MISSISSIPPI STATE UNIVERSITY

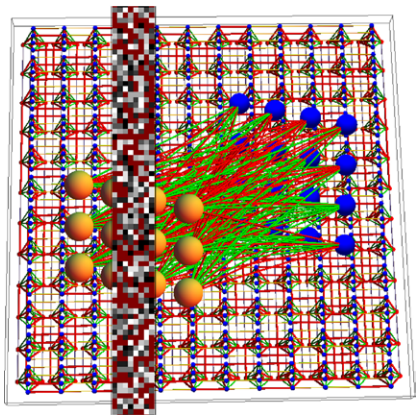
HIGH PERFORMANCE DATA ANALYTICS

DASI

Boltzmann Machines

CHALLENGE

In our connected world there are a number of bad actor who share the Internet with all users. Computers and other connected devices, including the ever-expanding Internet of Things, are wired through technology that make up the network backbone and network connections. All traffic passes along this network. It would be extremely advantageous to analyze the flow of network traffic, and even more advantageous to be able to classify the traffic over a particular network as normal traffic or as traffic from a bad actor. However, this type of network traffic classification is extremely difficult. One difficulty is network traffic at 100 Gbits/s or greater would need to be analyzed in real-time. Another difficulty is that as one detection and classification method becomes successful at removing traffic from bad actors the bad actors change their strategy.



A schematic of the theme of the development effort. Network traffic is the top picture representing the flow of bits in a network, here the colors are hexadecimal. A Boltzmann machine with 16 visible units (yellow) and 16 hidden units (blue) is the middle schematic, with colored connections being positive (green) or negative (red). The bottom schematic shows the Chimera lattice of a 1152-qubit D-Wave 2X. The D-Wave quantum computer plus high-performance classical computing provides the compute power to allow machine learning to be applied to cybersecurity.

Use Boltzmann machines, as implemented on an an adiabatic quantum computer and on a massively parallel classical supercomputer, to analyze and classify network traffic in real time

CURRENT PRACTICE

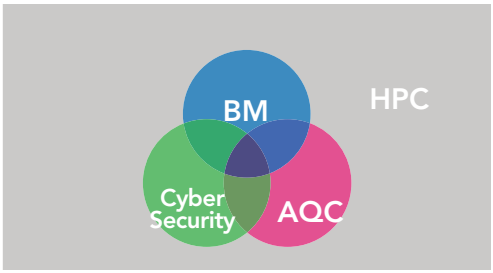
The research community is converging on the paradigm that network traffic classification can only be successful by using machine-learning techniques. One of the main emerging machine-learning techniques is Boltzmann machines. A Boltzmann machine is a stochastic neural network wherein some units (visible units) are set to the bits of the data being sampled and some units (hidden units) are free to equilibrate to a stochastic set of configurations. The main difficulty is to determine the set of parameters for the Boltzmann machine that optimally gives the classification of the data. In other words, the way the machine learns needs to be efficient. One type of connection, called the Restricted Boltzmann machine (RBM) allows only connections of the

visible-to-hidden type. A learning algorithm for the RBM can be written in a fashion such that an adequate way of approximating the required calculations for machine-learning of a RBM is possible. RBMs have been used in many types of environments that require machine-learning, including classification of network traffic.

We are at the dawn of a possible revolution in computers -- quantum computers may soon transition from laboratories to having a major effect on what calculations are feasible. Quantum computers rely on quantum principles, particularly quantum entanglement and quantum tunneling, to perform calculations that are impossible on classical computers. In technical jargon, classical computers can perform calculations in a class of problems labeled P, while quantum computers can perform calculations in a much larger class of problems labeled NP. Everyone assumes that P is contained in NP, but that NP is different from P. Quantum computers may change society as much in the current century as the wide availability of classical computers did in the last century. Currently one commercial quantum computer company in the world, D-Wave Systems. D-Wave makes a special-purpose type of analogue machine that is called an adiabatic quantum computer (AQC). An AQC is designed to solve one type of NP problem. This type of NP problem should have consequences for Boltzmann machines and hence for network traffic classification.

TECHNICAL APPROACH

The technical approach is to utilize Boltzmann machines, as implemented on a D-Wave AQC and on a massively parallel classical supercomputer, to analyze and classify network traffic in real-time. This involves efficient parallel programming of the classical supercomputer, devising and implementing novel algorithms made possible by availability of a D-Wave AQC, and applying the Boltzmann machine to network traffic classification and analysis. Mathematically our technical approach can be written as the intersection of four fields: Boltzmann Machines ∩ Cybersecurity ∩ High-Performance Parallel Computing ∩ Quantum Computing.



A Venn diagram of the task. The goal is to enhance cybersecurity (green). Machine learning methodologies are utilized, specifically Boltzmann Machines (BM) (blue). To enable solutions of hard problems, Computations are performed in a HPC (High Performance Computing) environment (gray). Calculations that are hard for HPC are enabled by AQC (Adiabatic Quantum Computers). The approach is at the intersection of these areas (purple).

IMPACT

Quantum computers hold the promise both of making all current computer and network security obsolete and of enabling heretofore impossible unbreakable security measures. Using an AQC to perform solutions of NP problems, and coupling these to machine learning may enhance cybersecurity related to network traffic. The impact would be in making our increasingly connected world more secure.

Contacts

Mark A. Novotny
William L. Giles Distinguished Professor
662.325.2806
man40@msstate.edu

Funding provided by a grant from Pacific Northwest National Laboratory.