



SANA – Security Analysis in Internet Traffic

Michael Hilker

University of Luxembourg, Campus Kirchberg
Interdisciplinary Lab for Intelligent and Adaptive Systems
Management of Information and Net-Centric Computing Group
6, Rue Richard Coudenhove-Kalergi
L-1359 Luxembourg

e-mail: michael.hilker@uni.lu
phone: +352-466644-5311
<http://wiki.uni.lu/mine/>



Agenda

- Who am I
- Introduction
- SANA
 - Artificial Immune System
 - Artificial Cells
- Architecture, Scenarios and Results
- Next Steps
- Conclusion

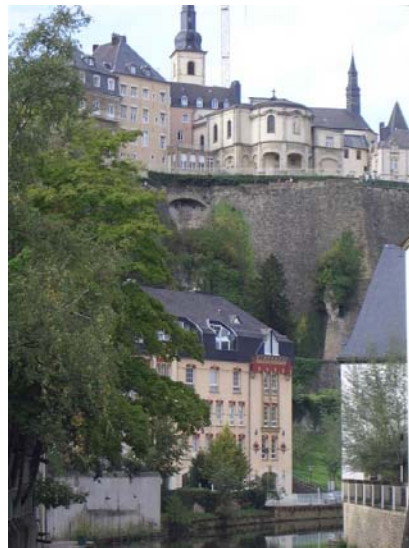


Who am I

Michael Hilker

- PhD-Candidate at the University of Luxembourg, supervised by Prof. Dr. Christoph Schommer, funded through a Scholarship of Luxembourg.
- Computer Scientist, graduated at the Johann Wolfgang Goethe-University Frankfurt, Germany in March 2005
- Working in the fields Biological Inspired Computing, Artificial (Immune) Systems (AIS), Intrusion/Anomaly Detection, Adaptive Systems, and Ant Colonies

Impressions of Luxembourg



- Area: 2,586 skm
- Habitants: 463,000
- Capital City:
Luxembourg
Habitants: 82,000
- Official Language:
German, French,
Luxembourgian

University of Luxembourg

- Three Locations – Kirchberg, Limpertsberg and Walferdange
- Computer Science approx. 70 Researchers
- Three Research Axes:
 - ComSys – Communicative Systems Laboratory
 - ILIAS – Interdisciplinary Lab for Intelligent and Adaptive Systems
 - LASSY – Laboratory for Advanced Software Systems
- MINE – Management of Information and Net-Centric Computing
 - 1 Prof., 1 Senior Researcher, 4 PhD-Candidates and approx. 10 Students



University of Luxembourg

MINE-Group



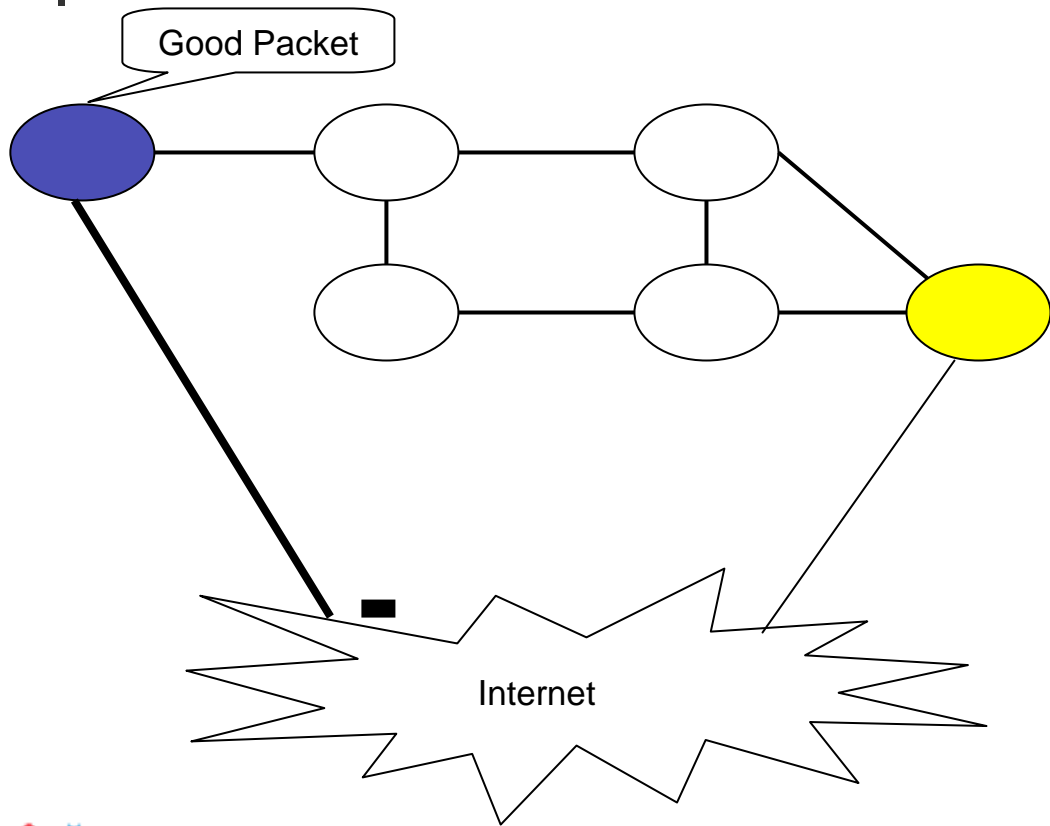
- 5 Research-Projects:
 - ADAM – Adaptive Information Memories for Agents in e-consultancy
 - ANIMA – Adaptive Netting in Stream Data
 - ICC – Inventing Communities of Communication
 - SANA – Security Analysis in Internet Traffic
 - TRIAS – Logic of Trust and Reliability for Information Agents in Science









