Helsinki University
of Technology

Protecting network infrastructures with strong cryptographic algorithms

The concept of Packet Level Authentication (PLA)

professor Hannu H. Kari
Laboratory for Theoretical Computer Science
Department of Computer Science and Engineering
Helsinki University of Technology (HUT), Espoo, Finland
email: Hannu.Kari@hut.fi

Agenda

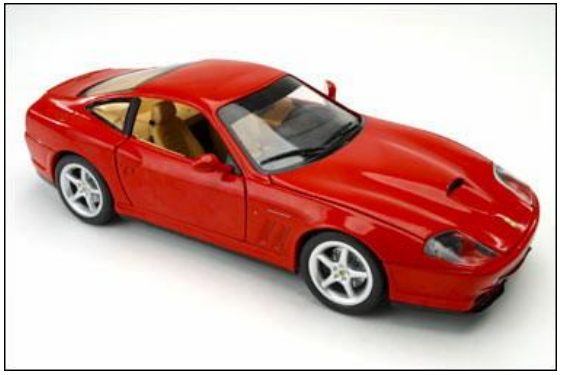
- Technology enhancements
- Fundamental design flaws of Internet
- Four technical levels to protect Internet
- Protecting network infrastructure
- PLA:
  - Packet Level Authentication –project
  - Project goals
  - Main operating idea
  - Performance estimations
  - Applications
- Conclusions

Helsinki University
of Technology

Technology enhancements

www.daimler.co.uk

~100 years



decorateyourgarage.com

www.macarthurcoal.com.au

Helsinki University
of Technology

Technology enhancements

www.route79.com

www2.jsonline.com

www.pennways.com

www.openfire.us

www.eia.doe.gov

en.wikipedia.org

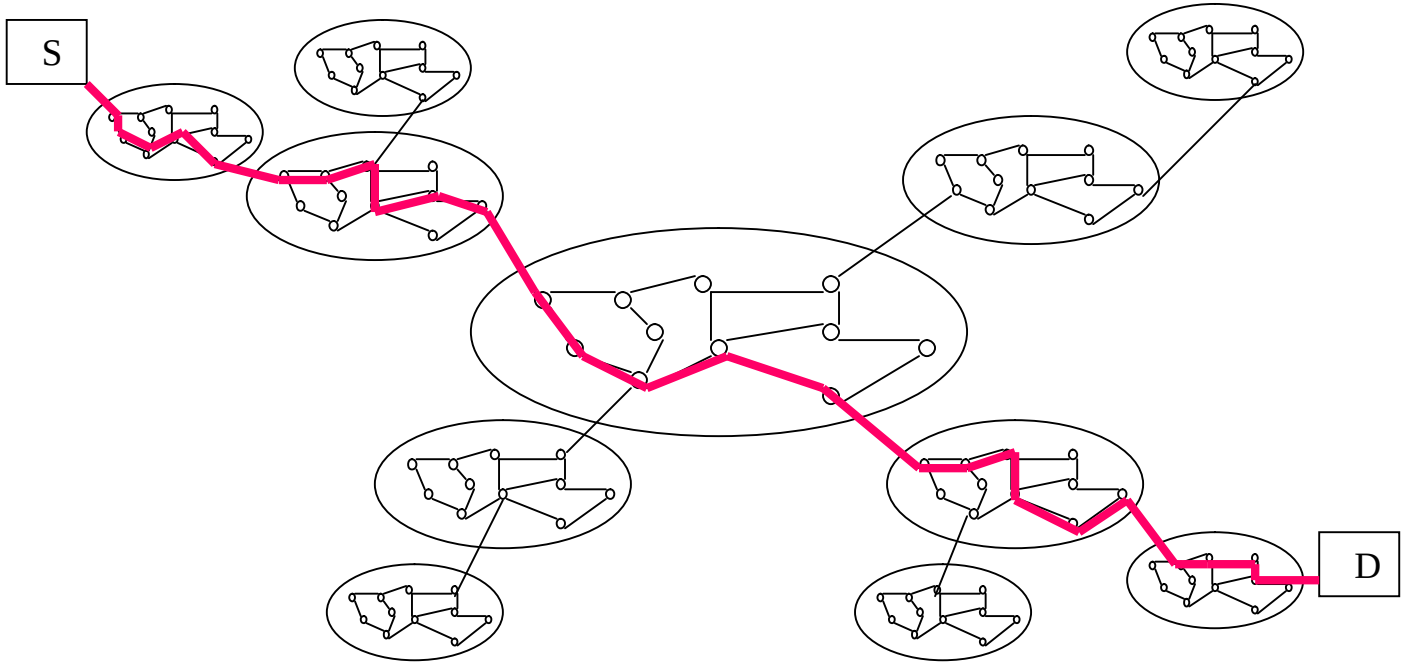
Technology enhancements

The same thing has happened in Internet in 10 years!

