WISDOM: Security-Aware Fibres

Elias Athanasopoulos,
Antonis Krithinakis, Georgios Kopidakis
ICS/FORTH
Greece
{elathan, krithin, kopidaki}@ics.forth.gr

Graeme Maxwell, Alistair Poustie
Centre of Integrated Photonics
United Kingdom
{graeme.maxwell, alistair.poustie}@ciphotonics.com

Bob Manning, Rod Webb
University College of Cork
Ireland
{bob.manning, rod.webb}@tyndall.ie

Martin Koyabe, Carla Di Cairano-Gilfedder
British Telecom
United Kingdom
{martin.koyabe, carla.dicairano-gilfedder}@bt.com

ABSTRACT

The network is becoming faster day by day. High-speed links, of many Gbps, are considered as commodity technology empowering the Internet. On the other hand, Moore's law still applies to current processing power. It needs about 18 months for CPUs to double the number of their transistors. A very fast network composed by not as fast processors is unable to perform basic operations needed in the security field, like firewalling and intrusion detection. In this paper, we propose a novel system, which promotes security operations in the optical domain. We describe all hardware components - optical and digital - and the software, which renders the system functional. We outline application scenarios in which a hybrid architecture of optical and digital parts, like the one we propose in this paper, can offer significant benefit to the network from a security perspective.

1. INTRODUCTION

Optical devices are not considered anymore as *exotic* network equipment. They are used as commodity hardware for high speed links, substituting their digital ancestors; namely, digital-based wired links[8]. The vision is the development of faster networks with speeds ranging from tens to hundreds of Gbps.

On the other hand, Moore's law[6] seems that still applies; the number of transistors on a chip is doubling about every two years. That is, the network evolves in terms of performance faster than microprocessors. Modern CPUs cannot cope with exhausting operations over network packets transmitted with many Gbps. For example, there is no easy way to perform pattern matching in network traffic of 40 or more Gbps throughput. Although some custom solutions exist in the market[4], they are upper bound limited in terms of throughput, and they certainly are not considered commodity systems.

Operations, like pattern-matching, are considered fundamental for security oriented applications like firewalls and Intrusion Detection Systems (IDSs). Thus, it is vital for the community to investigate new ways of performing these tasks for high speed links, like the ones provided by optical systems.

In addition, optical hardware is proved to be more environmentally friendly than the digital one. In a world profoundly penetrated by technology, it is vital to promote architectures that can coexist with the ecosystem having the least possible side effects.

Our motivation is summarized as follows:

- **Limitations of CPUs:** Current CPUs cannot perform packet inspection in high speed links.
- **Optical penetration:** Optical networks are becoming commodity technology.
- **Green nature:** Optical based technology is environment friendly.

In this paper, we present a complete system for performing basic security operations purely in the optical domain: the *WISDOM*[1] *firewall*. For the rest of the paper, we will use the terms *WISDOM firewall* and *optical firewall*, interchangeably, in order to refer to our system prototype.

Our primary goal is the development of a system that will significantly alleviate from the burden microprocessors working in the digital domain, by performing part of the necessary computation in the optical domain.

This paper outlines the basic characteristics of the first prototype under development. The prototype is expected to be delivered during the first quarter of 2009. Moreover, we present the software platform, which models the complete architecture and which, by the time of writing, is fully functional.

To summarize, our contribution in this paper is outlined as follows:

- To the best of our knowledge, for the first time we present a system that can handle basic security ori-

[1]WISDOM stands for WIrespeed Security Domains Optical Monitoring and it is funded by the European Union's FP6 call under the contract 033847[11].

EUROSEC '09 Nuremberg, Germany

ented operations in the optical domain; the optical firewall.

- We present a real implementation of a fully functional software framework for modeling the optical firewall in all of its practical aspects.
- We outline the basic challenges and the roadmap of the actual deployment of the system, which is expected to take place in the first quarter of 2009.

The paper is structured in the following order. We present related work in Section 2. In Section 3 we depict the basic architecture of the system. In Section 4 we briefly discuss the optical algorithms utilized by the optical components. We present in detail the software modeling platform and some application scenarios that can be modeled in Section 5. We discuss some important issues in Section 6 and we conclude in Section 7.

