

# **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  
wwei@njnet.edu.cn**





# Outline

---

- **Introduction**
- **Related work**
- **Our Work**
- **Conclusion**





# Introduction

- **The recent trend of high-speed networks**

- *2004 Dataquest Stat.*

- *14% of the links between core routers : OC-768(40 Gbps)*

- *21% of edge links : OC-192(10 Gbps)*

- **Increasingly complex intrusion detection methods**

- **Challenging the capability of a single NIDS**



# Introduction

## ■ Distributed architecture as an alternative

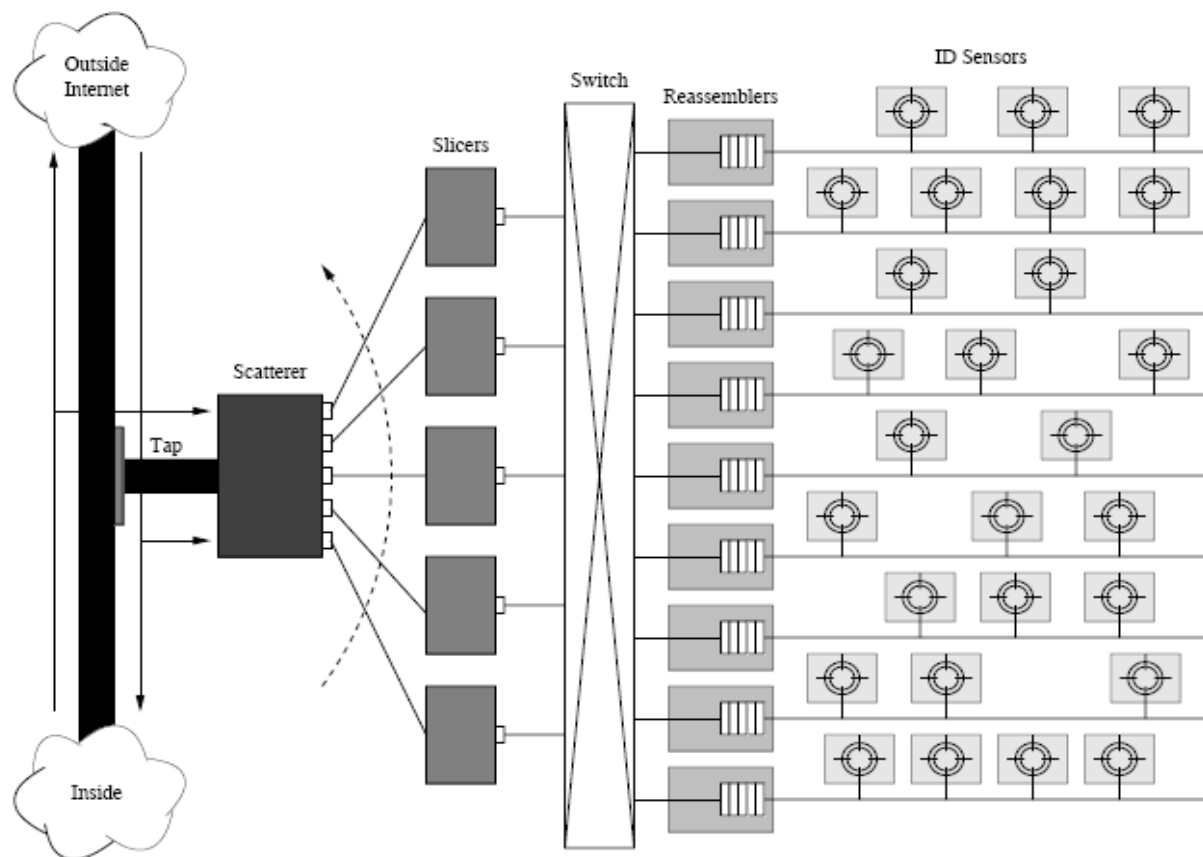
### ■ Basic idea

- *Traffic splitting*
- *Parallel process*
- *Reducing load on a single node*

### ■ Components

- *Network tap*
- *Traffic scatter*
- *Traffic slicer*
- *Switch*
- *Stream reassembler*
- *Channel*
- *IDS sensor*

# Introduction





# Introduction

---

## ■ Evaluation

- *Good scalability and flexibility*
- *The back end processing system can be managed in a form of a computer cluster, whose capability highly exceeds a single node*



# Related Work

---

## ■ Two key technologies

—*Traffic splitting*

—*Load balancing*





## Related Work

---

### ■ Traffic Splitting principles

- *To distribute packets of the same attack to the same sensor*
- *Efficient enough to keep up with the network speed*
- *To distribute the traffic among sensors as evenly as possible*
- *Adaptive to the variety of the network traffic*



# Related Work

---

- **Recent traffic Splitting approaches**

- **Mainly based on flows**

- *Hashing the triple of a flow to a specific sensor*

- **Some based on security policies and IDS characteristics**



# Related Work

---

## ■ Load balancing

- Unlike in other environments such as web servers or clusters
  - *Mainly concerned with the guarantee of appropriate sensor load much more than fairness of work distribution*