Introduction

- Networks are under a constant Assault from Intrusions, e.g. Viruses, Worms, Trojans.
- Infected Computers cause
 - high costs for removing the infection
 - often a stop for the usage of the computer
 - a risk for infection other machines
- Network Intrusion Detection Systems (NIDS):
 - Centralised, Semi-Automatic and Local Systems
 - Need plenty of Computational Power

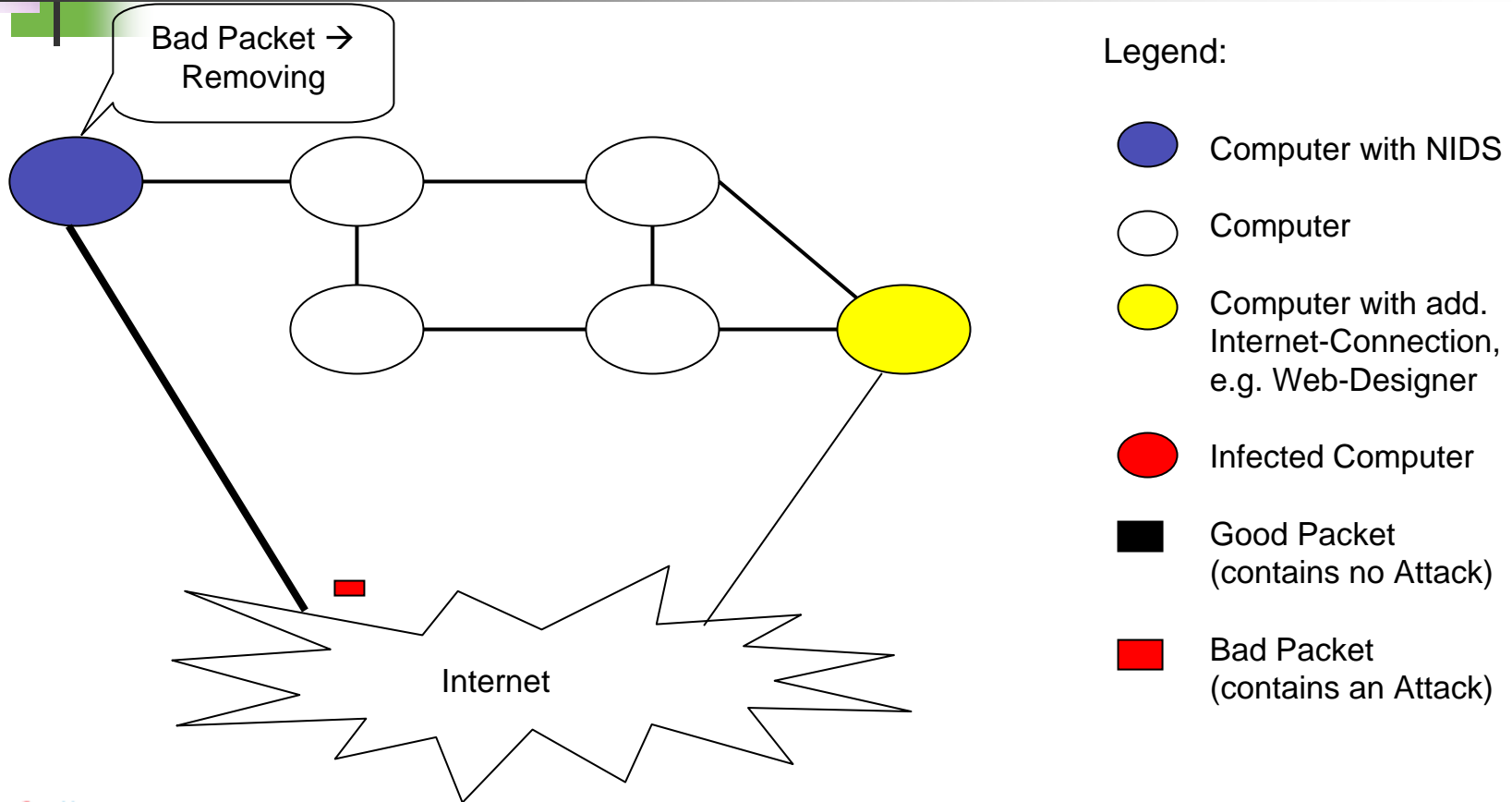
Example for a running NIDS



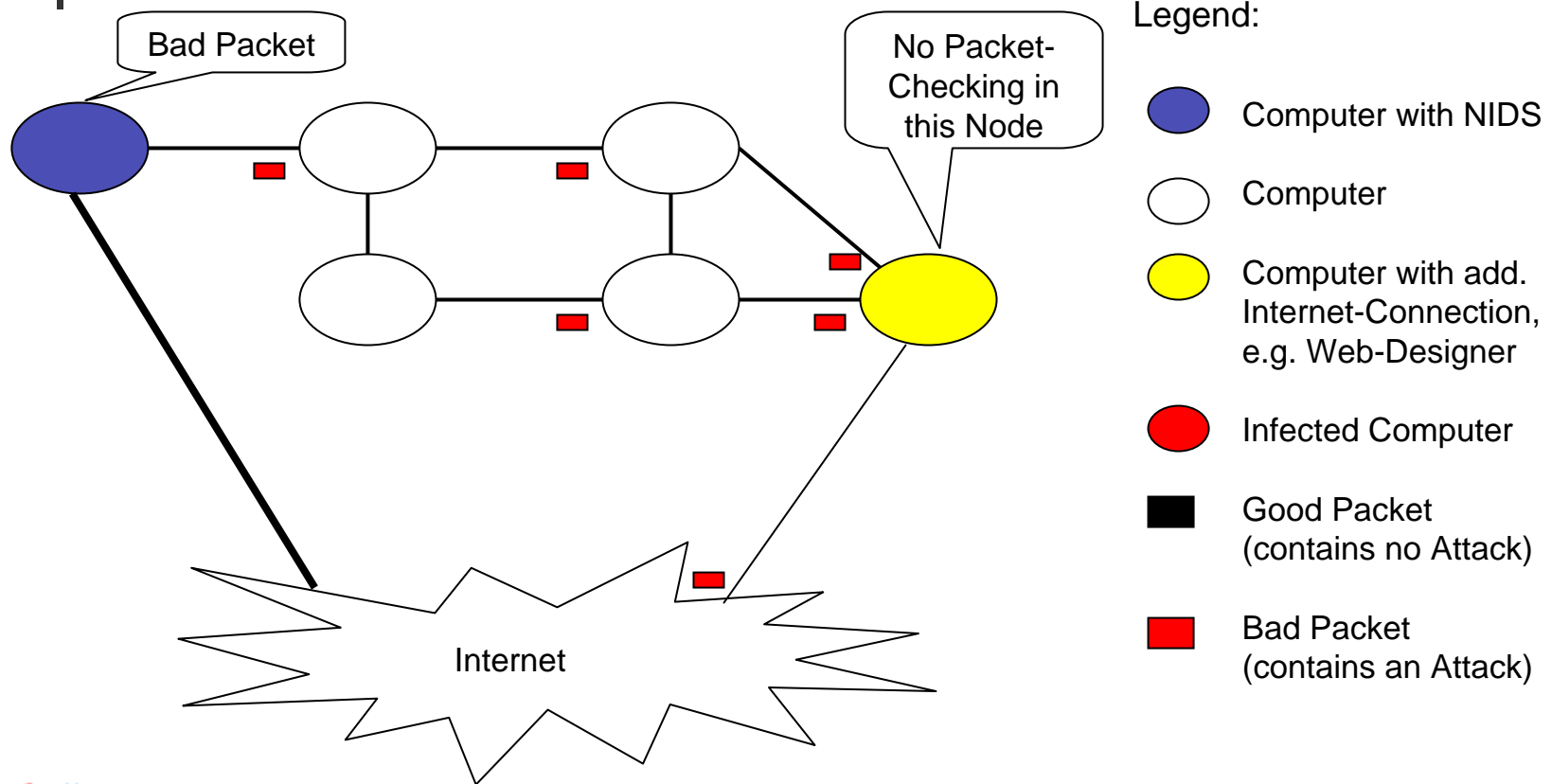
Legend:

