Hardware-Accelerated Framework for Security in High-Speed Networks

Jiří Novotný
CESNET, z.s.p.o.
Zikova 4, 160 00 Praha 6
Czech Republic
novotny@cesnet.cz

Pavel Čeleda
Masaryk University
Botanická 68a, 602 00 Brno
Czech Republic
celeda@ics.muni.cz

Martin Žádník
Brno University of Technology
Božetěchova 2, 612 66 Brno
Czech Republic
izadnik@fit.vutbr.cz

ABSTRACT

This paper presents hardware-accelerated framework for security in high-speed networks. To match the line rate performance requirements we use FPGA based COMBO acceleration cards. The NetCOPE platform enables to design new network security applications or accelerate existing one as well as shorten the time to develop these applications for COMBO cards. The network traffic is processed in real-time and available to intrusion detection applications, network monitoring tools etc. We describe the framework deployment in various projects and the possibilities how to meet current cyber threats.

1 INTRODUCTION

These days the problem of security in high-speed networks is of utmost importance. Massive cyber attacks targeting government and mission-critical servers can swiftly become an issue of national security like the attacks on Estonian infrastructure in 2007. The network enabled capability (NEC) pays attention to new security risks comming from cyberspace.

Various methods for cyber-defence used to date have been based on software solutions without hardware acceleration. With the increasing number of network users, services and the current generation of high-speed network links, the amount of transferred data has increased significantly. These facts have rendered many software solutions for network security obsolete and current high-speed networks lack of efficient technology for real-time traffic processing. The state-of-the-art methods for network intrusion detection, security analysis and forensics rely on combining and correlating data from various sources such as link utilization, statistics about IP flows and detailed packet payload inspection.

Hardware-accelerated devices are essential to meet the requirements of line rate network traffic processing without a packet loss. The presented framework allows to access network data at line rate, without packet loss and provides a reliable input for network security and anomaly detection tools. The system is based on commercial off the shelf server and hardware accelerator based on FPGA (*Field-Programmable Gate Array*) chips. The hardware accelerators are special network interface cards implementing time critical part of application in FPGA which performance is much higher than of a traditional CPU. Unique FPGA features (massive parallelism and on-the-fly reconfiguration) may be leveraged for network security analysis. For example, security engineer can switch the monitoring device from generating flow statistics to deep packet inspection.

The paper is organized as follows: After a short overview of the related work, we present the system architecture, the COMBO card family and describe major hardware and software parts. Then we discuss network applications where the acceleration framework is used. Finally, we conclude by describing FlowMon security use case, summarizing our experiences from security related projects and outlining our future plans.

2 RELATED WORK

The DAG project [4] at University of Waikato started in 1994 to combine hardware design (FPGA technology) with a PC based servers. Developed network measurement cards could capture packet headers with very high precision timing. The acceleration cards targeted the problem of capturing data at line rate into the host memory. In comparison with common network interface card, it uses simple ring buffer model [5] for data transfers and thus increases effectivity of DMA transactions. The proposed architecture is primarily designed for monitoring purposes, it connects the precise timestamp to each packet and make them accessible via modified PCAP library. Unfortunately, this architecture provides only fast data transfers from network into host memory. Firmware modifications of FPGA are not possible and the acceleration of third part applications is limited in this way. In 2001, Endace Measurement Systems was formed to commercialise the DAG project.

Similar commercial company that designs programmable network adapters with FPGA chips for purposes of network traffic monitoring is called Napatech [11]. Using an associative CAM memory placed on the acceleration card, it allows filter incoming traffic based on simple rules [10]. As the DAG card, this architecture is closed for implementing of own applications inside the FPGA chip.

Open platform intended for building of own network application is developed in the scope of NetFPGA project [12] at Stanford University. The architecture includes I/O blocks for packet reception, allows user to access an acceleration core via PCI system bus and implements basic packet transfers via DMA [8] [15]. Primarily, the platform is intended for education purposes and demonstrates two simple applications of network interface card and router. Alternatively, the card can be utilized for research activity [16]. Current bottleneck of the NetFPGA card is low throughput into host computer due to 33MHz/32bit PCI interface.

