

→ **Artificial Immune System for Network Monitoring**

Diploma Thesis

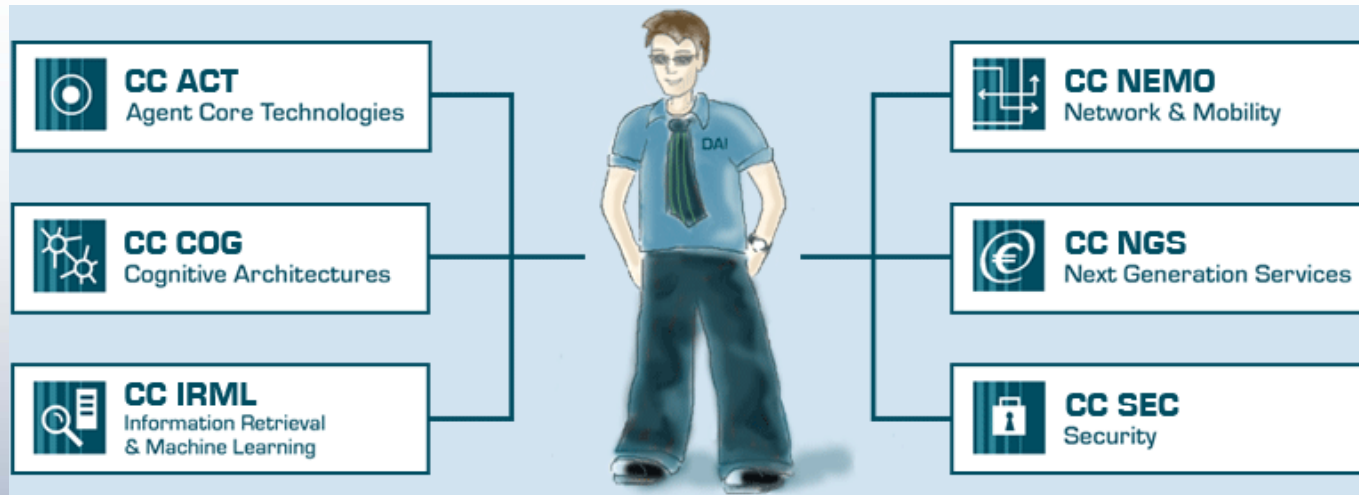
Katja Luther

katja.luther@dai-labor.de

Agenda

- ⇒ Introduction to network security
- ⇒ The biological immune system
- ⇒ Short introduction on artificial immune systems
- ⇒ AIS in a Multi-Agent System??
- ⇒ Integration in a Security System

Security at DAI-Labor



Focus Areas of CC Sec:

Computer security (operating systems, applications, exploits)

Distributed systems (trust, policies, middleware)

Agent security (mobile code)

Security analysis (computer installation, implementation testing)

Networks (wireless, wired, ad hoc, P2P, firewalls)

....

Signature based vs anomalybased intrusion detection

Signature:

- ⇒ only for known attacks
- ⇒ Signature describes characteristics of the attack (part of the code, sequence of process calls ...)

Anomalydetection:

- ⇒ Defintion of normal behaviour
- ⇒ Attacks are abnormal behaviour

Problems and advantages of signature based Intrusion Detection Systems?

Problems:

- ⇒ new attacks not detectable
 - some systems are able to detect similar attacks (fuzzy pattern matching)
- ⇒ need of an occurred attack to create a signature

Advantages:

- ⇒ low false positive rates
- ⇒ good detection of known attacks

Anomaly-based IDS

First attempts with anomaly-based Intrusion Detection

- statistical approach
- research on artificial immune systems (mostly research) and other artificial intelligence technics

Problems with high false positive rates and the definition of normal behaviour

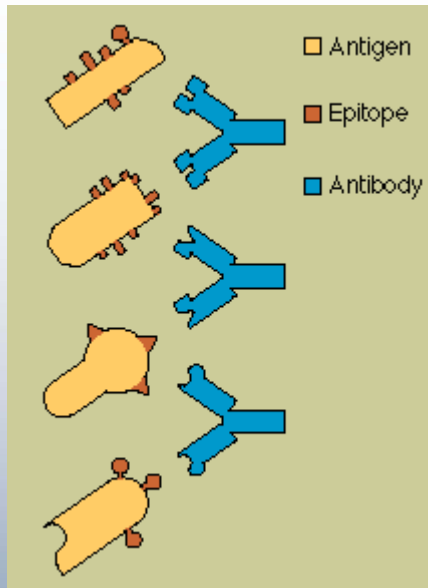
Advantages of the biological immune system

- ⇒ negative selection for differentiation of self and nonself
- ⇒ distributed system
- ⇒ able to learn new attacks
- ⇒ memory and adaption
- ⇒ multilayer security
- ⇒ autonomous system

