Cyber Analytics Researcher

Date: Sep 7, 2017
Location: MA, US

Group 58—Cyber Analytics and Decision Systems

The U.S. Government faces serious threats from sophisticated, evolving cyber adversaries who seek to access, compromise, and disrupt systems and the missions they support. The Cyber Analytics and Decision Systems Group strives to improve the security of these government systems through the development and deployment of innovative cyber security solutions using sound scientific and engineering principles and methodologies. The group develops quantitative threat models, metrics, and prototypes for securing current and future systems; novel Big Data analytics for discovery, characterization and prediction of cyber behavior; and improvements to operational cyber systems that enhance resilience and effectiveness. In each of the group's research and development (R&D) areas, emphasis is placed on realistic data and rigorous experimental evaluation of techniques. Projects are carried out by small, focused, cooperative teams that succeed together by participating in all phases of technical solution development, including systems analysis, innovative solution design, system architecture, solution prototyping and field-testing, and final technology transfer to Department of Defense (DoD) and Intelligence Community (IC) sponsors or industry. The Cyber Analytics and Decision Systems Group comprises computer scientists, mathematicians, machine learning researchers and practitioners, system analysts, software developers and security architects who firmly believe they can improve the security of the nation.

Cyber Analytics Researcher:

The Group seeks creative researchers and tool-builders to join our interdisciplinary team in driving intellectual and technical innovation in the growing field of big data cyber analytics. The successful candidate will work with a team of researchers to develop algorithms and analytics for discovery and characterization from voluminous and noisy data. This work will support all aspects of computer network operations and security, including intelligence, situational awareness, and decision support. Research will involve data mining, machine learning, natural language processing, statistical modeling, and software development to characterize cyber systems and user behavior at multiple scales and multiple levels of abstraction. Results will impact programs of national importance and be published in academic conferences and journals.

Requirements:

PhD in Applied Mathematics, Statistics, Computer Engineering, Computer Science, or a related field. In lieu of a PhD, an MS in a similar field and 3+ years of work experience will be considered. Must be able to design, develop, test, and analyze complex models and analytics to support national challenges. Ability to demonstrate effective communication skills with team members, managers and government sponsors is essential. Experience with machine learning, statistical modeling, user behavior modeling, data mining, and/or computational intelligence is required.

Desired skills:

Knowledge of Matlab, R, Java, or Python is highly desired, as is experience with Hadoop, MapReduce, or related big-data architectures. Experience with any combination of the following is desired: computer and network security, simulation modeling, cyber threat modeling, game theory, user behavior modeling, natural language processing, agent-based systems, visualization, and risk assessment. Strong written communication skills are highly desired, and candidates with a demonstrated publication history will be given strong consideration.

MIT Lincoln Laboratory is an Equal Employment Opportunity (EEO) employer. All qualified applicants will receive consideration for employment and will not be discriminated against on the basis of race, color, religion, sex, sexual orientation, gender identity, national origin, age, veteran status, disability status, or genetic information; U.S. citizenship is required.