-  Computer with NIDS
-  Computer
-  Computer with add. Internet-Connection, e.g. Web-Designer
-  Infected Computer
-  Good Packet (contains no Attack)
-  Bad Packet (contains an Attack)

Example for a running NIDS



Example for a running NIDS





Introduction

- Consequently, novel Approaches for Network Security are needed.
- The following Features are required:
 - Distributed, secures the whole Network
 - Computational Power is shared over the Network
 - Adaptive, learns how to detect new Attacks
 - Autonomous, works without central center



Immune System

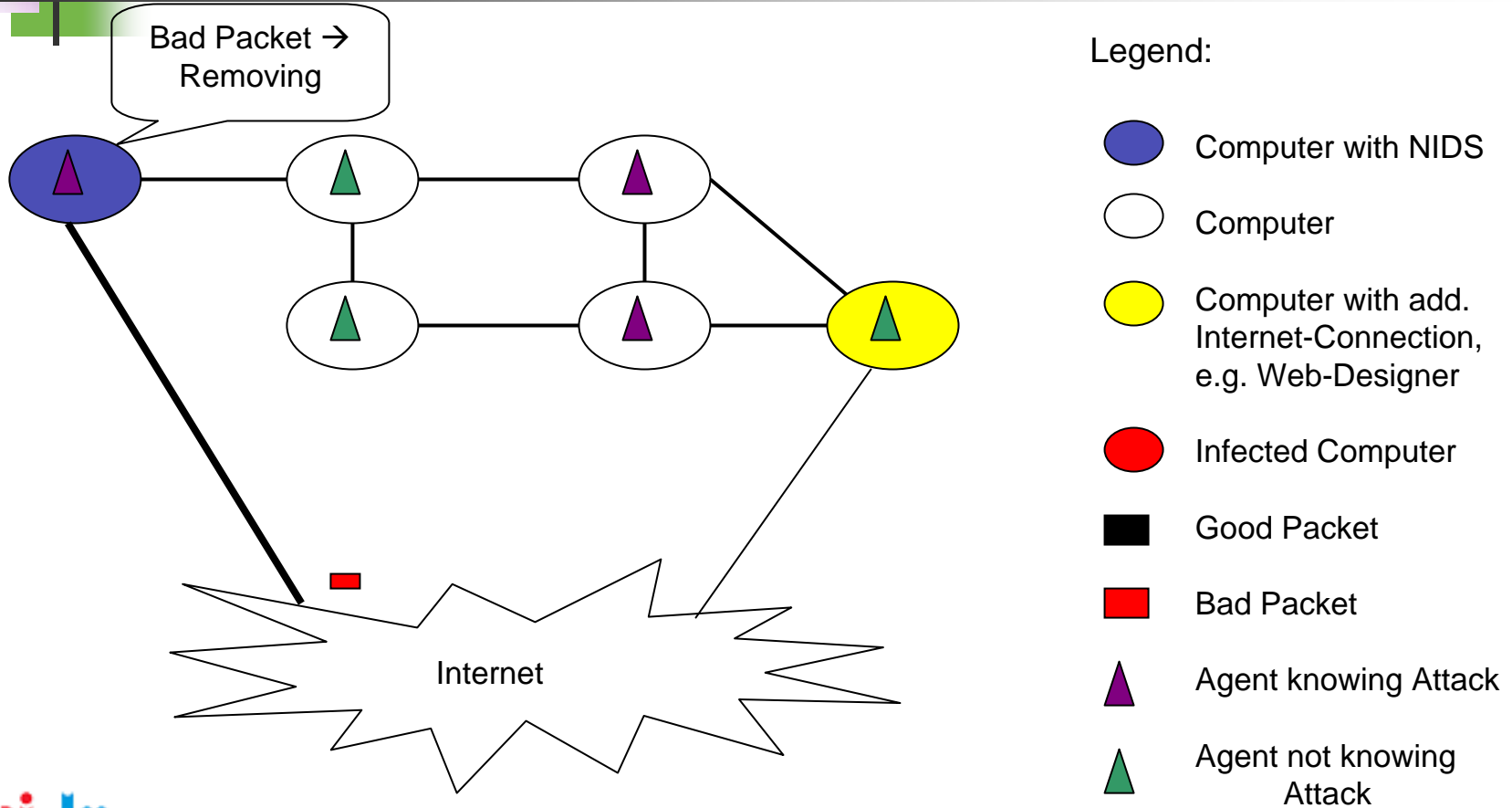
- Human Immune System (HIS)
- Protect the Human Body against Pathogens. It works efficient, unsupervised and it adapts quickly to new Pathogens.
“Nearly perfect Security-System for the Human Body”
- Building an Artificial Immune System (AIS) with the Advantages of the Human Immune System would enhance current NIDS.



