Fachhochschule Gelsenkirchen

Global View
→ Idea and Realization

Prof. Dr.
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Content

- Aim and outcomes of this lecture
- Idea of the Global View
- Realization of the Global View
- Results of the Global View
- Future Work
- Summary

Content

- **Aim and outcomes of this lecture**
- Idea of the Global View
- Realization of the Global View
- Results of the Global View
- Future Work
- Summary

Global view
→ Aims and outcomes of this lecture

Aims

- To introduce the motivation of the Global View for a Internet Early Warning System
- To explore the realization of a Global View
- To analyze the results the Global View
- To assess the challenge of the Global View

At the end of this lecture you will be able to:

- Understand what is meant by Global View.
- Know something of the possible realization of the Global View.
- Understand how to make the right interpretation of the Global View.

Content

- Aim and outcomes of this lecture
- **Idea of the Global View**
- Realization of the Global View
- Results of the Global View
- Future Work
- Summary

Idea of the Global View
→ Local view

- Networks are black boxes
- Only the links (connection) between different networks can be monitored by the providers or companies
- Traffic between nodes of the same network are not visible to the outside
- Local view is defined as the set of events, which have been identified within a network

$$E_{n_i} = \{e_1, e_2, \ldots, e_l\}$$

e_i := event

Idea of the Global View
→ Global view

- The global view is **union** of the different subsets of the events of all the local views

$$E_G = \bigcup_y E_{n_y}$$

- Not all events are interesting for a global perspective
  - e.g. breakdown of a redundant local network component
- Interesting events are e.g.
  - DDoS attacks, distribution of malware, spam, breakdown of a service like DNS, search service, …
- Special interest when for the subset of E_{n_i} the following term is valid:

