Beyond centralism: The Herold approach to Sensor Networks and Early Warning Systems

Axel Theilmann <theilmann@pre-sense.de>

PRESENSE Technologies GmbH
Sachsenstraße 5
20097 Hamburg

27.01.2010

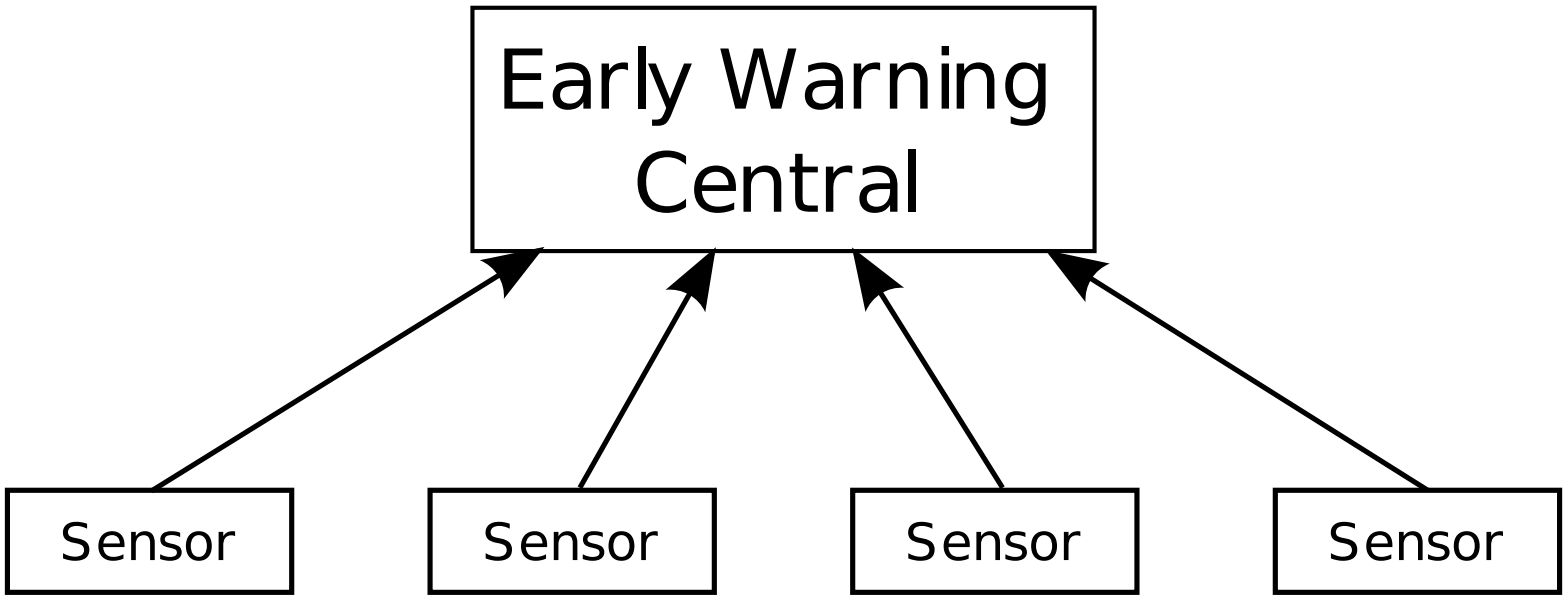
Outline

Outline

Early Warning Systems and Sensor Networks

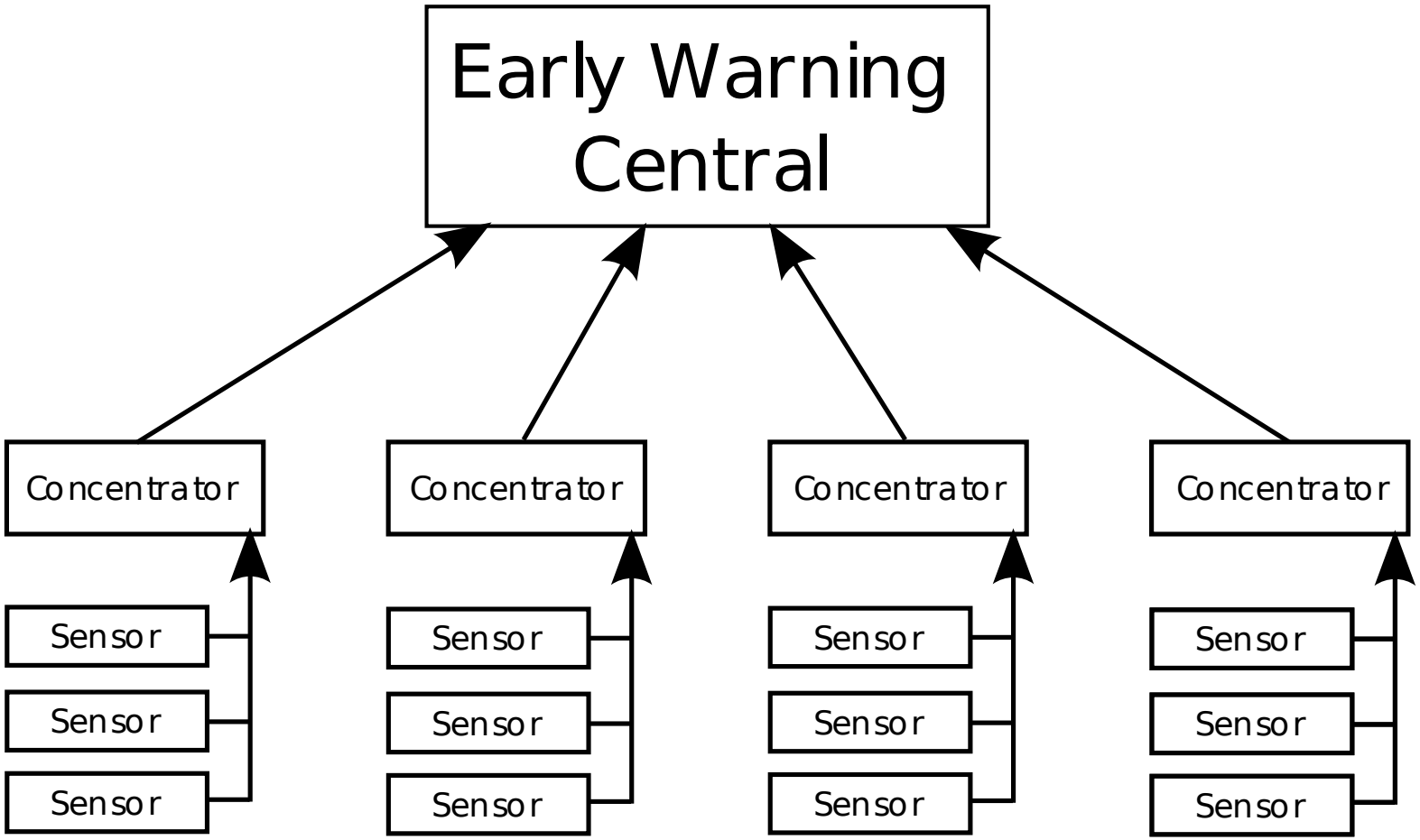
- Early Warning Systems (EWS) use Sensor networks to determine the current situation by collecting samples, much like TV ratings do.
- Sensors capture data in representative network areas and transmit to the Early Warning Center (EWC) for analysis.
- Approach and motivations differ from distributed IDS.

Data flow architecture of a Sensor Network



A simple Sensor network

Data flow architecture of a Sensor Network



A 3-level Sensor network

The Monolithic Approach

The Monolithic data flow architecture:

- Distribution is done purely for technical reasons.
  - Transmitting data from the place of observation to a common place of analysis.
  - Format conversion
  - Data reduction
- Data flows via a “dumb” infrastructure to an “intelligent” center.

Outline

Dealing with organisational structures

An EWS requires data from different types of networks and network operators.

Different networks and network operators have

- different goals and motivations for network analysis.
- different privacy and data protection requirements.
- different data rates.
- different storage requirements for recording of event histories.
- different requirements regarding access control.

Meeting operators' requirements (I)

For successful operation, an EWS must:

- satisfy the network operators' requirements.
- offer some kind of benefit in return.

Not surprisingly, network operators mainly care about *their* network. Also they tend to mainly be interested in a distributed IDS, rather than an EWS.