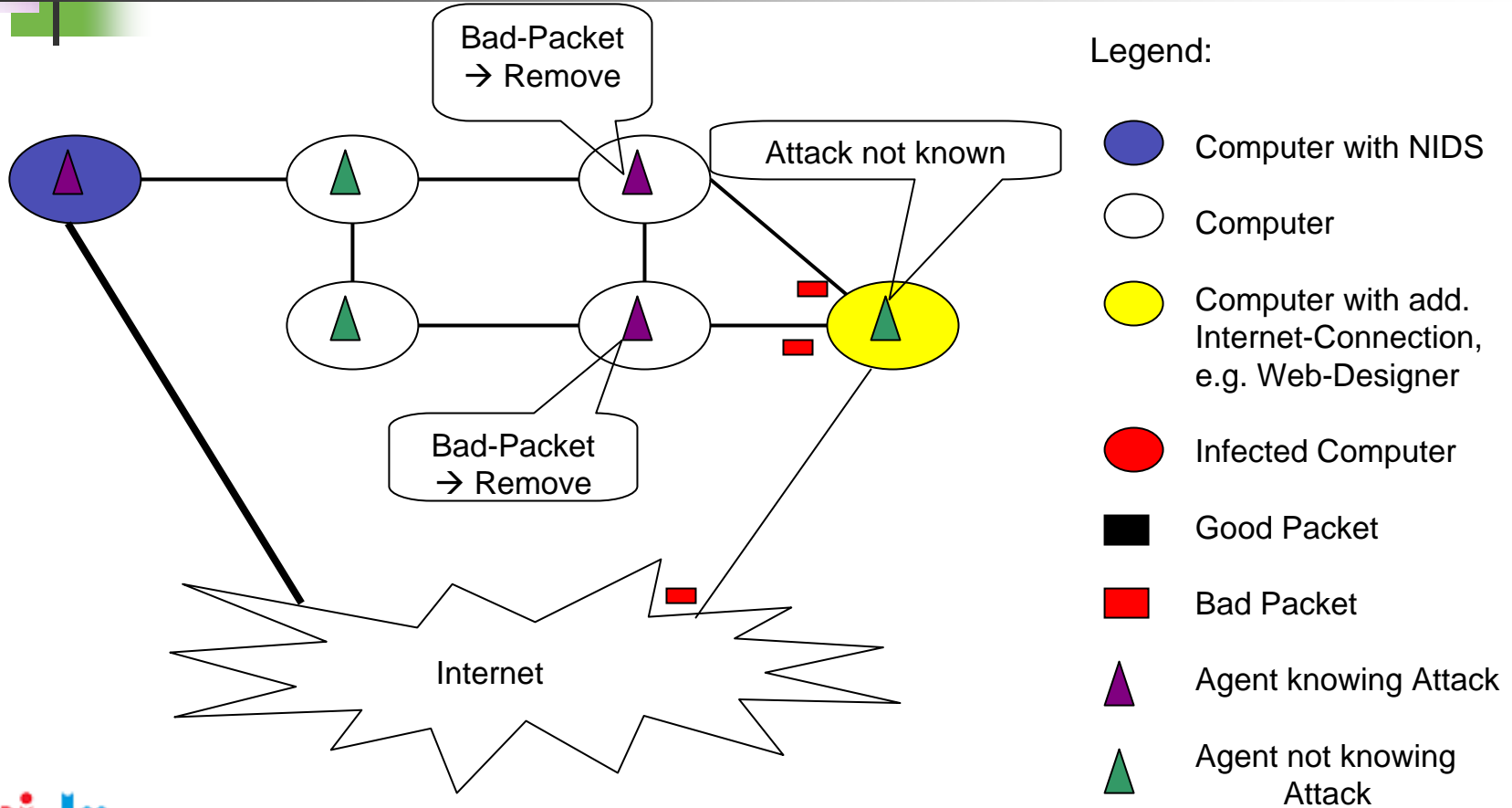
Artificial Immune System

- Artificial Cells – Agents – flow through the Network and perform Task in order to guarantee the Network Security.
- Some Features of Artificial Cells:
 - Lightweighted, Mobile
 - Autonomous
 - Adaptive
- Examples of Tasks:
 - Evaluate Packets whether they contain an Attack or not
 - Observe Status of a Network Node
 - Monitor Statistical Data about Network Traffic