$$e_d \in \bigcap_i E_{n_i}$$

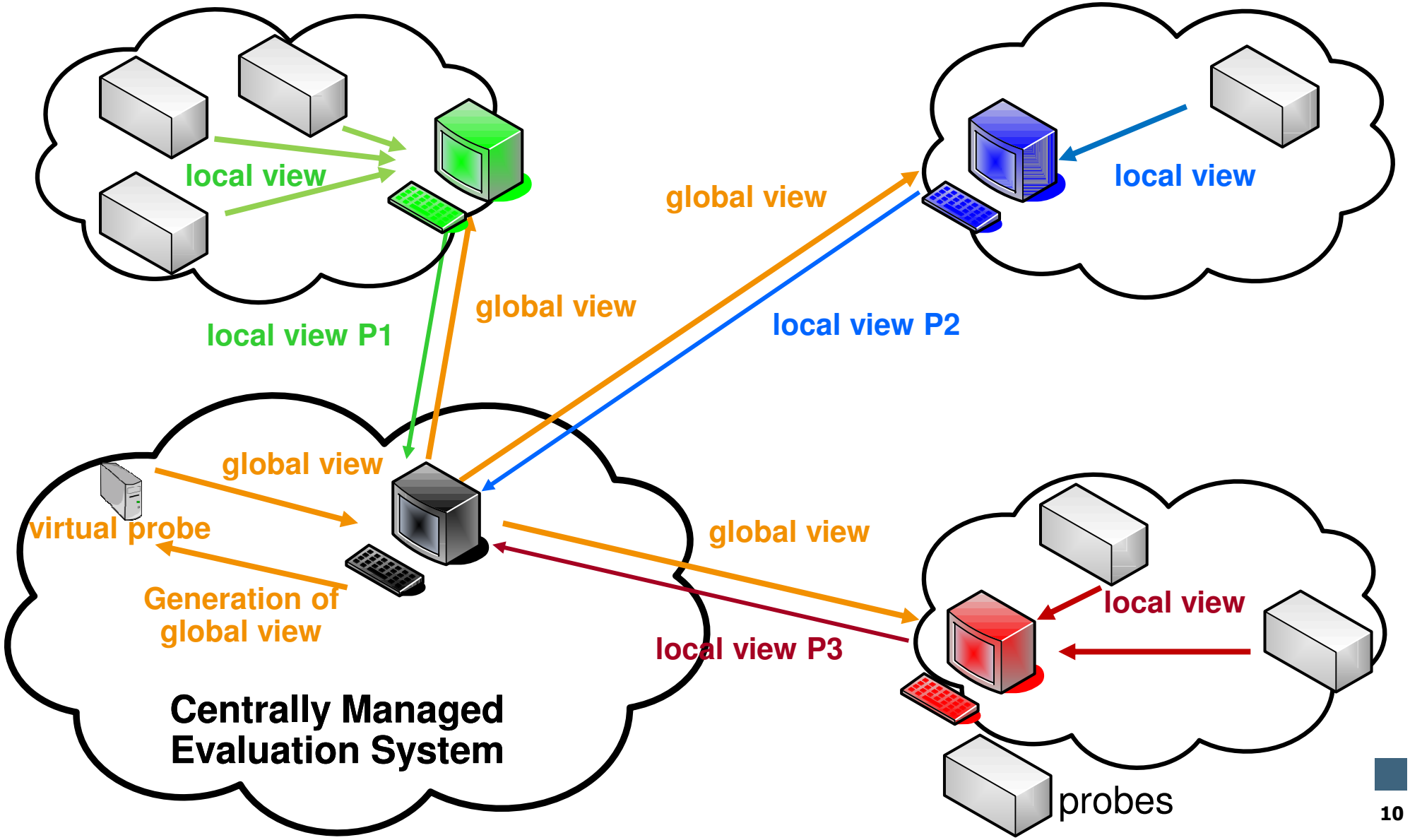
Content

- Aim and outcomes of this lecture
- Idea of the Global View
- **Realization of the Global View**
- Results of the Global View
- Future Work
- Summary

Realization of the Global View
→ Requirements towards a procedure

- Requirements towards a possible procedure to generate the global view
  - Enables **comparison between local and global view** nearly in real-time
  - Considers requirements of the operational environment of the sensor (e. g. data traffic)
    - Results in equal consideration of all partners
  - IAS already ensures privacy by design, but also important is the
  - Securing of the trustworthiness of the data of the individual partners