A monolithic EWS architecture cannot easily offer an attractive level of access to that data.

Meeting operators' requirements (II)

Possible changes to the EWC don't work well:

- EWC access for operators requires dumbing down the data, which hinders analysis.
- Multitenancy-support would drastically increase CPU and storage consumption.

But even then:

- User interface does not provide the view and analyses that operators are interested in.
- Administrational structuring of data and markup of infrastructure is missing.
- Single events are not easily accessible and processing not well automated.

Export of Data from Sensor Networks

Export of Early Warning Data

In a monolithic system, data only flows from the edges to the center, but getting data back out again is just as important for research and everyday use.

Export interfaces get added as an afterthought for specific requirements. Flexible export interfaces and query languages are missing. Automated exchange of data between sensor networks is difficult.

Cooperation and Integration of Sensor Networks (I)

Virtual Early Warning Systems

EWS are operated or planned on different levels (Company, National, International). Running them in parallel wastes resources.

An attractive alternative would be to create a federation of lower-level EWS and have them cooperate, forming a *Virtual EWS* that collects little to no original but accesses the data of its members.

Requests to the Virtual EWS are rewritten into sub-requests to its members' data, allowing each individual EWS to retain more control over its data.

Cooperation and Integration of Sensor Networks (II)

A new operational model for sensor networks is needed, that satisfies sensor and EWS operators' requirements and actively and flexibly supports exchange of data and cooperation between Early Warning Systems.

One such model is suggested by the Herold research project.

Outline

The Herold research project

- A research project in agent-based methods for distributed network monitoring and policy enforcement.
- Started in mid-2009 as a 2-year project.
- Partially funded by the German Federal Ministry of Education and Research
- Partners are:
  - PRESENSE Technologies GmbH
  - University of Hamburg / Group “Theoretical Foundations of Computer Science” (TGI)
  - n@work Internet Informationssysteme GmbH

The Herold research project (II)

The long-term goal is the interpretation of network nodes as independant *network agents* with individual

- knowledge (e.g. about network structure and current and past network events),
- goals (e.g. security policies and requirements), and
- capabilities (e.g. control over firewalls and IDS).

By connecting global policy, network and event models with local enforcement and monitoring capabilities, network agents can cooperate and provide network security as group efforts across organisational and network boundaries.