2. RELATED WORK

Data communications continues to grow exponentially as worldwide consumers and businesses rely ever more heavily on electronic and computer based communication systems. At the heart of these global systems are optical fibre links and optical equipment that allow very high data speeds ($> 40Gbps$) and very large information handling capacities (Tbps). Today there exist no tools or systems that implement security checks (e.g. filtering information) directly at these high data rates at the optical domain.

Implementing packet filtering capabilities at the optical domain can be a significant component in a network especially at peering points. Given that the average size of an IP packet is around 252 bytes, a Gigabit link needs to process about 1-2 million packets per second[23]. Current security approaches, based on the electronic techniques at wirespeed, are not scalable and effective. However, the ability to directly process high speed optical data at wirespeed would allow simplification of optical networks and strengthen security. Capacity of optical fibres for data transmission is increased by wavelength-division multiplexing (WDM), which allows multiple optical signals of different wavelengths (channels) to be carried on a single fibre. Filtering of specific channels is then possible during demultiplexing, giving some possibilities for traffic management[22]. The technology outlined in this paper relies on all-optical logic on demultiplexed pulses-bits. Bit-by-bit all-optical processing of packet headers is performed on a data channel in order to provide wirespeed pre-processing for efficient security operations.

Existing firewall implementations perform a linear search, and use caching to improve performance. Even assuming (very optimistically) an 80% hit rate[29], the cost of linear search through 20K filters is a bottleneck even if it occurs only 20% of the time. A number of algorithms - Boyer-Moore[17], E2xB[15], Wu-Manber[30] and Piranha[16] have been proposed for pattern matching in network intrusion detection systems. The performance of each algorithm may vary according to the case in which it is applied. These variations may be caused due to pre-processing cost per packet, depending on the size of the comparison string, sets or rules.

In recent years, the market of Network Intrusion Detection and Prevention Systems (NIDS) is moving towards a multi-functional one-in-all security platform capable of performing network intrusion detection and prevention, stateful firewall and several additional security functions. However as customer demand for multiple security services increases, there is a shift especially in large telecommunication operators and network providers to support multi-blade architectures such as the Advanced Telecommunications Computing Architecture (ATCA) chassis[1]. The ATCA architecture enables incorporation of the latest trends in high speed interconnects technologies, next generation processors, and improves reliability, manageability and serviceability. It therefore allows Telcos to offer best of breed virtual instances of NIDS including Netflow[3], McAfee HIPS[5], Snort[27], Sourcefire[10] and Check-Point[2].

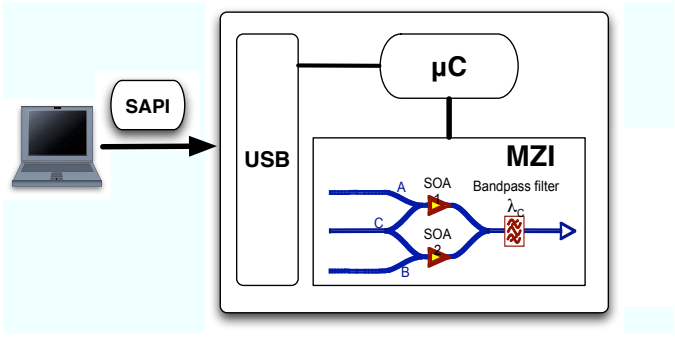

Figure 1: Schematic representation of the Optical Firewall architecture. In the scheme, the MZI (the core optical engine) is identified. The MZI can be instrumented using a standard PC via the USB interface, through SAPI.

3. SYSTEM ARCHITECTURE

Our system is mainly composed by (i) optical components, (ii) digital components and (iii) the software API. The optical part serves as the core engine, which is able to perform all-optical pattern matching. The optical part is instrumented by the software API, which communicates with the core implicitly using a digital interface. In this section, we present in detail each of the three domains of operation, namely, the optical, digital and software, which compose the system's architecture.

3.1 Optical Core

Semiconductor optical amplifiers (SOAs)[20] are the non-linear elements of choice in order to achieve all-optical logic at bit rates up to 160 Gbit/s. They are commonly used as non-linear elements in Mach-Zehnder interferometers (MZIs) [25], to make interferometric switching devices. It should be noted that these gates lack the flexibility of electronic digital gates, and have a considerably larger footprint.

