Deploying and testing the Multi-Agent Ranking Framework

Georgi Nikolov Thibault Debatty Wim Mees [1]

[1]Royal Military Academy, Brussels, Belgium

Cyber attacks have become a major factor in the world today and their effect can be devastating. To combat these new sophisticated attacks, the Multi-Agent Ranking Framework (MARk) aims to provide all the building blocks that are required to build a large scale detection and ranking system. It is the basis of the Multi-agent Anomaly-based Advanced Persistent Threat Detection Framework [1], developed as a means of detecting abnormal and malicious activity inside a network, through the combined analysis of APT characteristics and evidence aggregation. The framework was deployed to test its performance and evaluate its detection capabilities.

The MARk Framework

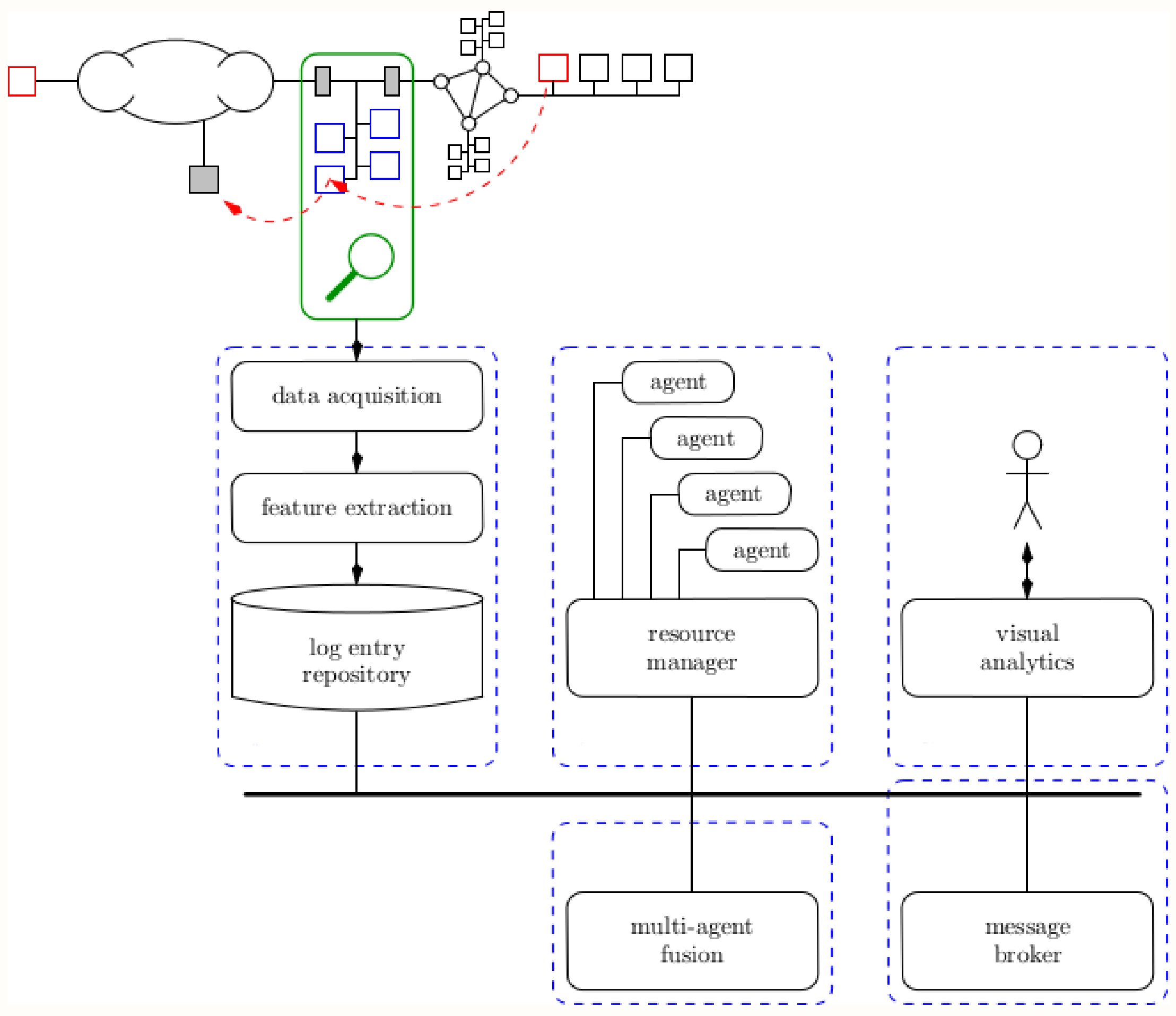

Figure 1: The MARk Framework

- Collect data from network log repositories
- Extract valuable features and store them
- When new data is available -> trigger corresponding agent
- Detector agents produce evidence when suspicious activity is encountered
- Evidences are aggregated and displayed via Visual Analytics

