2008

High Ppeed Circuit Techniques for Network Intrusion Detection Systems (NIDS)

Ajay Mohan Mahajan
University of Akron, main campus

HIGH SPEED CIRCUIT TECHNIQUES FOR NETWORK INTRUSION DETECTION SYSTEMS (NIDS)

by

Atul Mahajan

B.E., Electronics and Communication Engineering
Visveswaraiah Technological University, India, 2004

A Thesis
Submitted in Partial Fulfillment of the Requirements for the
Master of Science Degree

Department of Electrical and Computer Engineering
in the Graduate School
Southern Illinois University Carbondale
December 2008

THESIS APPROVAL

HIGH SPEED CIRCUIT TECHNIQUES FOR NETWORK INTRUSION DETECTION SYSTEMS (NIDS)

By

Atul Mahajan

A Thesis Submitted in Partial

Fulfillment of the Requirements

for the Degree of

Master of Science

in the field of Electrical and Computer Engineering

Approved by:

Dr. Haibo Wang, Chair

Dr. Ning Weng

Dr. Spyros Tragoudas

Graduate School
Southern Illinois University Carbondale
August 22, 2008

AN ABSTRACT OF THE THESIS OF

ATUL MAHAJAN, for the Master of Science in ELECTRICAL AND COMPUTER ENGINEERING, presented on August 22nd, 2008, at Southern Illinois University Carbondale.

TITLE: HIGH SPEED CIRCUIT TECHNIQUES FOR NETWORK INTRUSION DETECTION SYSTEMS (NIDS)

MAJOR PROFESSOR: Dr. Haibo Wang

This thesis presents a string matching hardware implemented on FPGA platforms for network intrusion detection systems. The proposed architecture, consisting of packet classifiers and strings matching verifiers, achieves superb throughput by using several mechanisms. First, based on incoming packet contents, the packet classifier scan dramatically reduce the number of strings to be matched for each packet and, accordingly, feed the packet to a proper verifier to conduct matching. Second, a novel multi-threading finite state machine (FSM) is proposed, which improves FSM clock frequency and allows multiple packets to be examined by a single FSM simultaneously. Design techniques for high-speed interconnect and interface circuits are also presented. Experimental results are presented to explore the trade-offs between system performance, strings partition granularity and hardware resource cost.

ACKNOWLEDGMENTS

I would like to express my deepest appreciation to my thesis mentor, Dr. Haibo Wang, who has guided and motivated me to this wonderful research area and given me a chance to work on this project. My sincere thanks also go to my committee members Dr. Ning Weng and Dr. Spyros Tragoudas who helped making this research more informed with their valuable comments and remarks.

I appreciate Southern Illinois University Carbondale and the Department of Electrical and Computer Engineering for providing necessary technical support for this work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

FIGURE PAGE

CHAPTER 1

INTRODUCTION

Over the past few years, there has been a manifold increase in the Internet applications. This increase has undoubtedly raised the standard of life all over the world. Most of the things can now be done while sitting at home and using the network, more commonly known as Internet. While the Internet brings enormous convenience, it also creates the possibilities for hackers or enemies to steal secretary information or derail the normal operation of organizations. Because of these Internet attacks, the Internet security becomes an important issue in the increasingly connected world.

There have been enormous cases in the recent history where the lack of network security has led to major fraudulent activities. The biggest and most famous case is the hacking of wireless networks of nine major retailers in USA. As a result, more than 41 million credit and debit card numbers were stolen. This case which happened in 2007 shocked the internet society all over the world. It clearly depicts that in spite of the highly sophisticated network security systems available nowadays, no one is guaranteed to be 100% safe in the Internet. Even the best available network security system can not provide 100% safety as everyday the intruders are developing newer ways of possible network attacks. This requires the security system to be updated periodically to keep up with all sorts of attacks.

In the near future, there will be more and more data transmitted over the networks. Not only financial information but all the official information related to the nation's security

is also available over the networks. As an instance, any intrusion in the network of Department of Defense of any nation can lead to dreadful consequences for the entire world. Hence, network security is the area which can never be ignored and need to be constantly updated.

One of the most promising techniques that provide the lacking security of the internet is Network Intrusion Detection System (NIDS) [8, 13, 18]. Although an NIDS normally contains various sub-systems, its most important component is a string matching engine. In order to detect any suspicious activity, the sting matching engine compares the incoming network packet with predefined patterns which are defined as a set of rules. According to the Snort version 2.4 there are a total of 3305 such rules. Each rule consists of two types of strings to be matched: one is header strings with determined position in packet header (e.g., source/destination network address and source/destination port number); another is payload strings with probabilistic position in packet payload (e.g., network worms and computer virus). A suspicious activity is detected when both header strings and at least one of payload strings are matched on the packet. This simple string matching engine was successful in detecting attacks when the network traffic was very low and also there were few possible attack rules. But in present day situation, where the network traffic is in the high range of ten Gigabit per second and also there are thousands of possible attack rules, this simple engine can become the bottleneck of the overall NIDS. Also, it is necessary to scan every byte of a packet as the starting position of payload string might be probabilistic.

The NIDS can be developed either in software or hardware. The existing software-based NIDS are very slow and they are capable to operate successfully only if the

network traffic is very low, in the order of hundred Megabits per second. In order to overcome the drawbacks of the software-based NIDS, various hardware approaches [4, 2, 6, 9, 12] have been proposed. However, all of them are either lacking performance, scalability to traffic rate and attack rules, or they are too complicated to design and operate.

To address these concerns, a simple but efficient architecture based on scalable classifiers and novel multi-threading finite state machines (FSMs) has been designed. The classifier arranges the incoming packet to three categories: malicious, suspected or benign. Malicious packets are directly discarded and the benign packets are forwarded to the network. Most of the incoming packets (85%) to the network are benign [3]. Only the suspected packets are sent to the string matching engine. FSMs in the matching engine are used to further verify whether the suspected packet is malicious one. The key to achieving high performance of this architecture is employing multiple small and fast FSMs. Each of these FSMs searches for a portion of rules on a suspected packet and accordingly marks it as benign or malicious.

The focus of this thesis is to design and implement the high-speed verifier on Field Programmable Gate Array (FPGA) platforms. The high-speed verifier is based on the concept of using FSMs to search a set of patterns. In order to improve the throughput of the verifier, a novel multi-threading FSM design has been proposed. A new circuit to feed the multi-threading FSM has also been developed. Investigations are conducted to study the granularity of the FSMs and experimental results have demonstrated that this proposed architecture achieves superb throughput.