Biological Immune System

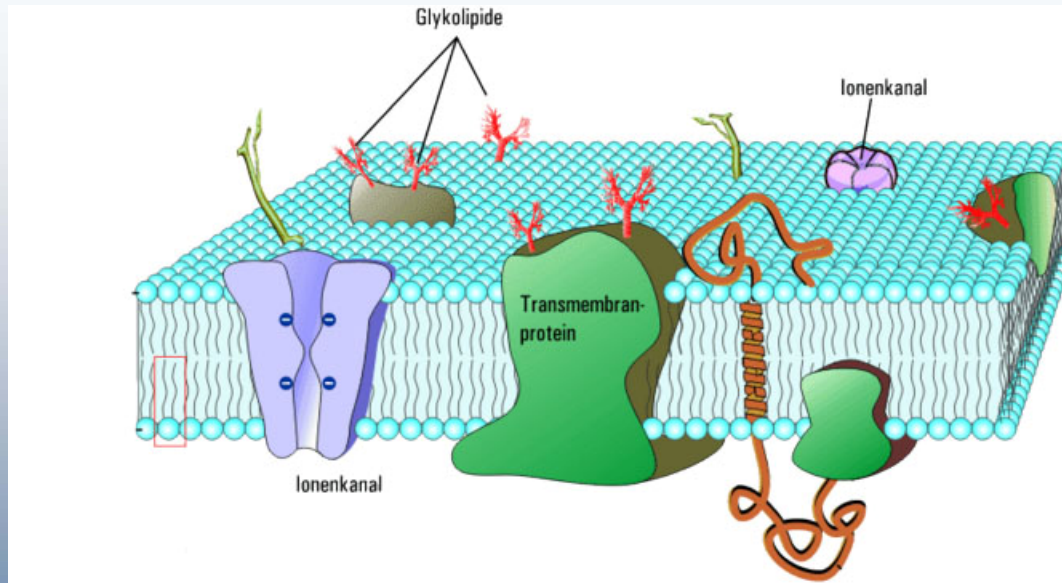
- ⇒ Chemical barriers: acid mantle of the skin, stomach acid
- ⇒ mechanical barriers: skin, mucosa (skin in nose and mouth)
- ⇒ non-specific immune mechanisms: defense cells in the skin and in the blood with non-specific receptors
- ⇒ specific immune mechanisms: T- and B-cells
 - negative selection
 - clonal selection

Pattern Matching of the biological immune system



- ⇒ Every cell has characteristic patterns on its surface (epitopes)
- ⇒ Receptors bind with different high affinity to these patterns
- ⇒ If the affinity is high, a immune response take place
- ⇒ Receptors can be integrated in the cell surface of immune cells or antibodies

Patterns of cells...



10.01.2006

Biological Immune System - Learning

- ⇒ Defence cells recognize nonself molecular patterns by receptors that bind features of these patterns
 - Antigen – receptor connection

- ⇒ Negative selection
 - receptors are produced with random configurations on the cell surface
 - training in thymus (negative Selection):
 - presentation of self-patterns
 - if a cell binds to these patterns, it will be destroyed
 - cells leaving the thymus, do not bind to self only to foreign patterns

- ⇒ Clonal Selection
 - Clonal reproduction of an activated cell, only activated cells will reproduce themselves

10.01.2006

Memory of the Immune System

- ⇒ Activated defence cells clone themselves and produce memory cells and antibodies (clonal selection)
- ⇒ During the next attack the memory cells allow a fast immune answer

Development of immune cells

1. clonal selection:

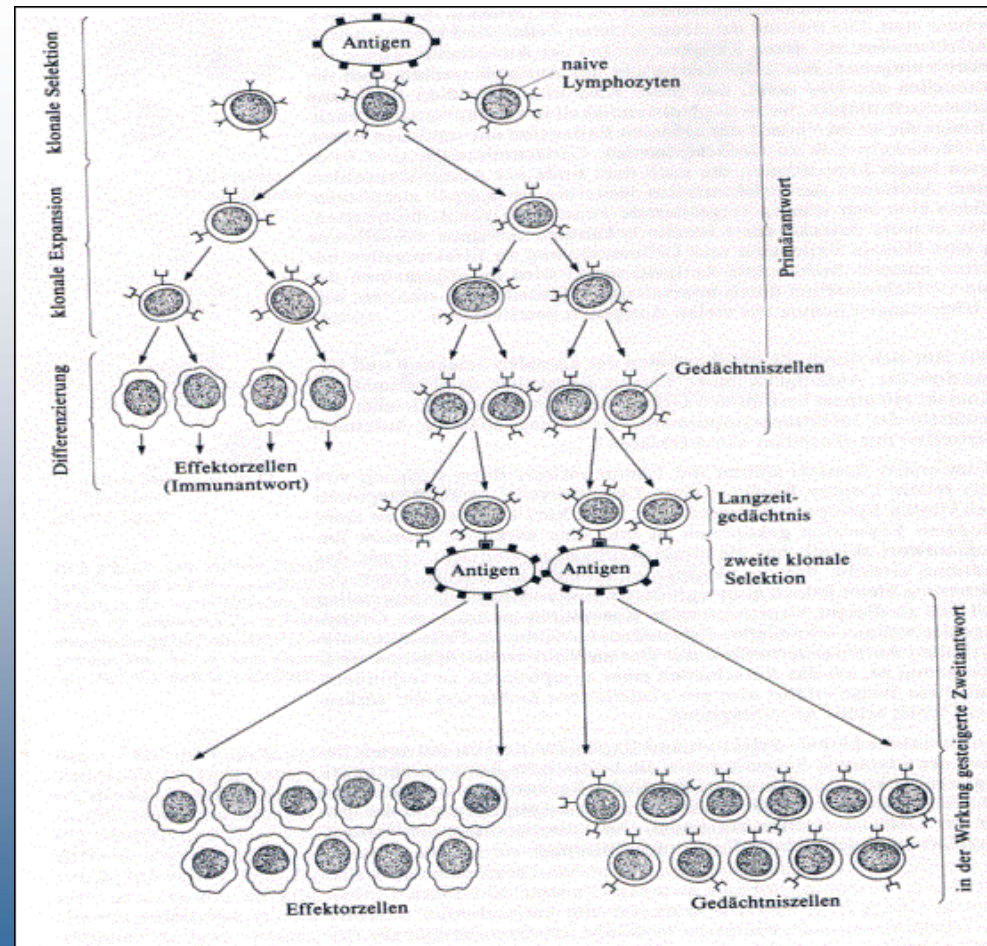
- binding to an antigen
- clonal reproduction