Realization of the Global View
→ Overview



Realization of the Global View
→ Using weighted average

- Local views from the database
- Determine a scaling factor for each parameter of every probe
- Preprocessing of the readings (subtraction of probe readings, sorting)
- Generation of global view
- Delegation to the transfer system

$$CountParameter_{x\,Global} = \frac{\sum_{n=1}^{N} \left(CountParameter_{x\,Probe_n} * ScalingFactor_{x\,Probe_n} \right)}{N}$$

$$ScalingFactor_{x\,Probe_n} = \frac{\sum_{t=p}^{q} CountParameter_{x\,ReferenceProbe}}{\sum_{t=p}^{q} CountParamter_{x\,Probe_n}}$$

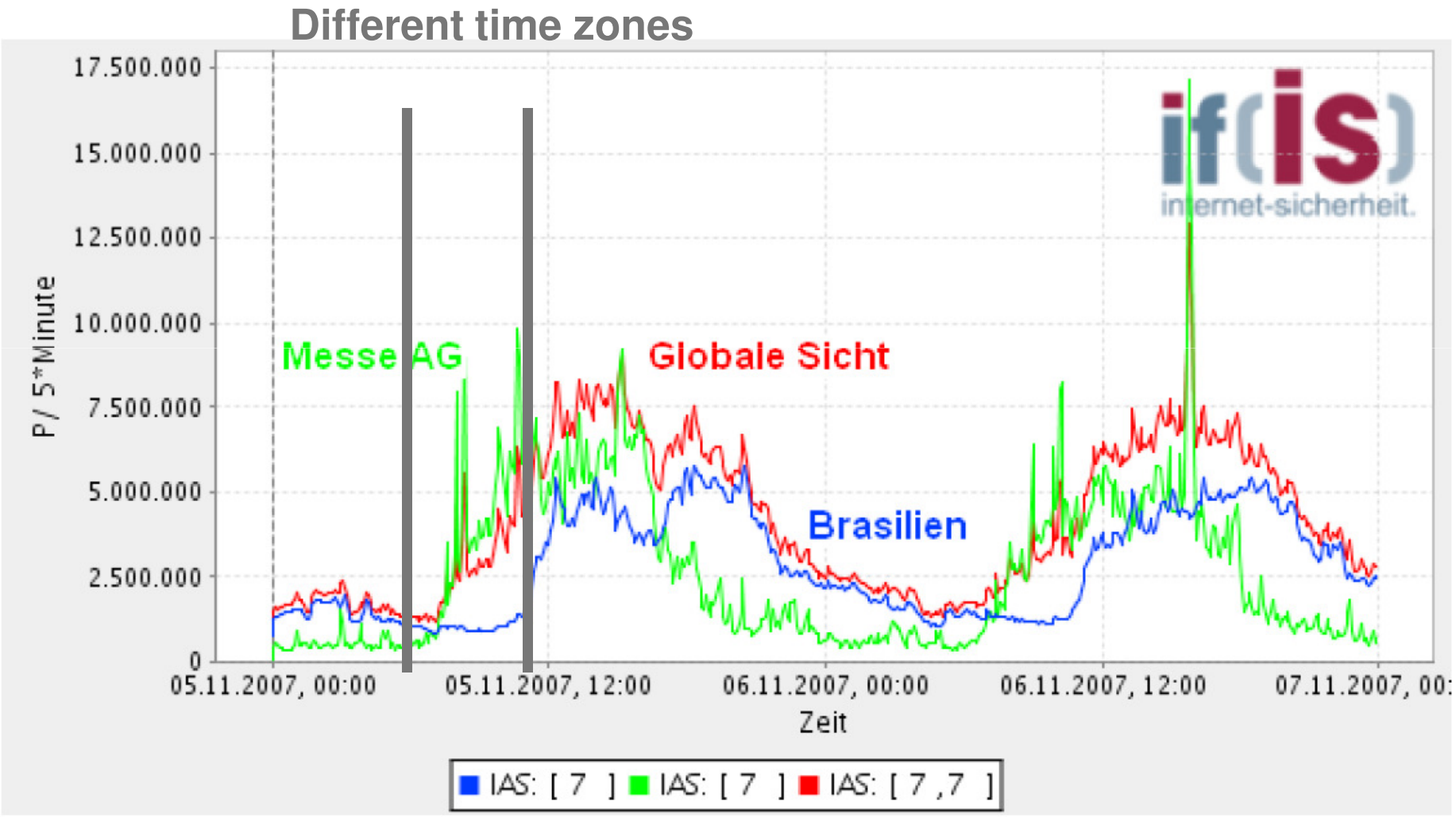
with N = number of probes, time slice t from p to q

