A Conversation with Heena Rathore: Building secure cyber-physical systems

INNOVATION LEADERS

by Bushra Anjum

Editor’s Introduction
Ubiquity's senior editor Dr. Bushra Anjum chats with Dr. Heena Rathore, assistant professor in the Computer Science Department at Texas State University, on how cyber-physical systems (CPS) are inherently similar to humans in their reliance upon sensing their environments and making decisions. They further discuss how this similarity motivates the exploration of novel AI algorithms inspired by the principles of cognition and neuroscience to ensure the security of critical CPS infrastructure, such as IoT networks, medical devices, and connected vehicles.
A Conversation with Heena Rathore: Building secure cyber-physical systems

INNOVATION LEADERS

by Bushra Anjum

Dr. Heena Rathore is an assistant professor in the Computer Science Department at Texas State University. Academically, she has worked as an assistant professor of instruction at The University of Texas at San Antonio and as a visiting assistant professor at Texas A&M University, Texarkana. She also worked as a data scientist and program manager at Hiller Measurements in Austin. Before that, she worked as a postdoctoral researcher for the US-Qatar Joint Collaborative Project between Temple University, the University of Idaho, and Qatar University. She received her Ph.D. in computer science and engineering on a Tata Consultancy Services Research scholarship at the Indian Institute of Technology Jodhpur, India. Her research interests include cognitive AI, cybersecurity of cyber-physical systems, and biologically inspired systems. She has been the winner of several prestigious awards, including Educationist Empowering India, IEEE Region 5 Outstanding Individual Achievement Award, IEEE Central Texas Section Achievements Award, IIT Alumni Award for Recognizing Excellence in Young Alumni, MPUAT Young Engineer Award, NI Global Engineering Impact Award, and NI Graphical System Design Achievement Award. Dr. Rathore can be reached via drheenarathore.wordpress.com and Twitter @heenarathore

What is your big concern about the future of computing to which you are dedicating yourself?

Cognitive-inspired machine learning is the interdisciplinary study of mind and intelligence, embracing psychology, machine learning, and neuroscience. This study can be understood at three levels: (1) comprehending the computational standards and mental capabilities such as perception, language, memory, attention, and learning [1]; (2) building intelligent systems and computational models to reach human intelligence; and (3) working on the mathematical descriptions of the brain that contribute to behavior and develop systems to reproduce that behavior. I believe theoretical understanding, developing mathematical algorithms along with building computational models all go hand in hand. My aim is to embed these three levels in building secure cyber-physical systems (CPS).

CPS systems are seen everywhere. Be it internet of things (IoT) networks, medical devices, or connected vehicles. These systems are designed for multitasking and coordinating sensor devices to make complex decisions independently while being energy efficient. However, these systems are capable of working independently only in pre-defined conditions, which means such systems
under attack scenarios should make quick decisions for threat detection and resilient solutions. Central to achieving the aforementioned goals, the systems should also acquire the ability to continuously monitor and efficiently adapt to the environment by integrating the dynamics of the physical processes with cooperative networking. Machine learning (ML) has the potential to provide CPS with an essential feature, namely cognition, which enables the learning of complex behaviors and interactions between the components of the system. However, the present state-of-the-art machine learning models require intensive computational power and large amounts of training and quality data to operate efficiently. I particularly struggled with choosing the number of neurons, hidden layers, weights, bias, and multi-stage objective functions for different CPS applications. Therefore, my attention drew towards developing cognitive-inspired intelligence in CPS to overcome the above-listed limitations and possess the ability to multitask and coordinate at a human level to provide security, improve system performance, and enhance productivity. I dedicate myself to building such secure systems to provide better real-time autonomous solutions in a coordinated manner without external intervention. Besides this, I dedicate myself to building intelligent CPS systems to enable the capability of self-adaptation, self-healing, and self-learning just like humans.

How did your journey start with the cyber-physical systems, and how has your interest evolved since?

