MUNI
C4E

On the Impact of Flow Monitoring Configuration

Petr Velan et al.

velan@ics.muni.cz

Institute of Computer Science, Masaryk University

April 20, 2020

Network Flow Monitoring

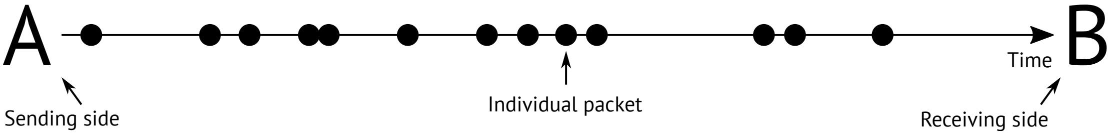
Network Flow Monitoring

- Used for monitoring of large networks
- Scales better than DPI
- Supported by network equipment (NetFlow and IPFIX protocols)

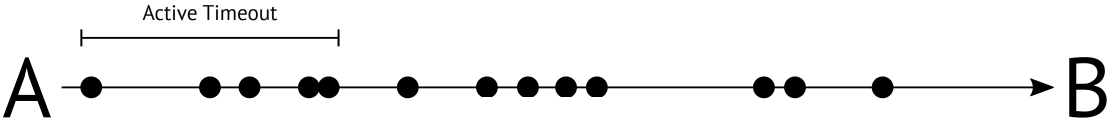
Use of Flow Monitoring Data

- Network management
  - Network planning (using long term statistics)
  - Network debugging
- **Security**
  - Incident handling
  - Policy verification
  - Attack detection
  - Anomaly detection

