

LA-UR-01-6185

Approved for public release;  
distribution is unlimited.

*Title:*

## **Gigabit Rate Network Intrusion Detection Technology**

*Author(s):*

Maya Gokhale, Dave Dubois, Andy Dubois, and Mike Boorman

*Submitted to:*

<http://lib-www.lanl.gov/cgi-bin/getfile?00783153.pdf>

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the University of California for the U.S. Department of Energy under contract W-7405-ENG-36. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

# Gigabit Rate Network Intrusion Detection Technology

Maya Gokhale

Dave Dubois

Andy Dubois

Mike Boorman

Los Alamos National Laboratory

Los Alamos, NM, U.S.A.

**keywords:** network intrusion detection, reconfigurable computing, FPGA.

**Contact Information:** Maya Gokhale maya@lanl.gov

## 1 Introduction

As digital network technologies become more advanced, the security issues related to these technologies also become more complex. To protect public and private networks, software-based intrusion detection systems have become the norm, with the goal of protecting against compromise to the network's integrity, the machines that form the network, and the information contained within it. However, with the widespread availability of 1 Gb/s Local Area Networks and 10Gb/s links, it has become clear that current software-based intrusion detection systems cannot process packets at those line rates, resulting in inadequate monitoring of network traffic and increasing the probability of an undetected attack. Available software-only systems can monitor at the very most 100Mb/s rate, an order of magnitude less than required.

In this work, we have designed and are currently prototyping a combination hardware/software network processor capable of detecting unauthorized intrusions into gigabit level networks.

## 2 Description

Our hardware platform consists of the SLAAC1V[1] card, a reconfigurable computer containing three Xilinx Virtex XCV1000 FPGAs, ten 256KBx36 SRAM memory modules, and a daughter Gigabit Ethernet card, the GRIP[2]. Packets pass from the line directly into the logic circuits programmed into the FPGAs. One set of logic circuits compare header fields from the packet with known attack features according to the "snort" rule database. A

second set of circuits compares packet content to desired content strings. Positive matches from comparisons on both circuits are processed in software, where more complex analysis can be performed. By filtering packet headers and content in hardware, we greatly reduce the burden of software processing.

Our circuits are a combination of state machines, banks of comparators (for port ranges), and Content Addressable Memories (CAMs). In the XCV1000 implementation, we can store 32 160-bit CAM entries (see Figure 1). The header comparison circuit occupies 34% of the on-chip RAM and uses 29% of the logic slices. The content comparison circuit uses 18% of the on-chip memory and 39% of the slices. The circuits operate at 66 MHz. Communication to the host program is performed at 66 MHz, with 32-bit data. We have measured 87MB/s bandwidth between the SLAAC board and PC using DMA.

We have modified the “snort” software to generate the Range Table and CAM configurations, and will extend the snort detection engine to process results from the hardware and complete logging/alerts in software. We are presently performing system integration and testing. At the workshop we will report on achieved performance.

## References

- [1] USC/ISI. SLAAC Project. [www.east.isi.edu/projects/SLAAC](http://www.east.isi.edu/projects/SLAAC)
- [2] USC/ISI. GRIP Project. [www.east.isi.edu/projects/GRIP](http://www.east.isi.edu/projects/GRIP)

Overview SLAAC Header & Content.igx

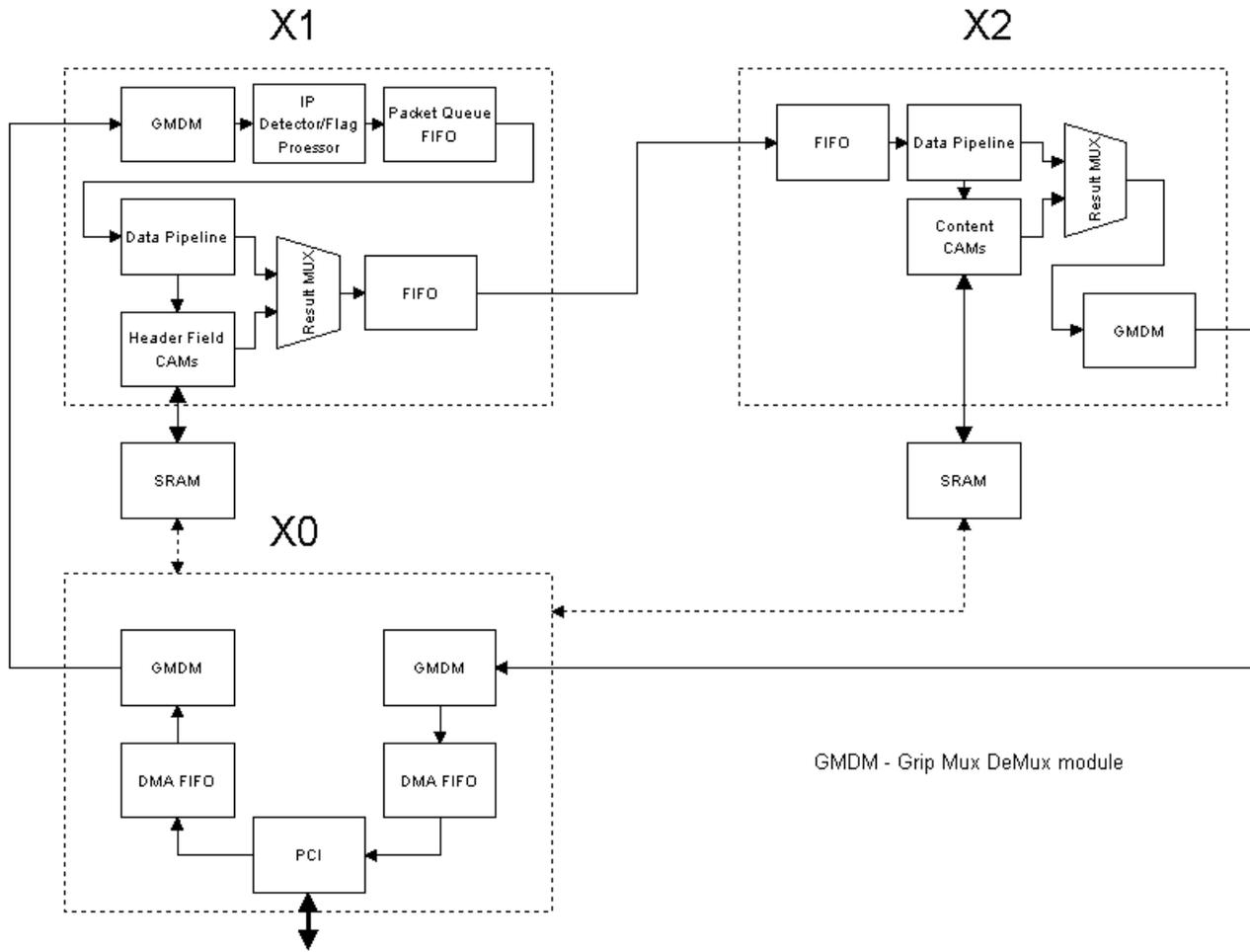


Figure 1: Header and Content CAMs