The optical core uses a SOA-based MZI as a logical switching element, with which we have managed to implement a pattern-matching algorithm (presented in section 4), as well as a CRC circuit (which has not yet been demonstrated experimentally in the project). The optical MZI has two SOAs, one in each arm. Using the MZI as a basic building block we are able to build an all-optical pattern-matching engine with the ability to look for patterns of size between 32-64 bits. Eventually, we believe that at the time of delivering the actual box, we will have managed to extend this limit. Another limitation is the ability to re-configure the patterns

of the box. For our experiments, we used fixed patterns, with the option of modifying them at a human-based scale and not in a real-time fashion. We further discuss these limitations in section 6.

3.2 Digital Interface

The optical box is assembled using digital components. Specifically, a micro-controller is used and a USB bus can interconnect the box with a commodity PC. Through the debugging phase we use a LabView[7] program in order to initialize and configure the search patterns for the MZI. All command instructions are transferred from the PC to the box via the USB bus.

3.3 Software API

The software API, which we refer to as SAPI (Security Application Programming Interface) is the mini operating system for the whole WISDOM firewall. Operations supported by SAPI are various low-level initialization functions (heating control, peltier control, etc.) as well as functions for setting and getting the search patterns used by the optical core.

SAPI is able to translate human rules to actual search patterns. For example, a rule that filters out e-mail traffic will produce the search pattern: *flag all packets with destination* `port 25`, or an ICMP[9] filter will produce the search pattern: *flag all packets with* `protocol 0x7`[2].

4. OPTICAL ALGORITHMS

In order to build a system for basic security operations in the optical domain, we need to have a basic toolkit for performing the fundamental operation of pattern-matching in an all-optical fashion. Although, efficient pattern-matching algorithms in the digital domain are almost straight-forward [17, 13], in the optical domain even a naive approach is quite challenging. In this section we highlight the basic challenges of building an all-optical pattern-matching algorithm and then we proceed in a brief presentation of the approach we use.

We have published a detailed description of our all-optical pattern matching algorithm in [26]. In this paper we briefly discuss the fundamental properties of our construct.

4.1 Challenges

The basic limitation in the optical domain is the absence of state. Practically, this means that it is not possible to build a state machine[18], which is a fundamental concept for seeking a sequential pattern in a stream of characters. Whilst electrons making up electrical data signals can be readily stored, photons, of which optical data signals are comprised, cannot, since light cannot be stopped without absorbing (and thereby destroying) the signal. Storage of data in optical form can only be achieved with the use of optical buffers (loops of optical fibre) in which it circulates continuously. Furthermore, even a naive matching of a specific pattern in a specific offset in the stream is challenging. For example, searching for a bit pattern `101` is contained in the bit string `1101` has to be done *on-the-fly* by comparing the value of each bit from the 2nd to the last one. In order to do this, bit-level synchronism between the bit pattern to be searched and the bit string is required, and the pattern matching has to be done sequentially.

[2]If the protocol field of an IP packet has the value of `0x7` the packet is identified as an ICMP packet.

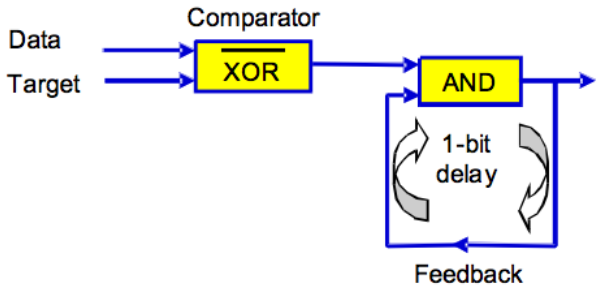

Figure 2: Serial pattern recognition system. The short feedback loop is only feasible with low-speed data.

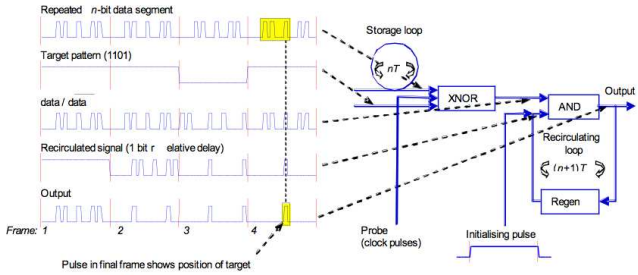

Figure 3: Schematic of pattern recognition system with example waveforms.