Example for AIS



Example for AIS



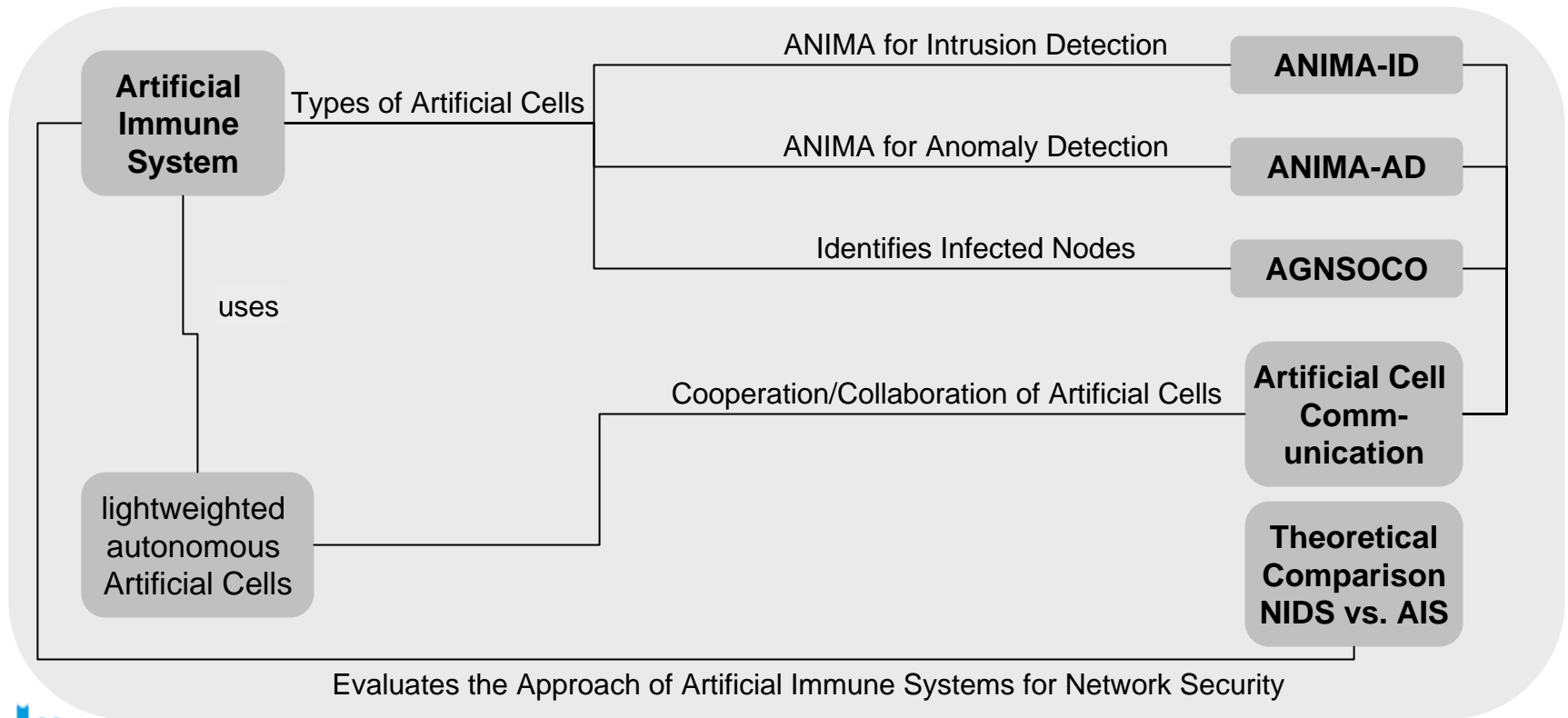


SANA

- SANA – Security Analysis in Internet Traffic BFR-Project funded by the Ministry.
- Introduce novel, non-standard Approaches for Network Security
- Several Sub-Projects which describe Components/Artificial Cells of the Artificial Immune System in SANA

SANA Overview

SANA





SANA in Detail

- SANA – AIS implemented in Java
- Bases on a Network Simulator which simulates a Packet-Oriented Network
- An Adversarial injects Packets with and without Attacks in order to stress the Network and the AIS.
- The artificial Cells check the Packets and remove the Packets containing an Attack. Additionally, artificial Cells may perform other Tasks as well.

SANA-AIS - Biological Inspired

