

# New Trend of Intrusion Detection System for High-speed Networks

Wei Wei

School of Computer Science and Engineering

East China (North) Regional Network Center (NENC) of CERNET

Southeast University, Nanjing, Jiangsu, China 210096

## 1 Introduction

Network Intrusion Detection System (NIDS) is an important and practical tool for network security. To guarantee a precise detection the NIDS must detect packets at a wire speed. However, with the recent trend of high-speed networks, the capability of a single NIDS can not meet the speed's demand, resulting in rising of false negatives.

To promote the NIDS performance and efficiency, present studies on IDSs for high-speed network monitoring have begun to choose the distributed architecture as an alternative, first suggested by Christopher Kruegel et al [1]. In such a design, the incoming network traffic is disseminated to a pool of sensors, which process a fraction of the whole traffic, reducing the possibility of packet loss caused by overload.

## 2 Related work

Two key technologies in the parallel IDS are traffic splitting and load balancing. To guarantee every sensor's independent intrusion detection, the splitting algorithm should distribute packets of the same attack to the same sensor, which means that packets belonging to one flow go to the same sensor. Meanwhile the splitting algorithm should be efficient enough to keep up with the network speed and distribute the traffic among sensors as evenly as possible. However, network traffic characteristics such as average packet size, inter-arrival time and protocols vary with time and environments. Consequently, the traffic splitting approach must be adaptive. Recent traffic splitting designs are mainly based on flows, hashing the triple consisting of source and destination IP addresses and port numbers, which is a unique identification of a flow, to a specific sensor. In addition, a design based on security policies and IDS characteristics is proposed and discussed [2].

In research of NIDS, unlike in web servers, distributed systems or clusters, load balancing is mainly concerned with the guarantee of appropriate sensor load much more than fairness of work distribution. As to the assignment of load balancing in NIDS, there are many different arguments around. Most researchers [4], [5], [6] suggest that the traffic splitter must be responsible for load balancing to keep the detecting capability of sensors and easily manage the overall system, while some others [7] argue that when assigned whole load balancing, the splitter implement should be based on expensive specific high-speed instruments to work at a full wire speed, and more may be likely the bottleneck of the system. Therefore they propose that load balancing should be achieved by each sensor based on the load balancing approach. Moreover how to predict overloading on nodes precisely and reduce the load smoothly to get a smallest packet loss rate is the main problem of load balancing. Studies of JIANG Wenbao and SUN Qin-dong both propose effective algorithms for load evaluation and adjustment [6], [7]. Unfortunately, the algorithm of JIANG's design is too complex and custom hardware must be used in the splitter, while the algorithm in [7] is impractical for practice for its relying on too many experiential parameters.

Besides the above working, there are several efforts on the improvement of the architecture. Early filtering, where a portion of the packets are processed on the splitter instead of the sensors, and locality buffering are used to increase the system performance [3]. And on the other hand, L Schaelicke, K Wheeler and C Freeland propose multiple levels of hashing to disperse the highly intensive traffic on one sensor [4]. Different to the two ideas above, LU Zhi-Jun et al's work proposes that an analyzing node, which receives messages issued by sensors, detects the

multi-object attack behaviors and adjusts the distribution of the network flow dynamically, should be added to the system<sup>[5]</sup>. However, there are still no complete set of practical schemes based on the architecture in general.

### 3 Our work

East China (North) Regional Network Center (NENC), one of the eight regional nodes of China Education and Research Network (CERNET), is an organization responsible for operating and maintaining the regional network. Security management is one of its important duties. By close monitoring the CERNET regional backbone, it acquaints security trend and responses in time.

For the need of network operation and management purposes, we have developed a misuse intrusion detection system-Monster 3.0, which supports Gigabit Ethernet links traffic processing. It has functions including security event detection, response and management, and has been applied to the construction of CERNET high-speed regional networks and an information service system for key disciplinary areas successfully. But the speed of our backbone network has reached up to 10G so that one single Monster can't be capable to monitor the whole network effectively. So we are investigating a parallel IDS for high-speed networks based on the distributed architecture.

