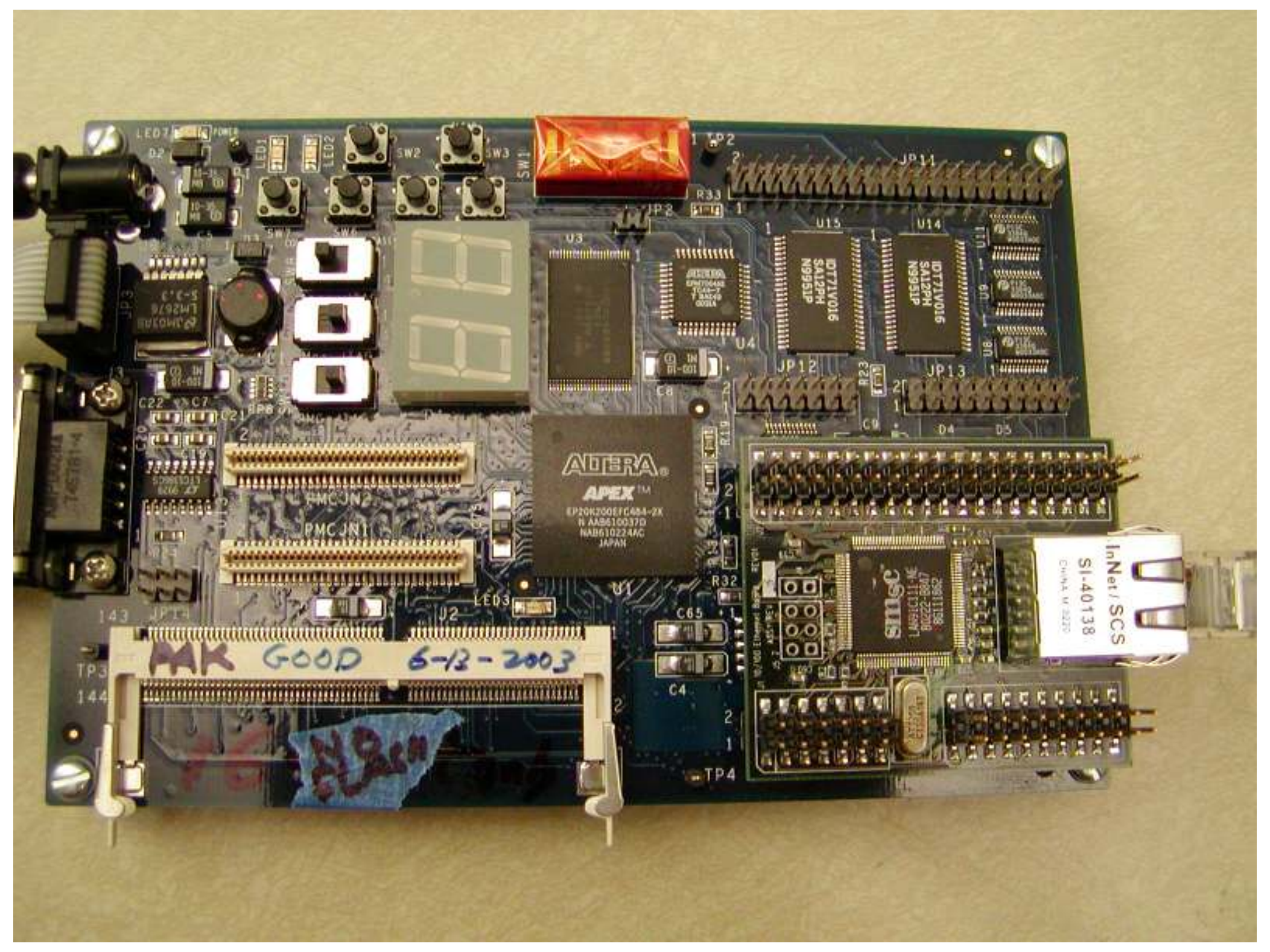