## ■ Assignment of load balancing in NIDS

### ■ Traffic splitter

- *To keep the detecting capability of sensors and easily manage the overall system*

### ■ Each sensor

- *Choosing packets to detect based on the load balancing approach*





# Related Work

---

## ■ Load balancing algorithm

— *How to predict overloading on nodes precisely*

— *How to reduce the load smoothly to get a smallest packet loss rate*



# Related Work

---

## ■ Improvement of the architecture

- Early filtering*
- Locality buffering*
- Multiple levels of hashing*
- Adding an analyzing node*



# Our work

---

## ■ Past work

### ■ A misuse intrusion detection system-Monster 3.0

— *Supporting Gigabit Ethernet links traffic processing*

— *Applied to the construction of CERNET high-speed regional networks successfully*



Beijing Node

Wuhan Node

Shanghai Node

National Backbone  
CRS1

Regional Backbone  
7609

Regional Backbone  
6503

10G Channel  
2.5G Channel

1G Channel  
100M Channel





# Our work

## ■ Our goal

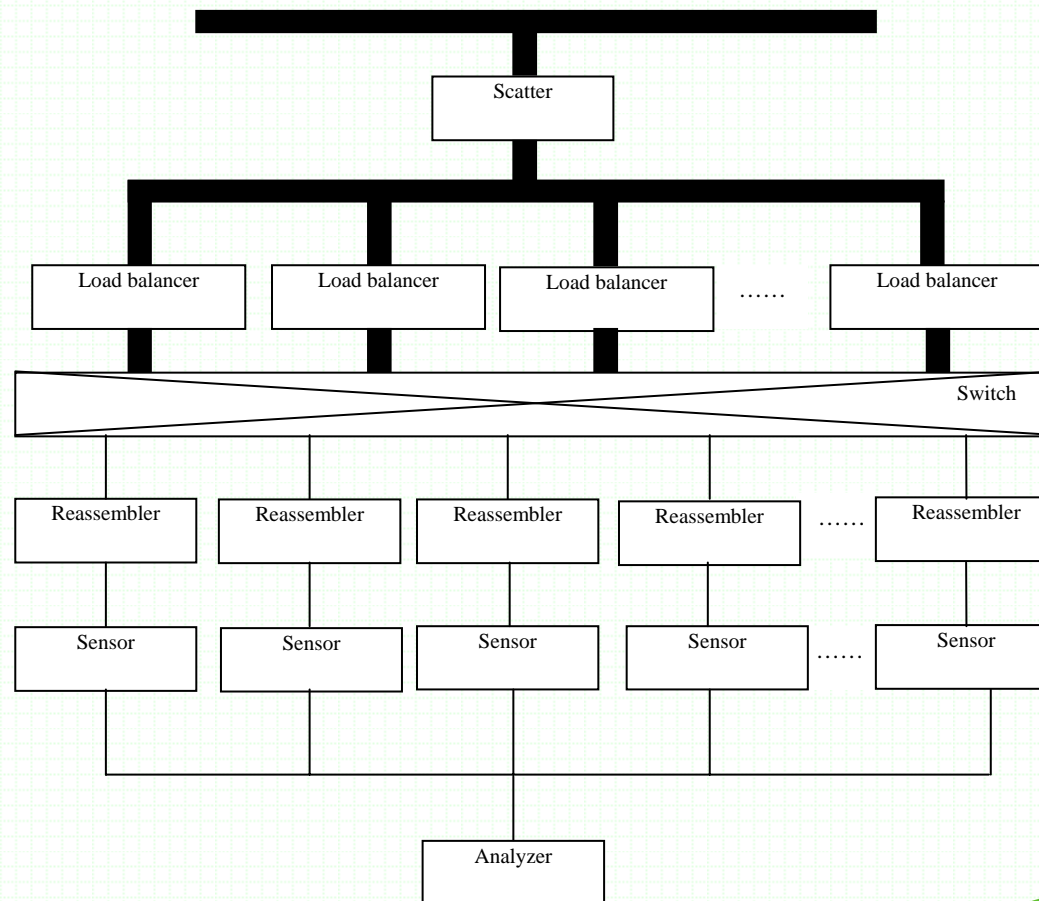
- **A parallel IDS for high-speed networks based on the distributed architecture**

## ■ Features of the system

- *Using common PC servers without requiring special hardware*
- *Running on high-speed networks steadily and assuring a low packet loss rate*
- *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*
- *A practical dynamic load balancing scheme to achieve a proper balance between the packet loss rate and the algorithm complexity*
- *Integrating the node-issued alert messages to detect multi-object attacks on the whole network*
- *Providing the high level report on objective network's macroscopic security trend analysis, response suggestions, and reactions at the same time*



# Our work





## Conclusion

---

- **The parallel IDS architecture effectively resolves the capability of process and analysis of network security for high-speed networks.**
- **It 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.**



*Questions?*

*Thank You*

