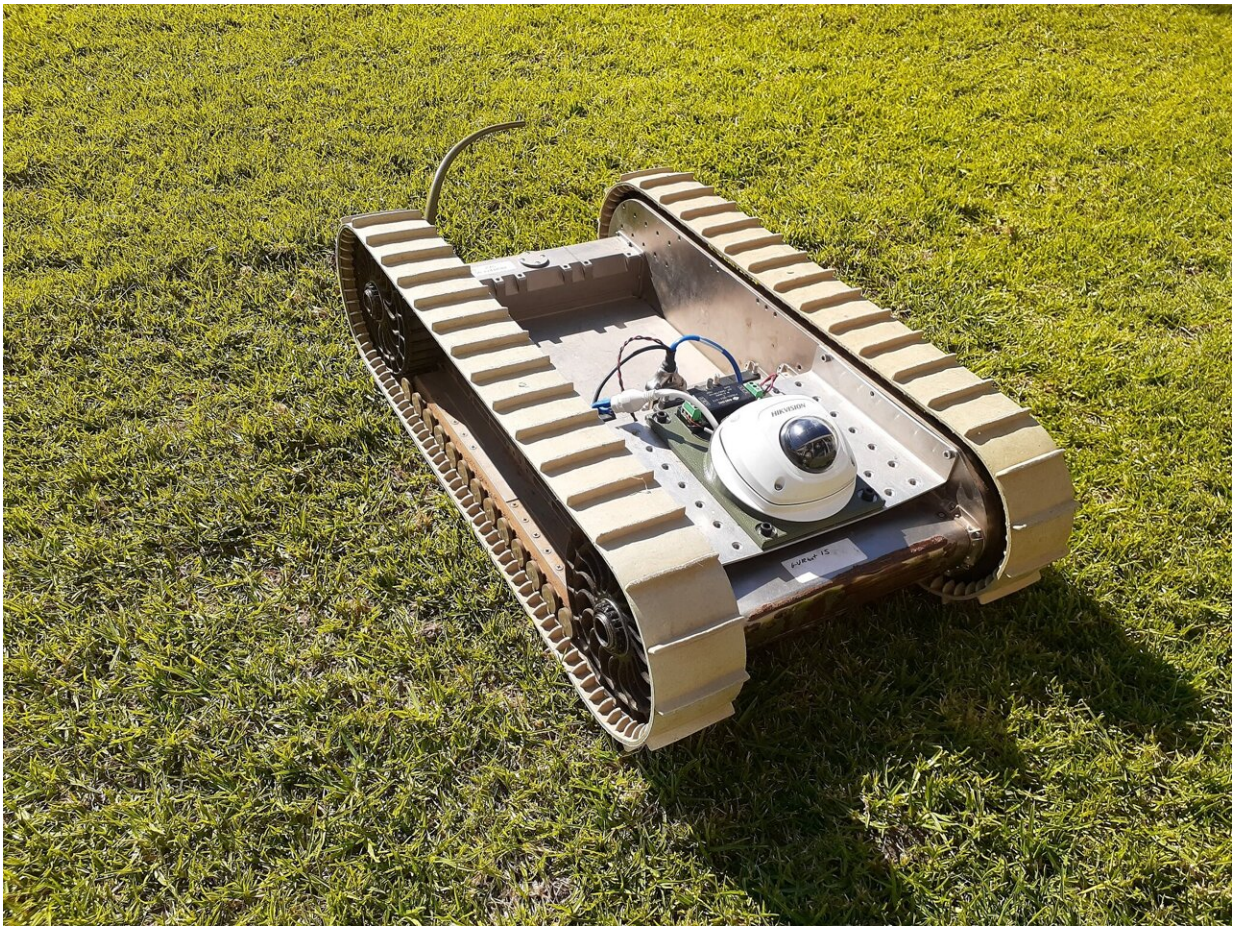
New cyber algorithm shuts down malicious robotic attack

October 12 2023



A replica of the US army combat ground vehicle used in the AI experiment. Credit: Fendy Santoso, Charles Sturt University

Australian researchers have designed an algorithm that can intercept a man-in-the-middle (MitM) cyberattack on an unmanned military robot and shut it down in seconds.

In an experiment using deep learning neural networks to simulate the behavior of the human brain, artificial intelligence experts from Charles Sturt University and the University of South Australia (UniSA) trained the robot's operating system to learn the signature of a MitM eavesdropping cyberattack. This is where attackers interrupt an existing conversation or data transfer.

The algorithm, tested in real time on a replica of a United States army combat ground vehicle, was 99% successful in preventing a malicious attack. False positive rates of less than 2% validated the system, demonstrating its effectiveness.

The results have been published in *IEEE Transactions on Dependable and Secure Computing*.

UniSA autonomous systems researcher, Professor Anthony Finn, says the proposed algorithm performs better than other recognition techniques used around the world to detect cyberattacks.

Professor Finn and Dr. Fendy Santoso from Charles Sturt Artificial Intelligence and Cyber Futures Institute collaborated with the US Army Futures Command to replicate a man-in-the-middle cyberattack on a GVT-BOT ground vehicle and trained its operating system to recognize an attack.

"The robot operating system (ROS) is extremely susceptible to data breaches and electronic hijacking because it is so highly networked," Prof Finn says.

"The advent of Industry 4, marked by the evolution in robotics, automation, and the Internet of Things, has demanded that robots work collaboratively, where sensors, actuators and controllers need to communicate and exchange information with one another via cloud services.

"The downside of this is that it makes them highly vulnerable to cyberattacks.

"The good news, however, is that the speed of computing doubles every couple of years, and it is now possible to develop and implement sophisticated AI algorithms to guard systems against digital attacks."

Dr. Santoso says despite its tremendous benefits and widespread usage, the robot operating system largely ignores security issues in its coding scheme due to encrypted network traffic data and limited integrity-checking capability.

"Owing to the benefits of deep learning, our intrusion detection framework is robust and highly accurate," Dr. Santoso says. "The system can handle large datasets suitable to safeguard large-scale and real-time data-driven systems such as ROS."

Prof Finn and Dr. Santoso plan to test their intrusion detection algorithm on different robotic platforms, such as drones, whose dynamics are faster and more complex compared to a ground robot.

More information: Fendy Santoso et al, Trusted Operations of a Military Ground Robot in the Face of Man-in-the-Middle Cyber-Attacks Using Deep Learning Convolutional Neural Networks: Real-Time Experimental Outcomes, *IEEE Transactions on Dependable and Secure Computing* (2023). DOI: 10.1109/TDSC.2023.3302807