4.2 Approach Used

We require, in the optical domain, an XNOR gate and an AND gate in series (see Figure 2). The XNOR gate should compare a predetermined data sequence (the target) with the incoming data packet, the result being passed to the AND gate. Using a 1-bit delay, the result for the previous bit may be compared with the next result. An output set of ones corresponding to the length of the target sequence sought indicates the presence of such a sequence in the packet data.

This approach works for low data rate, where the 1-bit feedback delay is achievable. For bit rates approaching 40 Gbit/s however, the bit period is $25ps$, which is less than the time taken to pass through the optical gate. These gates are based upon semiconductor optical amplifiers placed in planar silica Mach-Zehnder interferometers, which have a physical dimension of several cm, corresponding to a time-of-flight of $> 100ps$[25]. This constraint may be overcome through the use of parallel or pipelined circuits, but these architectures require at least one gate per target pattern bit. The length of target is therefore restricted by both the practicable level of integration and the acceptable power consumption.

To overcome this problem, the pattern recognition system shown schematically in Figure 3 is used. Data is held in a storage loop in order to permit interaction between adjacent bits without the need for an unfeasibly short feedback loop[14]. An n-bit segment of input data $a_1, ..., a_n$ is selected as the search field by switching it into the storage loop, which has a length, nT, where T is the bit period of

the input data. The loop repeats the data segment into N output frames, where N is the number of bits in the target pattern being sought. The target pattern is generated at the rate, lower than that of the data, of one bit per frame and both the repeated data and the target are compared by an XNOR gate (inverse exclusive OR). The feed-back loop is $(n+1)T$ long, so that, after each circulation, the data in the recirculating loop is gated with the results of the comparison of the a_i with the next target bit. A true bit in the final frame indicates an occurrence of the complete target pattern in the data. Since the output bit is aligned with the last bit of the target, it serves not only to detect but also to locate the target. The example shown is for a 4-bit pattern (`1101`). Multiple bits will be generated if the target appears more than once. A more detailed description of the algorithm may be found in[26].

5. SOFTWARE AND MODELING

In this section we present the software platform we have developed for modeling the WISDOM firewall. It is a custom framework developed specifically for the needs of our architecture. It runs in any PC, equipped with a network interface and a Microsoft Windows operating system. The framework does not aim in modeling the optical core of the system; there are options currently in the market for simulating optical devices[12]. Instead, our initial goal was to produce a software environment that illustrates the operation of our architecture as a whole system.

By using the framework we are able to reproduce application scenarios, we discuss later in this section, in a controlled software environment. We can estimate time costs and verify the pattern matching optical algorithm we presented in section 4.

This section is organized as follows. First, we present the framework's features through a quick guide using limited screen shots of the software environment, due to space constraints. We later proceed and depict some possible usage configurations and application scenarios. For a full description of the software platform we refer the reader to [21].

5.1 Overview

One of our first major concerns during the development of the framework was that it had to target a mixed scientific audience and not only computer scientists. This is, mainly, because our collaboration is composed by physicists, electrical engineers and computer scientists. Thus, we took the decision to develop a graphical user friendly application for the Microsoft Windows operating system. The framework can be used by anyone without requiring deep technical knowledge of computer software.

With the assistance of the graphical environment the user is able to construct instances of all-optical pattern matching boxes. We will further refer to such an instance as a *filter* or *rule*.

Each filter is configured using a dialog box. The user can specify the protocol of the filter, as well as the source and destination port of an incoming packet. In Figure 4 we depict a dialog box for the configuration of a filter that matches all e-mail packets. Specifically, an e-mail filter is interpreted as a rule that matches all TCP packets with destination port value `25`.

Once the user is satisfied with the setup, an icon of an MZI based all-optical pattern matching box is displayed in the user's desktop. In Figure 4 such an icon is depicted, which embeds a filter for ICMP packets. Note, that a filter for e-mail is considered as a *synthetic* rule, since it is consisted by two parts: the protocol and the destination port. Thus, the e-mail filter produces two instances of an all-optical pattern box. See Figure 5 for this clarification.