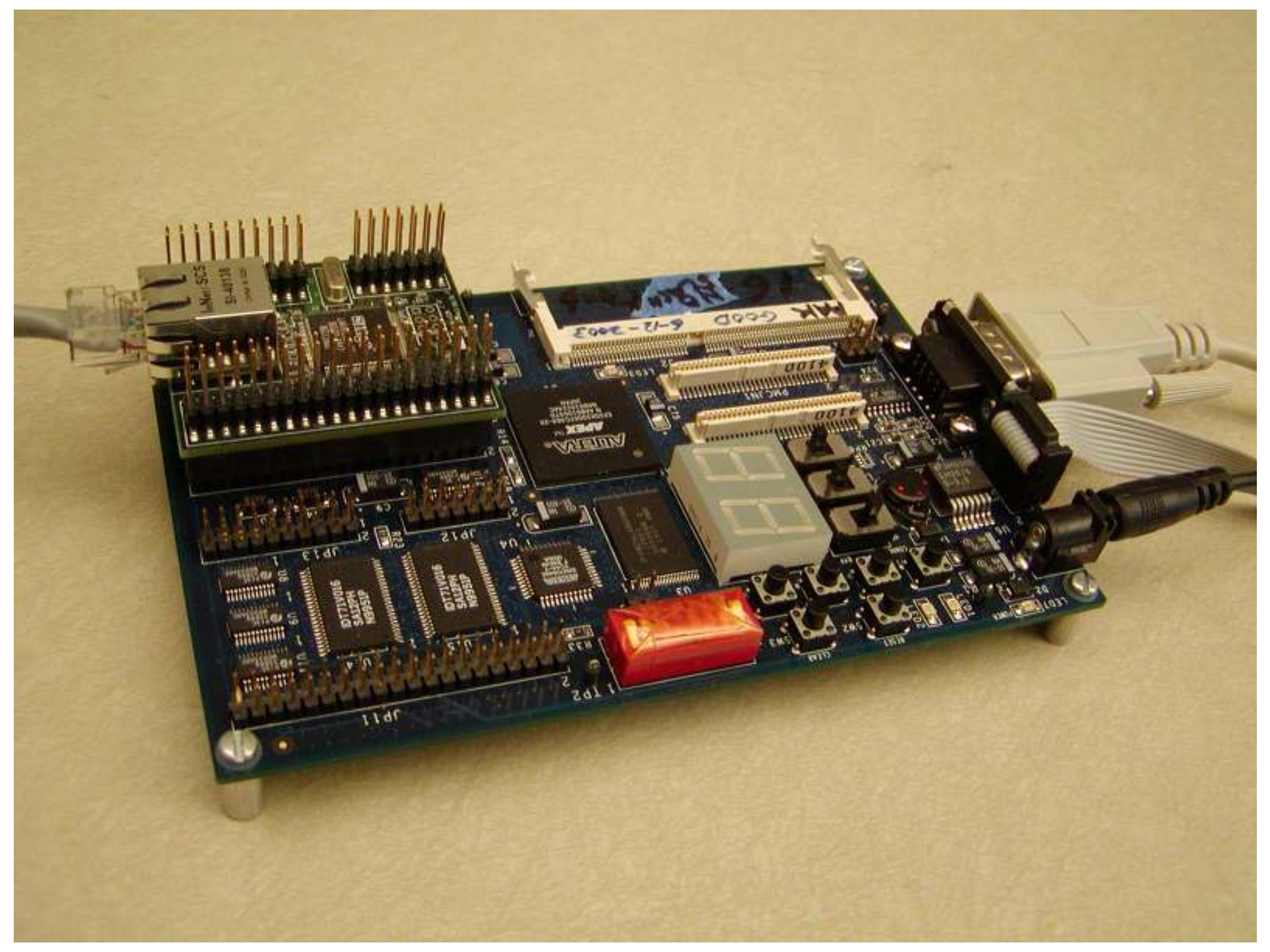