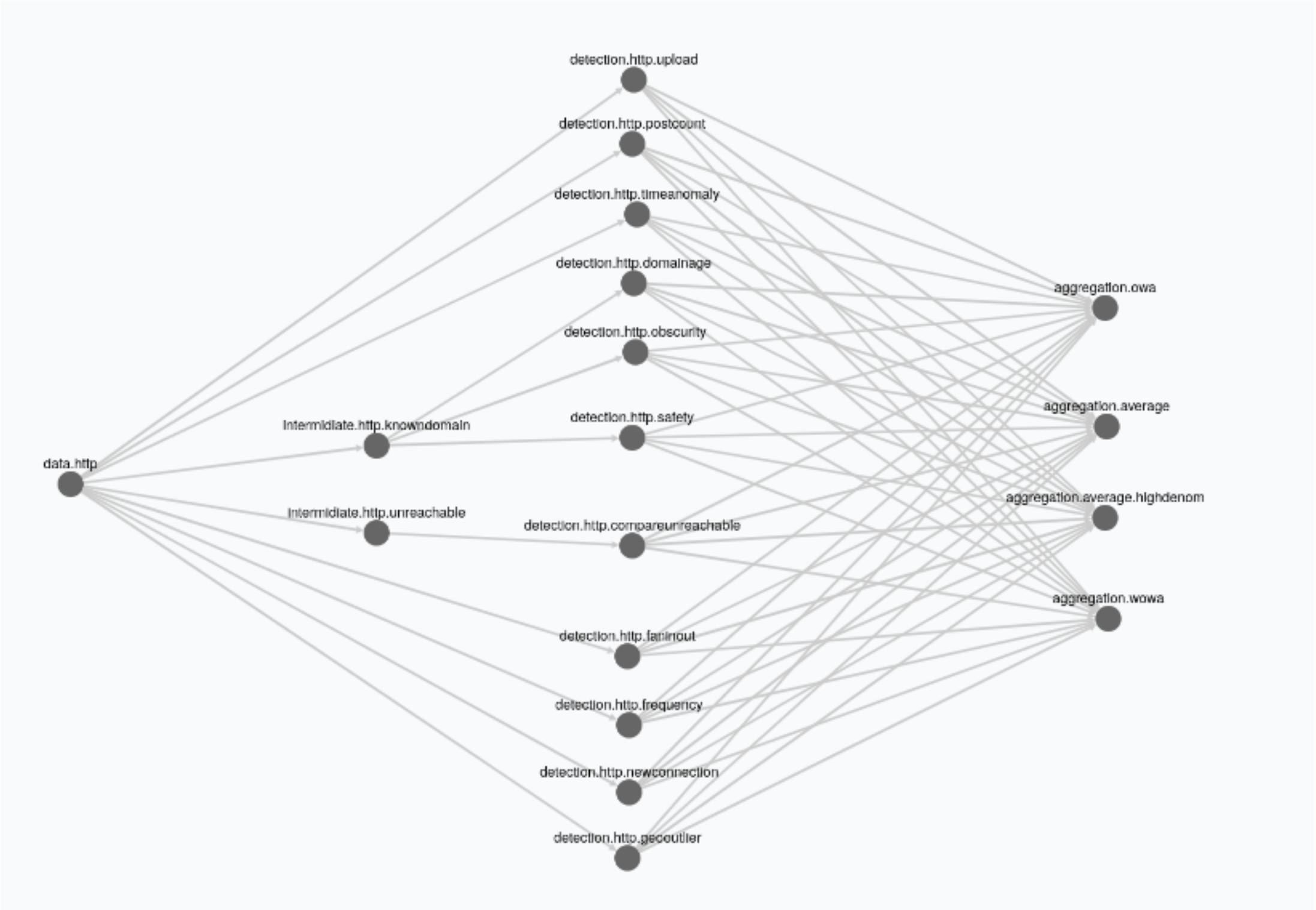

Figure 2: MASFAD Detection Cascade

An example of the Agent Detection Cascade is shown in Figure 2. The initial point in the cascade is the Data Source agent, which is responsible for retrieving new data and triggering the Detector agents. When a Detector agent produces an evidence, it can be passed to another Detector agent for further in-depth analysis, or aggregated by one of the Aggregation agents, which produces the final "suspiciousness score" after evaluation.

