Synergizing Human and Machine Intelligence

A key enabler for humankind’s success across the animal kingdom has been our ability to work in teams. This critical differentiator has allowed us to leverage shared knowledge and labor in a way that has catapulted us far beyond the course of natural evolution. Today we find ourselves at the edge of a new phase of our evolution, the coevolution of humans and robots. And in order for this phase to truly reach its potential, teamwork, both robots working for humans and robots working with humans, must be redefined. My vision is to create teamwork enabling technologies for robot-robot and human-robot teams. Since communication is the keystone of teamwork, my work will strive to develop new methods and technologies for effecting and securing knowledge transfer between teams of robots and their human counterparts. Towards the future, these technologies can apply beyond robots to machines, smart devices and general artificial intelligence.

Intuitive Communication across the Human-Robot Divide

In the case of robots working with humans, communication must be intuitive. This requires exploring new methods of communication across the human-robot divide. Many important applications of the future, such as coordinated manufacturing tasks, involve humans working in tight coordination with a single robot or multi-robot teams. For these cases, efficient and unambiguous communication between the human and robot will be essential for successful task completion. My newest research area is in exploring methods for intuitive communication between humans and machines. We are currently using “thought”, where the human’s brain signals are acquired via Electroencephalography (EEG) electrodes, as a form of communication to the robot. Our objective is to detect Error-Related Potentials (ErrP) generated by the human operator’s brain in response to an error committed by our Rethink Robotics Baxter robot in a collaborative building task. These ErrP signals are unique in that they are innately produced in the human brain in response to errors committed either by the human or the agent that the human is observing. For our human-Baxter collaborative task this meant that when Baxter reached for the incorrect object, an ErrP signal from the human operator’s brain could be detected. In this way, we can use human intelligence to augment machine intelligence in a seamless manner. Our most recent results show that these brain signals can be detected in the human brain within 400ms of a robot-committed error and can be fed back to the robot to correct its behavior in a tight loop. Interestingly, we have also been able to show that the robot can actively incite these error signals in the human brain if it is unsure of its decision and requires additional feedback; all without the need for deliberate communication such as language. This points to the ability of using human brain signals for real-time active learning of a robotic counterpart.

Securing Human-Robot Systems

In the case of robots working for humans, secure communication is of utmost importance. Take the example of fleets of autonomous vehicles that are poised to become man’s most ubiquitous robot. Communication in the wrong hands can turn an autonomous car from the world’s safest vehicle to the world’s deadliest vehicle by using its on-board sensors to target human pedestrians instead of avoid them; all with a simple bit flip. In the case of autonomous Uber rides, a malicious user could “spoof”, or falsely create, several pickup requests in a desired location in order to increase demand to certain geographical regions that best suit the malicious user, while depriving other legitimate users of a fair service. Real-world systems must be prepared to deal with security breaches. Multi-robot systems are particularly vulnerable to cyber-security attacks since effective coordination between multiple robots requires trust. Traditional cryptographic schemes require additional overhead of key generation and authentication which becomes unwieldy for multi-robot teams; whose nature is very dynamic due to new agents entering and exiting the network continuously. In response to this gap in security for multi-robot systems, I secured collaboration and funding through the MIT Lincoln Labs Cybersecurity group. My resulting work develops a theoretical and experimental framework for quarantining robot systems against spoofing attacks. We achieved this by using agent’s wireless transmissions themselves, as a fingerprint to determine whether the sender was a malicious adversary. The capability of using wireless signals as “fingerprints” was our discovery; a product of a cross-field collaboration at
MIT. Demonstrating that these wireless signal fingerprints could provide provable guarantees, bounding the impact of a malicious node in a robotic network, was a paradigm shift in the way security is approached for multi-agent systems.

Contributions and Impact

My work has been published at a premier robotics conferences such as Robotics Science and Systems Gil et al. (2015c), International Symposium on Robotics Research (ISRR) Gil et al. (2015a), and the IEEE International Conference on Robotics and Automation (ICRA), as well as top communication conferences such as the ACM Special Interest Group on Data Communication (SIGCOMM) and ACM Conference on Mobile Computing and Networking Kumar et al. (2014). The presentation of my work has on multiple occasions led to invitations to appear in top impact factor journals in robots such as the International Journal on Robotics Research (IJRR) Gil et al. (2015a) and the Autonomous Robots Journal (AURO) Gil et al. (2016), an opportunity presented to works that are deemed to be amongst the best research presented at top robotics conferences. Beyond publications, my work has led to U.S. patent filings Gil et al. (2015b), Kumar et al. (2015) and a recent startup Ubiety. I have secured funding in the form of grants for this startup effort; one from the MIT Deshpande Center and one from the National Science Foundation (NSF) for financing prototype development and an in-depth market exploration for our technology. This has allowed me to take my research all the way from theory to actual deployments in realistic environments such as the MIT Career Fair. I intend to continue along the track of producing cutting-edge research and not stopping at theory but rather taking my research all the way through to impact via the creation of new centers, university-wide and national initiatives, and startups.

Future

My future research plans center around synergizing human and machine intelligence by designing new technologies that bridge, secure, and facilitate collaboration of humans and their robotic counterparts. My experience in robotics, system modeling, and communication uniquely positions me to approach this problem from an interdisciplinary angle.

Scalable Security for Tomorrow’s Human-Robot Teams While my past and current work have shown the feasibility of this vision, they have focused on only a small aspect of the problem. With regards to security in multi-robot systems I have shown that for a specific security breach, the case of spoofing, we can guarantee that analyzing the wireless signals themselves allow detection and quarantining of the offending agents. However in the case of thousands or even millions of autonomous vehicles with millions of human users, the types of security breaches that must be mitigated quickly grow in number and as a consequence, we must begin to look at new technologies for augmenting machine intelligence.

Using Human Brain Signals to Augment Machine Intelligence Harnessing human generated brain signals that are detected via EEG holds great promise in providing a very low-latency and continuous form of feedback for our robot counterparts. Most intriguing would be the development of robot systems that can read and interpret human brain signals for the purpose of refining or repairing their own behaviors. This can unlock huge learning potential for robot systems. Imagine robots being able to learn from their mistakes by eavesdropping on a human observer’s thought patterns. This is hugely beneficial for artificial intelligence since a humans thought patterns represent a system that is already fully evolved for learning from mistakes. This form of seamless communication between man and machine could translate to many realms including those studied for prosthesis. In order for a human’s perception of his prosthetic limb to morph from viewing the limb as an external agent to a natural extension of his own body, seamless communication such as what exists through the nervous system of our bodies today, must be achieved. I would be very interested in investigating ways to continue seeking and refining intuitive forms of communication between men and machines as part of my research vision.
References