Each all-optical pattern matching box depicts an instance of a pattern matching operation that is based on the algorithm we presented in section 4. This means, that *each packet is processed using the complete optical algorithm for pattern matching and not using simple equality relations of computer programming.*

The user may construct unlimited filters in this fashion. However, the actual system's capacity is limited. The actual WISDOM firewall is expected to be able to serve simultaneously only a few filters.[3]

Upon having set the preferred filters, the framework can inject traffic to the simulated system. This can be achieved either by passively capturing the traffic experienced by the host, which runs the framework, or by processing already captured traces. The latter method is used mainly for debugging purposes. Each filter, depicted in the user's desktop as an optical firewall instance, updates its statistics in real-time. Statistics include packets captured, packets matched the filter and packets that did not. In addition, a global *tick* counter accounts for the cost of the whole session in terms of time spent. We define as a *tick* the amount of time spent for processing one bit of information in the optical domain. In the real case, a tick is in the scale of tens of *picoseconds*, but this can be slightly varied depending on the final intrinsic characteristics, specified in the actual construction phase of the optical devices (namely the SOAs), which will be used in the assembling of the prototype. The software framework supports the dynamic redefinition of the *tick* metric.

In Figure 5 we depict the framework, while running, using two filters, an ICMP and an e-mail one; the e-mail filter is expanded in two all-optical pattern matching boxes as it has already been explained.

5.2 Usage

Our custom framework is able to simulate specific application scenarios. In this way, it is a significant assistant for (i) producing effective rules that can be used in a hybrid firewall consisting of optical and digital components and (ii) verifying the correctness of the operation of the final prototype.

An application can be seen as a set of filters that will be eventually applied in a high speed link and will classify a significant volume of the traffic. Recall, that our goal is to push some of the firewall functionality in the optical domain and thus alleviate the computing effort of the digital hardware.

The correctness of operation is defined as the number of false positives and false negatives the optical firewall has. A false positive is defined as an event where a packet is flagged incorrectly and a false negative as an event where a packet is not flagged as it should. The expected number of false positives and negatives is *zero*. That is, an input trace, which we know in advance its contents, should be flagged identically both by the software framework and the actual prototype.

[3]Although, we have some re-configuration abilities, which in a sense extend the supported set of filters.

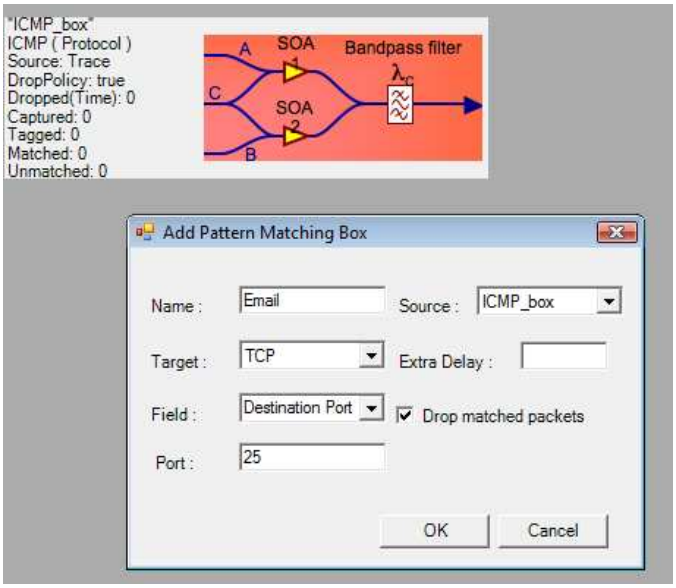

Figure 4: The configuration of all-optical pattern matching boxes. With the assistance of the environment the user is able to set up rules for a custom filter. In this Figure an ICMP filter has already been constructed (see the MZI icon displayed in the user's desktop) and an e-mail filter is in the process of its configuration.

