Design and Implementation of a High Speed Network Intrusion Detection System

Shruthi Sujendra

Department Of Electronics And Communication
CMRIT, BANGALORE

Abstract— **Network Intrusiion Dectection Systems (NIDS) plas a key role in protecting today's network security. The reprogrammable aspect of Field Programmable Gate Array (FPGA) makes t a technology in demnd as it can be used to update new rule sets and detect new attacks. However, scaling FPGA based NIDS implementations to faster network links is an important issue. Drawback in terms of linear increase in the resource occupation is seen when we try to balance traffic over multiple, but functionally equivalent, hardware blocks, each implementing several thousands of rule sets. Here we propose a different traffic aware design of FPGA-based NIDS in which Pattern Matching plays an important role. A modular approach is used wherein the traffic across the network is classified and grouped. This homogeneous traffic is dispatched to different capable hardware blocks, which support smaller rule set as per the homogeneous traffic type it supports. In recent types there are many FPGA based architectures for detecting malicious patterns. In this project more complex combinations of several patterns are used to describe intrusion activity. Importance is given to multi-pattern signatures and a FPGA based deep packet inspection engine for NIDS which supports both dynamic and static atterns is proposed. The results are shown in terms of trade-offs and advantages experimentally showing resource savings on a real network enviroment.**

Index Terms— NIDS, FPGA, Pattern Matching, Traffic aware, String Matching, hashing, DPI, NFA, Regular Expression, Multi-Patern Matching

I. INTRODUCTION

The global increase in the use of internet causes an increse in the demand for network security and protection against threats and attacks. One of the proposed solutions to overcome this demand is to use Network Intrusion Detection Systems (NIDS) also known as Network Intrusion Prevention Systems (NIPS). A NIDS is defined as a system that analyses the traffic crossing the network, classifies packets according to the header content or pattern matching and further inspects payload information with respect to regular expresson matching rules for detectingthe occurrence of attacks. Deep Packet Inspection (DPI) on which NIDS relies on is a mechanism which deeply searchess into packet payload for existence of predefined malicious pattern. However, the pattern-matching is more challenging due to the expanding signture sets and increasing line speed.

NIDS can be classified into software based NIDS and hardware based NIDS. Snort NIDS make use of software based NIDS whch are used mostly in relatively small scale networks as hey cannot manage multi Gbits/sec traffic rates of a typical network. Hardware based NIDS are a more realistic choice for high speed network links. However, Field Programmable Gate Arraya are most appealing technology as hardware implementations need to permit the frequent updation of the supported rule set, so as to cope with the new types of intrusions and attacks that the networks are subjected to. Parallel processing and reconfigurable capability are the two characteristics that make FPGA most suitable for this kind of application. In order to reduce the cost of implementation to deal with constant database updation, the property reconfiguration is used and in order to achieve multi-gigabit throughput FPGA-based system exploits the parallelism property.

In the past few years, studies based on pattern matching on reconfigurable device have been on only one type of pattern. In this project we address patterm matching in terms of combination of multiple patterns. Hashing approaches which have advantages in terms of hardware utilization and pattern updation is used. An architecture bsed on matching Regular expression based on Non-deterministic finite Automata which cn achieve gigabit throughput is proposed. However studies with respect to handling multi-pattern signature have shown only limited results. In this project we analyse a method for parallelization in FPGA-based NIDS traffic analysis wherein we see if there are ways other than balancing the traffic collected across multiple hardware modules devised to inspect packets using the same set of rules. A traffic aware approach is to be proposed. The header information of the packets are used by the disptcher to classify the traffic flow according to which the packets are routed into different content matching engines. A deep packet inspection approach is used for speeding up the NIDs on FPGA platform. The architecture is extended to support static and dynamic patterns of a multi-pattern signature and will also be designed to work on regular expression pattern matching and fixed string matching. Finally we have tried t show results in terms of system evaluation and resource utilization.