Fundamental design flaws of Internet

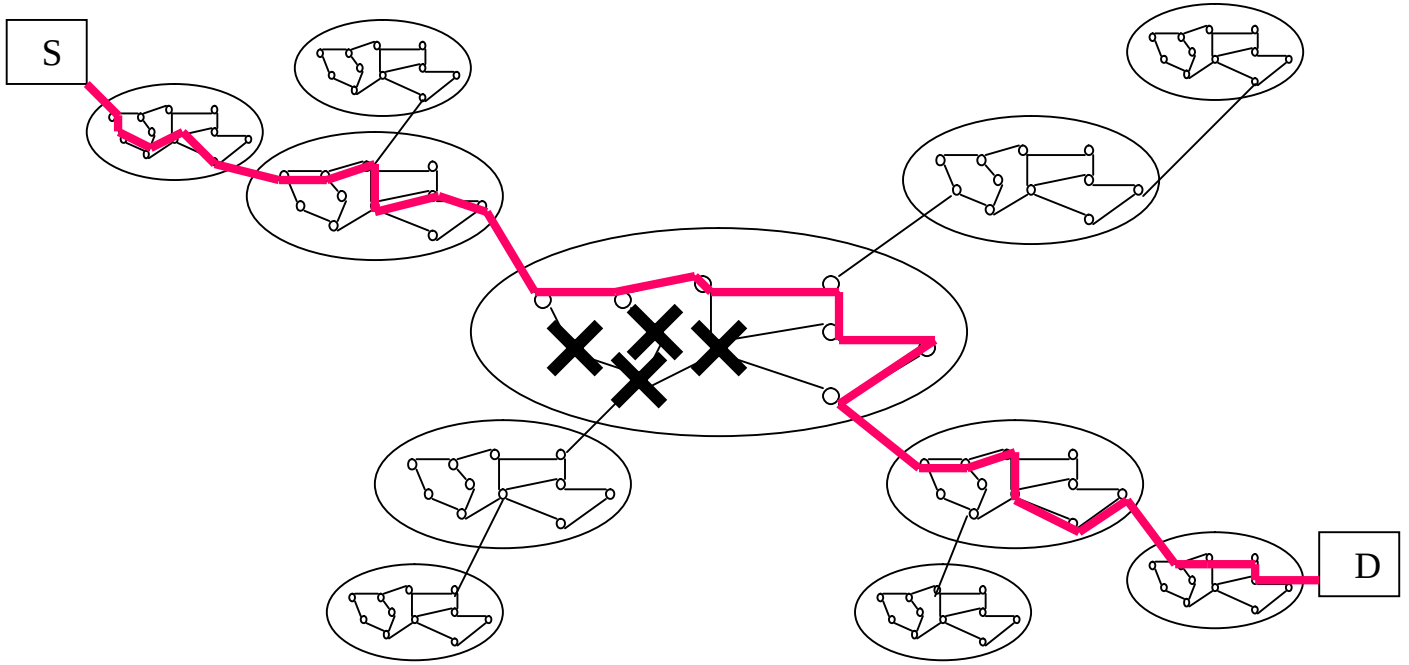
Internet

- **Internet was originally designed to survive nuclear war**



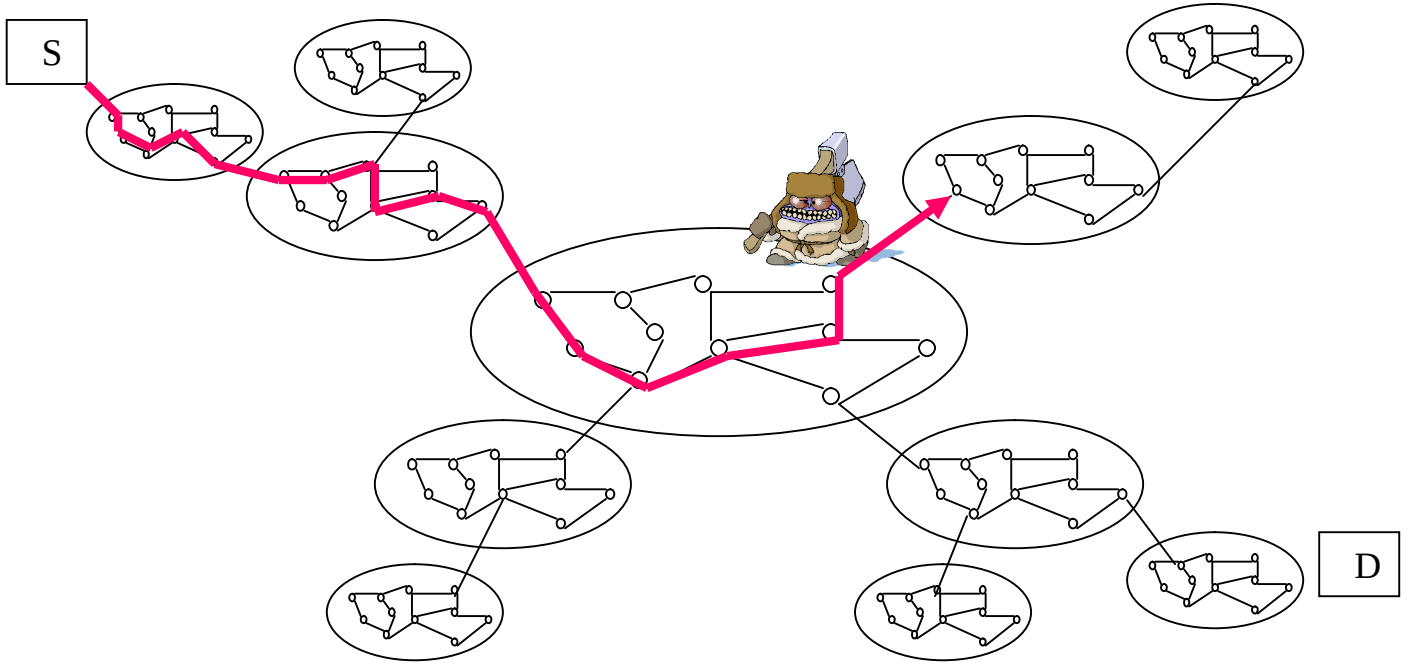
Internet

- **Packets can be rerouted quickly**



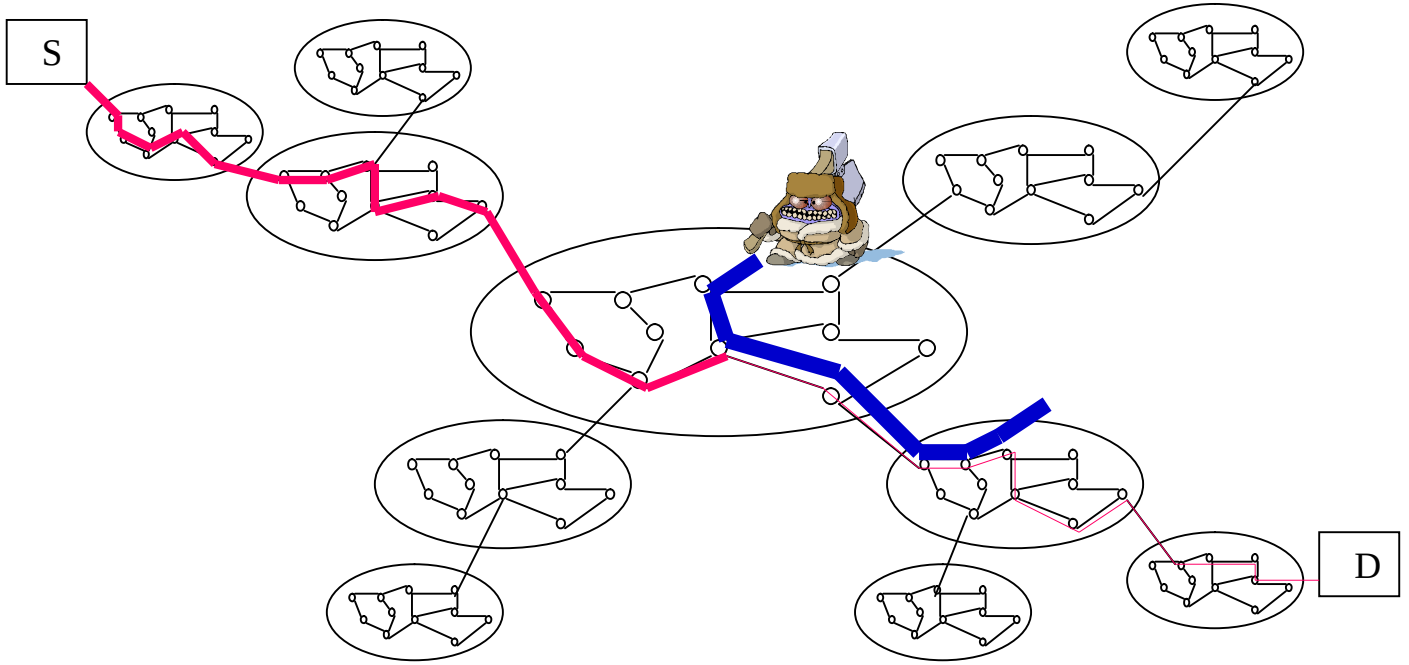
Internet

- **...but one mole can damage the routing**



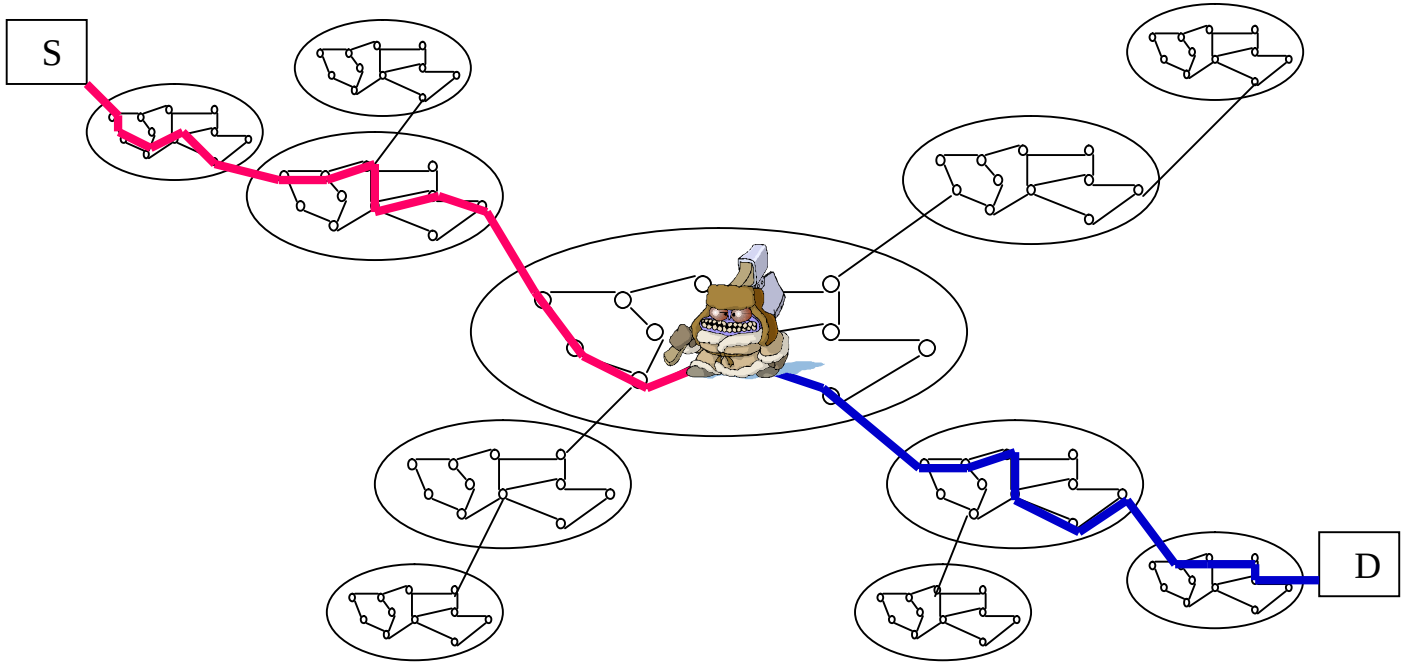
Internet

- **... or fill network with garbage ...**



Internet

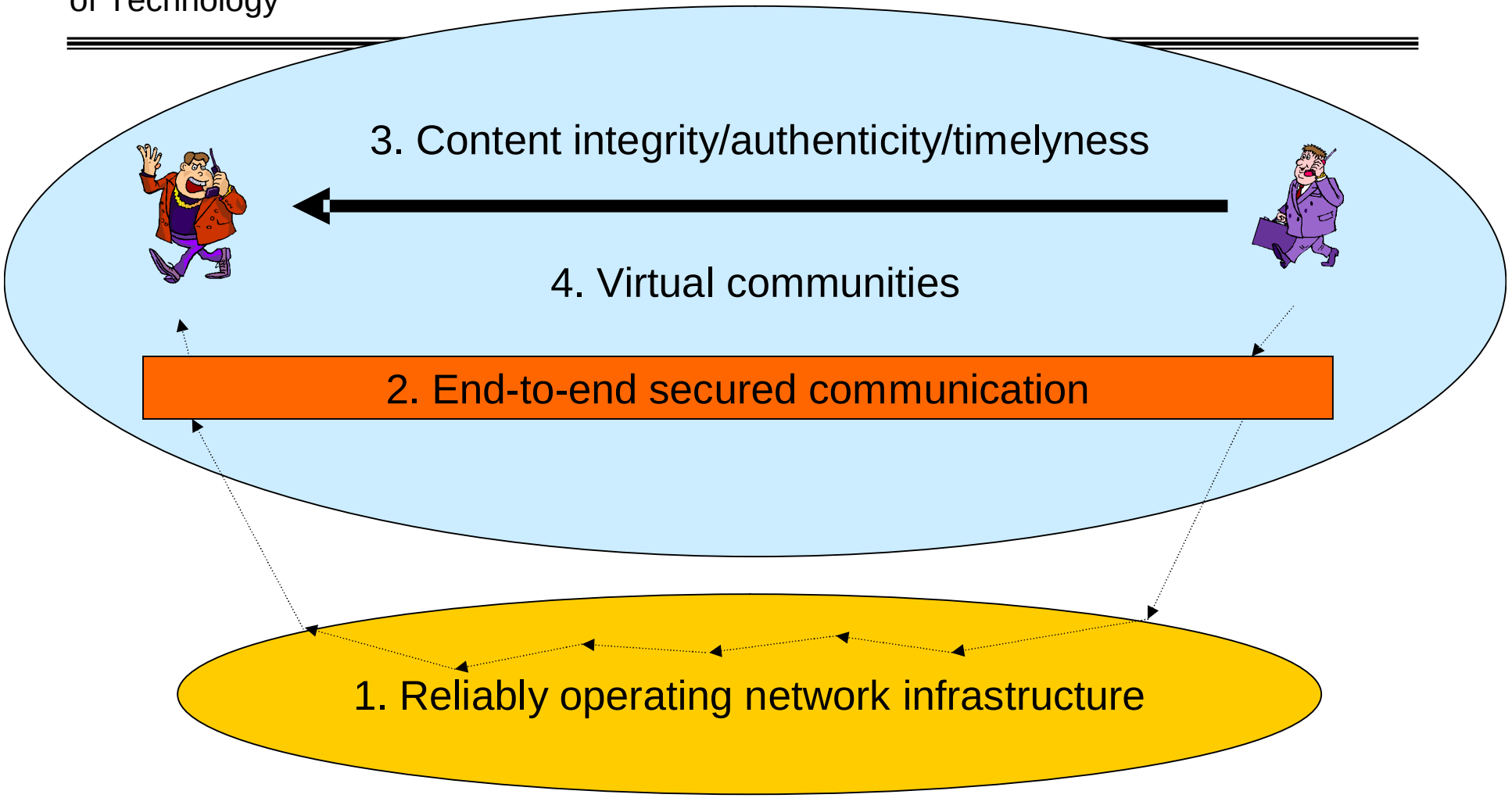
- **...or corrupt transmitted data**



Four technical levels to protect Internet

Helsinki University
of Technology

Four technical levels to protect Internet



Helsinki University
of Technology

Four technical levels to protect Internet

1. **Reliably operating network infrastructure**
   - **”Network-traffic-police” supervises traffic that networks operate and users/computers are following the traffic-rules**
2. **End-to-end secured communication**
   - **Unauthorized entities can’t see or change the content or know with whom we are communicating, and where we are**
3. **Content integrity/authenticity/timelyness**
   - **Automatic detection of forged information**
   - **Originator of WWW-page or email message can be verified**
   - **Integrity of the message can be verified**
4. **Virtual communities**
   - **Only the ”good guys” are members of the community**
   - **Communication is possible only between members**
   - **Missusers will be removed and punished**

Protecting network infrastructure

Helsinki University
of Technology

Protecting infrastructure: Main principle

- **Target**
  - **Communication between two legitimate computers shall work in all the time**
    - **despite any hostile attacks, that manipulate packets, jam the network, cut the communication links, or by other means try to disturb legitimate communication**

  ⇒ The network (i.e., routers) shall distinguish whether a packet is
    - **generated by a legitimate computer (and packet shall be forwarded further)**
    - **generated or modified by attackers (record/discard that packet and optionally rise an alarm)**

  - **Network shall be capable of prioritizing traffic based on importance of packets (Qos) and user**
