

A Granularity-adaptive System for in-Network Attack Detection



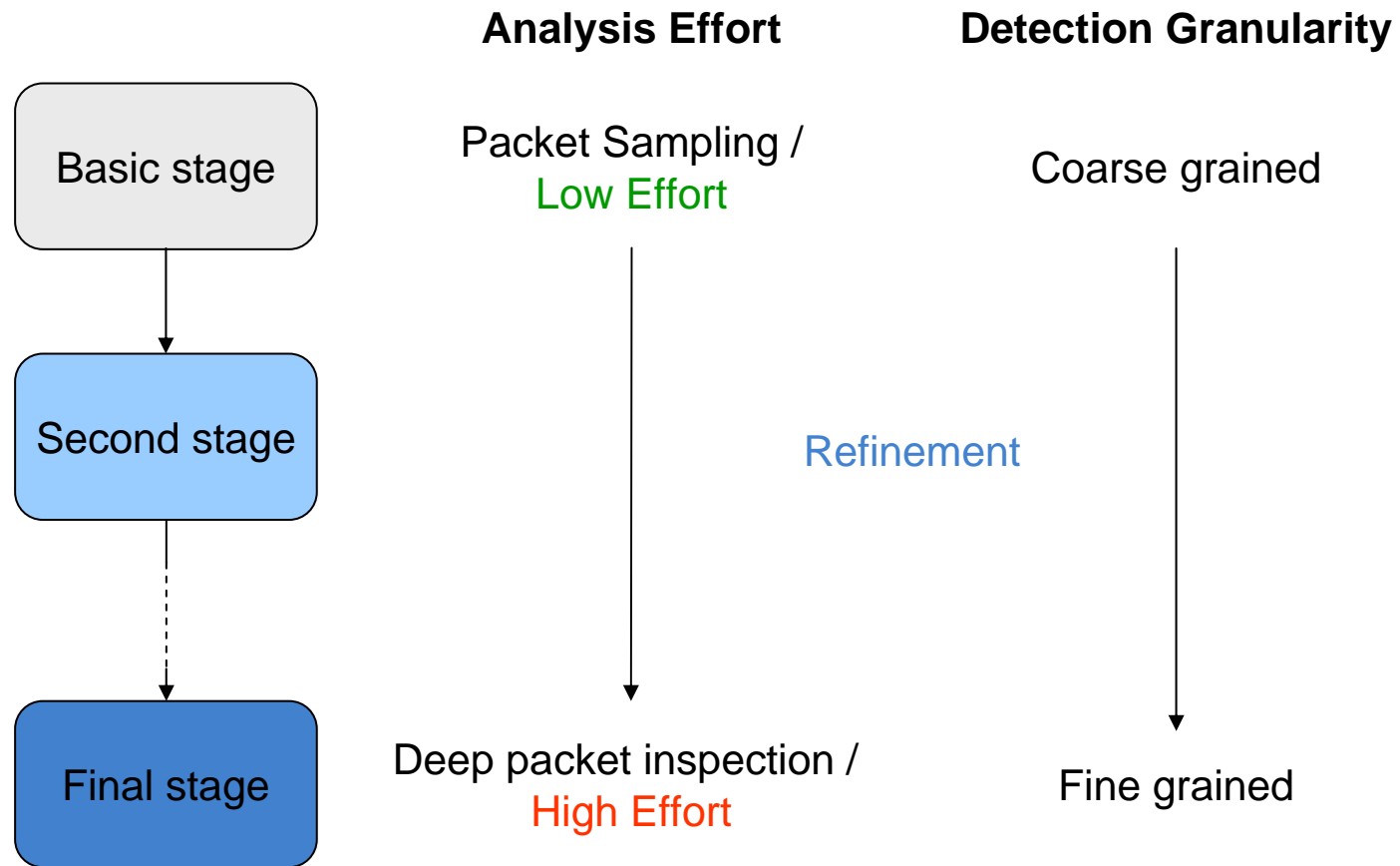
Thomas Gamer, Marcus Schöller, Roland Bless