Deployment

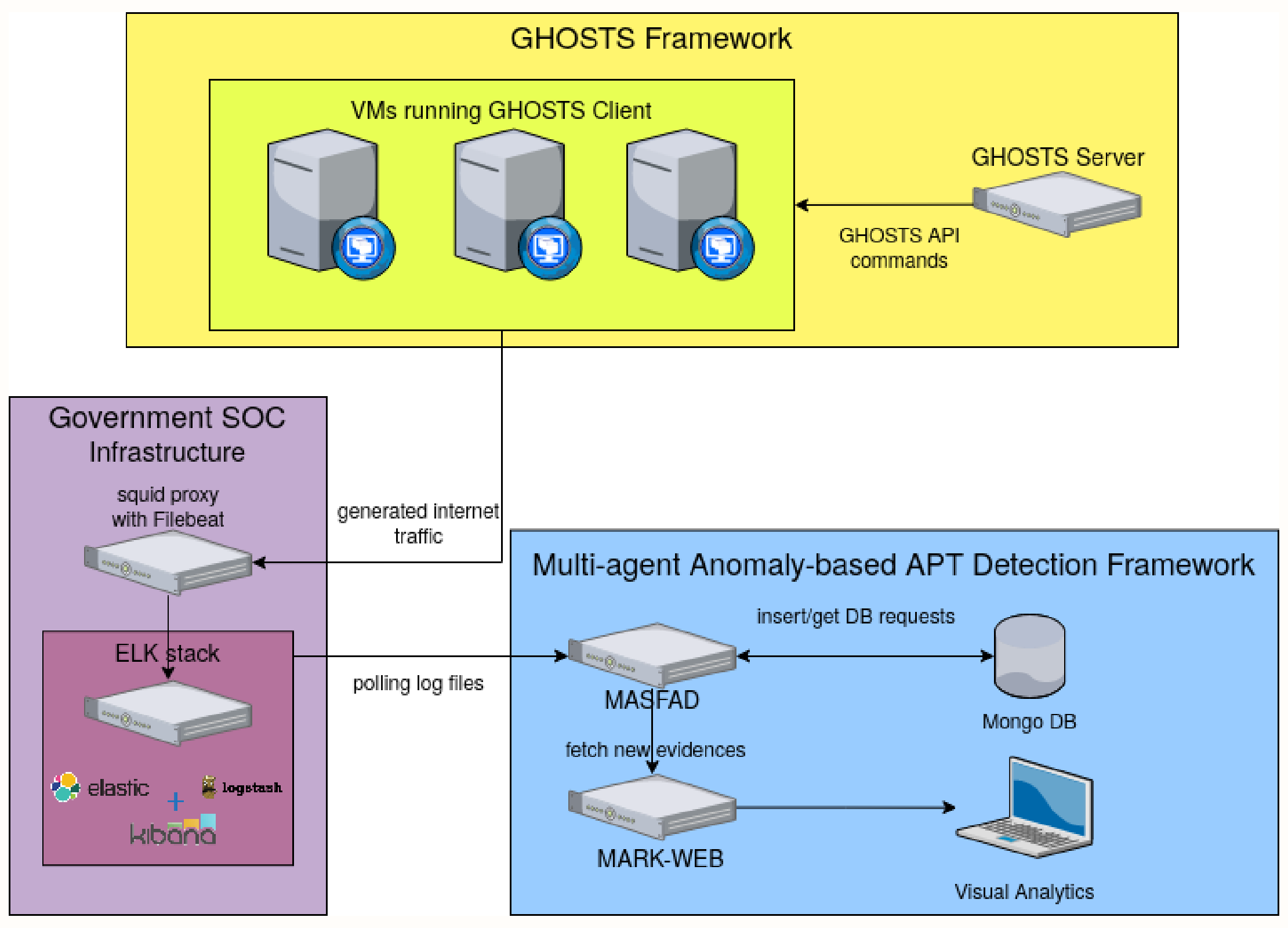

Figure 3: The MASFAD Deployment Architecture

The major components needed for the correct deployment of the testing environment are:

- A way to produce network traffic, done through the GHOSTS Framework
- Storing and filtering of the generated network traffic, done through the use of the ELK Stack
- Polling the network traffic and analysis, done through the MASFAD Framework

Data

To correctly test the framework, a large quantity of network traffic is needed for analysis. This has been achived through NPC automation, designed and implemented through the GHOSTS Framework [2]. The GHOSTS framework gives the possibility to configure a multitude of autonomous clients, each with predefined behavior, controlled by the GHOSTS server, through an API.

The generated network traffic is collected in squid proxy logs, via a deployed proxy server, and aggregated by Elasticsearch-Logstash-Kibana Stack (ELK Stack) [3], through the use of Filebeat. The ELK Stack module is closely modeled on the Security Operations Center, currently set-up at Belgian Defense.

Analysis and Visualization

The evidences produced by the Detector agents are aggregated by two Aggregation agents:

1. Ordered Weighted Average
2. Weighted Ordered Weighted Average

Each evidence aggregated by the OWA aggregation agent will be given a weight, a value that represents how significant it is for the aggregation. For the WOWA aggregator, not only do the evidences receive a weight, but also the Detector agents which have produced them. This helps to filter the reliability of the agents and attribute higher weights to the more precise Detector agents.

The evidence produced by the Aggregation agents is represented in multiple ways, through the use of the D3.js library [4], aiming to aid the domain expert in easily investigate it and gain insight in what has happened in the network. Examples of the representations are shown in Figures 4 and 5, the Bubble Graph and Radar chart respectively.