    - **not every computer or packet is equal**

PLA:
Packet Level Authentication-project

History

- **PLA-concept was originally introduced in 007-project by end of 2002.**
  - **Project was funded by Finnish Defence Forces**
  - **Original idea was to protect wireless communication in military grade wireless ad hoc networks**
- **Log of publicity:**
  - **May 2003: First public presentation of the idea at KTH**
  - **April 2004: Proof-of-concept implementation demonstration SFW2004**
  - **May 2006: Second proof of concept made as part of the PLA-project outputs**
- **No patents filed!**

Helsinki University
of Technology

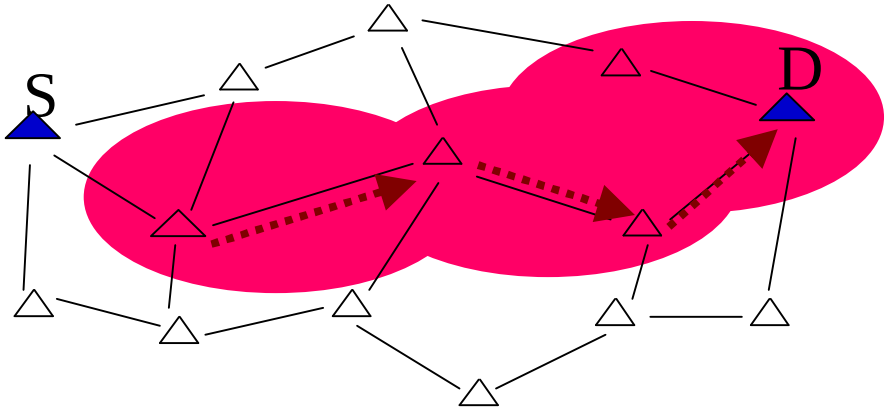
PLA-project

- **Strategic 2-year research project, 100%-ly Tekes funded (1.1.2006->)**
- **Four research topics:**
  - **Architecture**
    - **Concept design, scaleablity issues, Internet-wide deployment**
  - **SW implementation**
    - **Proof-of-concept with Linux –based routers**
  - **Crypto-methods**
    - **Optimized crypto-algorithms for PLA (e.g., elliptic curves)**
  - **HW acceleration**
    - **FGPA-based implementation of crypto-algorithms**
- **Three research groups from HUT**
  - **prof. Hannu H. Kari (mobility management, architecture, SW implementation)**
  - **prof. Kaisa Nyberg (crypto-algorithms, security analysis)**
  - **prof. Jorma Skyttä (crypto-accelerator, FPGA-implementation)**

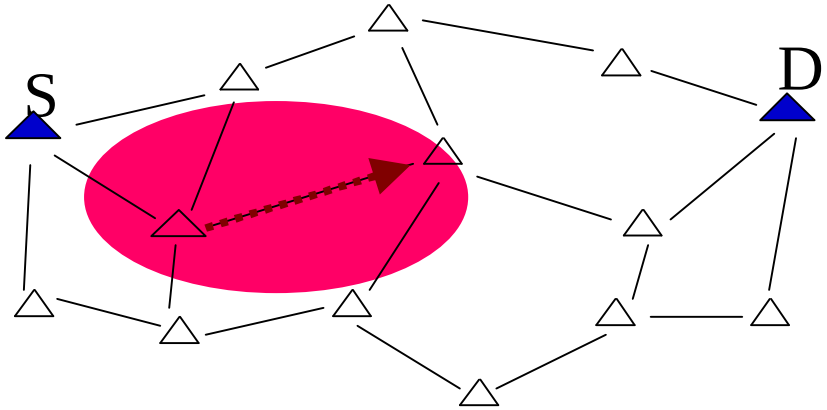
Helsinki University
of Technology

Original concept of PLA

Without PLA:
enemy uses our nodes to disturb our network



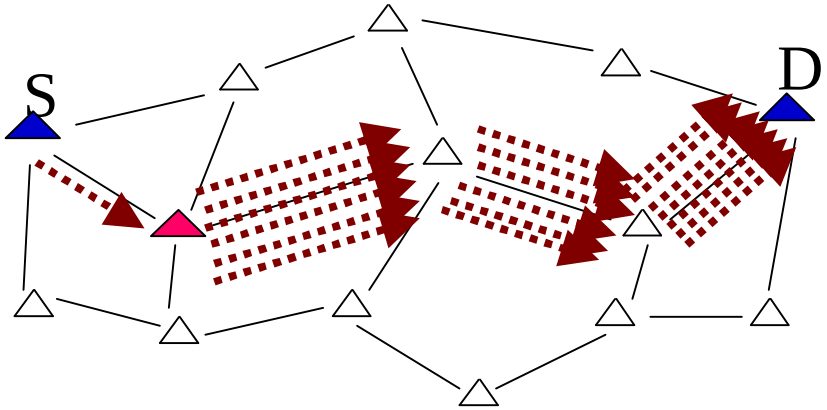
With PLA:
Interference is stopped at the first node



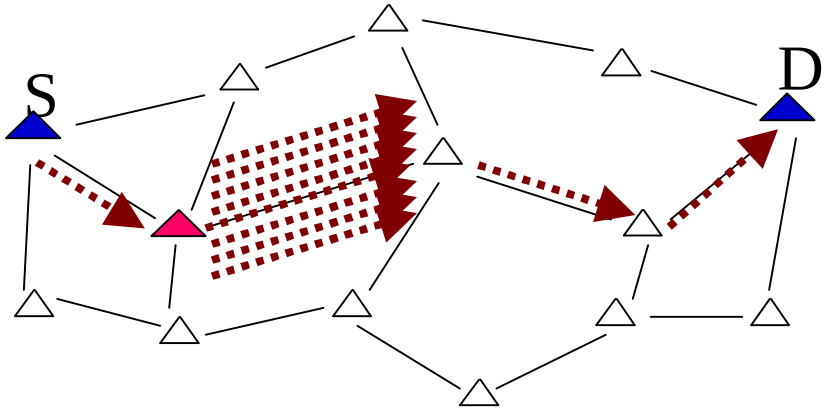
Helsinki University
of Technology

Original concept of PLA

Without PLA:
illegal duplicates cause flooding



With PLA:
discard illegal duplicates



PLA: Project goals

Goals

- To guarantee packet integrity
  - Undeniable proof of the origin of the packet
- To protect network infrastructures
  - Internet, in general
  - Wireless ad hoc networks, especially
  - Military networks, definitely
- Guarantee, that good packets can go through the network
  - Malicious packets shall be eliminated promptly
- PLA-solution should be part of every computer in the future