Institut für Telematik, Universität Karlsruhe (TH), Germany

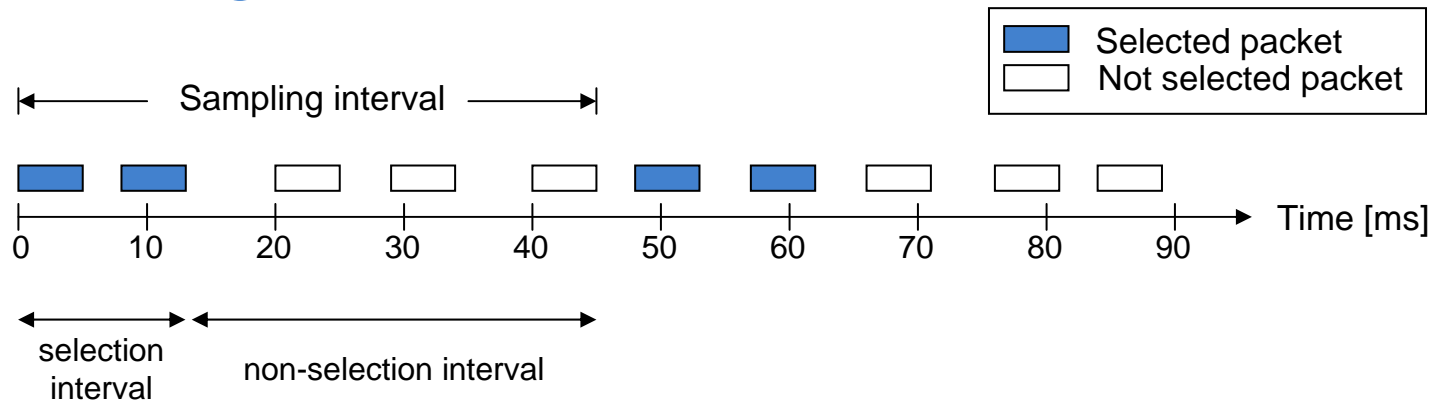


- Major threats in today's networks
 - DDoS attacks – commercialization
 - ▶ Main motivation: money, no longer fame
 - ▶ Blackmailing by DDoS attacks
 - Worm propagations
 - ▶ Preparation of DDoS attacks
 - ▶ Installation of botnets
- Early detection of these attacks
 - Support from network operators necessary
 - Victim cannot take effective countermeasures
 - Detection as early as possible
 - perform in-network detection

- In-network attack detection means
 - Detection in high-speed networks
 - Avoid forwarding delay by on-line analysis
- Possible Solutions
 - Special-purpose hardware (e.g., network processors)
 - ▶ Additional costs
 - ▶ Changing current infrastructure
 - Resource-saving detection system
 - ▶ Application of packet selectors
 - ▶ A hierarchical system using detection **refinement**



- Application of **Systematic count based sampling**



- Application of **Systematic count based sampling**
 - Introduces estimation errors
 - ▶ Limit error to predefined tolerance level
- Refinement reduces suspicious packet stream
 - Sampling probability has to be **increased** due to restriction of estimation error to tolerance level
 - Total number of selected packets, however, **decreases**

Interval rate (packets / interval)	Sampling probability	No of selected packets	Estimation error
125 k	4 %	5 k	14.62 %
12.5 k	30 %	3.75 k	14.75 %

- Architecture

- Basic stage detects stochastic anomalies

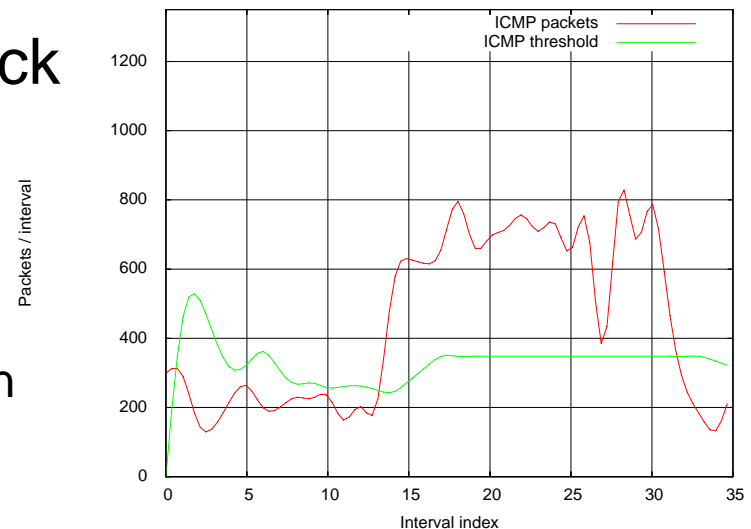
- ▶ Calculation of a dynamic **packet threshold**
 - ▶ Attack indication after **interval threshold** count of suspicious intervals
 - ▶ Due to self-similarity of Internet traffic

