Blackbird: a scalable and resource-efficient framework for distributed network monitoring

Elisa Arnoldi, Gabriele Merli, Marco Abbadini, **Michele Beretta**, Dario Facchinetti, Matthew Rossi, Stefano Paraboschi

INTRODUCTION

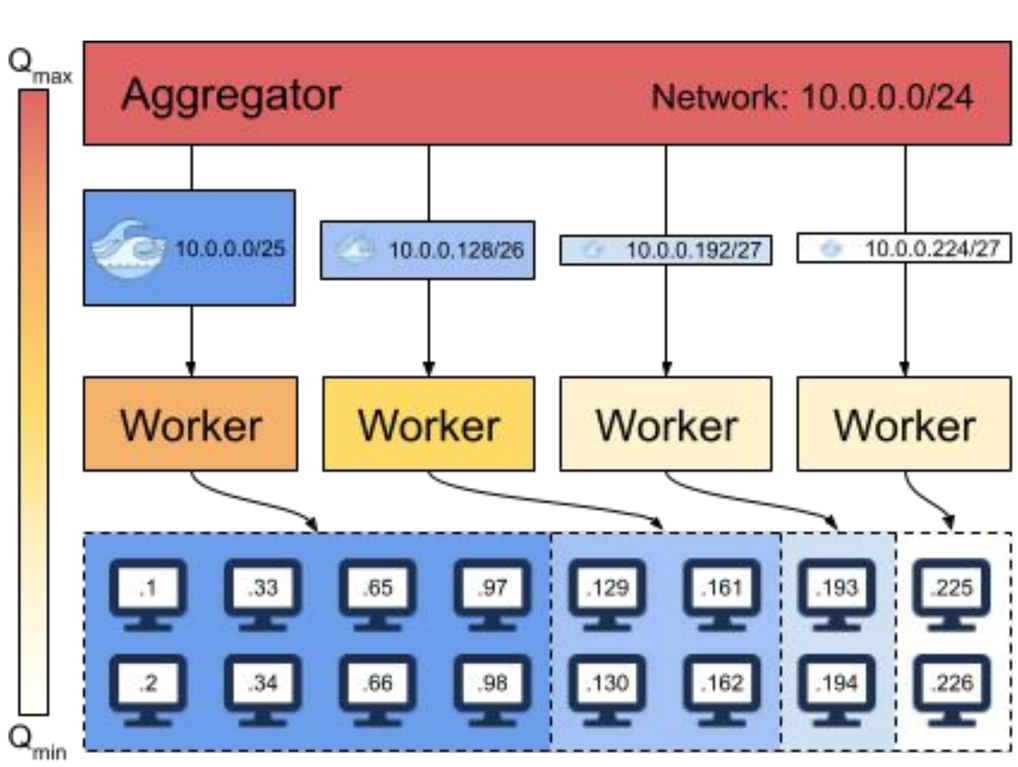
- Computer networks are increasingly large and complex
- Network monitoring is a useful technique to address security and management tasks

PROBLEM STATEMENT

- Existing monitoring tools are not up to par
- **Centralized tools**: simple, but generate a high volume of traffic and introduce a single point of failure
- **Distributed solutions**: resolve the high-volume traffic problem, but the need for aggregation re-introduces a central point of failure
- These methodologies can introduce prolonged monitoring gaps

CONTRIBUTION

- We introduce **Blackbird**, a new fully-distributed monitoring solution
- **No single point of failure**: scanned data is shared
- **Efficient**, and can run even on low-powered devices



IMPLEMENTATION

- Blackbird uses a set of agents deployed by the system administrator that are divided into **aggregators** and **workers**
- Aggregators, as the name suggests, collect data from workers and then share it with other agents
- Workers are tasked to scan their own section of the network through **waves**, a subdivision of the network address space
- All agents are able to **automatically self-organize** into aggregators and workers, even in case of failures