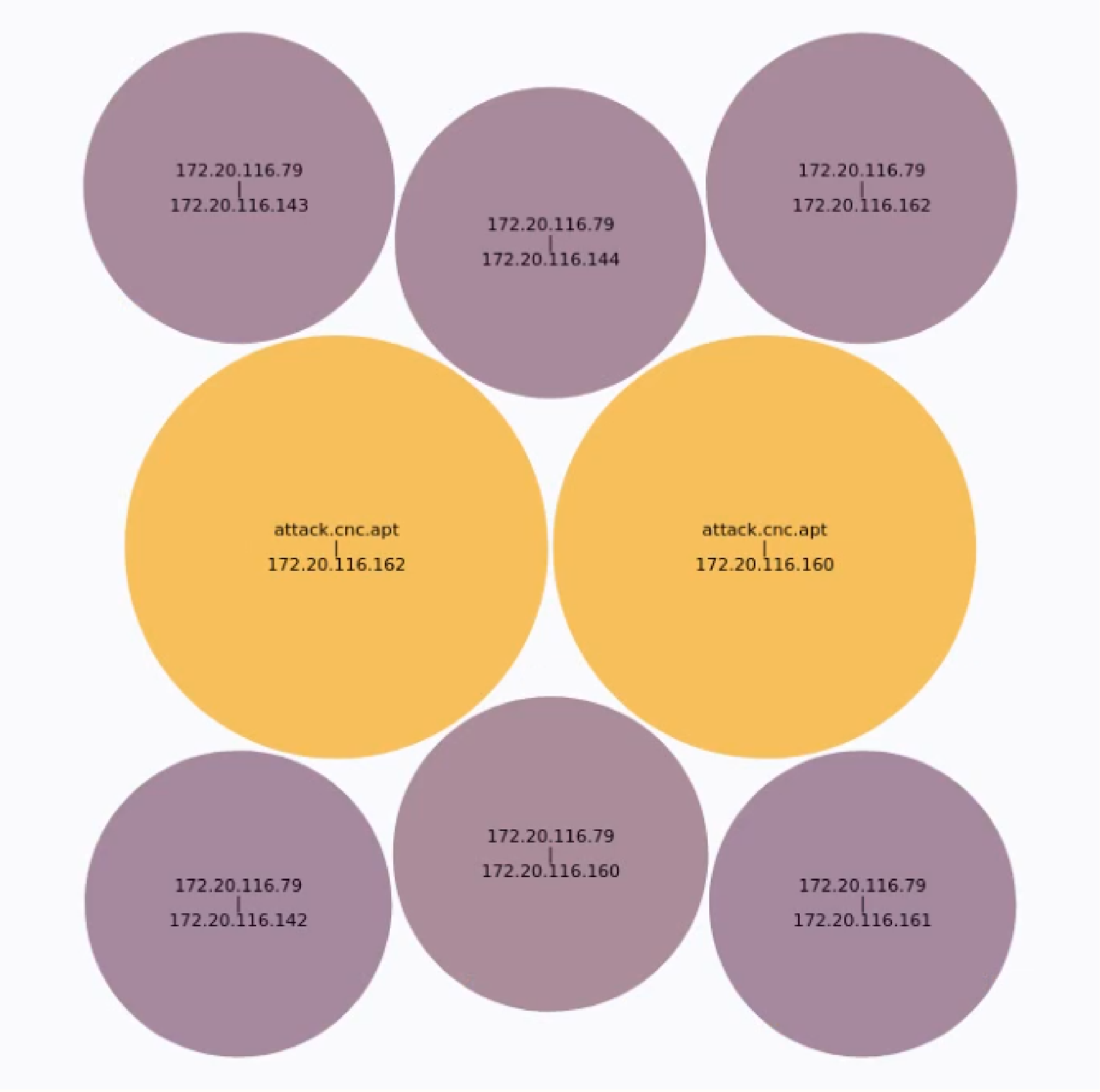

Figure 4: Example of Bubble Graph Visualization

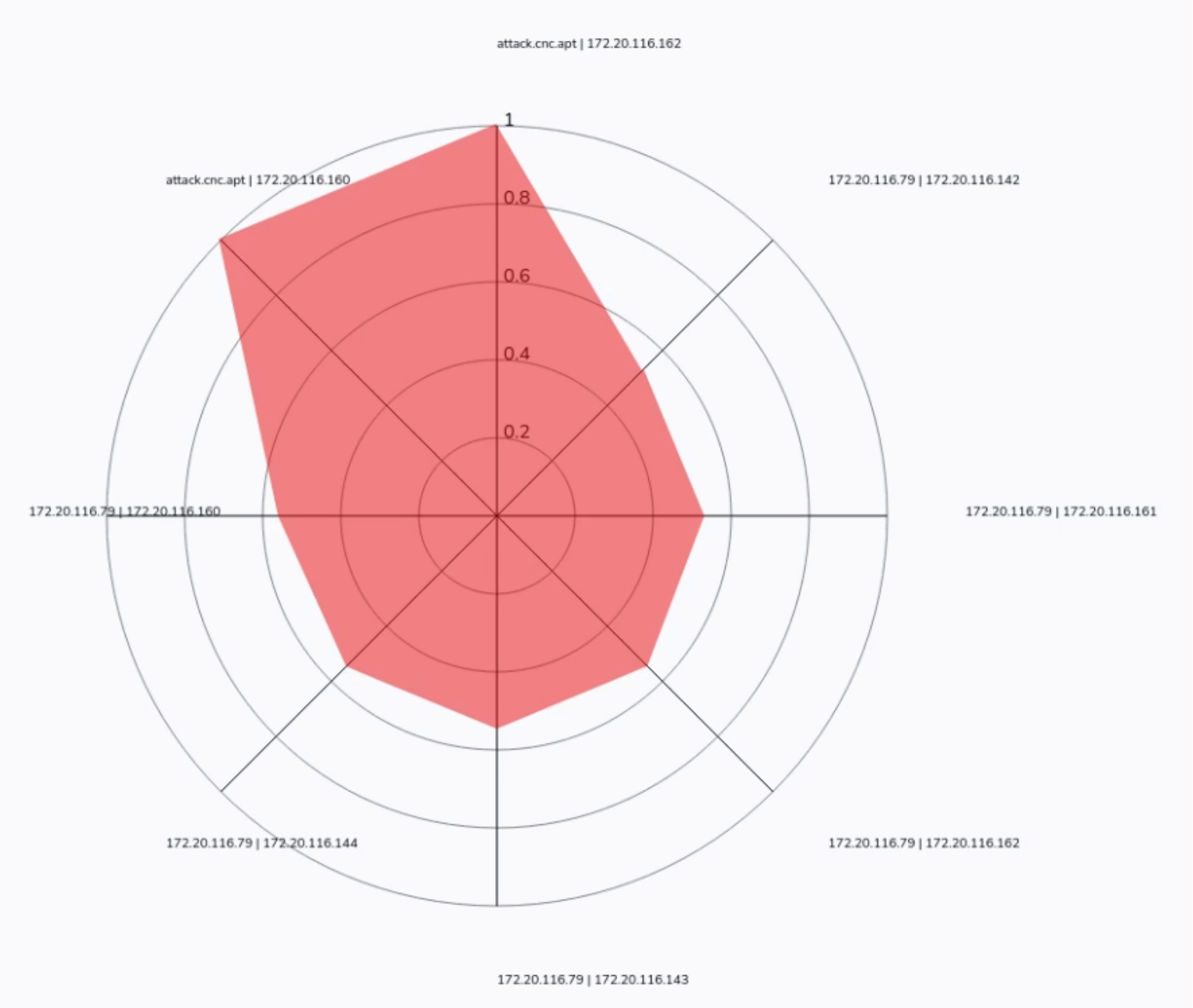

Figure 5: Example Radar Chart Visualization

Future Work

Possible future extensions of the testing scenario:

- Incorporate real-world data alongside the simulated network traffic
- Inject sophisticated real-world APT models
- Better integration with a variety of SOC applications
- Extend the available visualizations for more clarity and in-depth analysis

References

[1] G. Nikolov and T. Debatty and W. Mees, Evaluation of a Multi-agent Anomaly-based Advanced Persistent Threat Detection Framework, *The Twelfth International Conference of Evolving Internet (INTERNET 2020)*

[2] `https://github.com/cmu-sei/GHOSTS`

[3] `https://www.elastic.co/what-is/elk-stack`

[4] `https://d3js.org/`

DEFENCE

Cyber Defence Lab
Royal Military Academy
`www.cylab.be`

EUROPEAN DEFENCE AGENCY