- Loading of further analysis stages after finding an attack indication

- Objectives

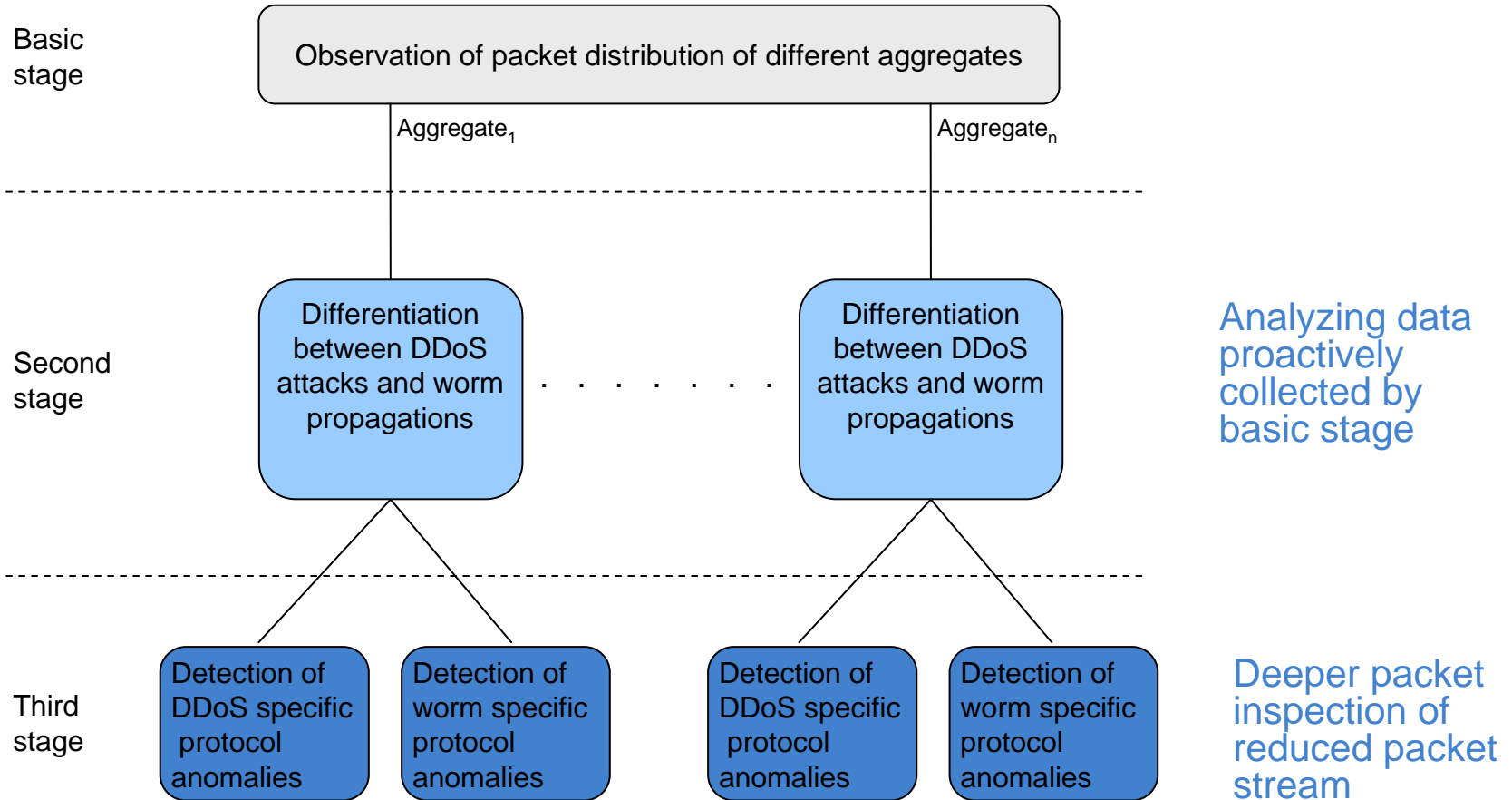
- ▶ Low resource consumption
 - ▶ Simple packet classification
 - ▶ Simple calculations

Packet distribution of an ICMP echo reply flooding attack (interval 60s)



- Further stages apply **Refinement**
 - **Deeper packet inspection** of suspicious packet stream
 - ▶ Reduction of packet stream by preceding stage
 - ▶ Sampling probability increases, but total number of selected packets decreases
 - Deeper packet inspection possible
 - **Analysis** of data **proactively** collected by preceding stage
 - ▶ History data has to be collected in preceding stage
 - ▶ Separation of data collection and analysis
 - Resource saving since calculations only performed if really required

Example: Small provider network



- Refinement enables
 - Attack detection in high-speed networks
 - Attack detection without adversely affecting a router's forwarding performance
 - No special-purpose hardware necessary
- Outlook
 - Adaptive sampling mechanism needed
 - ▶ Automatically adapt sampling probability to analyzed packet stream
 - ▶ Adaptation should limit estimation error to tolerance level