3 SYSTEM ARCHITECTURE

The facts described in previous section about availability and usability of programmable network adapters led us to design own acceleration framework. The framework was developed and deployed in frame of several international research projects since 2002. High-speed network processing requires an architecture that can handle large amounts of data and high data rates. The acceleration framework includes several building blocks which enables rapid development of algorithms for network traffic processing and consists of following parts:

- Hardware - family of COMBO acceleration cards.
- Firmware - NetCOPE development platform.
- Software - Linux kernel drivers and user space libraries.
- Security applications - traffic capturing, flow monitoring, IDS/IPS applications etc.

The NetCOPE [9] platform offers a set of IP (*Intellectual Property*) cores usable as basic building blocks for a wide range of network applications. Accelerated parts of target applications are integrated in form of plugins into NetCOPE platform. The plugins can perform various operations on network traffic like a packet classification, pattern matching, traffic statistics computation, precise timestamping, traffic processing (forwarding, capturing, filtering, encryption/decryption) etc.

These operations are time and performance critical in network monitoring applications, intrusion detection systems or traffic manipulation (routing, filtering). The layered architecture abstracts processing in each layer and significantly reduces the amount of data that are reported to higher-level layers. While the low-level layers need to be optimized to match the high performance during the network traffic preprocessing, the higher layers use the preprocessed data to complete the computation. Such approach allows to use commodity hardware to perform line rate deep packet inspection with SNORT or generate unsampled NetFlow data on heavy loaded links.

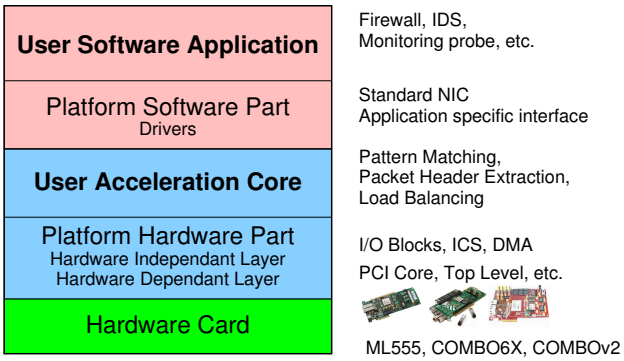


Figure 1: Layered architecture of NetCOPE platform.

4 FAMILY OF COMBO CARDS

The family of COMBO [2] cards has been developed at CESNET since 2002. The core of COMBO acceleration cards is based on FPGA chips connected to external memories and interface circuits. There are three types of COMBO cards:

- Mother cards - COMBO6, COMBO6X, COMBO6E, COMBO-LXT.
- Interface cards - COMBO-4MTX, COMBO-4SFP, COMBO-4SFPRO, COMBO-2XFP2.
- Special purpose cards - COMBO-PTM, COMBO-BOOT.

The mother card equipped with the connector for the interface card is connected to host computer via PCI bus. The interface card plugged into mother card has one or more network interfaces (1 Gbps, 10 Gbps) and provides interface-specific processing of incoming and outgoing packets. The special cards are used for the special purposes, like precise time stamp generation or standalone appliance without host computer. There are two generation of COMBO cards. First generation is widely used for the R&D activities as well as for commercial purposes. The second generation (currently under development) is designed to adapt to new technologies and increase throughput and flexibility of the first generation.

FIRST GENERATION OF COMBO CARDS

First generation of the COMBO cards was designed for the hardware acceleration of the IPv6 router in the frame of Liberouter project [3]. Next we have used the COMBO cards for network monitoring in the frame of SCAMPI [14] and GÉANT2 project [1]. The cards were designed mainly for the R&D activities and so we made decision to split the hardware accelerator in two parts to gain more flexibility. The main idea has been to use complex and expensive mother card with relatively inexpensive set of interface cards according the application needs. Vice versa, if the application demands more mother card resources, there is not necessary to design new interface card. Though the price of two cards is higher than in the case of one card, it allows us significantly decrease development time and costs for a new application. This way we were able to develop 10 Gbps programmable ethernet adapter in 2004.

All the mother cards of first generation are equipped with XILINX FPGA chips, three SRAM memories, CAM memory, socket for PC DRAM memory, PCI interface chip and power supplay. Each mother card has two 120 pin connectors for the connections with the interface card.

In the Liberouter project was packet forwarding provided directly in hardware, with relatively low demand for throughput over PCI bus. For this purpose we have developed COMBO6 mother card with PCI bus 33MHz/32bit. We have used ASIC PCI9054 chip for the PCI interface.