Helsinki University
of Technology

Packet level authentication

- **Analogy:**
- **Security measures on notes**
  - **Holograms**
  - **Microprint**
  - **Watermarks**
  - **UV-light**
  - **...**
- **Any receiver of notes can verify the authenticity of every note without consulting with banks or other authorities**

Helsinki University
of Technology

Packet level authentication

- **How about IP world?**
- **Each IP packet should have similar security measures**
  - **Receiver (e.g. a router) of a packet must be capable of verifying the authenticity of the IP packet without prior security association with the sender**
    - **I.e., receiver must be sure that the packet is sent by a legitimate node and the packet is not altered on the way**
    - **Just like with notes, each IP packet shall have all necessary information to verify authenticity**
- **In addition,**
  - **Since IP packets can be easily copied, we must have a mechanism to detect duplicated and delayed packets**

Helsinki University
of Technology

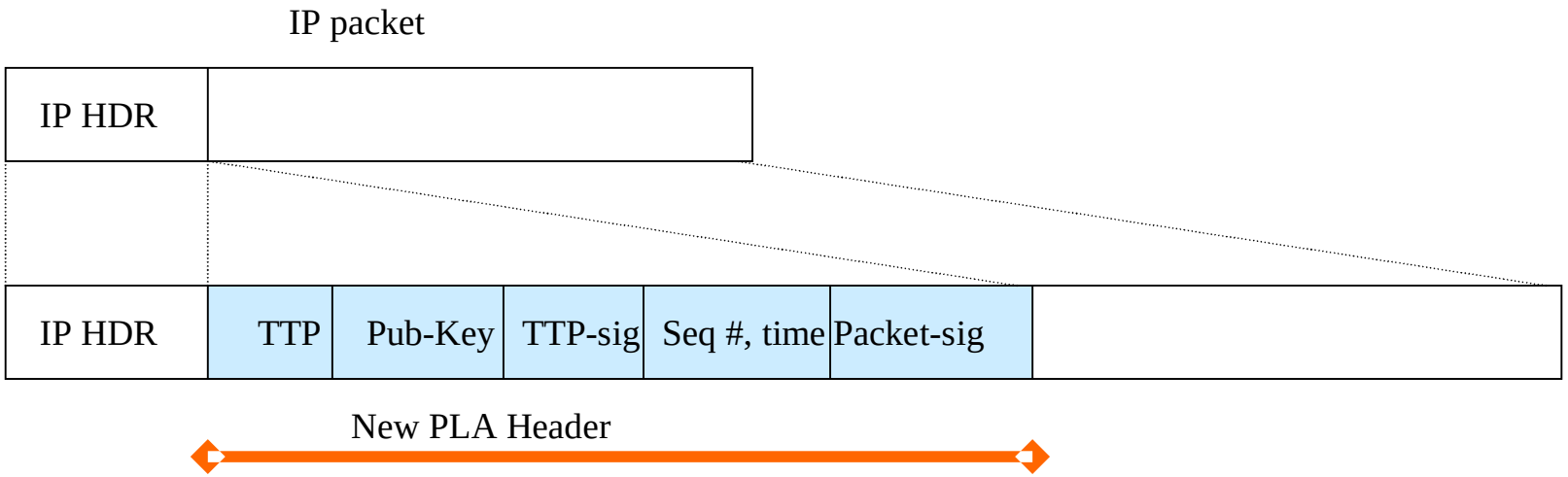
Packet level authentication

- **Why not IPsec?**
  - **Benefits of IPsec**
    - **Fast crypto algorithms and packet signatures due to symmetric keys**
    - **Well tested implementations and protocols**
  - **Disadvantages of IPsec**
    - **Can’t handle compromised nodes**
    - **IPsec is end-to-end protocol, intermediate nodes can’t validate packets**
    - **Requires several messages to establish security association between nodes**
    - **Scales badly to very dynamic networks**

PLA: Main operating idea

Helsinki University
of Technology

Packet level authentication: Implementation



PLA header inserted the same way as Mobile IP, IPsec, ... protocols

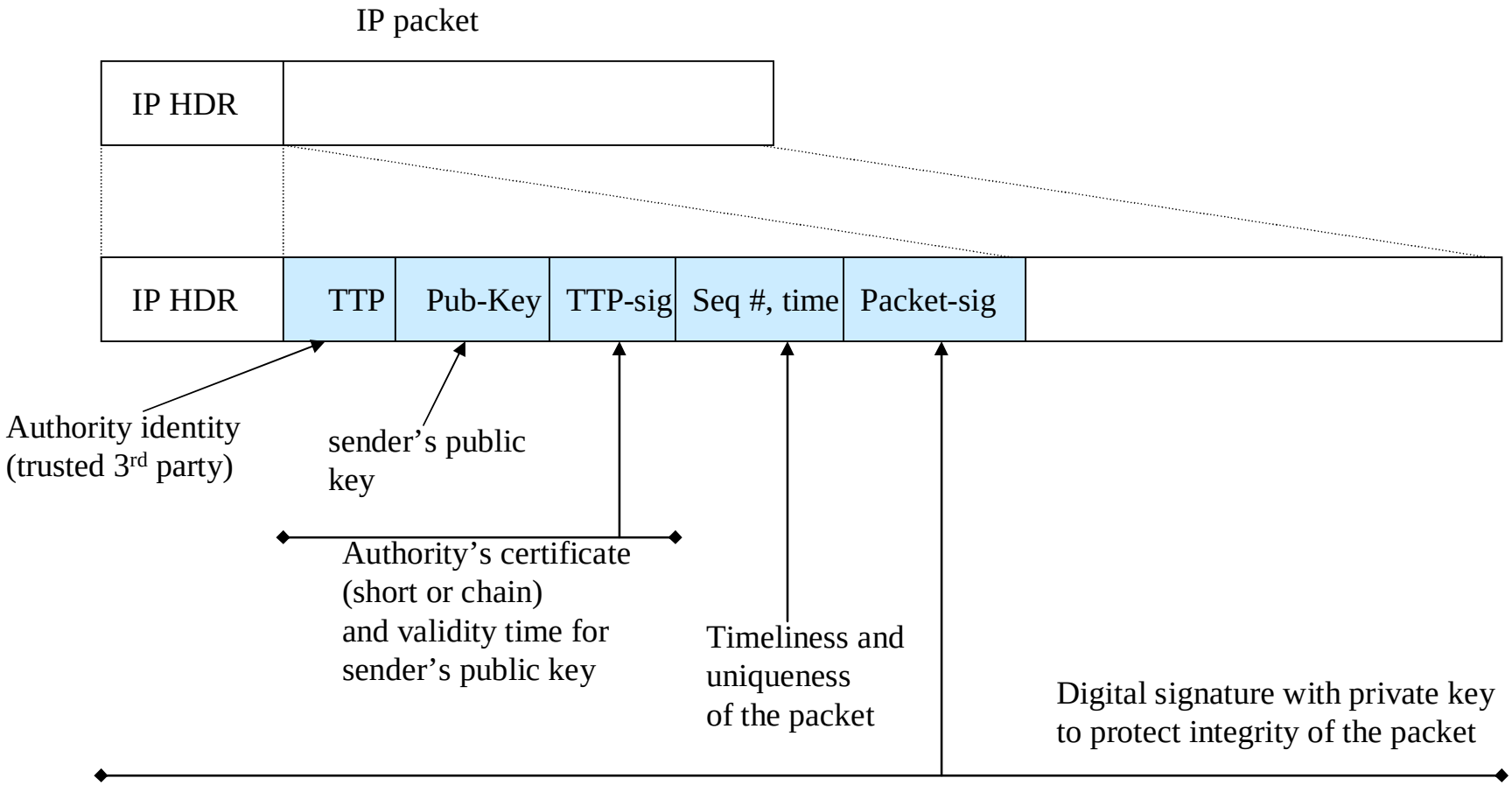
PLA header is transparent to standard IP routers (that do not understand PLA)

PLA header is transparent to all upper level protocols (UDP, TCP, SCTP, ...)