Realization of the Global View
→ What is imported?

- You **cannot buy** the **global view** on the market.

- We need a Private-Public-Partnership to provide the partner with a global view.
  - Only together the partners are able to generate the global view.
  - Than we can **generate added value** for the different partner.
  - The partner can use this global view to make the **better decision**.

Global View
→ Challenges (1/3)



Global View
→ Challenges (2/3)

- A part of the data flow is influenced by the communication behavior of humans and therefore indirectly by the local time
  - Different time zones and inconsequent daylight saving time regulations
  - cultural issues (sociological aspects) like the long lunch break in Spain (Siesta)

- Another part of the communication is created by machines and
  - might be not influenced by the local time and should therefore be examined in a global perspective or
  - might be run by “batch jobs” explicitly during night time, to save resources.

Global View
→ Challenges (3/3)

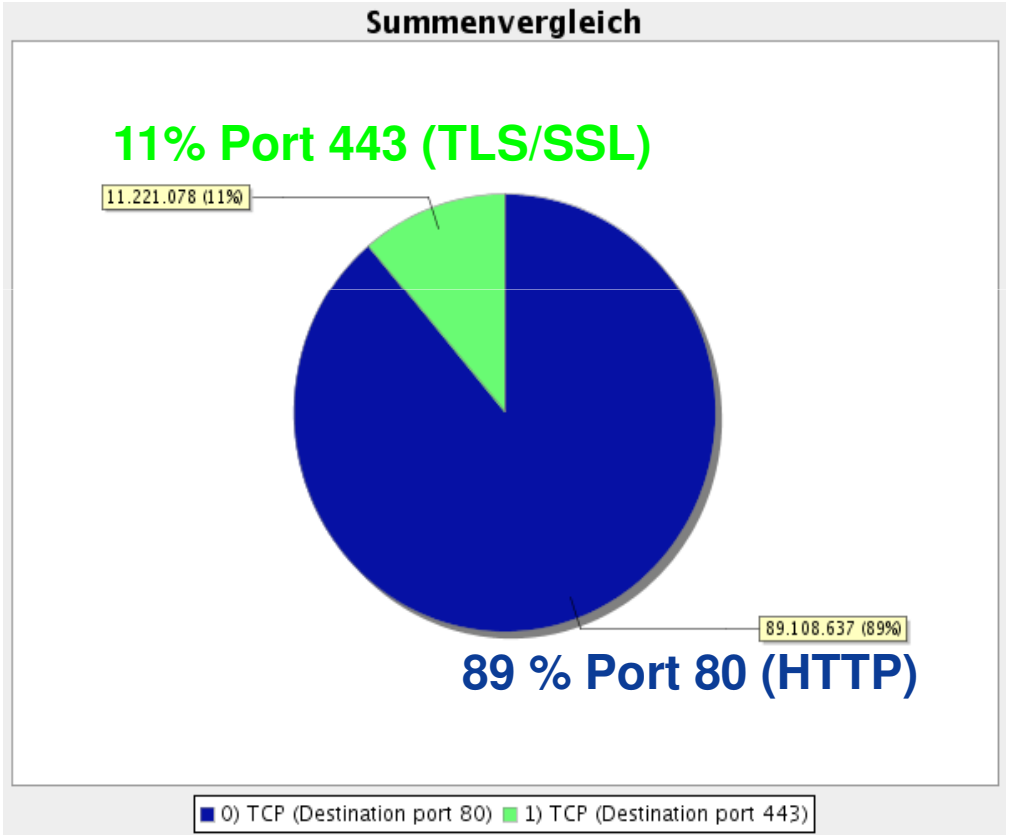
- Diversity of the possible partners and of the different natures of networks, that can be monitored with the sensor technology (to compare apples and oranges).
- Further research on the scaling factor, make challenges visible.
- To confirm research results, we need more distributed sensors.
- The selection of the correct number and position of sensors, to create a global view.