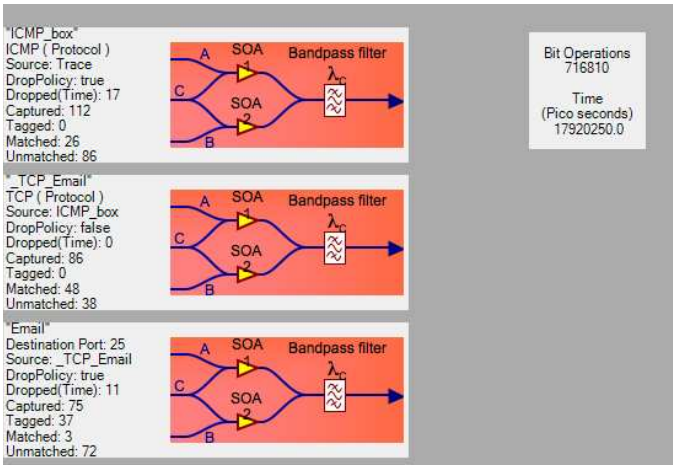

Figure 5: The environment during run-time. Two rules have been set up; an ICMP and an e-mail rule. Each rule takes as input real traffic and a global counter is accounting for time processing.

A possible application scenario is a hybrid optical-digital infrastructure to cope with SPAM[19], Web malware[24], as well as ICMP[9] filtering. We assume that our system operates in network links that exceed the throughput of 40 Gbps. The optical firewall is able to separate all e-mail and Web traffic natively in the optical domain. The pre-filtered traffic can be redirected in more sophisticated digital systems, that can perform SPAM processing and intrusion detection for Web requests. In addition, the optical firewall may drop all incoming ICMP packets, before they manage to reach any router operating in the digital domain.

6. DISCUSSION

In this section we highlight some important aspects of the proposed architecture. We first list some important limitations of the system and finally we discuss how compatible is the architecture with the fundamental principle of the Internet, widely known as *the end-to-end argument*[28].

Limitations. The WISDOM firewall can perform all optical pattern-matching only in the header of inspecting packets. This is, also, the case for most modern digital firewalls; they utilize rules that depend only in header fields. This imposes some constraints in the possible applications of the optical firewall. We presented some possible usages in section 5, which were based only in information located at the header of a packet. The limitation of header only searching comes from the fact, that, at least at the moment, we are not able to build rich in functionality state machines (this has been discussed in detail in section 4). Thus, deep packet inspection is something we can not achieve at this stage of development.

However, we expect that all-optical deep packet inspection will be possible in the near future. Throughout the development of the project we have pushed the size of the search pattern, at least three times. We started with the ability to perform pattern matching for search patterns of a few bits, and lately we have accomplished successfully experiments with search patterns of 64 bits. We expect that we are going to push this limit even further. Thus, our vision for the future, as optic devices become more powerful, is to have the ability, by using multiple instances of our architecture, to deploy the first all-optical Intrusion Detection System.

End-to-end argument. The fundamental principle of the Internet, widely known as the *end-to-end argument* [28] suggests that the functionality should be placed at the edges of the network, and not at the network itself. Since, our proposed architecture promotes security operations at the optical level, someone may argue that we violate this very important principle. Our position in that case, is that our architecture does not violate the *end-to-end argument*. More precisely, we propose to assist modern digital firewalls with all-optical ones, that may perform a significant pre-filtering. In fact, our proposed architecture *is to be used at the edges of the network*, in co-operation with digital routers.

7. CONCLUSION

In this paper, for the first time, to the best of our knowledge, we presented an architecture that promotes security operations in the optical domain. The motivation for such a construct is that digital hardware can not cope with modern high-speed optical links. Performing pattern-matching, a basic operation for all security software, in links experiencing throughput greater than 40 Gbps, today, is not trivial.

We analyzed in detail all characteristics of our proposed system. Namely, the optical core and the algorithm used for pattern-matching, the digital units and the software used for the control of the architecture. We, also, presented a custom software framework for the system modeling. The software framework is fully operational at the time of writing.

Throughout this paper we enumerated major constraints imposed in the optical domain, that make the construction

of an optical firewall quite challenging. The proposed system is real and the first prototype - available only for demonstration - is expected to be delivered during the first quarter of 2009. We believe, that our system is the beginning of a new generation of optical based hardware, that can perform sophisticated all-optical processing for security purposes.

8. ACKNOWLEDGEMENTS

We thank the anonymous reviewers for their valuable comments. We would also like to thank Lubomir Stroetmann, who contributed to this project while interning with FORTH. This work is funded by the FP6 EU project WISDOM. Elias Athanasopoulos, Antonis Krithinakis and Georgios Kopidakis are also with the University of Crete. Elias Athanasopoulos is also funded by the Microsoft Research PhD Scholarship project, provided by Microsoft Research Cambridge.

