FULL PROPOSAL

ARL BAA W911QX-19-R0044

Title:
SCRAMBLE: Secure, Real-Time Decision-Making for the Autonomous Battlefield

Proposer (PI):
Saurabh Bagchi
School of Electrical and Computer Engineering
Purdue University
465 Northwestern Ave., West Lafayette, IN, 47907
Ph: 1 (765) 494-1741 || E-mail: sbagchi@purdue.edu

Co-PIs:
Somali Chaterji, Mung Chiang, David Inouye
Purdue University

Prateek Mittal
Princeton University

Topic 2: AI/ML Research for Air/Ground Reconnaissance

Publicly Releasable Project Abstract

The battlefield of the near and the far future will involve autonomous operations among multiple cyber, physical, and kinetic assets, together with interactions with humans. Such autonomous operation will rely on a pipeline of machine learning (ML) algorithms executing in real-time on a distributed set of heterogeneous platforms, both stationary and maneuverable. The algorithms will have to deal with both adversarial control and data planes. The former means that some of the nodes on which the algorithms will execute cannot be trusted and have been compromised for leaking information or violating the integrity of the results. An adversarial data plane means that the algorithms will have to operate with uncertain, incomplete, and potentially, maliciously manipulated data sources. This project will design secure algorithms that can provide probabilistic guarantees on security *and* latency, under powerful, rigorously quantified adversary models, moving away from the trend of one-off security solutions for specific attack vectors. The project will provide a robust, scalable, and usable software suite that can execute on today's standard and custom execution platforms plus on ARL CISD's (Computational and Information Sciences Directorate) autonomous battlefield testbed.

The project will make fundamental research contributions under three pillars—*robust adversarial algorithms*, *interpretable algorithms* aiding the trust of the warfighter on the results of the autonomous algorithms, and *secure, distributed execution* of the autonomy pipeline among multiple platforms.

The research contributions in these three pillars will combine to achieve the end deliverable of secure-by-design autonomous algorithms that can operate under the constraints, and uncertainties, of a battlefield environment. The instantiation will be in a prototype software system called SCRAMBLE (**Se**C**ure** **R**eal-time Decision-Making for the **A**utono**M**ous **B**att**LE**field). The proposed work will leverage significant current work by various members of the team, individually and jointly, on security, distributed algorithms, and machine learning, part of which is joint work with ARL. The project will address part of two themes underlined in the 2018 National Defense Strategy "Sharpening the American Military's Competitive Edge", namely, C4ISR and advanced autonomous systems. This project will provide a critical building block for introducing *secure autonomy* in today's and emerging C4ISR workflows.