcester Polytechnic Institute**
Address: 100 Institute Rd., Worcester, MA 016092280
Country: USA
DUNS Number: 041508581 EIN: 042121659

Report Date: 30-Sep-2021 Date Received: 24-Aug-2021
Final Report for Period Beginning 01-Apr-2021 and Ending 31-Aug-2021
Title: Verification and Synthesis of Assured Dynamic Cyber Defense with Deception and Counter Deception
Begin Performance Period: 01-Apr-2021 **End Performance Period:** 10-Sep-2021
Report Term: 0-Other

Submitted By: Jie Fu Email: fujie@ufl.edu
Phone: (352) 392-0912

STEM Degrees: 0 **STEM Participants:** 3

Major Goals: The project consists of three key goals:

Thrust I: Develop a game-theoretic modeling framework for cyber networks equipped with dynamic defense and deception mechanisms. The modeling framework will enable the development of novel algorithms for verifying and synthesizing proactive defense systems given security specifications in high-level formal logic;
Thrust 2: Develop game-theoretic synthesis methods for constructing assured active cyber defense strategies with novel deception mechanisms;
Thrust 3: Develop effective dynamic defense strategies against learning-based attacks in repeated interactions.

Accomplishments: 1) Major activities:

Activity 1: Formal modeling and verification of proactive cyber defense with moving target defense and deception

This activity is closedly related to the proposed research tasks I-1 and I-2.

- We developed a formal security model that captures the attack decision-making problem in a cyber network equipped with time-based or event-triggered randomization. We showed that due to network randomization, an attack action will have probabilistic outcomes. Because of such unpredictability and uncertainty, the attack success probability can be reduced.

- Based on the formal security model, we investigated the verification problem. That is, given a randomization protocol as proactive network defense and intrusion detection sensors, how shall the attacker optimally plan his multi-stage attacks to achieve an attack objective in linear temporal logic, while evading detection? The attack policy computed herein can provide information for network defenders to assess the effectiveness of the moving target defense.

- Based on the formal verification and attack synthesis, we then investigated how to optimally allocate two types of sensors for attack detection and mitigation. Specifically, we consider 1) intrusion detection sensors, which are observable by the attacker but randomly and dynamically (re)-allocated in the network; 2) stealthy sensors, which are not observable by the attacker. The stealthy sensors correspond to a class of cyberdeception techniques called "honey patching", with which the defender patches a vulnerability, but from the attacker's perspective, the vulnerability is unpatched. Any exploitation of a honey-patched vulnerability will trigger the detection of an attacker.

- We analyzed the optimal sensor allocation problem with these two types of sensors and developed mixed-integer linear programming to solve the allocation of (attacker observable) sensors and (attacker unobservable) stealthy sensors.

Finally, we demonstrated the optimality of the proposed method in a small-scale network. We are currently investigating scalable solutions to larger networks.

We are planning to submit this work to a network security conference. Our preliminary results are detailed in the technical report, submitted in the Other Products section.

Activity 2: Qualitative planning with active sensing against reactive sensor attacks

In this activity, we investigate the impact of cyber attacks on autonomous systems. This study is motivated by the discussion with our ARL collaborators that many cyberattacks aim to not only compromise the network but also disrupt the mission of an autonomous system that depends on the network for mission-critical information. Therefore, we analyze a class of imperfect information games that capture the interaction between an autonomous agent, who aims to carry out missions using a distributed cyber sensor network, while a cyber attacker purposefully jams the sensors within the network so as to prevent the agent from completing its mission. We analyzed the case of an attack-unaware agent who misperceives the sensor attacks as probabilistic sensor failures and showed that the cyber attacker can exploit this unawareness to achieve his attack objective.

- We modeled such an adversarial interaction using a formal model--a reachability game with partially controllable observation functions. A zero-sum, reachability game means that the agent aims to reach a subset of target states while the attacker is to prevent the agent from reaching the target set. The results from reachability games extend to a subclass of games with syntactically co-safe linear temporal logic objectives.

- We extended probabilistic model checking in partially observable games to answer, from which set of information states, the agent has an observation-based control and active sensing strategy that ensures the task can be achieved with probability one given probabilistic action outcomes and probabilistic sensor failures.