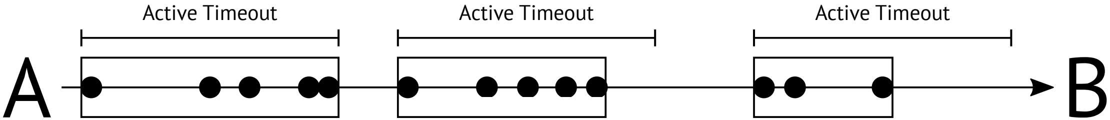
Flow Record Creation



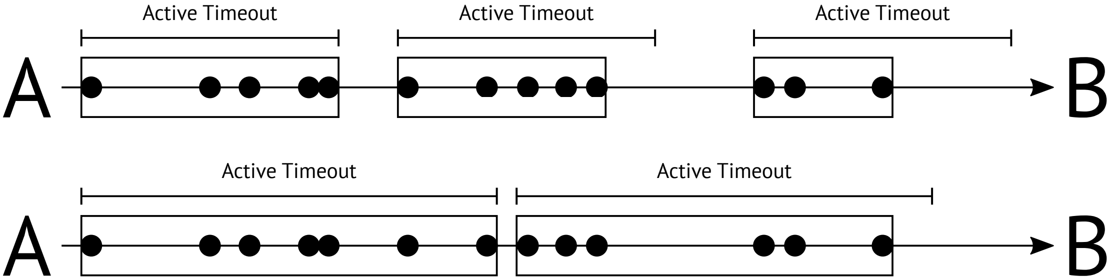
Flow Record Creation



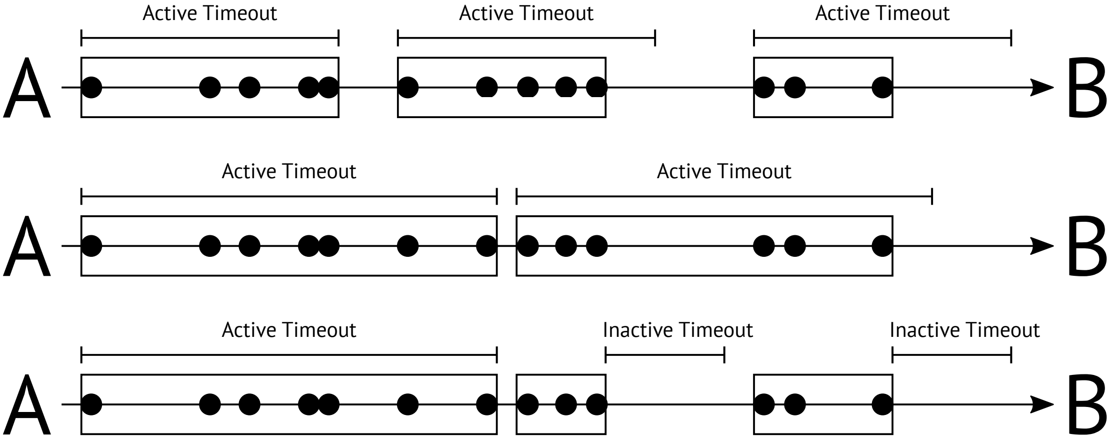
Flow Record Creation



Flow Record Creation



Flow Record Creation



Flow Record Creation

Flow Expiration Conditions

- Active timeout
- Inactive timeout
- Protocol specific reasons (e.g. end of TCP connection)
- Resource restrictions (e.g. limited flow cache size)
- Exporter shutdown

The Important Lesson

Configuration of flow monitoring is essential!

If you are publishing results based on flow data:

Always include description of flow monitoring configuration.

Flow Expiration Configuration Impact

What is affected by flow expiration timeouts?

- Flow export
  - Larger inactive timeout causes flows to be cached longer which increases computing and memory requirements
  - Smaller timeouts increase number of generated flow records, which increases computing and export bandwidth requirements
- Flow collection
  - Larger number of flow records increases computing and storage space requirements
- Flow analysis
  - Larger number of flow records increases computing requirements
  - Different number of flow records with different properties influences analysis results

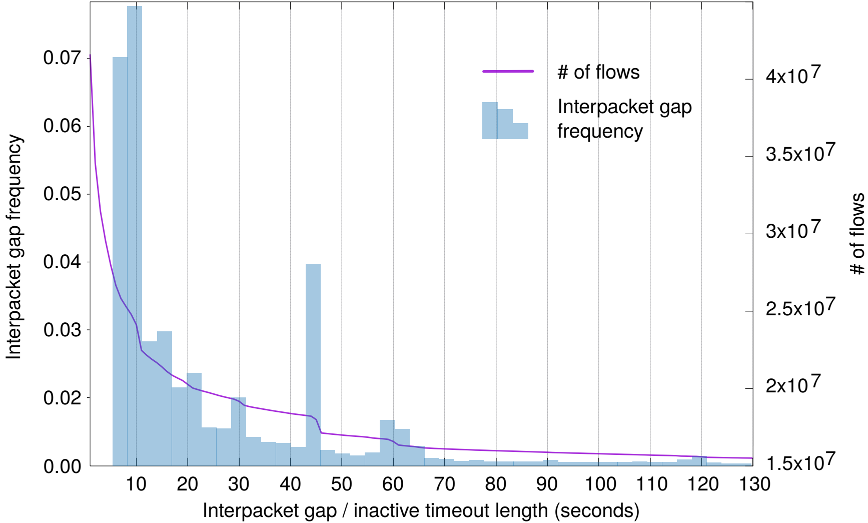
Number of Created Flows

How large is impact of flow expiration timeouts on flow creation?

To find out, we:

- Selected datasets
  - The CAIDA Anonymized Internet Traces 2015 Dataset (1.1 billion of packets)
  - A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018) (3.6 million of packets)
- Computed flows using a range of different timeouts
  - We were interested only in number of flows
  - Python tool – unsuitable for the CAIDA dataset (too slow, large memory consumption)
  - C++ tool, fast computation the flow records
- Analysed the results

Impact of the Inactive Timeout (CAIDA Dataset, TCP)