The system has those features:

- 1) Using common PC servers without requiring special hardware
- 2) Running on high-speed networks steadily and assuring a low packet loss rate
- 3) A simple and efficient splitting design to meet the demand of high speed, assign the traffic across nodes as evenly as possible and adapt itself to the variety of the network traffic
- 4) A practical dynamic load balancing scheme to achieve a proper balance between the packet loss rate and the algorithm complexity
- 5) Integrating the node-issued alert messages to detect multi-object attacks on the whole network
- 6) Providing the high level report on objective network's macroscopic security trend analysis, response suggestions, and reactions at the same time

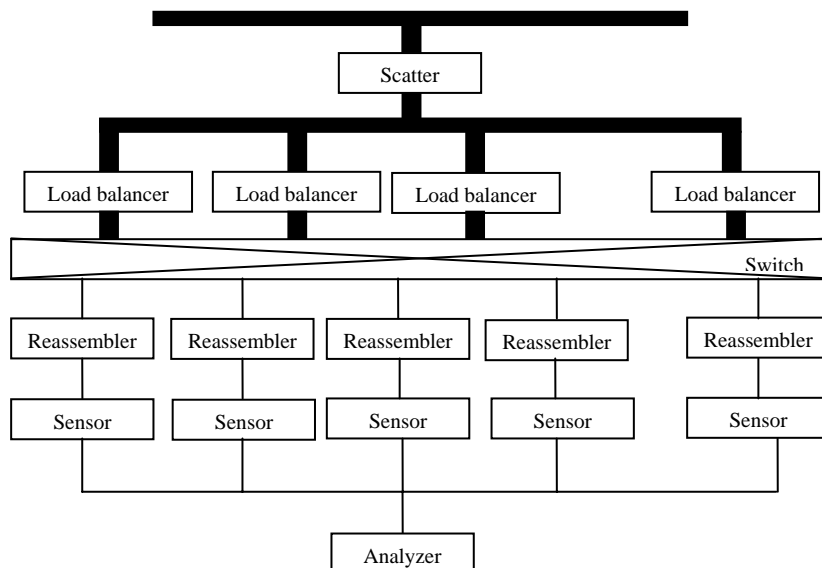


Figure 1 the architecture of the system

Figure 1 shows the architecture of our system. To keep up with the high traffic throughput the scatter only distributes the packets to load balancers evenly in a round-robin. Each load balancer first discards the packets containing no payload and matching no rules, which do not require content matching by an early filtering to reduce

the load on the sensors, then assigns its traffic to corresponding sensors by the splitting algorithm, and makes dynamic load balancing by the feedbacks from sensors. The original order of two packets could be lost if the two frames took different paths over distinct load balancers to the same sensor. Therefore, thereassemblers associated with each sensor make sure that the packets appear on the sensor in the same order that they appeared on the high-speed link. At the last step, the analyzer integrates the alert messages from sensors and detects possible missed multi-object attacks. It can also evaluate the network's macroscopically security trend and gives out its response suggestions and reactions.

#### **4 Conclusion**

Effectively resolving the capability of process and analysis of network security for high-speed networks, the parallel IDS architecture has a better scalability and flexibility with a hierarchical structure. Based on this architecture, the IDS will effectively monitor our backbone network for security and helps us in the evaluation and forecast of network security situations.

#### **References**

- [1] C. Kruegel, F. Valeur, G. Vigna, R. Kemmerer. Stateful Intrusion Detection for High-Speed Networks. Proceedings of the IEEE Symposium on Security and Privacy. Los Alamitos, Californias: IEEE Press, May 2002. 285- 293.
- [2] Tarek Abbes, Alakesh Haloi, Michaël Rusinowitch. High Performance Intrusion Detection using Traffic Classification. Proceedings of the IEEE International Conference on Advances in Intelligent Systems (AISTA2004), Luxembourg , Nov 2004.
- [3] I.Charitakis, K.Anagnostakis, E.Markatos. An Active Traffic Splitter Architecture for Intrusion Detection. Proceedings of the 11th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS 2003), Orlando, October 2003. 238- 241
- [4] L.Schaelicke, K.Wheeler, C.Freeland. SPANIDS: A Scalable Network Intrusion Detection Loadbalancer. Proceedings of the 2nd Conference on Computing Frontiers, Ischia, Italy, 2005.
- [5] LU Zhi-Jun, ZHENG Jing, HUANG Hao. A Distributed Real-Time Intrusion Detection System for High-Speed Network. Journal of Computer Research and Development, 2004, 41(4):667-673.
- [6] JIANG Wenbao, HAO Shuang, DAI Yiqi, LIU Tinghua. Load Balancing Algorithm for High-speed Network Intrusion Detection Systems. Journal of Tsinghua Univ (Sci&Tech), 2006, 46(1):106-110.
- [7] SUN Qin-dong, ZHANG De-yun, GAO Peng and ZHANG Xiao. Study of Parallel IDS Load Balancing Algorithm. Mini-microsystems, 2004, 25(12):2215-2217.