The SCAMPI project was targeted to network monitoring with the significantly higher demand for the PCI throughput. In the frame of SCAMPI was developed COMBO6X card with PCI-X 66MHz/64bit and COMBO6E with PCI-E x4. Both cards use the XILINX FPGA with PCI core as the PCI interface chip.

The portfolio of COMBO interface cards consists of bunch of 1 Gbps and 10 Gbps cards. The 1 Gbps interface cards have four interfaces while the 10 Gbps versions have two interfaces. All of interface cards are equipped with the smaller FPGA, SRAM memories and some of them also carry CAM memory. For the first versions of 1 Gbps cards and for all 10 Gbps we have used phyter chips for the interfaces. The development of the 1 Gbps cards was without great issue. The situation with 10 Gbps was more complicated. First 10 Gbps card COMBO-2XFP was developed in 2004. At this card we found the issue with the heat dissipation an availability of phyter chips. We have solved that issue with the redesign using phyter chips from the other vendor.

For the 1 Gbps application we use COMBO-4SFPRO with 4x1 Gbps ports, XILINX X2CVP20 FPGA, two SRAM's and CAM memory. The 10 Gbps applications use COMBO-2XFP2 with 2x10 Gbps ports, 1x1 Gbps port, XILINX X2CVP30 and two SRAM's. COMBO-PTM card was developed for the precise time stamp generation. It is 33MHz/32bit PCI card with XILINX X3S200 FPGA, TI MSP430FI49IPM processor, precise crystal and RS232/485 interface for the external GPS receiver. COMBO-BOOT card is used for the simple standalone applications running at interface card without the host PC and mother card. The information about the portfolio of COMBO cards is available at [2].

For the most of today applications we use COMBO6X, COMBO-4SFPRO, COMBO-2XFP2 and COMBO-PTM cards.

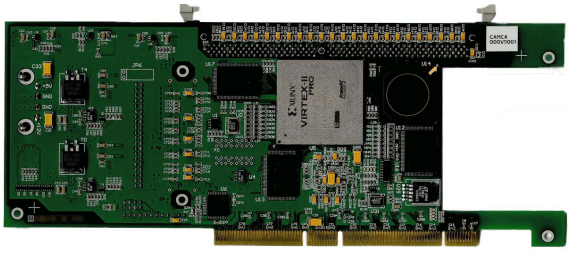


Figure 2: COMBO6X Mother card - back side.

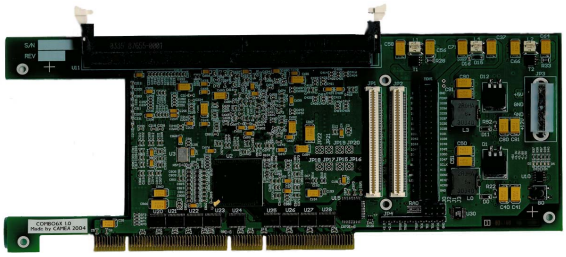


Figure 3: COMBO6X Mother card - front side.

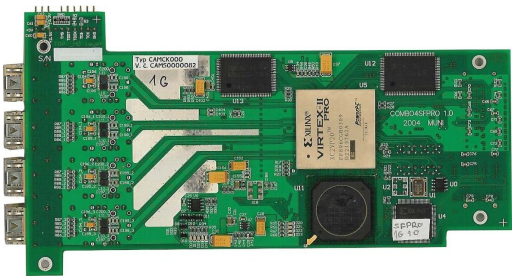


Figure 4: COMBO-4SFPRO 4x1 Gbps interface card.

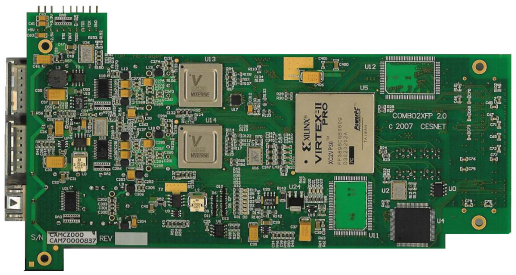


Figure 5: COMBO-2XFP2 2x10 Gbps, 1x1 Gbps interface card.