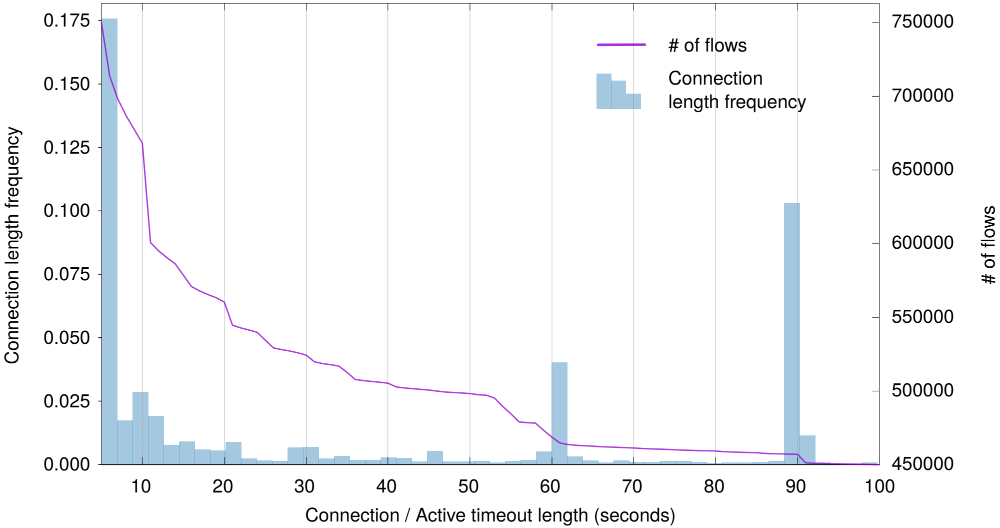
Impact of the Inactive Timeout (CAIDA Dataset, TCP)

Changing inactive timeout setting:

- 30 s -> 10 s causes an increase of almost 26% flows records
- 60 s -> 30 s causes an increase of almost 16% flows records
- 60 s -> 10 s causes an increase of almost **44%** flows records

A 45 second interpacket gap is quite common. Number of generated flows increases by 1.2% for 46 s and 45 s inactive timeout setting.

Impact of the Active Timeout (CSE-CIC Dataset, TCP)



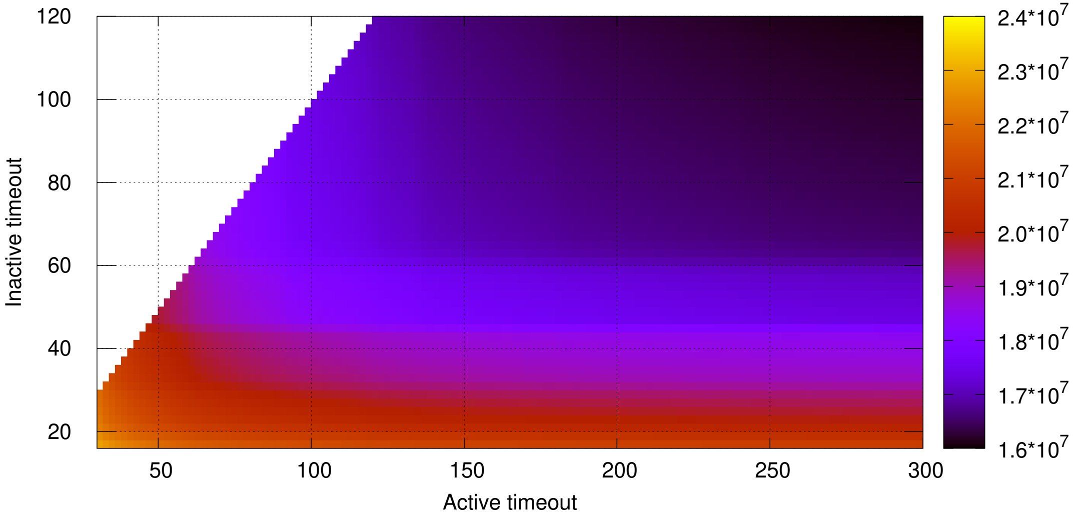
Impact of the Active Timeout (CSE-CIC Dataset, TCP)

The impact of active timeout is more complicated to evaluate

- Correlation between active timeout and connection length is weaker
- Number of multiples of active timeout that can fit into a connection length is also important (e.g. 10 s active timeout)
- Interpacket gaps influence the result as well

Decreasing the active timeout from 300 seconds to 120 seconds increases the number of flow records only by 3% (for this dataset).