PLA can be used in both IPv4 and IPv6 networks

Helsinki University
of Technology

Packet level authentication: Implementation



Helsinki University
of Technology

Packet level authentication: Implementation

- **Extra header per packet**
  1. **Authority**
     - **General, TTP, Access-network operator, home operator,...**
  2. **Public key of sender**
     - **E.g., Elliptic curve (ECC)**
  3. **Authority's signature of sender key and validity time**
     - **Authority's assurance that the sender's key is valid for a given time period**
  4. **Sending time (+sequence number)**
     - **Possibility to remove duplicates and old packets**
  5. **Signature of the sender of this packet**
     - **Sender's assurance that he has sent this packet**

PLA: Performance estimations

Performance

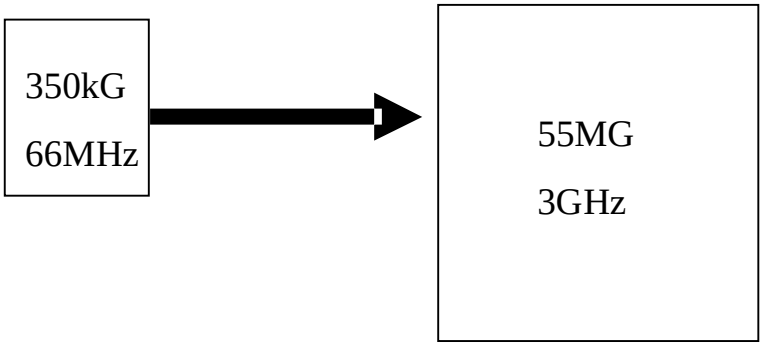
- **Sending node**
  - **One digital signature per packet**
- **Verifying node/Receiving node**
  - **First packet:**
    - **One certificate validation & One digital signature verification**
  - **Next packets:**
    - **One digital signature verification per packet**
- **Digital signature requires one hash and one elliptic curve operation**

Performance

- **Elliptic curve HW implementation at ECE department of HUT**
  - **FPGA with 350 000 gates**
  - **Clock speed 66MHz**
  - **167 bit ECC multiplication on 100 μs using 167 bit arithmetics**
  - **Estimate: one signature in less than 1 ms**
    - **Actually it is closer to 200 μs**
- **Performance is thus (in order of magnitude)**
  - **1000 packets/s**
    - **With 500 Byte packet size, 4 Mbps**

Performance

- **How about scaling up?**
  - **Pentium IV class silicon**
  - **Clock speed**
    - **66MHz -> 3 GHz**
    - **(speedup factor 45)**
  - **Dice size**
    - **350 000 gates -> 55 M gates**
    - **(160 parallel signature units)**



$$\frac{1}{1ms} \times \frac{C_{new}}{C_{ref}} \times \frac{G_{new}}{G_{ref}} = \frac{1}{1ms} \times \frac{3GHz}{66Mhz} \times \frac{55\,000\,000}{350\,000} = 7.14\ Msignature/s$$

Helsinki University
of Technology

Performance

- **Throughput of ”Pentium IV-class” PLA HW accelerator**

Throughput [Gbps]			
Signatures	Packet size		
validated			
per packet	150B	500B	1500B
One (*)	8.6	28.6	85.7
Two (**)	4.3	14.3	42.9
(**) For the first packet from a given sender			
(*) For the subsequent packets from the same sender			

Helsinki University
of Technology

Methods to improve performance

- **Parallel HW (multiple chips)**
- **Sending node**
  - **Every packet must be signed by the sender in order to minimize security problems**
- **Receiving/Verifying node**
  - **Check packets randomly**
  - **Check only every Nth packet**
  - **Checking can be adaptive**
    - **Check fewer packets from trusted nodes**
    - **Check more packets at the beginning of the stream of packets**
    - **More packets from same node of a flow, fewer checks done**
    - **When you feel paranoid, check more**

PLA: Applications

Applications for PLA

- Protecting network infrastructures
- Securing wireless ad hoc networks
- Restricting DoS and DDoS attacks
  - I don’t like messages from this sender, block it at nearest router
    - Nearest PLA-capable router to the attacker blocks the traffic
- Handling compromised nodes
- Delegation of command chain
- Reestablishing core network after military strike
- ...
- Handling access control
- Replacing firewalls
- Handle charging/accounting

Conclusions

Helsinki University
of Technology

Conclusions

- **PLA is part of HUT's Context Aware Management/Policy Manager (CAM/PM) –architecture, which is a rule based system that adapts node's behavior according to its surrounding**
- **Packet level authentication (PLA) provides scalable method to eliminate most of the faulty, forged, duplicated, and otherwise unwanted packets**
- **PLA can be implemented in HW with gigabits/s authentication capacity for core network routers**

Thank you,
Questions?

Some background material

Some PLA details

Helsinki University
of Technology

Packet level authentication

- **General requirements**
  - **Security mechanism shall be based on public algorithms**
    - **No security by obscurity!**
  - **Public key algorithms and digital signatures provide undeniable proof of the origin**
    - **Symmetric keys can’t be used since nodes may be compromised**
  - **Protocol must be compatible with standard IP routers and applications**
    - **Standard header extensions shall be used**
  - **Solution must be robust and scaleable**
    - **It shall be applicable both in military and civilian networks**

Helsinki University
of Technology

Packet level authentication

- **Benefits**
  - **Strong access control**
  - **Only right packets are routed**
  - **Easy to implement in HW (”Secure-CRC”)**
  - **Less packets in the network**
  - **Can be combined with QoS, AAA, firewalls, ...**
  - **Secures all routing protocols**
- **Disadvantages**
  - **Increased packet size (~100 bytes)**
    - **transmission overhead, processing delays**
  - **Requires strong crypto algorithms**
    - **Elliptic curves, digital signatures, ...**
  - **More computation per packet**
    - **One or two digital signatures, one or two hashes per packet**

Helsinki University
of Technology

Packet level authentication: Implementation

- **Sending:**
  1. **Authority**
     - **Constant field**
  2. **Public key of sender**
     - **Constant field**
  3. **Authority's signature of sender key and validity time**
     - **Constant field**
  4. **Sending time (+sequence number)**
     - **Update per packet**
  5. **Signature of the sender of this packet**
     - **Calculate per packet**

Helsinki University
of Technology

Packet level authentication: Implementation

- **Reception, 1. packet:**
  1. **Check sending time**
     - **Check time**
  2. **Authority**
     - **Verify that you know the authority (or ask your authority is this trustworthy)**
  3. **Public key of sender**
     - **Store this**
  4. **Authority's signature of sender key and validity time**
     - **Check validity**
  5. **Signature of the sender of this packet**
     - **Verify**
  6. **Sequence number**
     - **Store sequence number**

Helsinki University
of Technology

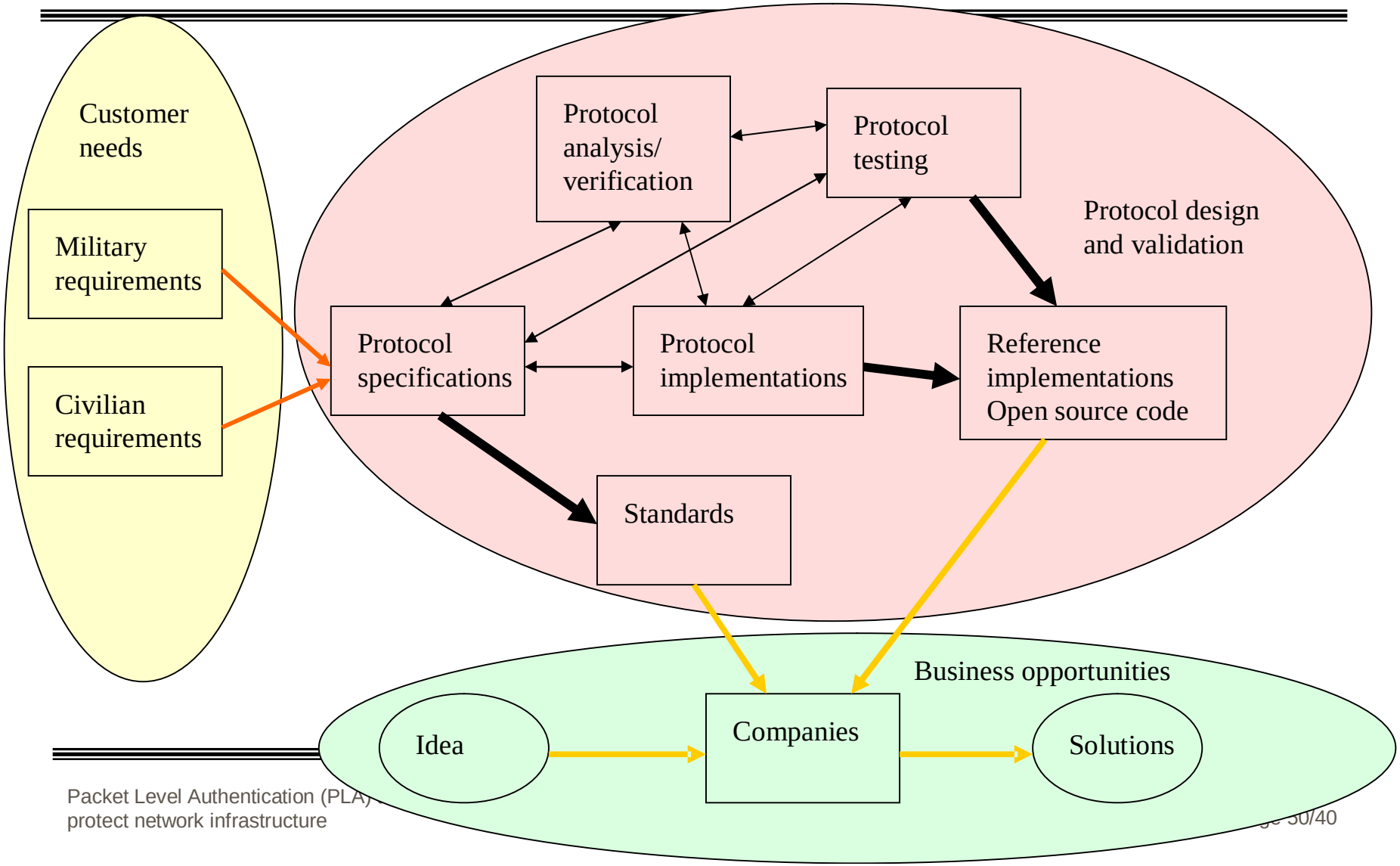
Packet level authentication: Implementation