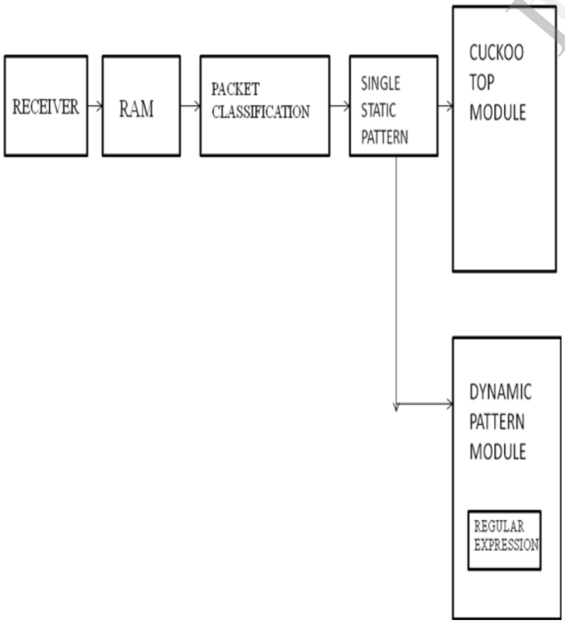
II. NETWORK INTRUSION DETECTION SYSTEMS

Network traffic is data in a network. In computer networks, the data is encapsulated in network packets. The network traffic control is the process of managing, prioritising, controlling or reducing the network traffic, particularly internet bandwidth. In terms bandwidth management, network administrators reduce congestion, latency and packet loss. To determine the cause of network congestion it is necessary to measure the traffic of the network.

Communication between two hosts using a network may be encrypted to maintan privacy. Network security consists of plicies and provisions adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification or denial of network accessibility. Network security starts with authentication, commonly with a username and a password. Users choose or are assigned an ID and password. Networks can be private or public. Security management for networks is different for all kinds of situtuions. A homme or small office may require the basic security only but a large businessess may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

The network traffic is analysed by Network Intrusion Detection Systems (NIDS). NIDS are network security appliances that monitor networks for malicious activity, log information about this activity, attempt to block it and report it.

III. PROPOSED BLOCK DIAGRAM



Firstly receiver module receives the data serially like FIFO and gives to RAM. The RAM stores the data in address locations. If data is valid, analyzer analyses the data in the form of packet send it to the multi pattern agents.

The receiver module receives data and calculates for maximum number of data. Since 8 bit data has been sent the max number of bits will be 608 bytes/8 bit it will be 76 bytes. The data are checked for error. The data that have no error are stored in RAM storage. The data are passed to frame formation from RAM that has no errors. The frame formation separates IP error and Ethernet error and is sent to frame extraction. When IP and Ethernet are eliminated the frame extraction sends only required data to cuckoo algorithm.

In this project we use the Cukoo-hashing method to implement static string matching engine which usually consist of 16 modules. Each module will detect patterns with specific length relative to their position. The Cuckoo 1 will detect all pattern having one byte length, Cuckoo 2 will detect pattern which have 2 bytes in length. The priority circuit will select the longest matched pattern among 16 modules. The output will be the value consisting of matched module and the index of pattern stored in that module.

The incoming character is derived from packet classification and feeds Character Matching Module for matching against all existing characters and character classes. Then, output signals from this module are routed to all Regular Expression Matching Engine (REME) being inside PCRE Matching Module. Each REME presents one regular expression and is constructed from some Building Blocks (BB). Common prefix sharing is directly implemented inside PCRE Matching Module. Common infix sharing is handled separately in Infix Matching Module. Eventually, all matching signals are collected and encoded by Encoder Module.

IV. APPLICATIONS

The NIDS system proposed finds applications in various networks in different fields such as –

- Data security
- Military communication
- Authentication process

V. CONCLUSION

There is significant savings in the design of hardware Network Intrusion Detection systems (NIDS) due to the traffic classification. The dispatcher forwards different types of traffic to the pattern matching engines which support different rulesets in the proposed architecture. A FPGA-based deep packet inspection engine is used in the NIDS for speeding up our application. Our architecture is designed such that it supports both static and dynamic patterns of multi-pattern signature matching. The fixed string pattern and NFA-based matching engine for regular expression pattern is processed by expanding the cuckoo-hashing architecture. The proposed system is applied to real network traffic to show results in terms of resourse savings and throughput.

REFERENCES

1. “Traffic-aware Design of a High Speed FPGA Network Intrusion Dectection System”, Salvatore Pontarelli, Giuseppe Bianchi, Simone Teofili Consorzio Nazionale InterUniversitario per le Telecomunicazioni (CNIT), University of Rome “Tor Vergata”, Via del Politecnico 1, 00133, Rome, ITALY
2. .” Ultra-High Throughput Low-Power Packet Classification”, Alan Kennedy and Xiaojun Wang
3. http://en.wikipedia.org/wiki/Network_security
4. http://en.wikipedia.org/wiki/Network_intrusion_detection_system
5. http://en.wikipedia.org/wiki/Network_traffic
6. Sourcefire, “Snort: The Open Source Network Intrusion Detection System”, available at http://www.snort.org.
7. Xilinx Website, available at http://www.xilinx.com/
8. COMBO Product Brief, available at http://www.inveatech.com/data/combo/combo pb en.pdf
9. Virtex-5 Family Overview, available at
10. http://www.xilinx.com/support/documentation/datasheets/ds100.pdf