- Packet Filter – Check only Packet-Header – Modeling the innate Immune System
 - Innate Immune System detects and removes basic Intrusion quickly.
- Artificial Cells – Check whole Packet and perform additional Tasks – Modeling the adaptive Immune System
 - Adaptive Immune System detects and removes complex Attacks and performs other Tasks.



SANA Architecture

- Using the Implementation of SANA, it is possible to add complex Attacks and simulate complex Scenarios.
- In the SANA-AIS, it is possible to model nearly all immunological Processes.
- Currently, the Second-Signal/Co-Stimulation and a first version of Cytokines are implemented.

SANA Architecture

Workflow in Node

Packet arrives at a node

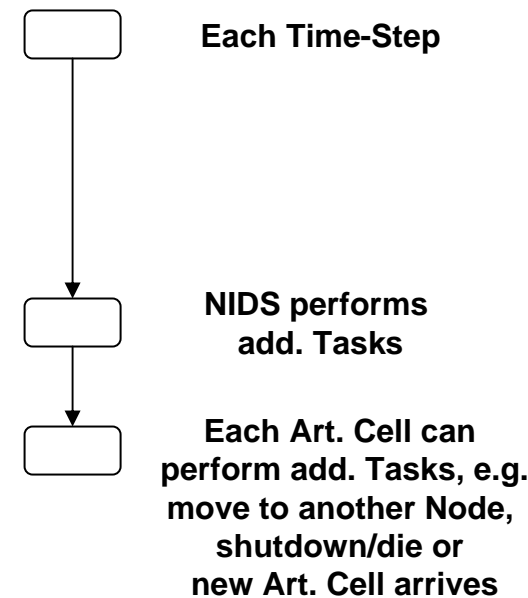
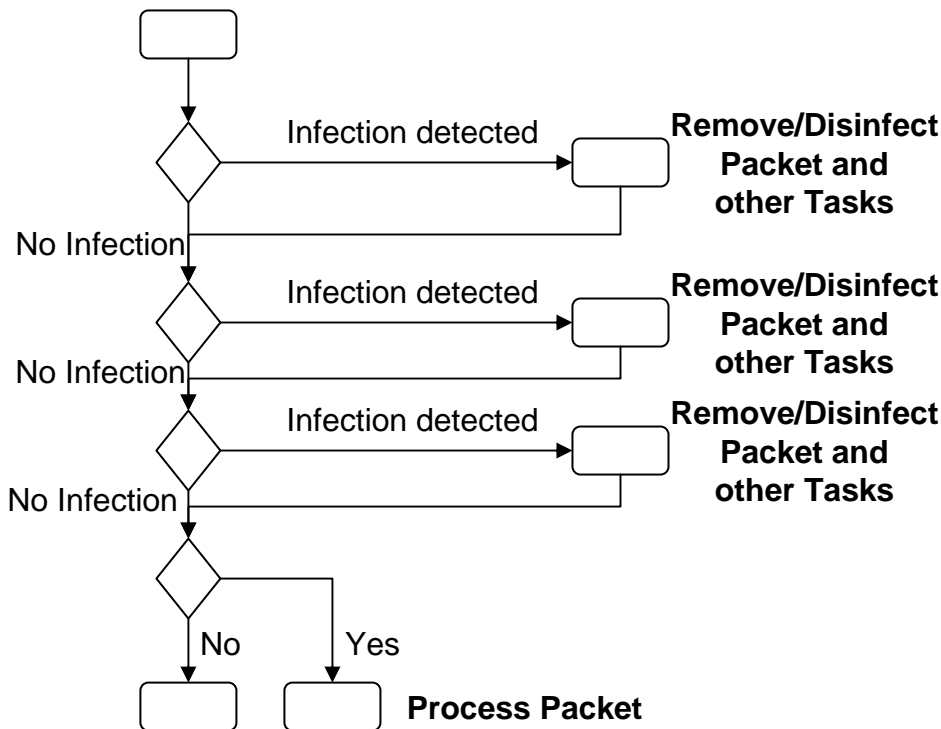
Packet-Filter: Checking Header