- **Reception, next packets:**
  1. **Sending time**
     - **Verify time and sequence numbers**
  2. **Authority**
     - **Verify data in cache**
  3. **Public key of sender**
     - **Verify data in cache**
  4. **Authority's signature of sender key and validity time**
     - **Verify data in cache**
  5. **Signature of the sender of this packet**
     - **Verify**
  6. **Store time and sequence number**

Open Software Research - principle

Helsinki University
of Technology

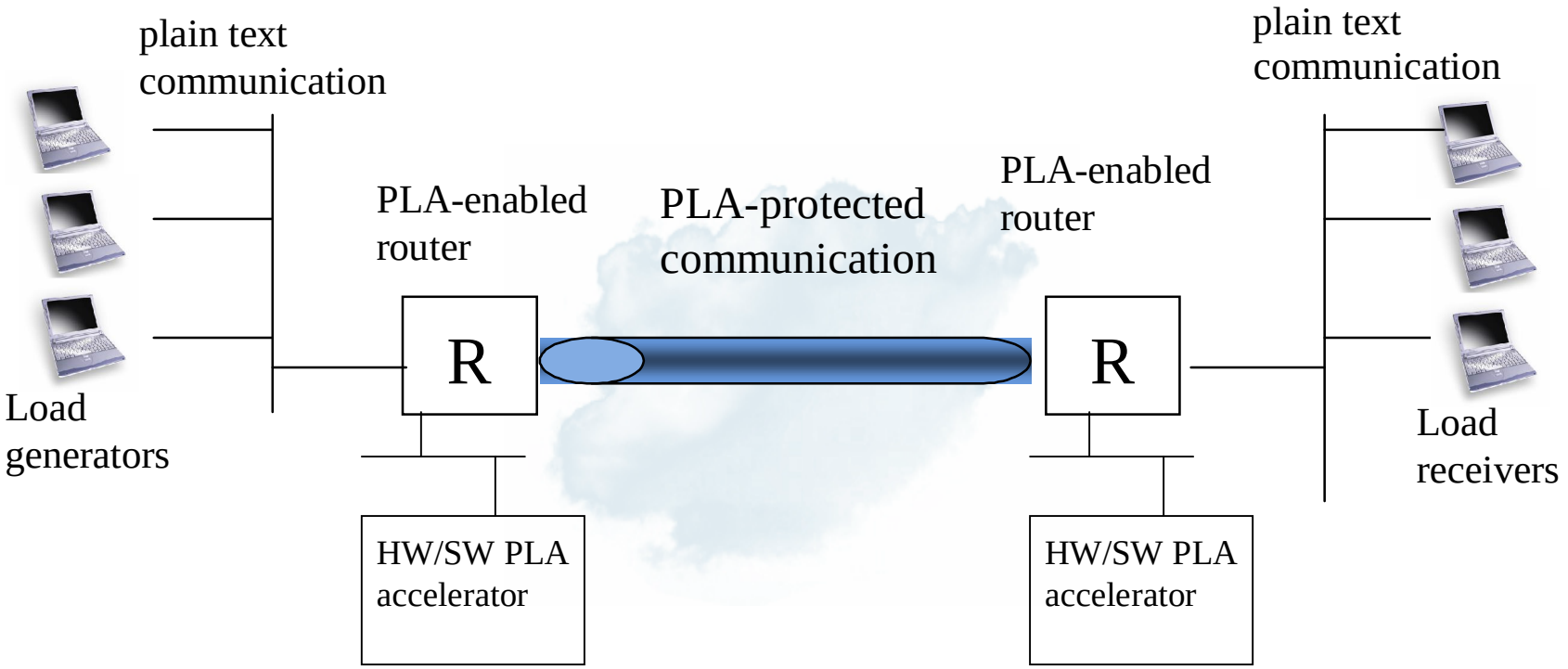
Operating model for open source research