Outline

Sensor Networks from a network agent point of view

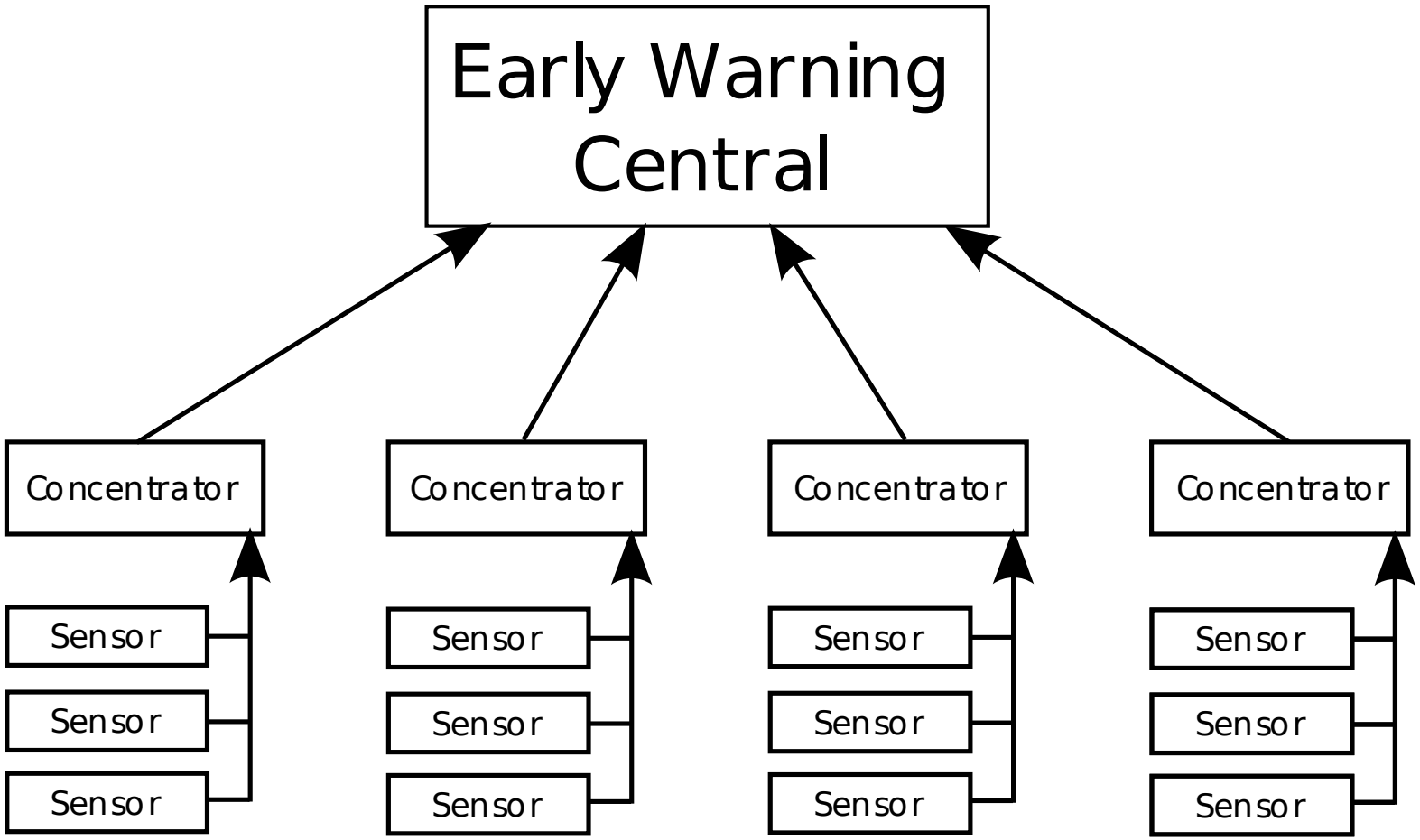
Applied to sensor networks, this suggests to model each crossing of an organisational boundary as a relationship between independent network agents. Each agent then operates as an independent sensor network.

Each agent individually:

- maintains a description of the network,
- maintains early warning algorithms,
- analyses and records incoming events,
- offers a user interface suitable for its operator
- offers an agent interface that other agents can use.