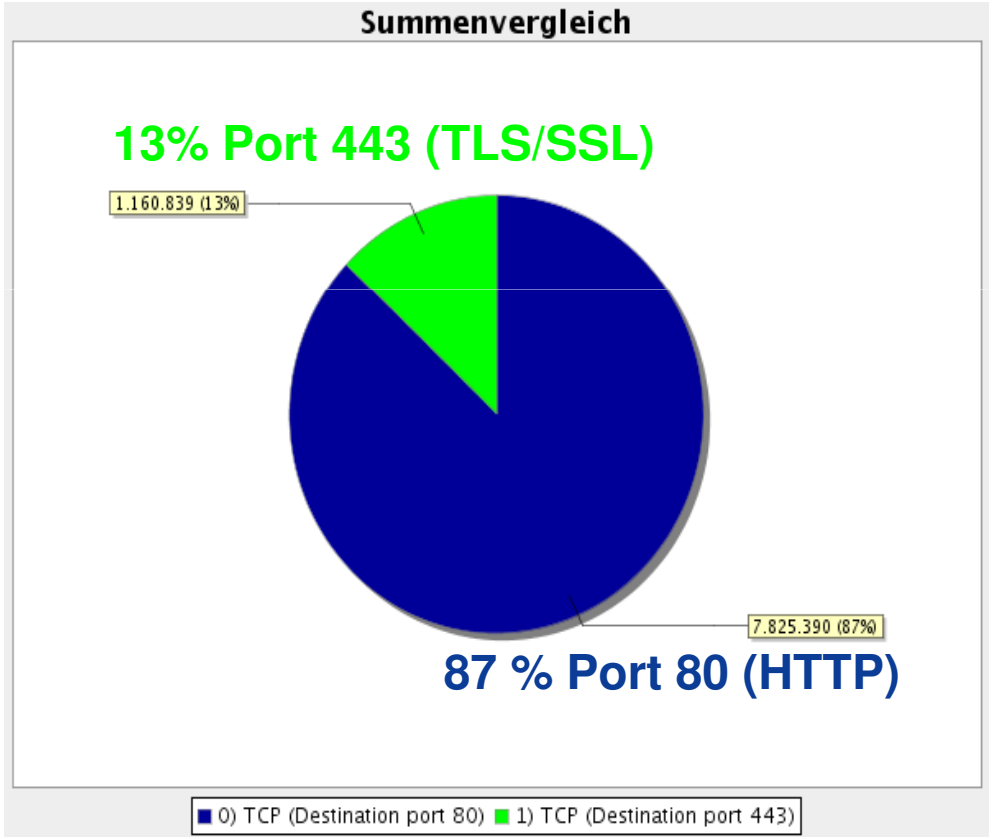
Content

- Aim and outcomes of this lecture
- Idea of the Global View
- Realization of the Global View
- **Results of the Global View**
- Future Work
- Summary

Results of the Global View
→ Relation of used protocols

- Global representation of the relation of different protocols (Example: Web communication)