Test environment

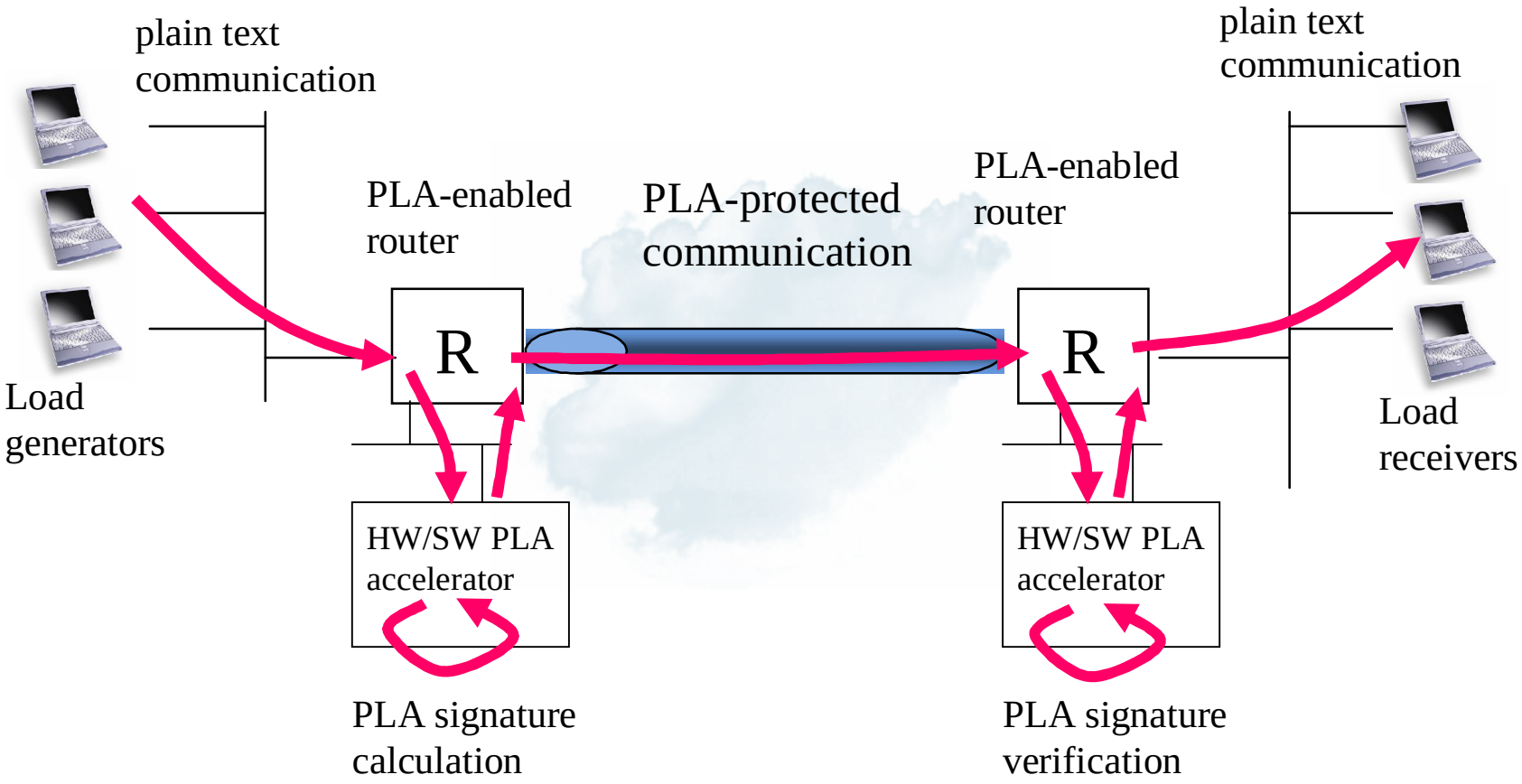
Helsinki University
of Technology

Test environment



Helsinki University
of Technology

Test environment: PLA operations



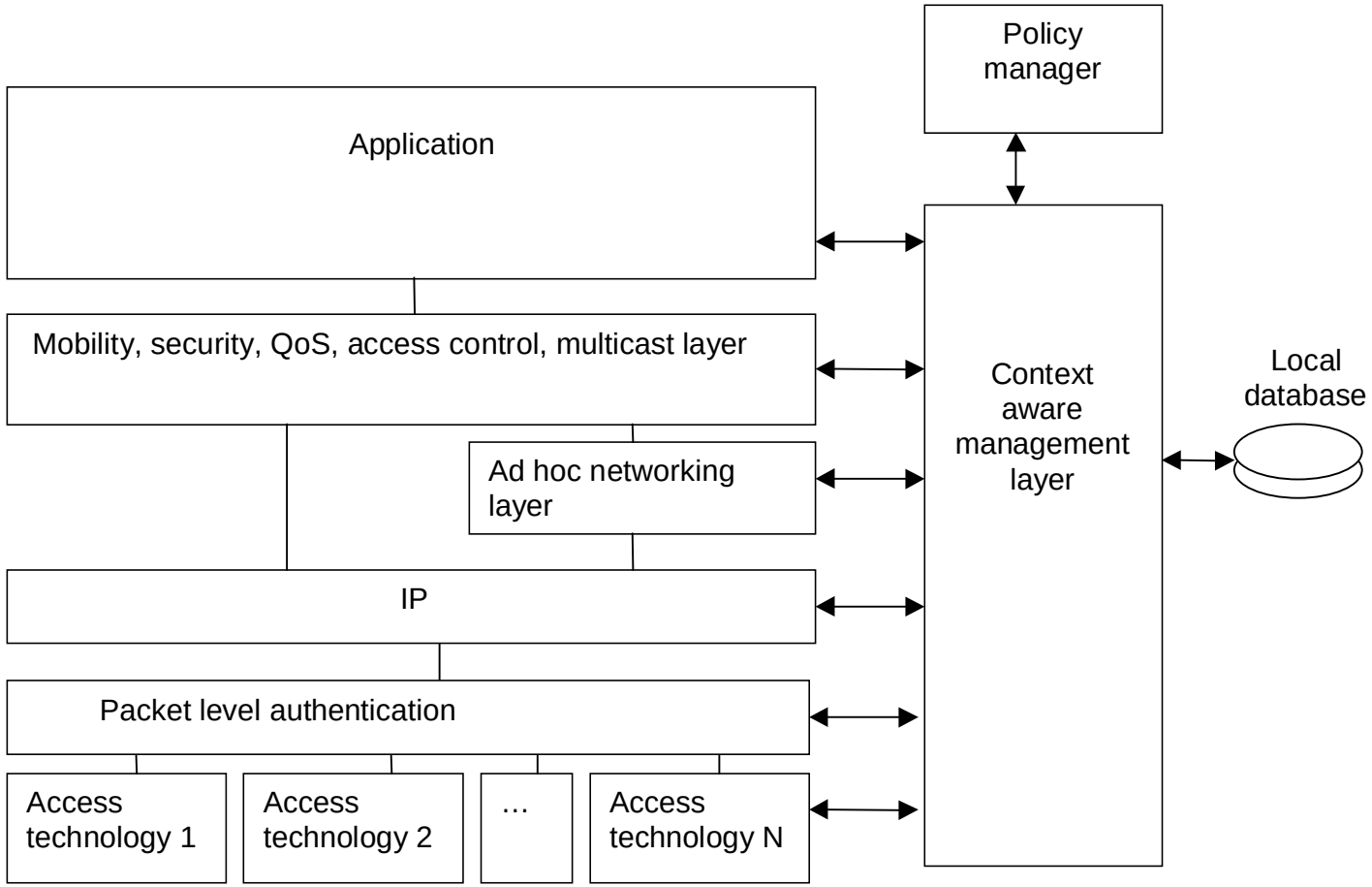
Context Aware Management/ Policy Manager (CAM/PM) architecture

New solution

- **Context Aware Management/Policy Manager**
  - **Each node (computer) has a rule based policy manager that controls the behavior of the node and adapts it to environment changes**
- **Adaptive trust model**
  - **Trust on nodes is not static but changes on time**
- **Packet level authentication**
  - **A mechanism to ensure that only correct and authentic packets are timely processed**

Helsinki University
of Technology

Context Aware Management/ Policy Manager



Helsinki University
of Technology

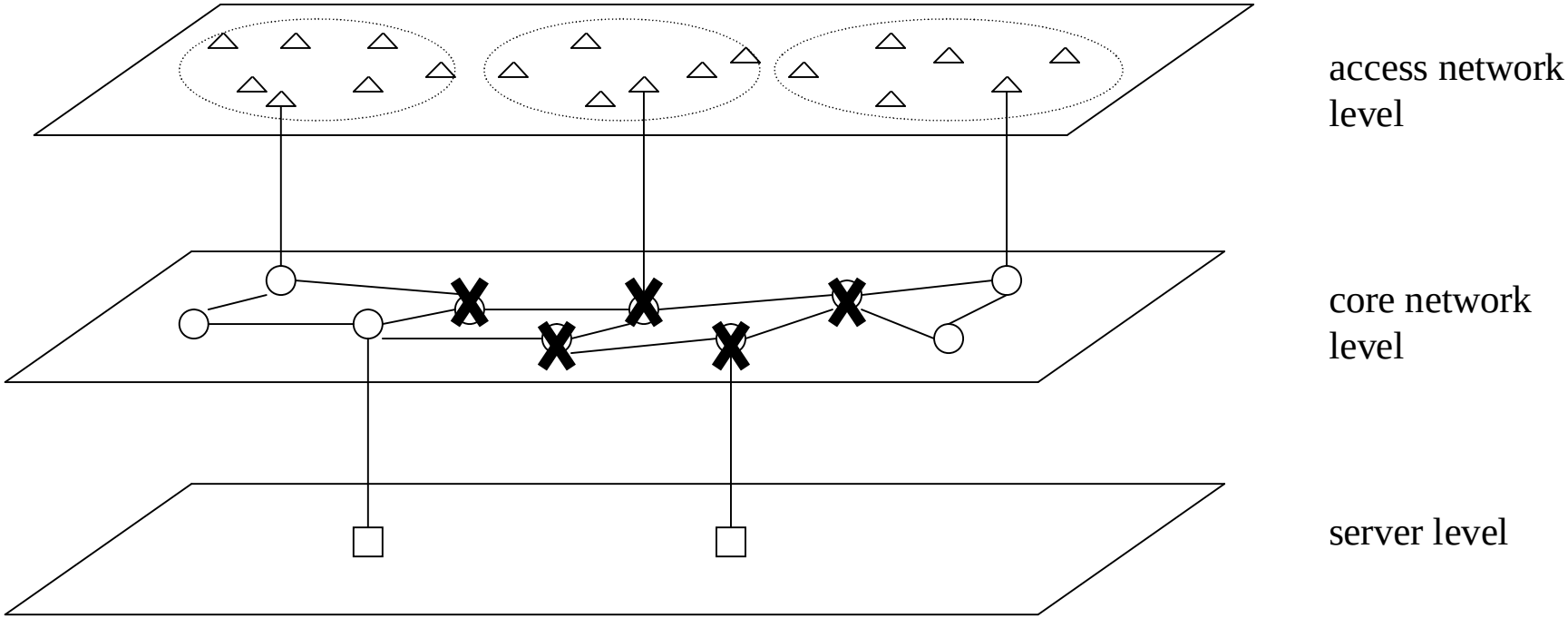
Context Aware Management/ Policy Manager

- **Context Aware Management layer**
  - **Interfaces with all protocol layers and applications**
- **Policy Manager**
  - **Decisions are based on policy rules**
  - **Collects information from all protocol layers and applications**
  - **May have local user interface**
  - **Can negotiate with neighboring PMs or take commands from remote entity**
- **Policy rules**
  - **Formal representation of decision methodology**
  - **New rules can be sent by authorized entity (e.g., owner of the node, civil/military authority)**

Utilizing CAM/PM with PLA and adaptive trust model: New rules to fix damaged core network with wireless network