Human ingenuity is centered around our core abilities to dream, inspire, and communicate. Together, we learn from our past, capitalize on the present, and plan for the future. Rapid technology advancements have allowed us all to become connected and share information at the touch of a single button. Such an inspiration could be the catalyst for the transformation to bridge the chasm between smart machines and humans. Growing up as a child in Udaipur, India, I was deeply drawn to the field of biology, to the extent that I dreamt of becoming a physician. This deep interest in the subject matter has constantly made me wonder how we can bring such ingenuity into machines through advances in sensing, communication, and processing. Although my career took a different trajectory toward engineering, I never drifted far away from my interests. I continued to look at nature for inspiration, be it in the area of the human immune system, or how dolphins use communication and sensing to look for prey, or how ants always manage to find the shortest distance to food. I used theories and concepts from the human immune system and social psychology to develop security solutions for IoT devices. I developed a mathematical trust model inspired by social psychology for IoT devices, which were flagged as anomalous or benevolent based on the measurements they provided. Once these were flagged as anomalous, they were removed using an adaptive mathematical model inspired by the human
immune system. The models were 99 percent [more] efficient than other existing state-of-the-art ML algorithms [2]. As part of a literature survey for my research, I noticed that researchers mainly focused on advancing state-of-the-art machine learning algorithms without paying attention to the implementation and computational cost of these algorithms. Most of the research focused on running algorithms on expensive, power-hungry processors. This is especially true when these algorithms are being designed for massive CPS applications in areas such as healthcare, transportation, and smart cities. For part of my post-doc work, I implemented a multi-layer perceptron model on FPGA [field-programmable gate array] to provide access control, classification, and predictions of the stimulations for medical devices such as cardiac defibrillators, insulin pumps, and deep brain stimulators respectively. The model was 98 percent accurate and more reliable than standard machine learning algorithms for the aforementioned problems [3]. My research led to numerous awards, namely IEEE Region 5 Outstanding Individual Achievement Award, NI Global Engineering Impact Award, NI Graphical System Design Achievement Award, and others. My research work was also featured in professional and trade publications such as *Microwave Journal*, *EverythingRF.com*, and *Indian Science Journal*. Likewise, journalists of major newspapers, such as the *Financial Express*, *Science Reporter*, *Times of India*, *Economic Times*, and *India Today*, have written news stories about my original research and its significance. As a researcher what excites me the most is how, through novel approaches and interdisciplinary research, we can keep up with advancing technologies to overcome network vulnerabilities.

**What cognition and neuroscience-inspired projects are you currently leading to develop secure cyber-physical systems?**

Recently I won the NSF CRII grant for “Cooperative Neuro-Inspired Actor-Critic Model for Anomaly Detection in Connected Vehicles.” Connected vehicles (CV) are an integral part of the future of intelligent transportation systems. They utilize wireless and sensing technologies to enable communication and cooperation between vehicles and infrastructure. Nonetheless, sensor reliability and data integrity play a crucial role in these vehicles. As vehicles and infrastructures grow increasingly networked and automated, there is a pressing need to identify sensor-related malicious activities to mitigate potential safety hazards. The overarching goal of this project is to protect the CV network against anomalous sensor readings and/or malicious cyber-attacks to ensure the safety of vehicles and passengers. Intuitively, you can think of it in this way. If you are driving a car, you have years of experience to make informed decisions about the next driving action you will take. For example, if the car starts skidding, then you explore the environment to see if the road is wet or slippery. If yes, you attribute the skid to the condition of
the road. If not, you know that there is something wrong with the tire. In a span of a few seconds, you process tons of historical evidence and make informed decisions. How does an autonomous vehicle do this? How does it know the root cause of the event and take the right action? My NSF-funded research precisely aims to address this. The aim is to protect and ensure the safety of vehicles and passengers due to unauthorized modifications to vehicle-reported measurements and build the vehicle's reputation [4]. Actor-Critic Model, a type of reinforcement learning model, is one example of a neuro-inspired machine learning algorithm. They serve to provide dopamine instantiated communication and control movement. It has been studied that dopamine plays a critical role in predicting future rewards, which can help in planning and executing profitable behaviors and decisions. The underlying thrust area of my research group is to model novel algorithms based on dopamine learning to address the limitations of present challenges in connected vehicles. Broadly, this work would enable a diverse and inclusive community of scientists and engineers to work in multidisciplinary areas such as cognitive and neuroscience-inspired machine learning and CPS. Feel free to reach out if you want to know more about my research group. Let's together build a smarter and more intelligent system with learnings from us.

References

[1] Rathore, H. and Bhadauria, V. Intelligent decision making in autonomous vehicles using cognition aided reinforcement learning. IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2022.

[2] Rathore, H., Badarla, V., and Shit, S. Consensus-aware sociopsychological trust model for wireless sensor networks. ACM Trans. Sen. Netw. 12, 3 (2016).

[3] H. Rathore, H., Wenzel, L., Al-Ali, A. K., Mohamed, A., Du, X., and Guizani, M. Multi-layer perceptron model on chip for secure diabetic treatment. IEEE Access 6 (2018).

[4] Rathore, H., Samant, A., and Jadliwala, M. Tangle. CV: A distributed ledger technique for secure message sharing in connected vehicles. ACM Trans. Cyber-Phys. Syst. 5, 1 (2021).

Biography

Bushra Anjum, Ph.D., is a health IT data specialist currently working as the Senior Analytics Manager at the San Francisco based health tech firm Doximity. Aimed at creating HIPAA secure tools for clinicians, she leads a team of analysts, scientists, and engineers working on product and
client-facing analytics. Formerly a Fulbright scholar from Pakistan, Dr. Anjum served in academia (both in Pakistan and the USA) for many years before joining the tech industry. A keen enthusiast of promoting diversity in the STEM fields, her volunteer activities, among others, involve being a senior editor for ACM Ubiquity and the Standing Committee’s Chair for ACM-W global leadership. She can be contacted via the contact page bushraanjum.info/contact or via Twitter @DrBushraAnjum.

DOI: 10.1145/3570516