If available: Check by NIDS

Packet checked by each Artificial Cell

Destination is this Node

Send Packet to Destination





SANA Scenarios

- Defined in a Scenario:
 - Topology of the Network
 - Behaviour of Adversarial / Artificial Cells
 - As the case maybe Topology / Behaviour of NIDS
 - Number of Time-Steps to simulate
- After the Simulation:
 - Number of founded Attacks
 - Number of finished Attacks
 - Number of False-Positives
- Currently at least 15 Simulations with different Attacks, Adversaries, Agents and Networks.



SANA Results

- SANA performs well in most Scenarios.
- SANA identifies about 60% - 80% of the Attacks.
- In cooperation with a NIDS, the Network is secured against nearly all Attacks (approx. 85% - 95%).

SANA –

Some types of Artificial Cells

- ANIMA-ID
Art. Cell which stores different Signatures of Attacks and identifies these again.
- ANIMA-AD
Art. Cell which stores the behaviour of normal Network Traffic and identifies abnormal.
- AGNOSCO
Art. Cell basing on Ant Colonies which identifies Zombie-Nodes.
- Second Signal
Cooperation of two Art. Cells in order to reduce False-Positives.



Next Steps

- Currently, there exist two different Approaches for Network Security:
 - Centralised (e.g. NIDS):
A Server which checks each Packet routed over it. All other Nodes are not secured.
 - Distributed (e.g. AIS):
A System which runs on each Node and all Packets on all Nodes are checked.
- In this Sub-Project, I compare the two Approaches theoretically. Therefore, I compare the two Approaches in different Models.
- However, the best Approach is a Combination of Centralised and Distributed Network Security Systems, e.g. a NIDS and SANA.



Next Steps

- The Human Immune System consists of lot of Cells. These cells cooperate/collaborate in order to secure the Human Body properly.
 - Example: Minimizing False-Positives – the Body would remove itself – using cooperation between Cells and Redundancies.
- In this Sub-Project, I analyse the Cell Communication in the Human Body in order to reuse the used Techniques for SANA and for Computer Science generally.



Publications

- M. Hilker, C. Schommer: Description of Bad-Signatures for Network Intrusion Detection. Proceedings, Fourth Australasian Information Security Workshop (AISW-NetSec 2006) during the Australasian Computer Science Week January 2006, Australia, Hobart. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 54.
- M. Hilker, C. Schommer: A new queueing strategy for the Adversarial Queueing Theory. Proceedings, IPSI-2005 December 2005, Slovenia, Bled.
- M. Hilker: Queueing Strategien im Internet Routing. Diploma Thesis at the JW Goethe-University Frankfurt, Germany, March 2005.



Conclusion

- More Information:
<http://wiki.uni.lu/mine>
- Thanks for Your Time!

Questions?