2. differentiation:

- effector cells
- memory cells

3. new infection:

- memory cells become new effector and memory cells



Danger Theory (Matzinger 1994 and 2002)

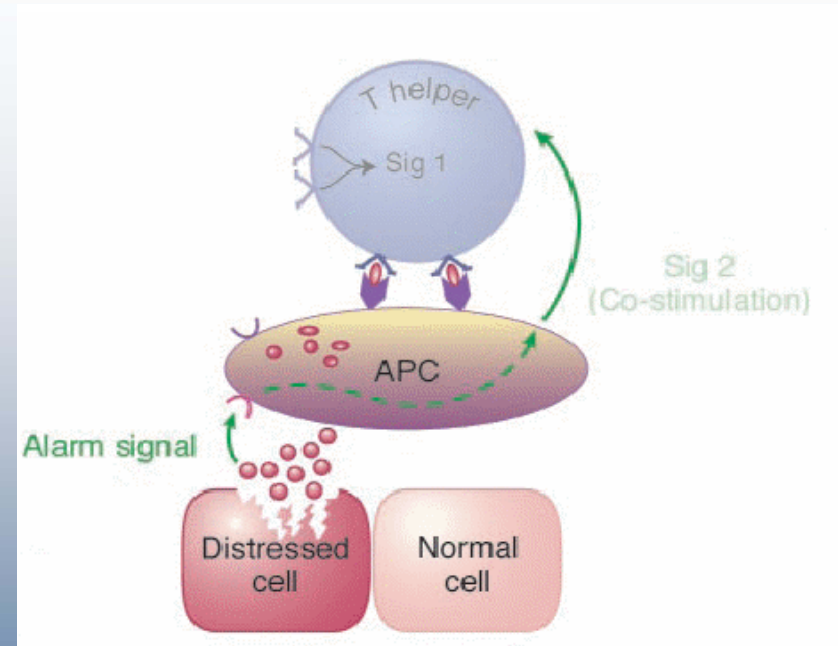
No immune response to foreign cells of embryos or transplantations

⇒ Additional signal?

Danger Theory of Polly Matzinger (1994 and 2002):

⇒ Distressed or injured cells produce „danger signals“

⇒ Immune response only in conjunction with danger signals



Advantages of the biological immune system

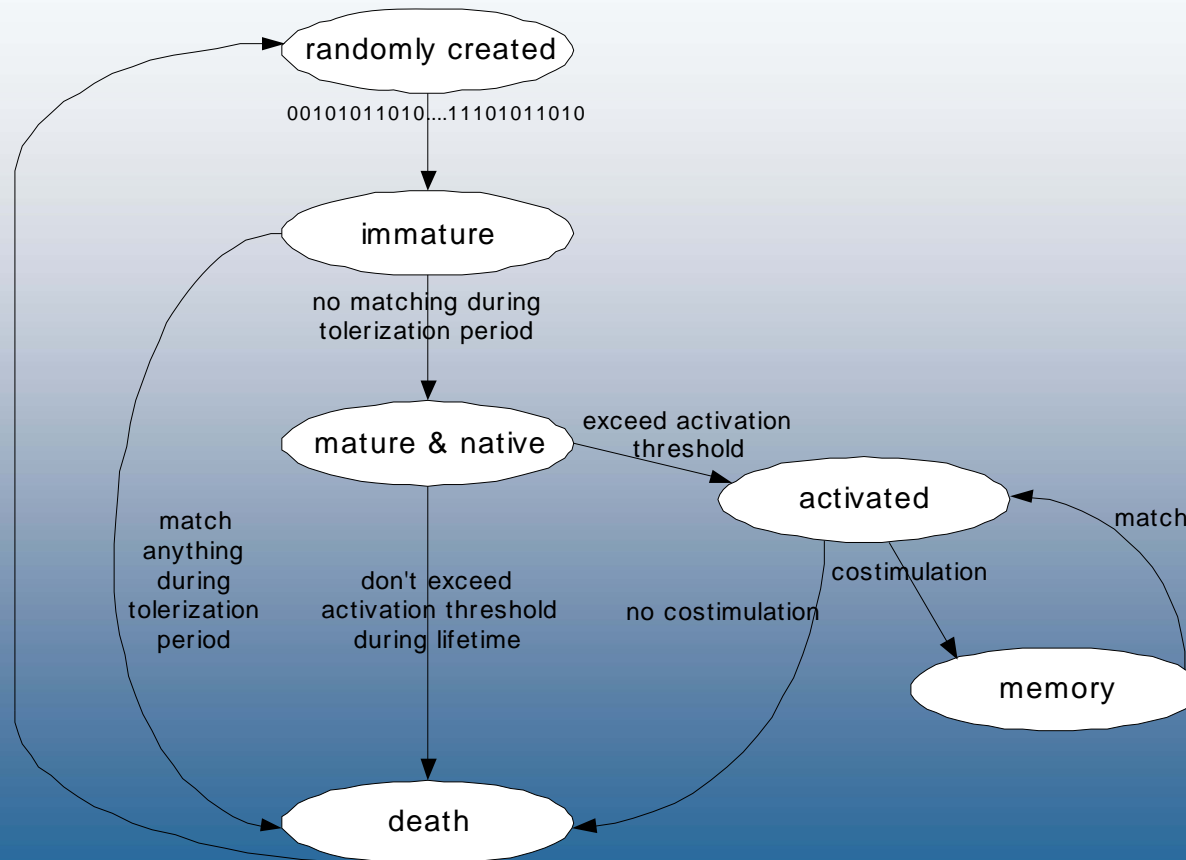
- ⇒ negative selection for differentiation of self and nonself
- ⇒ distributed system
- ⇒ able to learn new attacks
- ⇒ memory and adaptation
- ⇒ multilayer security
- ⇒ autonomous system