COMBOv2 – NEW GENERATION OF COMBO CARDS

Growing throughput of computer networks (speeds up to 40-100 Gbps) and complexity of network algorithms raised the needs for more powerfull hardware acceleration cards. The main bottleneck of the existing COMBO cards is throughput between the mother and interface card on 10 Gbps speeds. This approach is still sufficient due to built-in preprocessing on interface card for many applications even at 10 Gbps speeds. The

new FPGA chips support serial transfers and eliminate the bottleneck. XILINX V5-LXT family achieves up to 4 Gbps on one pair of wires (based on Rocket I/O), the new V5-FXT supports up to 6.5 Gbps. There are announcement for speeds over 10 Gbps. Demand for higher throughput is main reason for the redesign of the COMBO family which have started in 2007. The COMBOv2 family will use several serial lines together with LVDS pairs (up to 1 Gbps) between the interface and mother card. This way we can transfer up to 28 Gbps in one direction on one IFC (*Interface Connector*) with V5-LXT chip. The throughput is enough for two 10 Gbps links. To increase the flexibility we placed on mother card LSC (*Low Speed Connectors*) connectors with 10 LVDS pairs and throughput up to 8 Gbps. The new COMBO-LXT mother card has PCI-E x8, two IFC connectors, four LSC connectors, two QDRAM chips and connector for SODIMM PC memory.

Interface card COMBOI-1G4 has four 1 Gbps ports. COMBOI-10G2 has two 10 Gbps ports. We are working on design of four port 10 Gbps (COMBOI-10G4) card and 40 Gbps (COMBOI-40G1) card. The COMBO-LXT, COMBOI-1G4 and COMBOI-10G2 are in manufacturing phase now, while the COMBOI-10G4 and COMBOI-40G1 are in design phase.

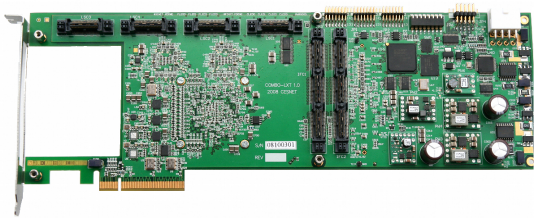


Figure 6: COMBO-LXT - front side.

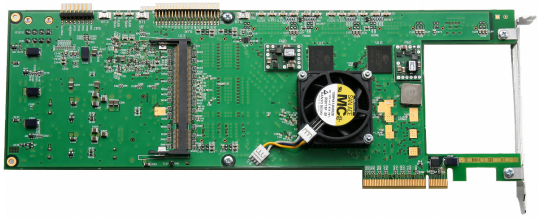


Figure 7: COMBO-LXT - back side.

5 NETCOPE - PLATFORM FOR NETWORK APPLICATIONS

COMBO hardware was used in several R&D projects. In first stage many software and firmware blocks were modified or even rewritten from the scratch with new project. To avoid this situation we have developed NetCOPE [9] platform. The platform is based on basic building blocks commonly used in network applications. The designer can focus his effort just on the application core and use advantages of the platform with well-defined API. The firmware of NetCOPE platform is written in VHDL. The application core can be written in any hardware description language like VHDL, Verilog or in higher-level language like SystemVerilog, HandelC, etc. The NetCOPE provides a set of input/output interface blocks, packet processing units, memory controllers, interconnecting system and fast DMA engines.

I/O BLOCKS

The input/output blocks implement packet receiving and transmitting via Ethernet IEEE 802.3 at speeds 10 Mbps - 10 Gbps. Packets are transferred from/to user core via local link protocol. Each incoming packet can be processed with additional information like precise timestamp, packet length and interface number.

INTERCONNECTION SYSTEM

The interconnection system connects all blocks placed in FPGA with I/O blocks, memories, and PCI bus. The architecture has tree structure, likewise PCI-E bus. It is capable read and write transaction coming from system bus and transfer them among the components. A set of LocalLink tools were developed for streaming operations (split, join, change data stream width, etc.), data storage (FIFO, buffers), data modifying and debugging.