Impact of the Combination of Both Timeouts (CAIDA Dataset, TCP)



Impact of the Combination of Both Timeouts (CAIDA Dataset, TCP)

Following can be derived from analysing the timeouts:

- Specifics of used transport protocols such as timeouts and common connection lengths (e.g. HTTP keepalive) can be observed as faster changes in the number of flows (colour changes)
- Different protocols (UDP, TCP, ICMP) and networks (datasets) behave differently

Decreasing the active timeout from 300 seconds to 120 seconds and the inactive timeout from 30 seconds to 10 seconds increases the number of flow records by **26%** (for this dataset).

Impact on Flow Data Analysis

The magnitude of impact of flow timeouts depends on a type of analysis, for example:

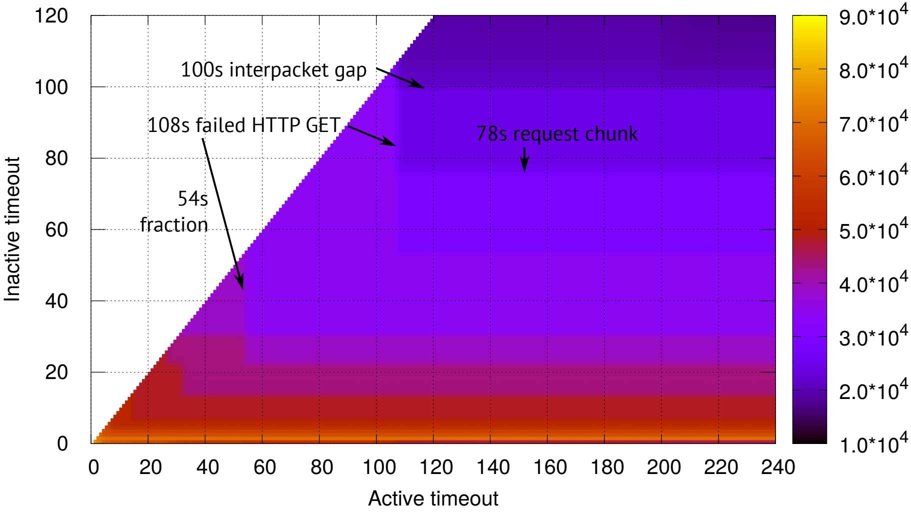
- Port scan detection will not be affected because port scans always generate only short flow records
- Covert dictionary attack can run slowly from multiple attackers to avoid detection. Their detection might be be affected by flow timeout settings
- DDoS attacks detection such as Slowloris detection will be affected the most

Impact on a Slowloris Attack Detection

There is a Slowloris attack in the CSE-CIC dataset, which we analysed:

- Successful attack establishes a TCP connection, sends first part of HTTP header and continues to send a small part of request header every 100 seconds (first after 78 s). The server responds with Bad Request response after approximately 2470 seconds.
- When the attack is successful, attacker does not get response for initial part of GET request and closes connection after 108 seconds
- In the most severe case, TCP connection cannot be established and attacker gives up after sending tree SYN packet in 3 seconds.

Impact on a Slowloris Attack Detection



Impact on a Slowloris Attack Detection

Caution is required when relying on flow data for Slowloris detection

- Large enough timeouts should be used
- Preprocessing using flow aggregation might be needed
- When using machine learning, ensure that flow expiration conditions remain the same throughout the whole process

Recommended Flow Expiration Configuration

When determining the flow expiration timeouts, the following should be taken into consideration:

- Timeouts should be tuned for different protocols (e.g. TCP, UDP) separately
- Timeouts must be based on processing delay requirements (data freshness)
- The number of generated flows must be within performance limitations of the monitoring system
- Timeouts must be accounted for by all network data analysis tools

Take Away Message – Reminder

Configuration of flow monitoring is essential!

If you are publishing results based on flow data:

Always include description of flow monitoring configuration.

Thank you for your attention

MUNI
C4E

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

C4E.CZ