Why an artificial immune system?

- ⇒ Inspiration from nature, only as a metaphor
- ⇒ Very effective classification algorithm
- ⇒ Try to apply the advantages of the biological immune system to the properties of a computer network

Artificial Immune System (AIS)

⇒ First approaches of S. Forrest (Forrest et al. 1994)



10.01.2006

Negative Selection Algorithm

First approach with binary strings (datapath-triple: IP-adresses and protocol)

pattern-matching over the whole string, searching for the longest matching string

detector	011010101101001
monitored string	110100101100100

new approach: real-value vectors (n-dimensional space)

- n-dimensional vector as centre and real value as radius
- Pattern matches if it is inside the radius of a detector

every detector has status informations: age, matches, threshold

AIS- Clonal Selection

Initialisation: 1. creation of randomly produced detectors (binary strings)

Population loop: 2. selection of detectors with high affinity
3. reproduction and genetic variation
4. Affinity evaluation

Cycle: Repeat Step 2 until a convergence criterion is met

Genetic variation?

binary string

110100



randomly chosen mutation point

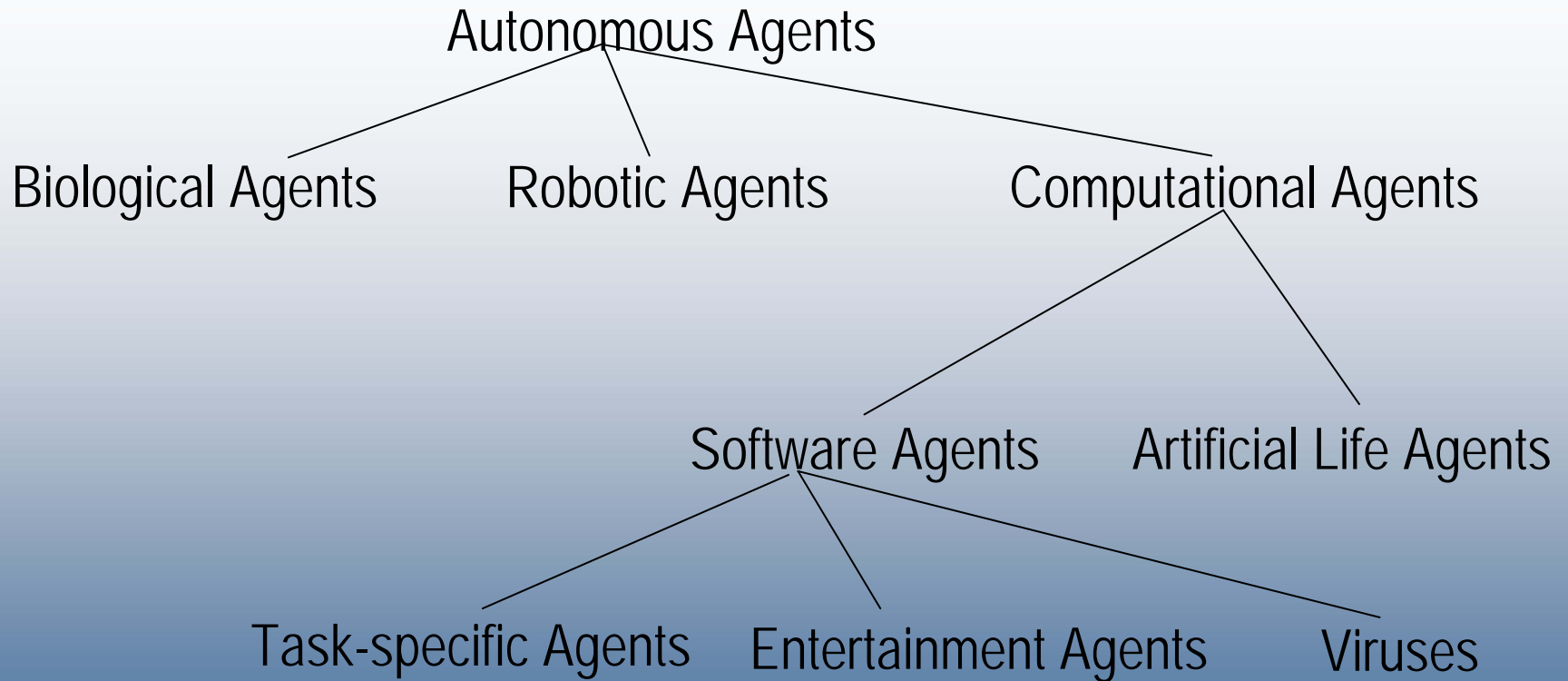
110100



mutation

110110

Agents



10.01.2006

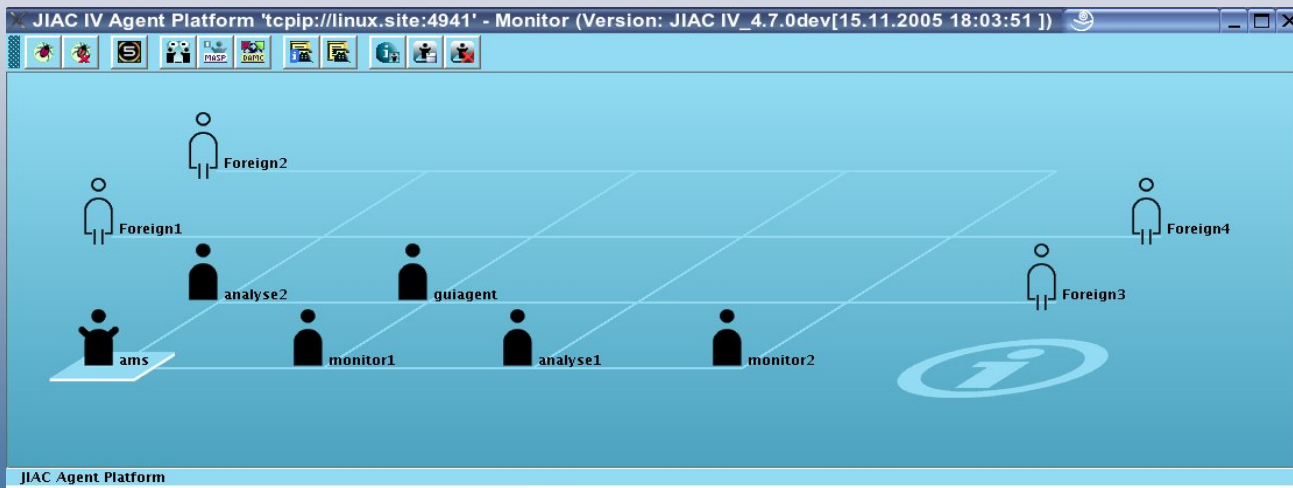
Agents - characteristics

reactive	responds in a timely fashion to changes in the environment
autonomous	exercises control over its own actions
goal oriented	does not simply react to the changes in the environment
temporally continuous	a continuously running process

JIAC

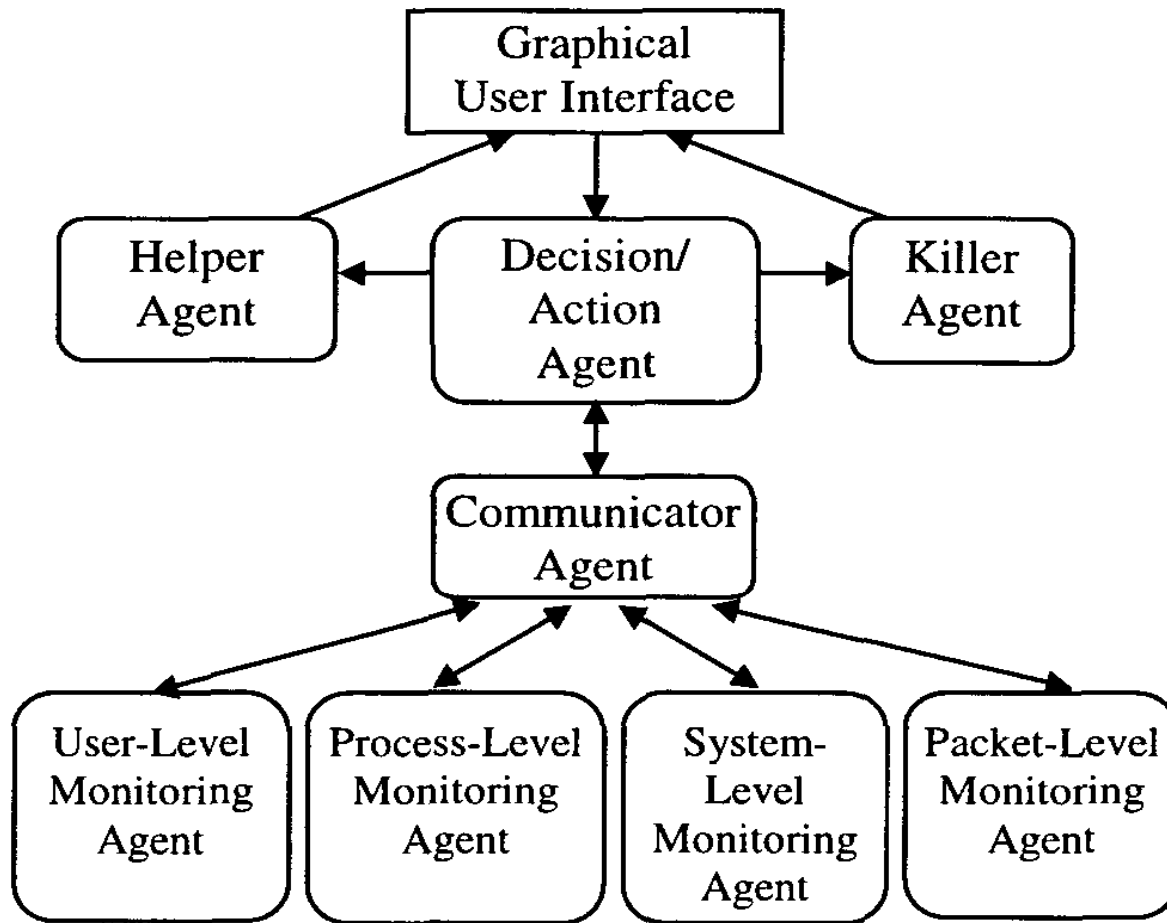
(Javabased Intelligent Agent Componentware)