Pattern Matching in Network Intrusion Detection Systems

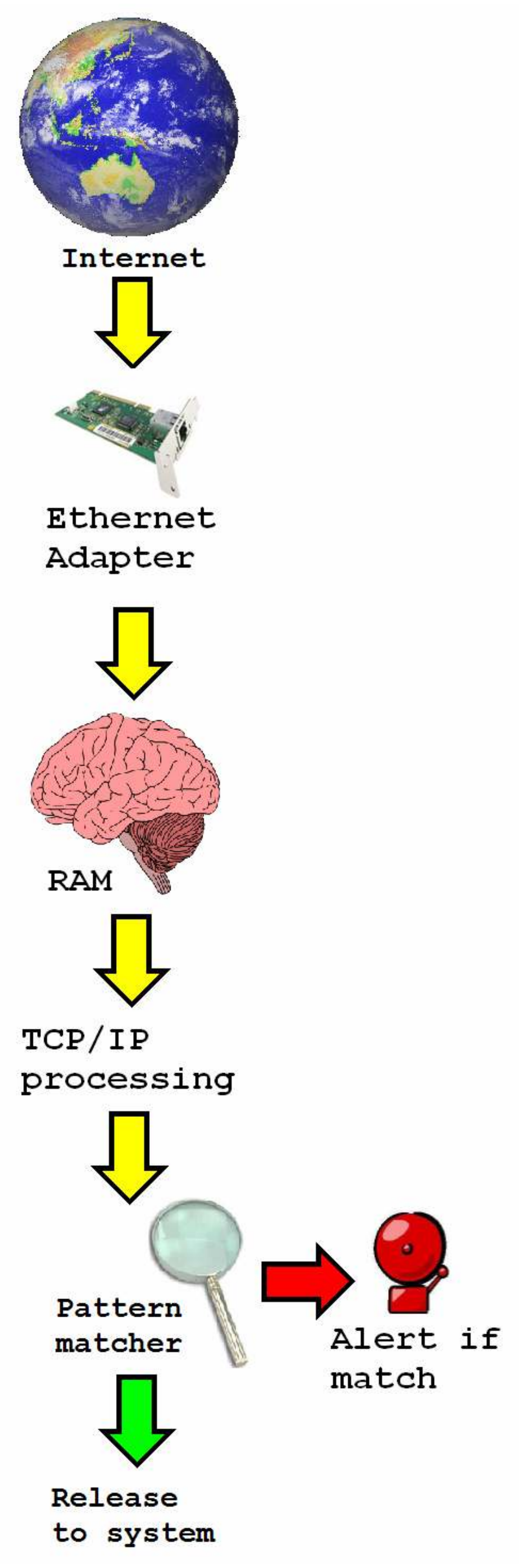


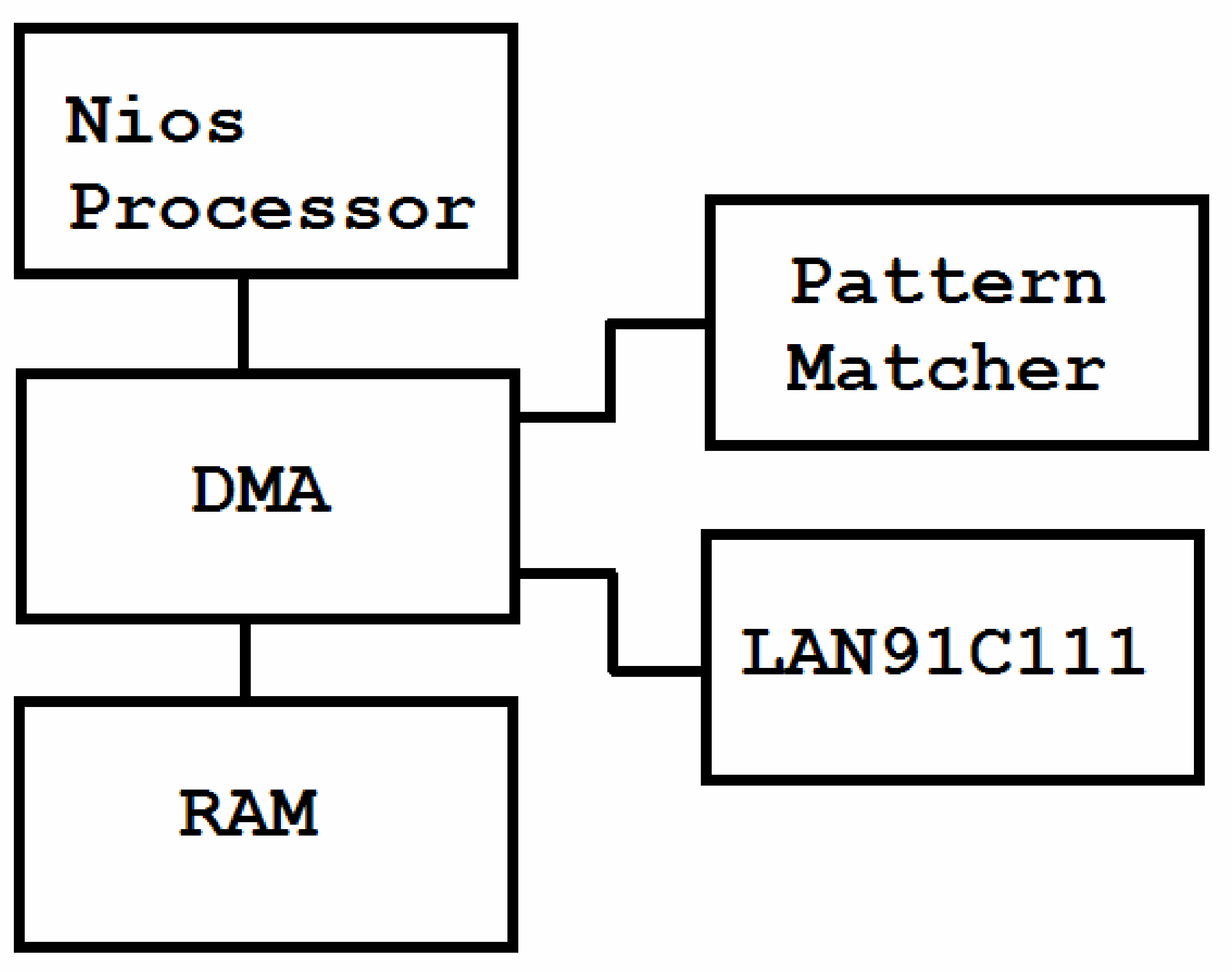
Abstract

The objective of this research is to assess the effectiveness of offloading the pattern matching functionality of a network intrusion detection system (NIDS) to hardware, such as field programmable gate arrays (FPGA). Effectiveness can be measured by the growth in complexity of patterns versus the number of required logic elements to support the design and the speed at which this design can function.