FAST DMA TRANSFERS

Fast data transfers from/to host computer memory is key feature for many networking applications. NetCOPE supports standard network interface and application specific interface which adds additional control data (e.g. precise timestamps). Standard network interface communicates via network sockets. The incoming/outgoing data are processed by IP stack. This way the framework can be used as standard NIC with extended functionality like hardware packet filtration. While using of standard network interface is straightforward there are issues with insufficient speed and lack of flexibility. This overcomes application specific interface which delivers data to ring buffer accessible from user space application.

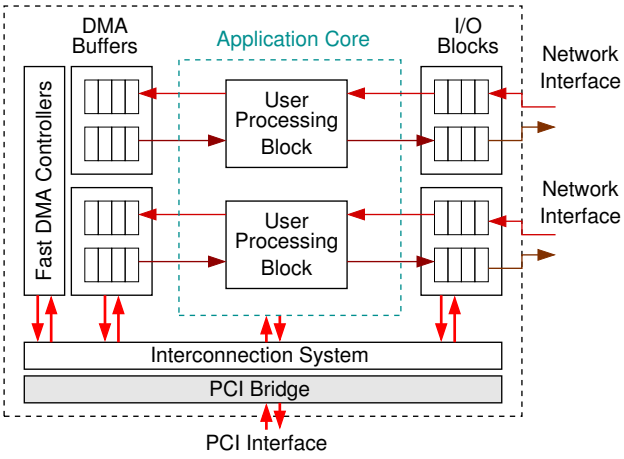


Figure 8: NetCOPE platform block schema.

SOFTWARE

The software includes Linux kernel drivers, set of libraries and basic tools for uploading the firmware, controlling the hardware and applications. These platform specific drivers, libraries and tools are necessary to handle unique features provided by COMBO cards. It leads to using of dedicated tools. On the other hand developed software follows the rules and practices valid for UNIX like operating systems. The majority of source code is written in C language.

To support third party applications like various network monitoring tools, intrusion detection systems etc. standardized PCAP interface is available. The PCAP interface allows to use any libpcap based application without source code modifications. The upper software layer of proposed platform is formed by security applications like the NIFIC (network interface card with packet filtration), SNORT accelerator (deep packet inspection) and FlowMon (monitoring of network flows). The system is based on Linux, which means unlimited potential for extensions.

APPLICATIONS

The acceleration framework was used in the following applications:

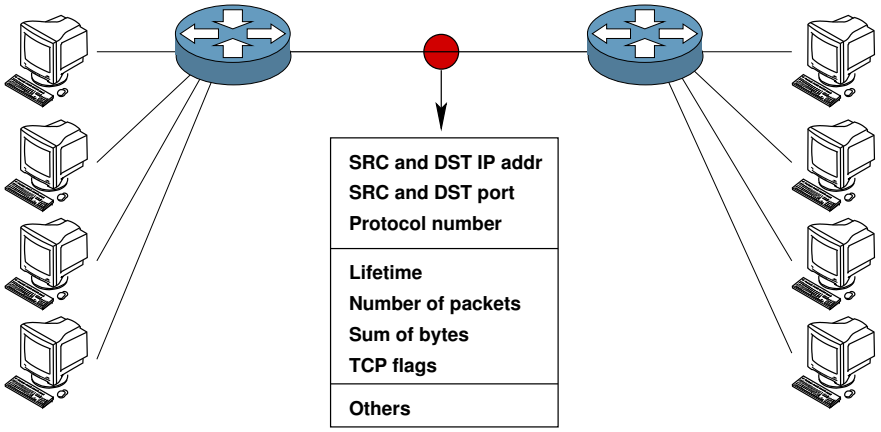
- Liberouter - IPv6 router.
- IDS - payload checking and preprocessor for SNORT.
- NIFIC - network interface card with packet filtration.
- FlowMon - advanced NetFlow monitoring.

The Liberouter project used COMBO cards for the development of IPv6 based router. In 2002 there was not sufficient support for IPv6 in commercial available routers. The project was successfully finished, but the big vendors catch up missing IPv6 functionality in their current generation of routers.

The IDS, NIFIC and FlowMon are targeting new area - network traffic observation and processing. The applications for network monitoring are much more interesting now, as there is lack of line rate compliant appliances on the market, especially for security purposes. In the frame of GÉANT2 [1] project new security toolset was developed. Based on FlowMon probe with NfSen collector [7] the network operators are able to watch network traffic in real-time. Next section describes in detail the FlowMon probe use case.

