COVER PAGE

SBIR Project -- ARMY-2023-AIWADE			
Project Name	AI-driven Wireless Attack Detection and Escape (AI-WADE)		
Topic No.	A234-007 Artificial Intelligence (AI)/ Machine Learning (ML) Open Topic		
Project No	ARMY-2023-AIWADE		
Contract No	W5170123C0145	**Project Type**	SBIR Phase I
Report Type	Non-Proprietary Project Summary Report		
Period Covered	08/15/2023 – 11/15/2023		
PI	Dr. Sastry Kompella Chief Scientist, Nexcepta 301-693-7616 skompella@nexcepta.com		
Contract POC	ASA(ALT) Applied SBIR Contracting Center of Excellence (CCOE) – **SAAL-ZT** Sarah Abdul-Wahab, Contract Specialist Email Address: Sarah.a.abdul-wahab.civ@army.mil Robert Waible, Contracting Officer Email Address: robert.c.waible.civ@army.mil	**TPOC**	DEVCOM Army Research Lab, FCDD-RLA Ananthram Swami, Technical Point of Contact (TPOC) Phone: 301-394-2486 Email: ananthram.swami.civ@army.mil
Security Classification	Unclassified		

DISTRIBUTION STATEMENT A: Approved for Public Release. Distribution is Unlimited.

The summary report should not exceed 700 words and must include: the technology description; anticipated Department of Defense (DoD) and/or non-DoD customers; the plan to transition the SBIR developed technology to the customer; anticipated applications/benefits for the Government and/or private sector use; and an image depicting the developed technology.

1 PHASE I PROJECT SUMMARY

Technology Description: Spectrum battlefield is characterized by a complex multi-domain environment with fast and unknown dynamics. Wireless channel, network topology, user mobility and traffic, and interference effects, which includes in-network and out-network interference as well as adversarial jamming, changes over time. Conventional statistical and rule-based methods cannot be effectively applied for attack detection and prediction due to the complexity of the spectrum environment. Deep Learning (DL), particularly Deep Reinforcement Learning (RL) has emerged as a powerful means for spectrum awareness by learning from and adapting to spectrum dynamics. However, DL models can forget the behavior and the appropriate responses to a known threats as they learn to adapt to a new unseen type of wireless threat.

Continual learning is a type of learning solution that has been developed mainly in the computer vision domain to continuously learn and acquire new skills building on previously acquired knowledge. The goal of AI-WADE is to develop a wireless network security solution with continual RL capabilities that can learn on-the-fly the appropriate response to a jammer and does not suffer from catastrophic forgetting. During Phase I, we have developed the system architecture and the simulation environment along with reinforcement learning algorithms that are applied to relevant scenarios for AI-WADE system.

Figure 1 shows the AI-WADE system. There are blue force communications nodes and adversarial nodes within the area of interest. Each blue force node has an RL agent. It first senses the spectrum, then detects and classifies over-the-air signals. The adversarial nodes jam channels with varying jamming patterns with certain power budgets. The goal of a blue force node is to determine the appropriate transmit parameters which maximizes its operational efficiency. Its reward function is designed to reflect this goal in decision making. Each agent uses only the locally observed information without explicitly estimating the jamming patterns and parameters of the jammer in advance, and thus formulates a model-free problem.

Jamming patterns may change over time and the blue force nodes are expected to learn and adapt to this change in a short time. For this, we integrated a continual learning mechanism called PackNet together with reinforcement learning. PackNet “packs” multiple tasks into a single network by iteratively pruning, freezing, and retraining parts of the network at task change. It is closely related to progressive neural networks, developed in the RL context and it does not suffer from catastrophic forgetting while allowing beneficial transfer of knowledge of past tasks to the new ones (called as forward transfer). For Phase I, we will leverage and adapt publicly available open-source implementation of PackNet algorithm in AI-WADE project.

Anticipated Applications / Benefits: AI-WADE has significant potential for anti-interference application in areas such as perimeter security, border patrol and enterprise security. Commercial applications include detection and subsequent evasion of rogue Wi-Fi, 5G/6G cellular base stations and drone/UAS activities in protected areas. AI-WADE can enhance Environmental Sensing

Capability (ESC) sensors used in CBRS bands for spectrum coexistence between military and 5G commercial systems.

Anticipated DoD and Non-DoD customers: AI-WADE provides state-of-the-art wireless security solution against smart jammers. Current solutions are based on statistical and rule-based methods and often lack the prediction component for wireless threats. AI-WADE is complementary to other vendor solutions and provides a flexible integration path. Anticipated customers include dual use cases with proper customization to 5G/6G and IoT market needs by following the industry standards and developing the necessary APIs for hassle-free integration for vendors. The SDR implementation and field experimentation in future phases will pass the main hurdle for the acceptance of our technology with high TRL by both Government and commercial customers.

SBIR Transition Plan: Our strategy to transition our SBIR technology includes: (i) establishing close relationships with the transition PMs on the government side and of the large primes managing the transition programs of record; we have identified program managers from C5ISR and initiated the transition discussion with them (ii) establishing transition goals/requirements and integrating them into our Phase II project milestones; (iii) working towards TRL 5+ by the end of Phase II and using internal R&D as needed to meet this goal; and (iv) identifying contract vehicles such as IDIQs and BAAs that will be needed to support the transition.

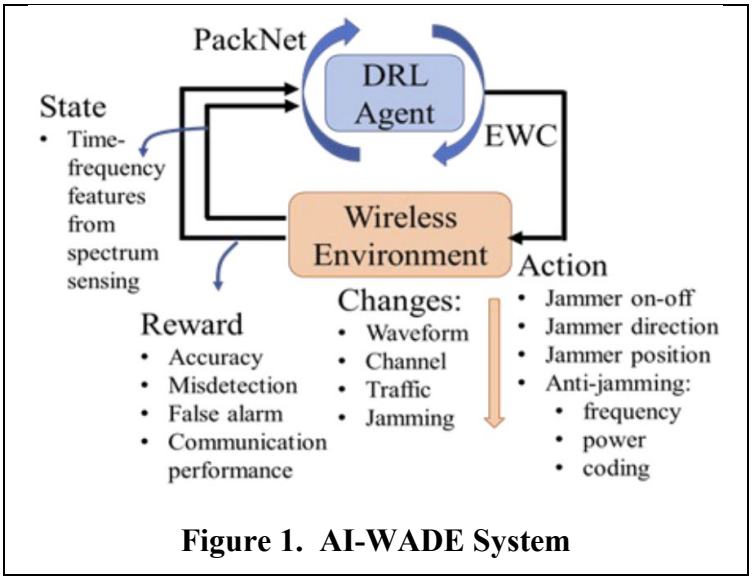

Figure 1. AI-WADE System