Data Flow

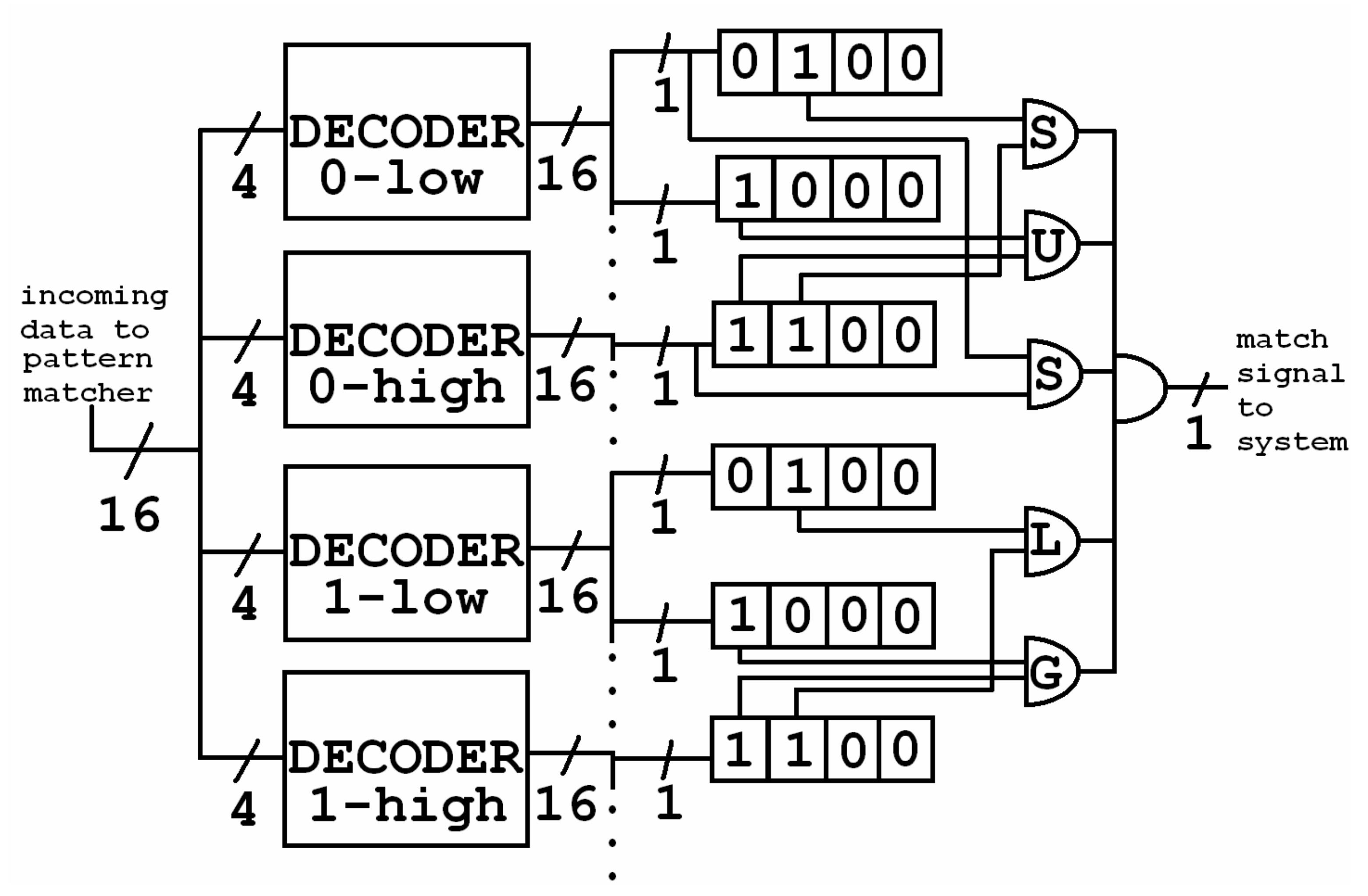
1. Data flows from the internet through the Ethernet adapter to the memory
2. All the headers are processed and removed
3. The payload of the packets get scanned
4. If there is a match the packet gets drop and the system receives an alert otherwise the packet is release to the system





Architecture

The experiment is carried out on the Altera development board with a Nios processor, an APEX 20K200E fpga with 8,320 logic elements, and a LAN91C111 Ethernet adapter. The dataflow of the design consists of a direct memory access unit that carries data to and from the Ethernet adapter bus to random access memory and then to a pattern matcher.



Example discrete comparators for the pattern "SLUGS"

Number of Patterns	Size of Shift Registers (bits)	Number of Logic Elements	Time of Most Critical Path (ns)
1	5	2,561	---
2	11	2,607	---
3	11	2,623	---
14	11	2,805	29.464
38	24	3,059	33.001
44	24	3,197	34.130
78	24	4,397	34.562
108	24	5,027	36.690
148	24	5,576	39.581

Results and Future Work

The growth of the number of logic elements is relatively low compared to the increase in the number of patterns. When the number of patterns exceeds 200, the development board was not able to fit the design due to routing failure. The possibility for NIDS to be developed in hardware exists. It would offer a better solution than software due its operating speed. At the same time there is still much work to be done before a feasible hardware-based NIDS can be created. Even though pattern matching would be faster in hardware, an Ethernet packet comes with a huge overhead. The processing of the packet headers alone takes up many CPU cycles.

Khi Lam
University of California, Santa Cruz
Mentors: Pak Chan and Martine Schlag
SURF-IT Summer 2005