- ⇒ includes development methodologies, software development tools and a runtime environment
- ⇒ framework for service-oriented agentbased applications



10.01.2006

Agentbased AIS – Dasgupta et al. 2001

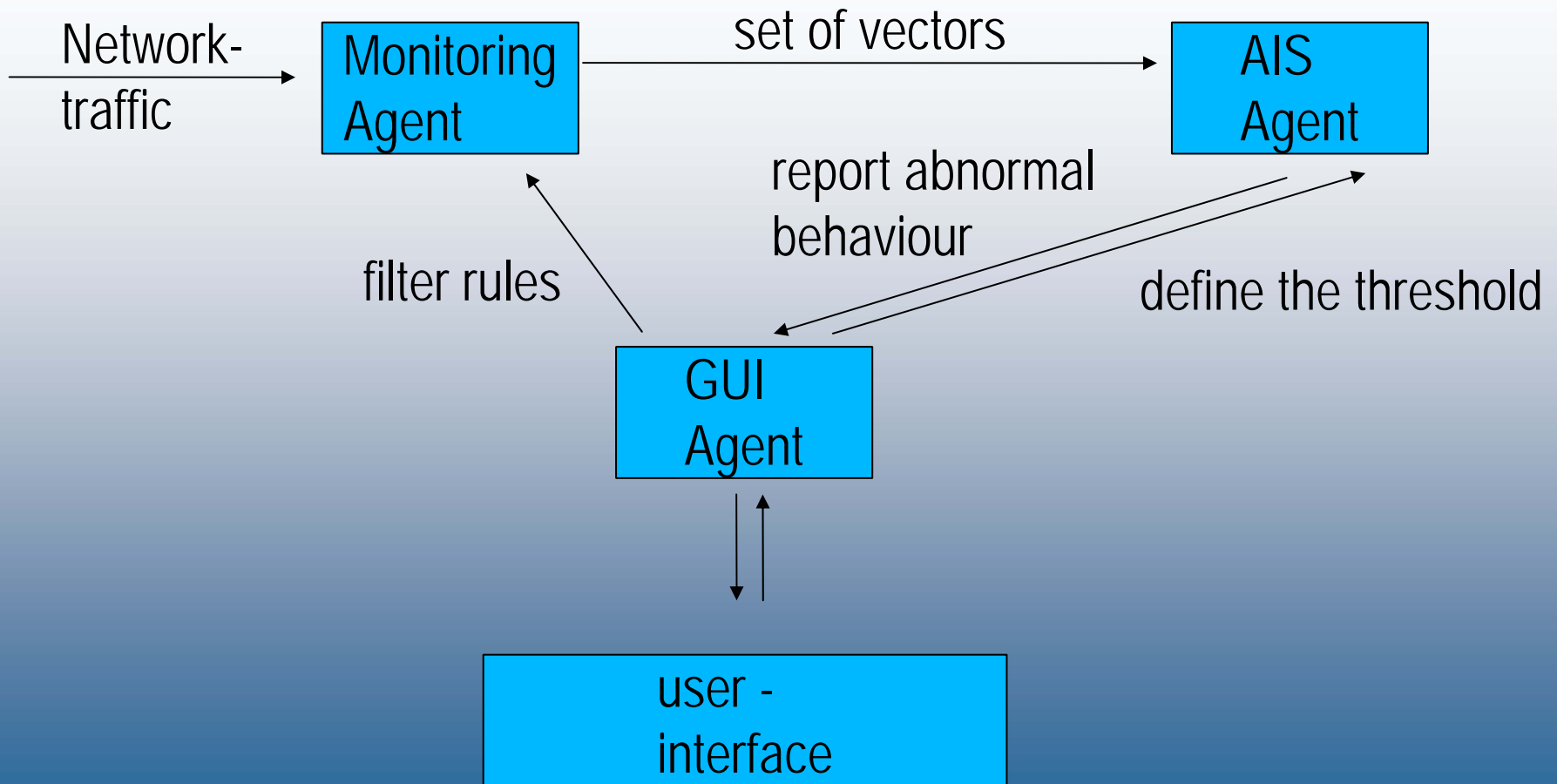


- hierarchical approach
- distribution of tasks
- expandability

Goals for a new agentbased AIS

- ⇒ avoid the Single Point of failure (hierarchical agent-system)
 - ⇒ selforganized system without central management
- ⇒ integration and coordination of different applications
- ⇒ real-value negative selection (RNS) (Gonzalez et al. 2002) in combination with agent-system
- ⇒ integration of Danger-Theory (Aickelin et al. 2003)

Architecture of one network node



10.01.2006

Agent roles

Monitoring-Agent

- Sniffer, tcpdump rules, uses jpcap library
- administrator is able to set filter rules

AIS-Agent

- analysis of network-packets with AIS-algorithms
- threshold of nonself traffic-behaviour
- if threshold is reached message to the GUI-Agent

