SAND2017-7534C

The Center for Cyber Defenders

Expanding computer security knowledge

Eratosthenes

Samuel Richter, Missouri University of Science and Technology , M.S. Comp Sci
Frank Conlon, Texas Tech University, PhD Computer Science

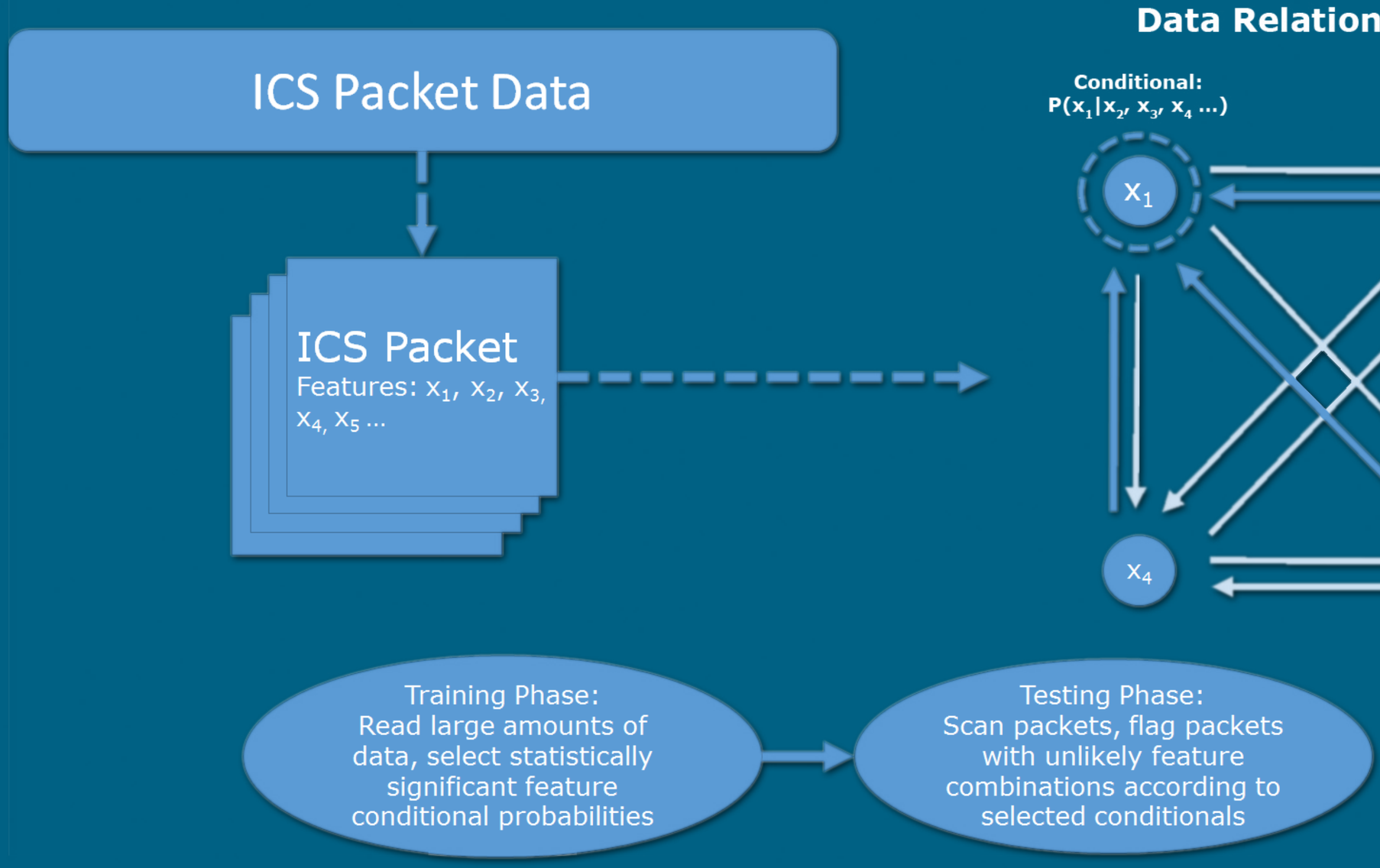
Project Mentor: John Mulder, Org. 5828

Problem Statement:

Industrial Control Systems (ICS) are specialized computer systems used to monitor and control modern industrial infrastructure. Many of these systems were not created with security in mind because they were never intended to be connected to the internet. As the World Wide Web grew though, it became extremely convenient to attach remote ICSs to the internet to facilitate easy access for maintenance. Unfortunately, this also made it very easy for the bad guys to access these systems. Our goal with Eratosthenes is to create a framework that can be used to detect malicious activity across a network that an ICS is attached to.

Approach:

We created a statistical anomaly detection method that is based on conditional probabilities in our feature space. Our data set consisted of unlabeled ICS packets captured during a training exercise run by SNL. We calculated the conditional probabilities of each value in a packet, given the values that the rest of the features in the packet took on. We then pruned that list of probabilities to include only the sets of feature values that have a statistically significant chance of occurring. This allowed us to quickly determine if a given feature set was anomalous by checking to see if it existed in our set of likely features.



Impact and Benefits:

This system can help alert managers of ICS systems when a malicious agent attempts to access or interfere with the devices in their ICS. The system can provide information on what is being changed, what devices are acting anomalously, and other details regarding the anomalous behavior that is occurring. Additionally, the system can detect anomalous events that could indicate malfunctions or other undesirable behavior in the system. This can greatly enhance the monitoring tools currently available to managers of ICS's.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.