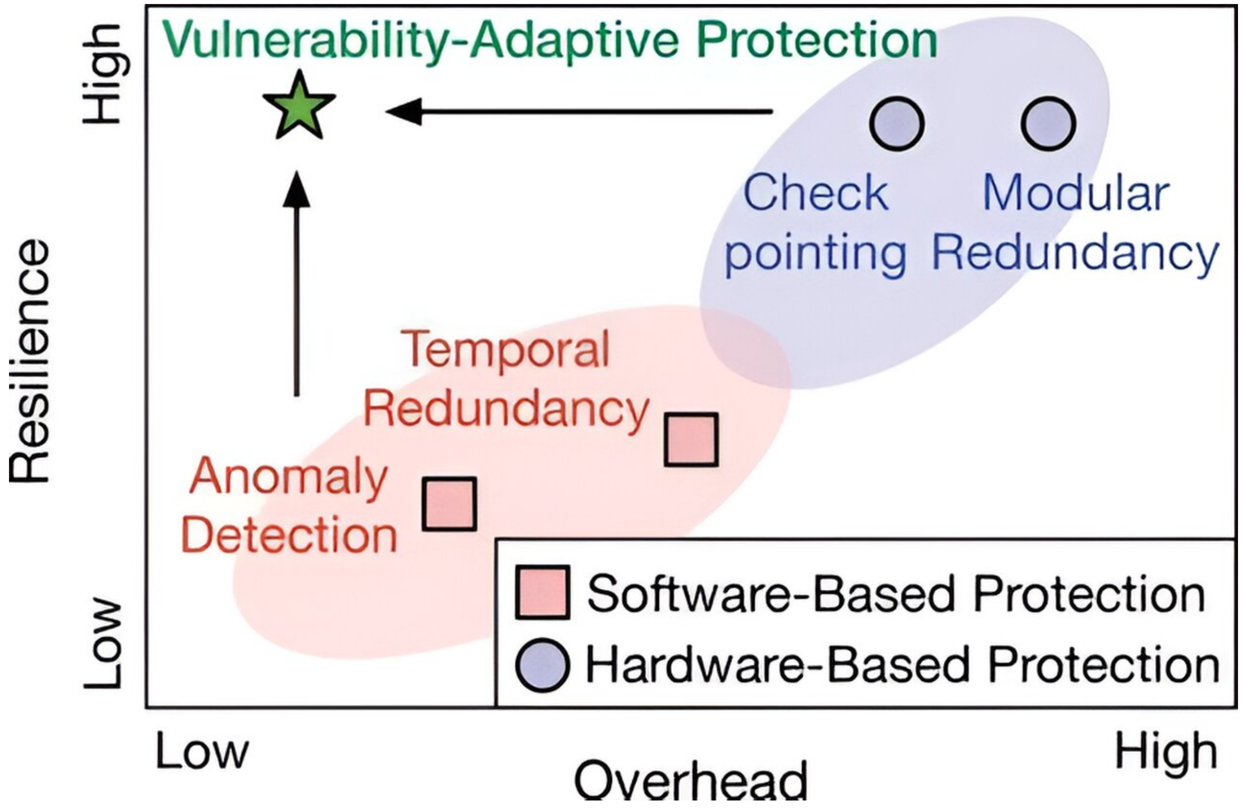
Balancing cost and reliability in autonomous machine design

October 3 2024, by Luke Auburn



Design landscape of different software and hardware-based protection techniques for resilient autonomous machines. Our proposed vulnerability-adaptive protection design paradigm co-optimizes performance, energy efficiency, and resilience. Credit: *Communications of the ACM* (2024). DOI: 10.1145/3647638

With millions of self-driving cars projected to be on the road in 2025 and autonomous drones generating billions in annual sales, safety and reliability are important considerations for consumers, manufacturers, and regulators. But solutions for protecting autonomous machine hardware and software from malfunctions, attacks, and other failures also increase costs. Those costs arise from performance features, energy consumption, weight, and the use of semiconductor chips.

Researchers from the University of Rochester, Georgia Tech, and the Shenzen Institute of Artificial Intelligence and Robotics for Society say that the existing tradeoff between overhead and protecting machines against vulnerabilities is due to a "one-size-fits-all" approach to protection. In a paper published in *Communications of the ACM*, the authors propose a new approach that adapts to varying levels of vulnerabilities within an autonomous machine system to make them more reliable and control costs.

Yuhao Zhu, an associate professor in Rochester's Department of Computer Science, says one example of a current "one-size-fits-all" approach is Tesla's use of two Full Self-Driving Chips (FSD Chips) in each vehicle—a redundancy that provides protection in case the first chip fails but doubles the cost of chips for the car. By contrast, Zhu says he and his students have taken a more comprehensive approach to protect against both hardware and software vulnerabilities and more wisely allocate protection.

"The basic idea is that you apply different protection strategies to different parts of the system," says Zhu. "You can refine the approach based on the inherent characteristics of the software and hardware. We need to develop different protection strategies for the front end versus the back end of the software stack."

For example, Zhu says the front end of an autonomous vehicle's software stack is focused on sensing the environment through devices such as cameras and light detection and ranging (LiDAR), while the back end processes that information, plans the route, and sends commands to the actuator.

"You don't have to spend a lot of the protection budget on the front end because it's inherently fault tolerant," says Zhu. "Meanwhile, the back end has few inherent protection strategies, but it's critical to secure because it directly interfaces with the mechanical components of the vehicle."

Zhu says examples of low-cost protection measures on the front end include software-based solutions such as filtering out anomalies in the data. For more heavy-duty protection schemes on the back end, he recommends things like checkpointing to periodically save the state of the entire machine or selectively making duplicates of critical modules on a chip.

Next Zhu says the team hopes to overcome vulnerabilities in the most recent autonomous machine software stacks, which are more heavily based on neural network artificial intelligence, often from end to end.

"Some of the most recent examples are one single, giant neural network deep learning model that takes sensing inputs, does a bunch of computation that nobody fully understands, and generates commands to the actuator," says Zhu. "The advantage is that it greatly improves the average performance, but when it fails, you can't pinpoint the failure to a particular module. It makes the common case better but the worst case worse, which we want to mitigate."

More information: Zishen Wan et al, The Vulnerability-Adaptive Protection Paradigm, *Communications of the ACM* (2024). DOI: 10.1145/3647638

Provided by University of Rochester

Citation: Balancing cost and reliability in autonomous machine design (2024, October 3) retrieved 4 October 2024 from https://techxplore.com/news/2024-10-reliability-autonomous-machine.html