6 FLOWMON - SECURITY USE CASE

FlowMon is a network probe dedicated for measurement of flow statistics (see Figure 9), such as duration of the flow, sum of bytes transferred in the flow etc. The flow is defined as a sequence of consecutive packets with the same IP addresses, ports and protocol number. Measurement of flow statistics was first introduced by Cisco which created de facto standard of flow monitoring represented by NetFlow protocol. NetFlow protocol is used to export flow information from so called exporters to collector.



Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flags	Pack.	Bytes
0.000	TCP	192.168.195.164:1086	192.168.10.12:445	.A....	2	84
0.577	TCP	192.168.195.132:2544	194.228.32.3:80	.A.R..	3	126
0.576	TCP	192.168.195.132:2545	194.228.32.3:80	.A.R..	3	126
0.000	UDP	192.168.60.31:4021	192.168.60.1:53	.....	1	55
0.000	UDP	192.168.60.31:4020	192.43.244.18:123	.....	1	72
30.276	TCP	192.168.192.170:61158	71.33.170.53:1358	.AP...	307	368627

Figure 9: Collecting statistics about endpoints communication.

NetFlow can be enabled on routers which constitute primary source of NetFlow data today. On the other hand utilization of standalone dedicated systems such as FlowMon seems to have several benefits. Offloading of resource intensive NetFlow measurement to dedicated hardware probe is probably the most important one. Often the routers suffer of huge system load when NetFlow is enabled. Dedicated probe allows routers to perform their primary task, i.e. to route packets and keep mission critical applications up and running.

FlowMon probe provides information about who communicates with whom, for how long, which protocol, how much data and so on. Typical application areas of FlowMon for security and NEC activities includes:

- Information about the network behavior at any time and any point.

- Monitoring of network traffic in real-time.
- Securing the network against internal and external threats.
- Recognition of anomalies like worms or DDoS attacks.
- Detection of cyber crime and cyber attacks.

Flow monitoring capabilities enable deployment in many other application areas, like traffic billing, capacity planning, lawful intercept, etc.

FLOWMON ARCHITECTURE

FlowMon consists of two parts, firmware (FPGA) and software (host PC). Firmware part is dedicated to time critical measurement itself which means aggregation information about packets into flow records. The software part constitutes of several types of exporters capable of sending flow records to collectors using various protocols, such as NetFlow v5, v9, IPFIX.

FlowMon is one of the first applications on COMBO6X cards that leverages hardware and software NetCOPE interfaces in order to efficiently retrieve packets from hardware interface, to abstract accesses to external on board memories and to transfer measured flow records into host PC using DMA. The software interface allows to hand over measured flow records with nearly zero overhead to several software exporters. Layered model of the used architecture is displayed on Figure 10.

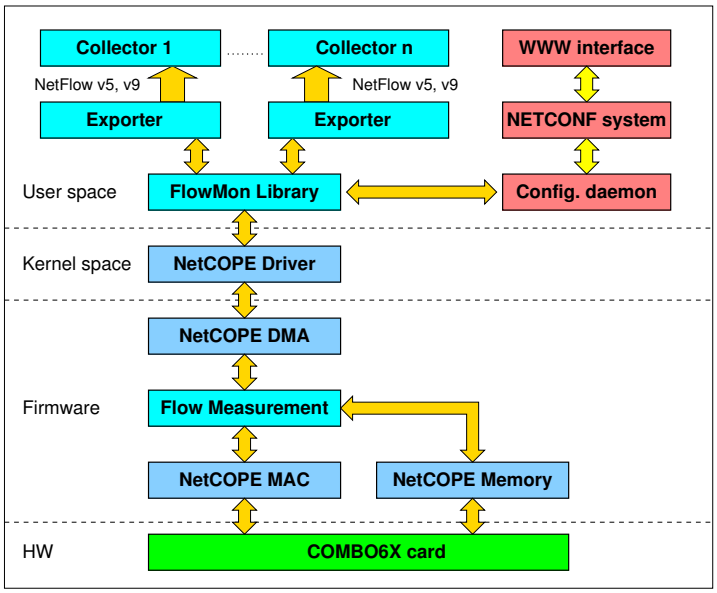


Figure 10: FlowMon system architecture.

The FlowMon firmware is composed of data-driven modules which are chained in a processing pipeline. Each module is designed to perform its unique task necessary to transform received packets into flow records at line rate.