GUI-Agent

- connection to the user interface/administrator
- relay the commands to the monitoring- and AIS-agent

Used Algorithms

Negative selection with vectors for selection of detectors

- Production of detectors randomly but only in possible space
- Distance measurement: binary hamming distance for every vector element
- Vector represents the tcp header information

Clonal selection for analysis of network-packets

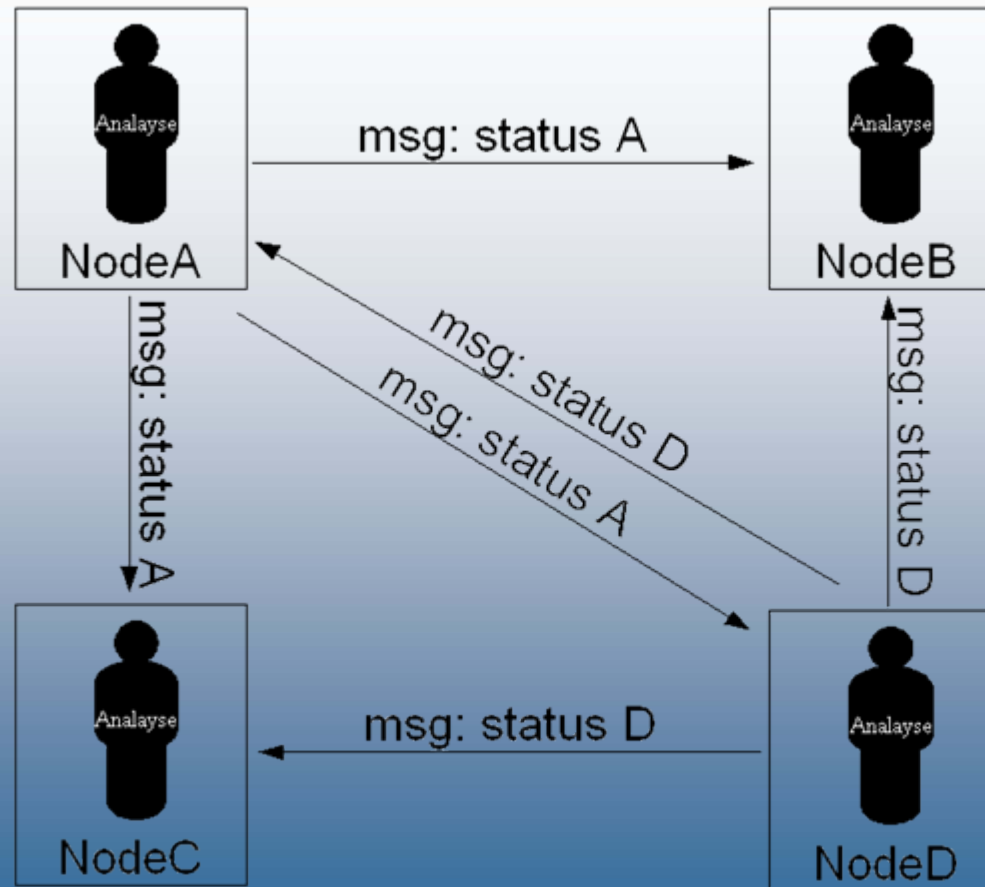
- similar to evolutionary algorithms
- fitness evaluation by affinity
- mutation on binary representation of the vector elements

Coordination of different nodes

- ⇒ Agents of different nodes send status to their neighbours, if their threshold is reached or after a defined time period
- ⇒ Thresholds can be adapted, if rate of abnormal traffic at the neighbour nodes is high
- ⇒ Administrator gets a message if the threshold is reached

Coordination of nodes

Threshold is reached!



Threshold is reached!