SELF-ORGANIZATION OF AGENTS

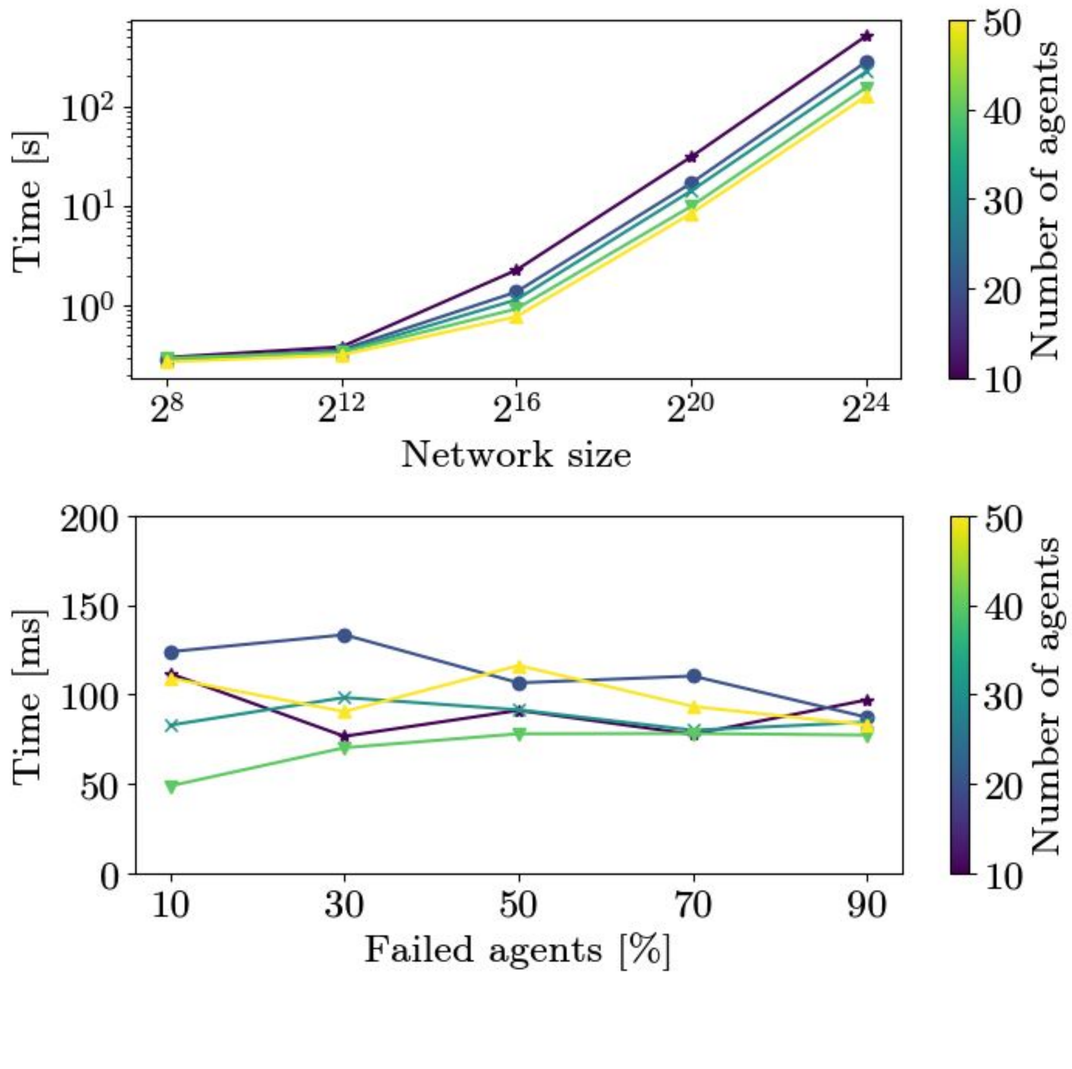
- Once distributed on some nodes of the network, agents will **self-organize** into aggregators and workers based on their **quality value**:

$$Q_i(t) = \alpha q_i(t) + (1-\alpha) Q_i(t-1) \quad \alpha \in [0,1]$$
$$q_i(t) = \sum_k w_k m_{i,k}(t) \quad w_k, m_{i,k} \in \mathbb{R}$$

- Quality indicates how **trustworthy** the node is, and is based on a historic average of weighted metrics (link quality, performance, and so on)
- The **most trustworthy** agents will become **aggregators**, the remaining ones will be workers
- After a failure, the agent tree will **self-heal** without any data loss

PRELIMINARY EVALUATION

- The number of agents highly influences **network scan times**
- With 10 agents, it is possible to scan a /12 network in under 30 s
- Agents are able to **self-organize** in under 100 ms, even when 90% of nodes fail



Unibg Seclab