To this end, the design exploits unique features of FPGA chips. For example, packet-parsing engines are instantiated multiple times in parallel to guarantee the full throughput during packets processing for 10 Gbps lines. Moreover the reconfiguration ability of an FPGA allows to modify the measurement process any time the new requirements arise. High flexibility of the system allows to support various protocols (IPv4, IPv6, VLAN, MPLS) and to follow standards for flow information export IPFIX, or Cisco NetFlow v9. Software of the probe allows to postprocess transferred flow records (filtering, anonymization) and export them to the collector using various protocols, such as NetFlow v5, v9, IPFIX. Software implementation of export process

allows to easily add extra features, e.g. export information via encrypted channel. FlowMon probe provides secure remote configuration via command line (SSH) or from any web browser using NETCONF protocol [6].

FLOWMON DEPLOYMENT

NetFlow is traditionally used for routing optimization, application troubleshooting, traffic mix monitoring, accounting and billing and others. Besides these running-up applications new utilization attracts the attention. Among the most widely known belongs detection of security incidents and denial of service attacks, already embedded in some collectors. The simplest heuristic for detection of DoS is based on detection of deviations of statistics from their expected values. More sophisticated methods are based on search through IP address and port space which is constructed out of NetFlow data.

Traffic behavioral analysis is an alternative approach to traditional pattern matching. The analysis is based on specific behavior of different types of applications rather than on pattern detection which is sometimes difficult concerning encrypted connections or simply applications where no significant pattern signature can be identified. Main motivation for statistical analysis is its robustness for certain kind of applications. For example, if the analysis is focused to detect interactive communication by monitoring interval between consequent packets it would be very hard for application to deceive detection mechanism by generating packets with larger interval between consequent packets as the quality of communication would suffer.

The FlowMon probe was successfully used in CAMNEP project [13] supported by the European Research Office of the US Army under Contract No. N62558-07-C-0001. The CAMNEP system is a network intrusion detection system based on a self-adaptive ensemble of multi-layer detection agents. The system fuses the decisions provided by a set of network behavior analysis algorithms, which identify the anomalies in the NetFlow data.

The FlowMon probe is recognized as part of security toolset defined by GÉANT2 project. The toolset is used by National Research and Education Networks (NREN) to generate NetFlow data and to supervise network traffic. NETSEC project running on Masaryk University uses FlowMon probes to monitor and track all security incidents in the university network.

Measurement of connections quality is yet another application that could benefit from flow monitoring, especially where multimedia application are utilized. The advantage is that such measurement is non-invasive (no extra packet have to be launched in the network) and at the same time performed upon multiple hosts and applications during real traffic utilization. Gathered data can be correlated afterward which can help with troubleshooting and optimizations.

7 FUTURE WORK

Described applications operate with ordinary NetFlow data which works fine up to transport layer of TCP/IP model. But there are new security applications that require flow-like data with more or different information. For some of them standard items of flexible NetFlow v9 or IPFIX would suffice, another need further extensions and customization which we try to incorporate into FlowMon probes.

First of such extension is so called L7-decoder. Its function is to identify applications that are communicating via network. Some of them are naturally identified by its transport port number but a larger group of nowadays applications either utilize unprivileged ports (dynamically) or hide its traffic on ports assigned to other applications. Ordinary NetFlow data can report only applications running on well-known ports with consequence of joining legitimate with malicious traffic on the same port.

The task of the decoder is to distinguish between various applications by inspecting the data at application layer (payload of transport layer) where it may look for specific patterns using regular expressions. The implementation of the network application decoder directly in the FlowMon probe would be only a natural extension since it was the original intent to provide information about application traffic mix. Moreover the

core of decoder is based on well studied problem of pattern matching which was shown to be suitable for FPGA implementation.

Our future work will focus on currently proposed 40-100 Gbps high-speed links. We will look for a new approaches how to get more detailed traffic information (e.g. interpacket gaps) to support anomaly detection mechanisms. Well preprocessed data can significantly improve performance and detection abilities of network monitoring and intrusion systems.