9. REFERENCES

[1] Asis. `http://www.asis-pro.com/Default.asp`.
[2] CheckPoint. `http://www.checkpoint.com/`.
[3] Cisco, Netflow. `http://www.cisco.com/`.
[4] endace - NinjaBox-Z Series. `http://www.endace.com/our-products/ninja-platforms/ninjabox-z-series`.
[5] McAfee, HIPS. `http://www.mcafee.com/`.
[6] Moore's Law. `http://www.intel.com/technology/mooreslaw/`.
[7] NI - LabView. `http://www.ni.com/labview/`.
[8] Optical hardware market holds steady at $2.7 billion in 3Q05. `http://findarticles.com/p/articles/mi_hb4766/is_200601/ai_n17355712`.
[9] RFC792 - Internet Control Message Protocol. `http://www.faqs.org/rfcs/rfc792.html`.
[10] Sourcefire. `http://www.sourcefire.com/`.
[11] The WISDOM Project. `http://www.ict-wisdom.org`.
[12] VPIphotonics. `http://www.vpiphotonics.com/`.
[13] A. V. Aho and M. J. Corasick. Efficient string matching: an aid to bibliographic search. *Commun. ACM*, 18(6):333–340, 1975.
[14] A.J. Poustie et al. All-optical parity checker. In *Optics Communications, 162, 37*, 1999.
[15] K. Anagnostakis, S. Antonatos, M. Polychronakis, and E. Markatos. A domain-specific string matching algorithm for intrusion detection, 2003.
[16] S. Antonatos, M. Polychronakis, P. Akritidis, K. G. Anagnostakis, and E. P. Markatos. Piranha: Fast and memory-efficient pattern matching for intrusion detection. In R. Sasaki, S. Qing, E. Okamoto, and H. Yoshiura, editors, *SEC*, pages 393–408. Springer, 2005.
[17] R. S. Boyer and J. S. Moore. A fast string searching algorithm. *Commun. ACM*, 20(10):762–772, 1977.
[18] C. C. Carroll. R68-40 sequential machines and automata theory. *IEEE Trans. Comput.*, 17(9):922–923, 1968.
[19] L. F. Cranor and B. A. LaMacchia. Spam! *Commun. ACM*, 41(8):74–83, 1998.
[20] D. Cotter et al. Non-linear optics for high-speed digital information processing. In *Science 286, pages 1433-1636)*, 1999.
[21] A. Krithinakis, L. Stroetmann, E. Athanasopoulos, G. Kopidakis, and E. P. Markatos. WSIM: A Software Platform to Simulate All-Optical Security Operations. *European Conference on Computer Network Defense*, 0:41–47, 2008.
[22] R. A. Lauder and R. A. Halgren. Optical firewall. Technical Report EP1263154, December 2002.
[23] P. Newman, G. Minshall, and T. L. Lyon. IP switching — ATM under IP. *IEEE/ACM Transactions on Networking*, 6(2):117–129, 1998.
[24] M. Polychronakis, P. Mavrommatis, and N. Provos. Ghost turns zombie: Exploring the life-cycle of web-based malware. In *Proceedings of the 1st USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET)*, April 2008.
[25] A. Poustie. Semiconductor devices for all-optical signal processing. In *Proceedings of European Conference on Optical Communication*, volume 3, pages 475–8, 2005.
[26] R. P. Webb et al. 42gbit/s all-optical pattern recognition system. In *Proceedings of Optical Fibre Communications (OFC)*, 2008.
[27] M. Roesch. Snort: Lightweight intrusion detection for networks. In *LISA*, pages 229–238. USENIX, 1999.
[28] J. H. Saltzer, D. P. Reed, and D. D. Clark. End-to-end arguments in system design. *ACM Trans. Comput. Syst.*, 2(4):277–288, 1984.
[29] S. Suri and G. Varghese. Packet filtering in high speed networks. In *SODA '99: Proceedings of the tenth annual ACM-SIAM symposium on Discrete algorithms*, pages 969–970, Philadelphia, PA, USA, 1999. Society for Industrial and Applied Mathematics.
[30] S. Wu and U. Manber. A fast algorithm for multi-pattern searching. Technical Report TR-94-17, 1994.