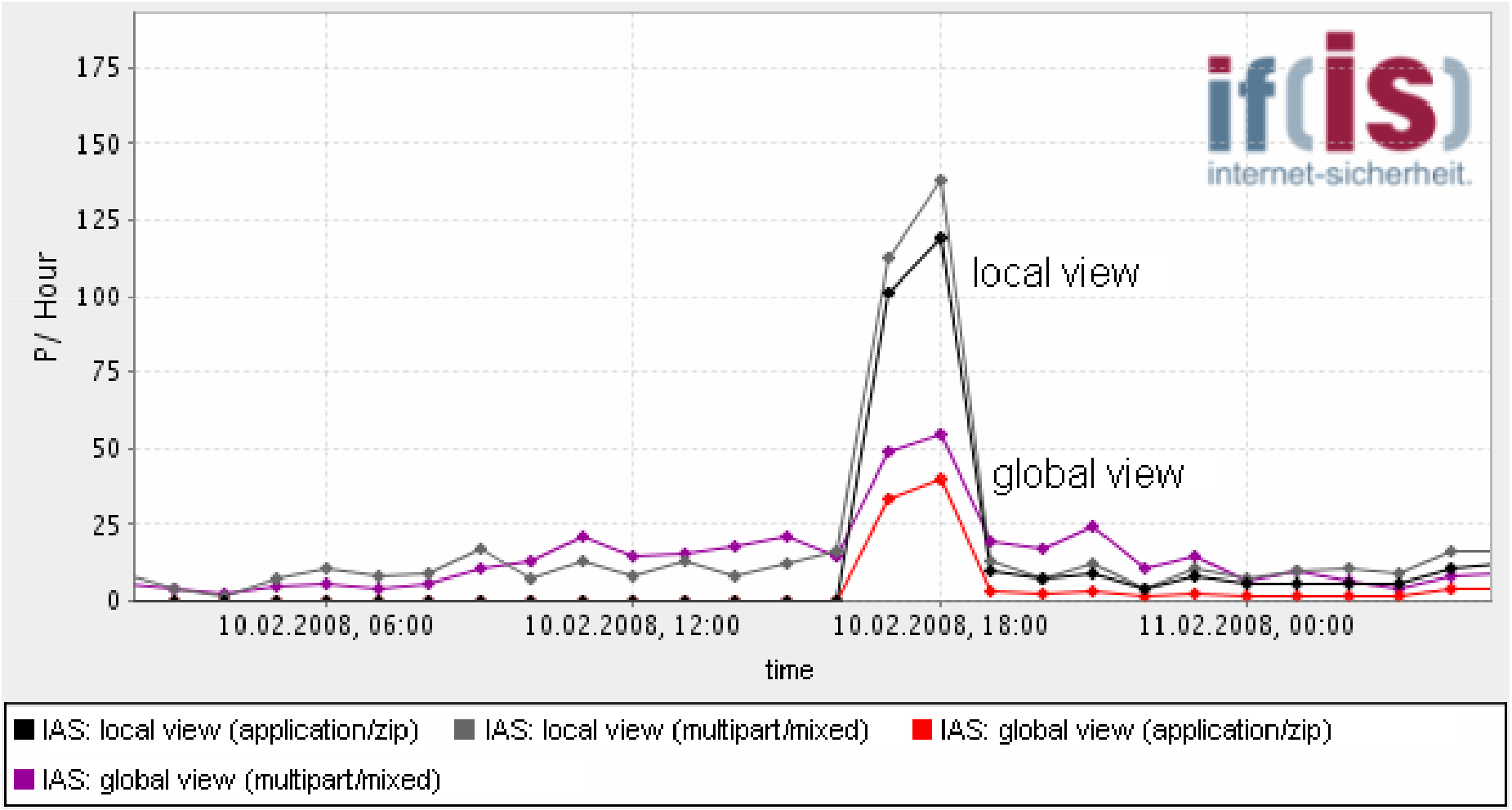


local view

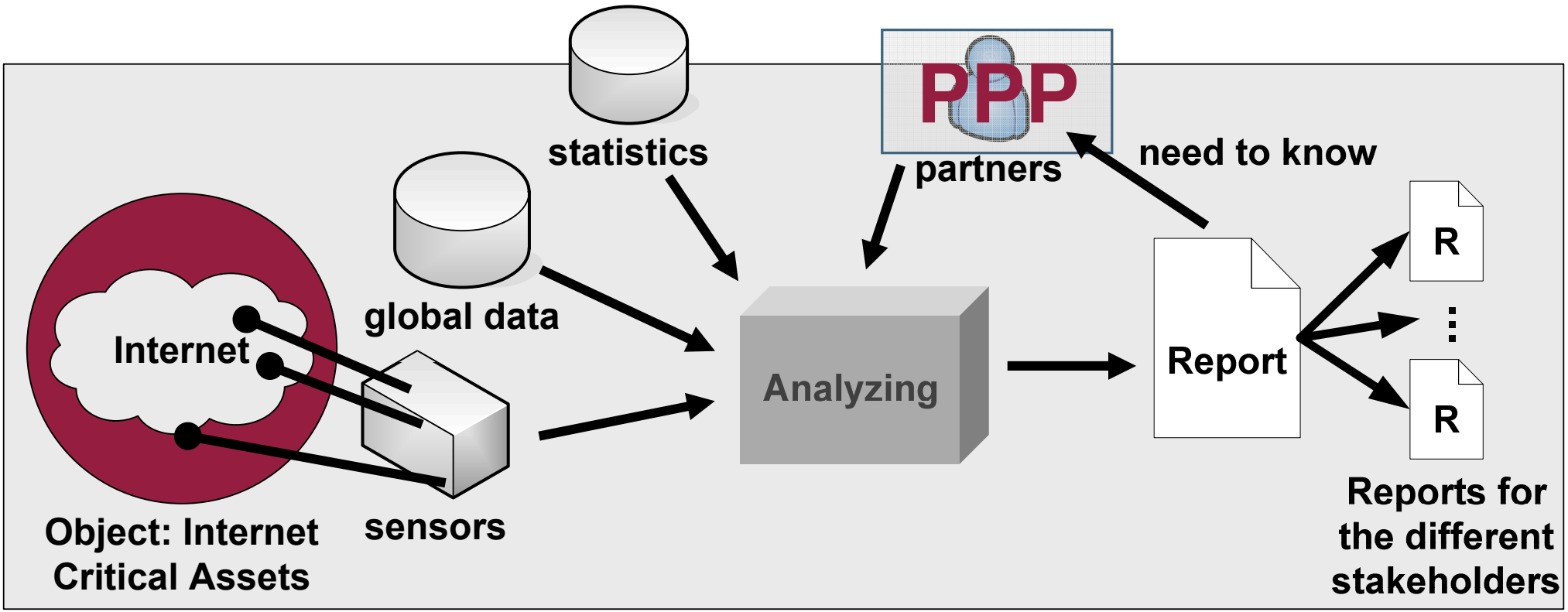
global view

Results of the Global View
→ Anomaly detection: Malware

- Dangers on the internet (e.g.: attachment ZIP)



Internet Security Status
→Project idea



- **This will help to:**
  - improve the stability and trustworthiness of the European Internet,
  - raise awareness for critical processes or components, and
  - find out more about the European Internet and its users in order to better support to their needs and service demands

Content

- Aim and outcomes of this lecture
- Idea of the Global View
- Realization of the Global View
- Results of the Global View
- **Future Work**
- Summary

Future Work

- Find more partners!
- Discussing different scenarios for a time zone comprehensive global view (global and local attacks …)
- Limitation to a useful number of parameters
  - Determine, whether the parameters can be grouped into those caused by humans and those created by machines – whether this is even necessary.
- Grouping of partners (apples to apples and oranges to oranges)
  - Improves the detection of anomalies and creates added value for partners
  - Grouping by different sectors (global view of financial institutes …)
  - Grouping by the type of network (e.g. global view of content providers, of enterprises, of internet service providers …)
  - Merge to one comprehensive global view

Content

- Aim and outcomes of this lecture
- Idea of the Global View
- Realization of the Global View
- Results of the Global View
- Future Work
- **Summary**

Global View
→ Summary

- The Global View generates added value.
- With the help a Global View you can make the better decision.
- It is not easy to produce the right Global View.
- You cannot buy the Global View on the market.
- Only together the partners are able to generate the Global View.

Fachhochschule Gelsenkirchen

Global View
→ Idea and Realization

Thank you for your attention!
Questions?

Prof. Dr.
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Global view
→ Literature

- [1] Sven Tschöltsch, Konzeption und Realisierung einer globalen Sichtweise auf das Internet zur Bewertung der eigenen Sicherheit (concept and realization of a global view of the internet for a better evaluation of the local security situation), Diploma Thesis, University of Applied Sciences Gelsenkirchen, 2008

Links:

Institute for Internet Security:
http://www.internet-sicherheit.de/forschung/aktuelle-projekte/internet-frhwarnsysteme/globale-sichtweise/