8 TECHNOLOGY TRANSFER

The presented framework was partly developed under the SCAMPI project [14]. The reviewers of SCAMPI recognized the potential of the framework and recommend commercial exploitation. CESNET transferred the developed technology into spin-off company INVEA-TECH. The INVEA-TECH shareholders are Masaryk University, Brno University of Technology, commercial partner UNIS and the the key persons working on the project. INVEA-TECH cooperates closely with CESNET and academic comunity. The goal of the spin-off company is to finish the technology into successful products and provide feedback from the commercial experiences to the academic world.

9 CONCLUSION

The presented hardware-accelerated framework overcomes the limitations of software-based security solutions. The acceleration framework is suitable for research and development work in current networks. Provided performance enables deployment in worst case scenarios like a heavy loaded backbone links or denial of service attacks.

New security applications can be designed on top of the NetCOPE platform or third party applications can be run over the accelerated NetCOPE application interface. Such applications enable the network operators and security engineers to know their network at any time and any point. Network traffic can be observed in real-time, without packet loss and anomalies like worms or DDoS attacks can be recognized.

ACKNOWLEDGEMENT

This work is joint research effort of CESNET- Czech NREN, Brno University of Technology and Masaryk University. The work is currently supported by the EU Sixth Framework GÉANT2 project (FP6-IST 511082) and by the Research Intent of the Czech Ministry of Education (MSM6383917201). The projects we were part includes SCAMPI (IST-2001-32404) and 6NET (IST-2001-32603).

REFERENCES

[1] GÉANT2 project. *Official Web Pages of GÉANT2 Project – EU FP6 project GN2 (contract No. 511082)*, 2005. `www.geant2.net`.

[2] CESNET, z.s.p.o. *Description of COMBO Cards*. `www.liberouter.org/hardware.php`.

[3] CESNET, z.s.p.o. *Official Web Pages of Liberouter Project*, 2008. `www.liberouter.org`.

[4] DAG Project, 2008. `http://dag.cs.waikato.ac.nz/`.

[5] Loris Degioanni and Gianluca Varenni. Introducing scalability in network measurement: toward 10 gbps with commodity hardware. In *IMC '04: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*, pages 233–238, New York, NY, USA, 2004. ACM.

[6] Rob Enns. *NETCONF Configuration Protocol – RFC 4741*. IETF, Network Working Group, 2006. `www.ietf.org/rfc/rfc4741.txt`.

[7] Peter Haag. *NfSen - NetFlow Sensor*, 2008. `nfsen.sourceforge.net`.

[8] John W. Lockwood, Nick McKeown, Greg Watson, Glen Gibb, Paul Hartke, Jad Naous, Ramanan Raghuraman, and Jianying Luo. Netfpga–an open platform for gigabit-rate network switching and routing. In *MSE '07: Proceedings of the 2007 IEEE International Conference on Microelectronic Systems Education*, pages 160–161, Washington, DC, USA, 2007. IEEE Computer Society.

[9] Tomas Martinek and Martin Kosek. Netcope: Platform for rapid development of network applications. In *Proc. of 2008 IEEE Design and Diagnostics of Electronic Circuits and Systems Workshop*, pages 219–224. IEEE Computer Society, 2008.

[10] Napatech. NT Family 4 or 8 x 1 Gbit/s Protocol and Traffic Analysis Network Adapter, 2007. `http://www.napatech.com/composite-214.htm`.

[11] Napatech, 2008. `http://www.napatech.com`.

[12] NetFPGA, 2008. `http://www.netfpga.org`.

[13] Martin Rehak, Michal Pechoucek, Karel Bartos, Martin Grill, Pavel Celeda, and Vojtech Krmicek. CAMNEP: An intrusion detection system for high-speed networks. *Progress in Informatics*, (5):65–74, March 2008.

[14] SCAMPI project. *Official Web Pages of SCAMPI Project – IST-2001-32404*, 2005. `www.ist-scampi.org`.

[15] Greg Watson, Nick McKeown, and Martin Casado. Netfpga: A tool for network research and education. In *2nd workshop on Architectural Research using FPGA Platforms (WARFP)*, 2006.

[16] Nicholas Weaver, Vern Paxson, and Jose M. Gonzalez. The shunt: an fpga-based accelerator for network intrusion prevention. In *FPGA '07: Proceedings of the 2007 ACM/SIGDA 15th international symposium on Field programmable gate arrays*, pages 199–206, New York, NY, USA, 2007. ACM.