- We then analyzed the attacker's game to compute, given the strategy from an attack unaware agent, when to attack which sensors so that the agent cannot achieve the task with probability one, even the agent believes it can do so.

- We demonstrated the results with a partially observable game and show the cost of being attack unaware in the presence of cyber sensor network attacks.

This work is our preliminary result to investigate the consequence of cyber attacks for security and safety in cyber-physical systems. We have one paper accepted by IEEE Conference on Decision and Control 2021 and attached it in the Products section. Our ongoing work is to investigate the formal synthesis of attacker-aware defense strategies in this class of partially observable games with partially controllable observations. We will also move from toy examples in this conference paper to more realistic robotic and sensor network applications for experimental validation in the journal extension.

2) Specific objectives:

In this reporting period, our specific objectives are mainly on the formal modeling and verification of cyber defense systems and defense/attack objectives in temporal logic, stated in the proposed research Thrust I. Our focus is on proactive defense, where the goal of the cyber defense is to use sensors (observable or stealthy), combined with network configuration randomization, to enable early detection of the attacker and thereby protect critical network infrastructure. The research activities are closely related to the objectives proposed in research Task I-1, I-2.

3) Significant results:

[1] A. N. Kulkarni, S. Han, N. O. Leslie, C. A. Kamhoua, and J. Fu, “Qualitative Planning in Imperfect Information Games with Active Sensing and Reactive Sensor Attacks: Cost of Unawareness,” presented at the submitted to IEEE Conference on Decision and Control, May 2021. Accessed: Jul. 06, 2021. [Online]. Available: http://arxiv.org/abs/2104.00176

[2] L. Li, S. Han, N. O. Leslie, C. A. Kamhoua, and J. Fu, "Optimal Sensor Allocation for Proactive Cyber Defense with Deception", Technical report, 2021.

Training Opportunities: During this reporting period, we have involved three Ph.D. students to perform related research. The students have learned fundamental definitions of attack graphs and related graphical security models and the software tools to generate attack graphs from real networks using MulVal. The students have been directly involved in the algorithm development and experimental validation for major research activities.

Results Dissemination: Nothing to Report

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Through this reporting period, we have collaborated with Dr. Charles Kamhoua from the Army Research Lab. The software and code developed in major activities will be shared with ARL after testing and proper documentation.

PARTICIPANTS:

Participant Type: PD/PI
Participant: Jie Fu
Person Months Worked: 4.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Abhishek N. Kulkarni
Person Months Worked: 4.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Lening Li
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Sumukha Udupa
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

RPPR Final Report
as of 19-Oct-2021

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 3-Accepted
Conference Name: IEEE conference on Decision and Control
Date Received: 24-Aug-2021 Conference Date: 13-Dec-2021 Date Published: 13-Dec-2021
Conference Location: Austin, Texas, USA.
Paper Title: Qualitative Planning in Imperfect Information Games with Active Sensing and Reactive Sensor Attacks: Cost of Unawareness
Authors: Abhishek N. Kulkarni, Shuo Han, Nandi O. Leslie, Charles A. Kamhoua, Jie Fu
Acknowledged Federal Support: **Y**

Partners

,

Shuo Han, University of Illinois Chicago, Illinois, USA.Charles A. Kamhoua, Army Research Laboratory, Maryland, U

I certify that the information in the report is complete and accurate:
Signature: Jie Fu
Signature Date: 8/24/21 4:10PM

The accomplishments in this project period are concluded in “Accomplished” section. The main algorithms and figures/charts are included in the our conference paper [1] and technical report [2], which are uploaded into the “Product” section of this report.

[1] A. N. Kulkarni, S. Han, N. O. Leslie, C. A. Kamhoua, and J. Fu, “Qualitative Planning in Imperfect Information Games with Active Sensing and Reactive Sensor Attacks: Cost of Unawareness,” presented at the submitted to IEEE Conference on Decision and Control, May 2021. Accessed: Jul. 06, 2021. [Online]. Available: http://arxiv.org/abs/2104.00176

[2] L. Li, S. Han, N. O. Leslie, C. A. Kamhoua, and J. Fu, "Optimal Sensor Allocation for Proactive Cyber Defense with Deception", Technical report, 2021.