Future: Integration of AIS

- ⇒ Agents specialised for different fields (application, network, resources etc.)
- ⇒ Danger Signals like high CPU load or high frequency of port use
- ⇒ Agents report their warnings and the threshold of the AIS-agents falls down

Next steps

- ⇒ analysing of different pattern-matching algorithms (in bioinformatics different pattern matching algorithms are in use, performance?)
- ⇒ analysing of different detector shapes
- ⇒ identification of danger signals (timerelated events, user behaviour, resource usage)
- ⇒ analysing of performance (the probe of every packet is not feasible, improvement of detector-production)
- ⇒ realisation of an integrated agentbased security system

10.01.2006

Thank you ...
Questions??

10.01.2006

Quellen

Dipankar Dasgupta and Hal Brian. Mobile Security Agents for Network Trac Analysis. In Proceedings of DARPA Information Survivability Conference and Exposition II, volume 2. IEEE Computer Society Press, 2001.

<http://ieeexplore.ieee.org/search/wrapper.jsp?arnumber=932184>.

Stan Franklin and Art Graesser. Is it an Agent, or just a Program?: A Taxonomy for Autonomous Agents. In Proceedings of the Third International Workshop on Agent Theories, Architectures, and Languages. Springer-Verlag, 1996.

<http://www.msci.memphis.edu/~franklin/AgentProg.html>.

Stephanie Forrest, Alan S. Perelson, Lawrence Allen, and Rajesh Cherukuri. Self-nonsel discrimination in a computer. In Proceedings of the IEEE Symposium on Research in Security and Privacy. IEEE Computer Society Press, 1994.

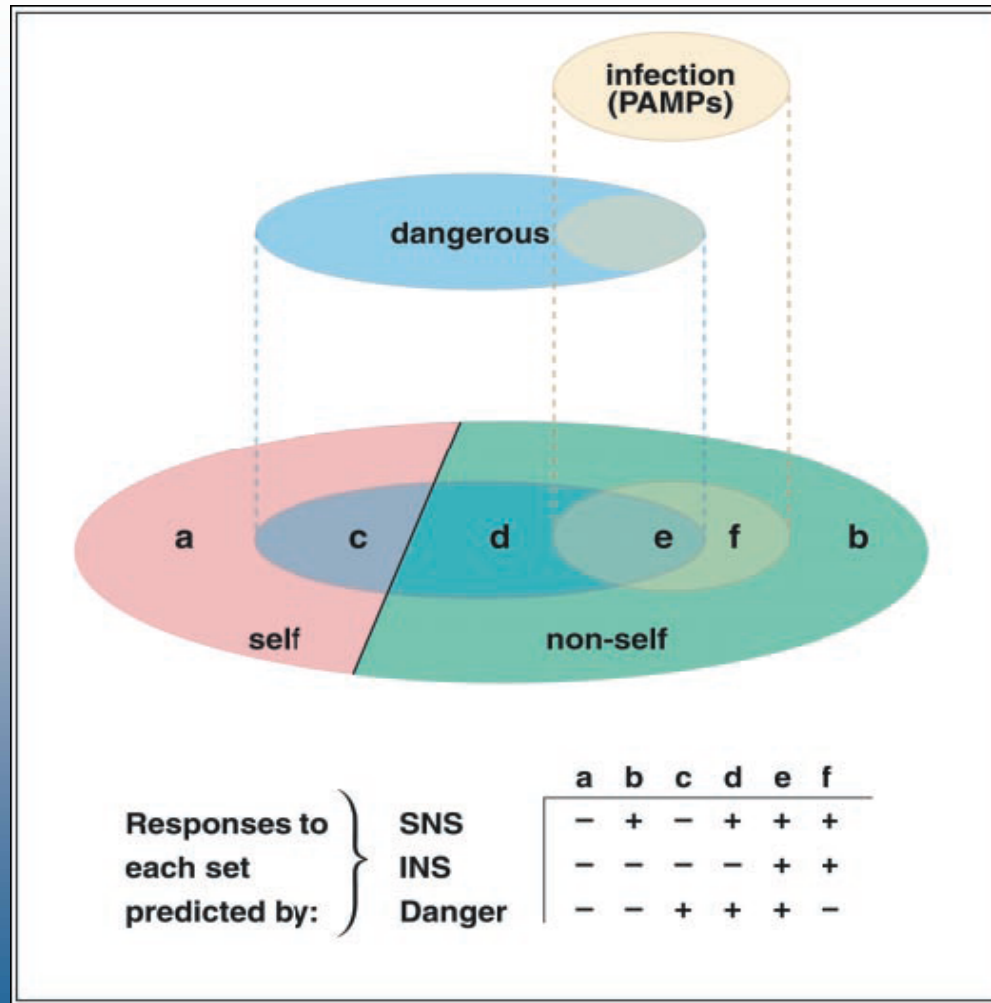
<http://www.cs.unm.edu/~immsec/papers.htm>

Quellen

Fabio A. Gonzalez and Dipankar Dasgupta. Anomaly detection using real-valued negative selection. In special issue of the Journal of Genetic Programming and Evolvable Machine, 4(4):383-403, December 2003.

Polly Matzinger. Tolerance, danger and the extended family. Annual Review of Immunology, (12), 1994.

Polly Matzinger. The Danger Model: A Renewed Sense of Self. Science, April 2002.



Jadl:

- ⇒ knowledge representation language
- ⇒ for description of ontologies, functions, goals and services

Planelements:

- ⇒ speech acts, actions and conditions
- ⇒ scripts combine planelements, protocoll scripts for interaction