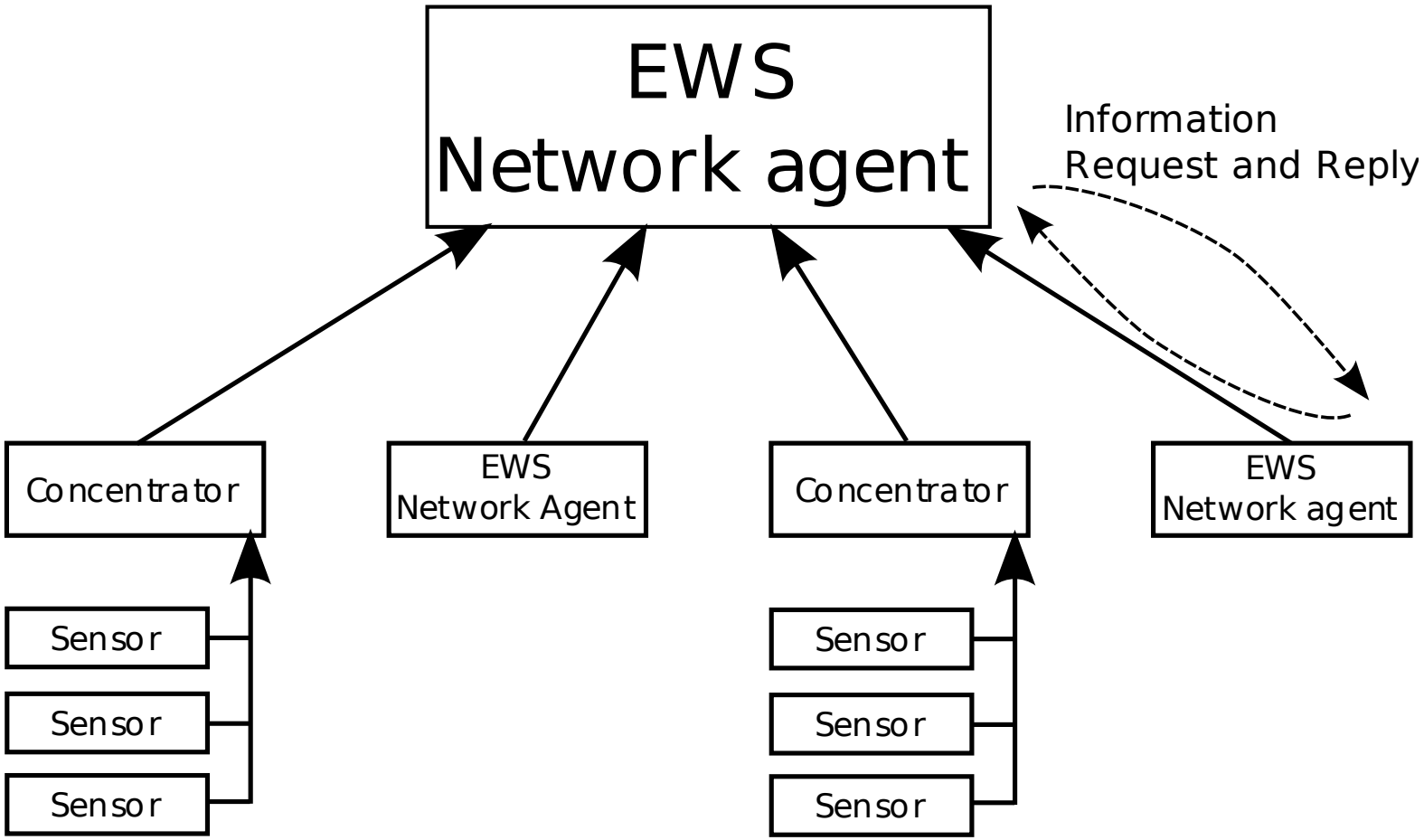
These network agents can now be organised into different topologies.

Hierarchical network agents (I)



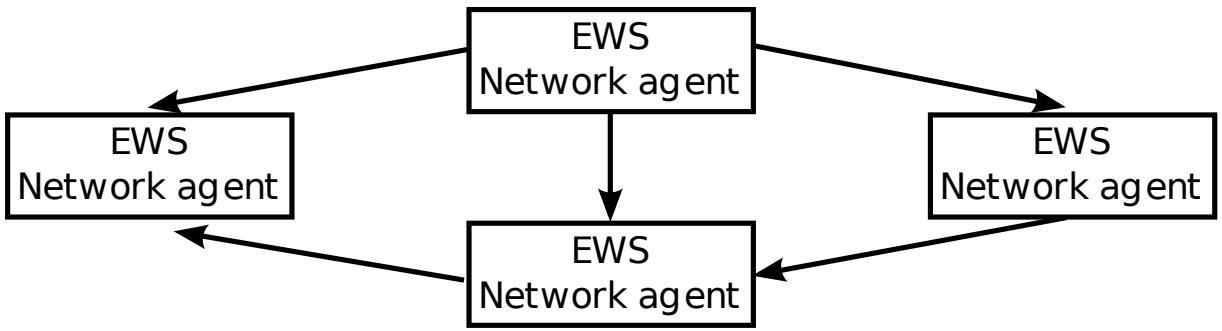
A 3-level Sensor network

Hierarchical network agents (II)



A hierarchical sensor network based on network agents.

Non-Hierarchical network agents



A non-hierarchical sensor network based on network agents.

The Herold project will create models and a software infrastructure to run network agents and have them exchange information and services for a truly cooperative approach to network security.

Outline

Conclusion

- Large sensor networks must satisfy requirements arising from the crossing of organisational boundaries.
- Further cooperation and data exchange between EWS is needed.
- The Herold project suggests a network agent approach for cooperative network security.
- Uniform interfaces allow for different topologies
- Hierarchical structures to match organisational structures.
- Non-hierarchical structures for flexible cooperation.

Questions, Remarks, Discussion?

The Herold project can be reached under

info@herold-security.org.

Further results and tools will be published at

www.herold-security.org

as the project continues.

Thank you!

Questions?