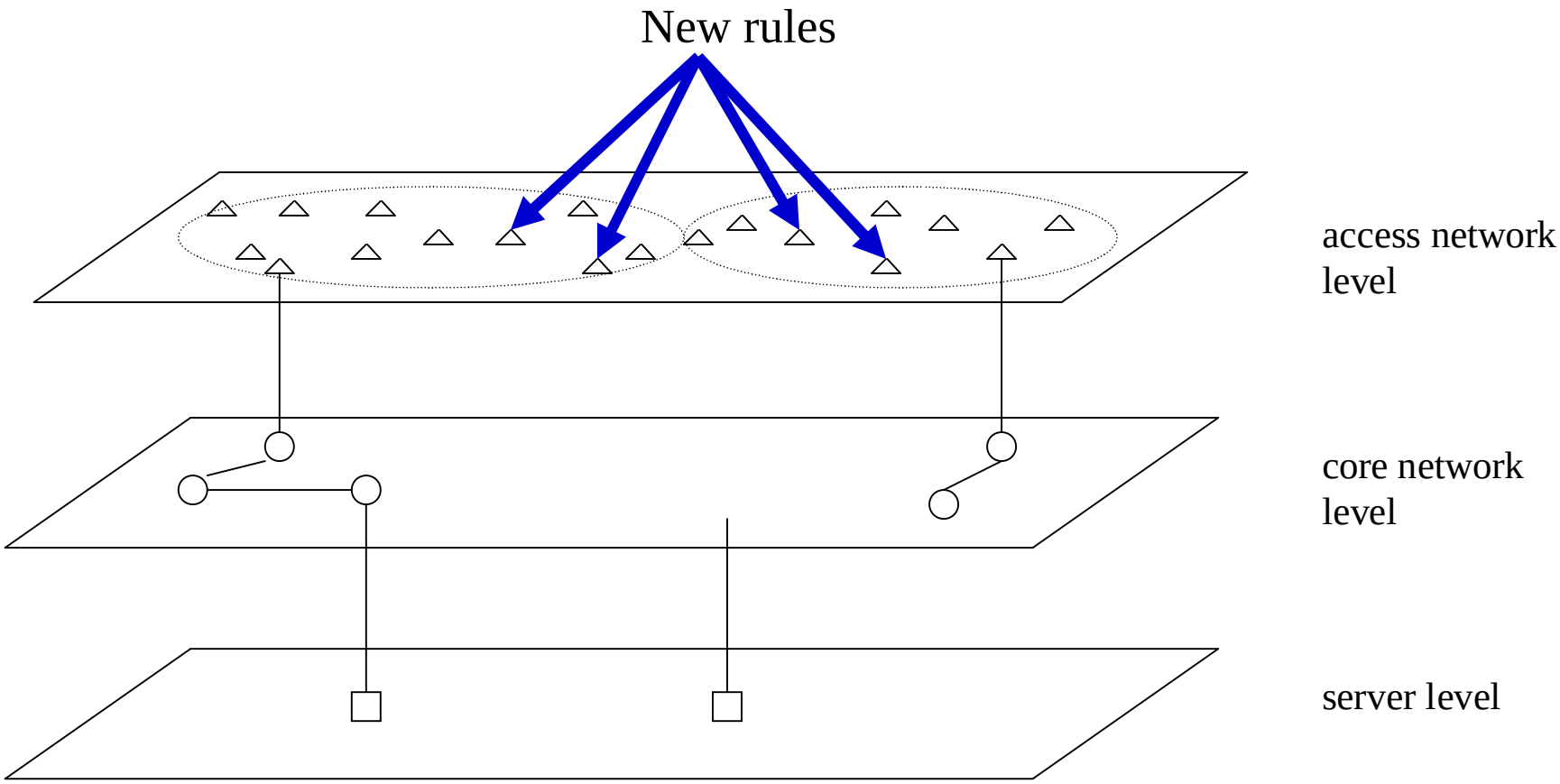
Helsinki University
of Technology

Application: New core network: Military strike



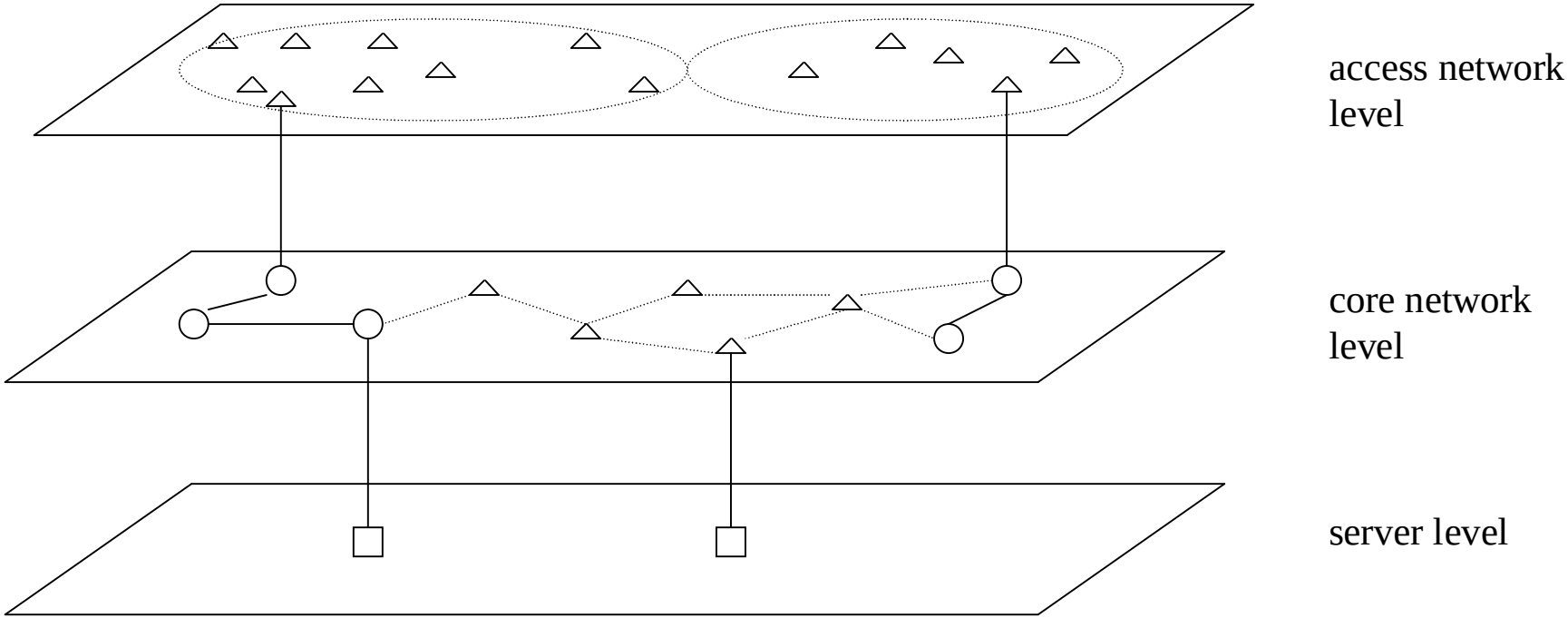
Helsinki University
of Technology

Application: New core network: Reconfiguration



Helsinki University
of Technology

Application: New core network: After military strike

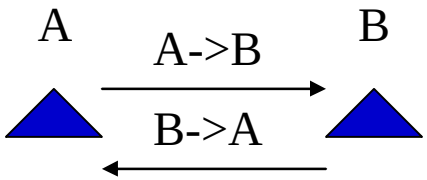


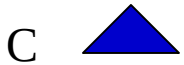
Utilizing CAM/PM with PLA and adaptive trust model: Fast communication in a dynamic wireless network

Helsinki University
of Technology

Application: Quick secured communication in battle field

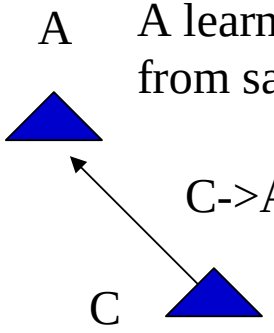
Any communication





C learns that both A and B are from same group

First message from C to A

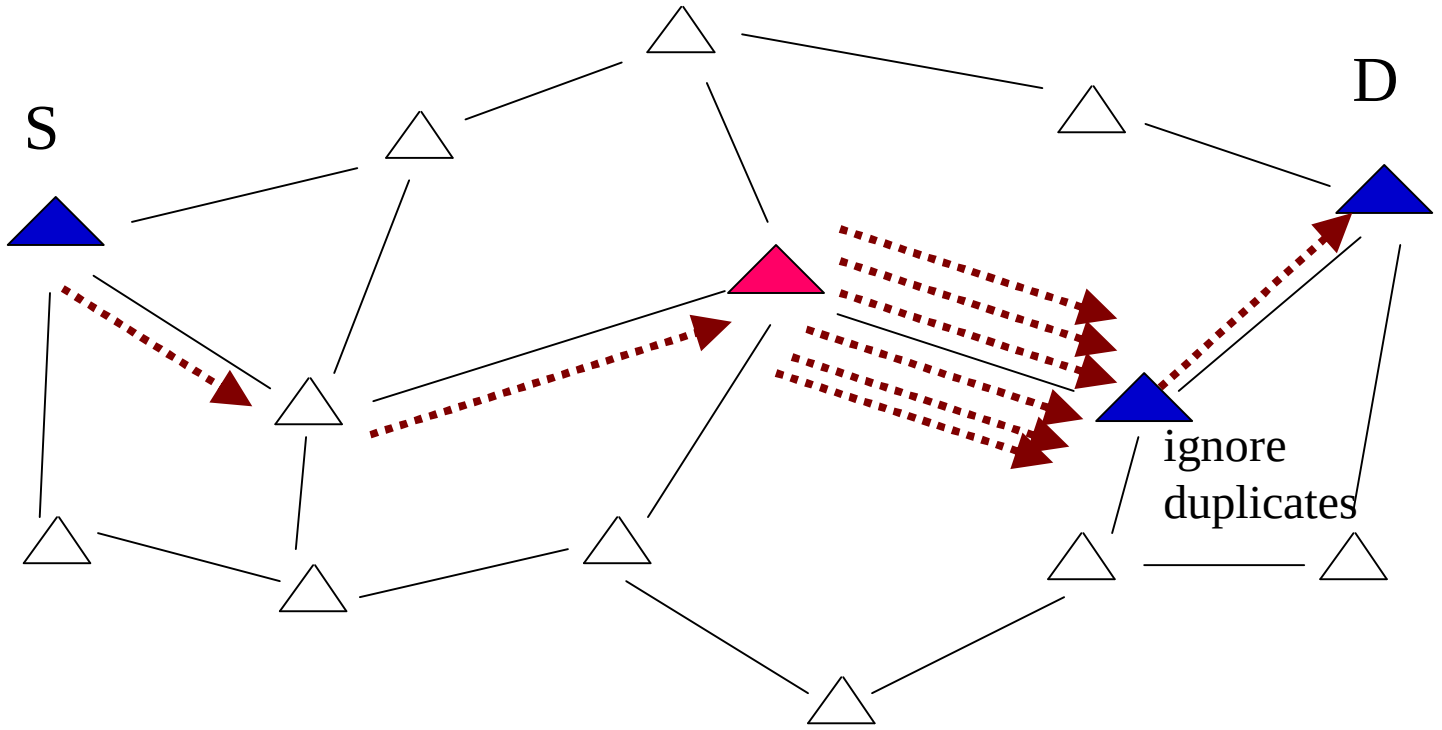


A learns that C is from same group

C->A (message encrypted with A's public key)

Utilizing CAM/PM with PLA and adaptive trust model: Detecting replayed packets

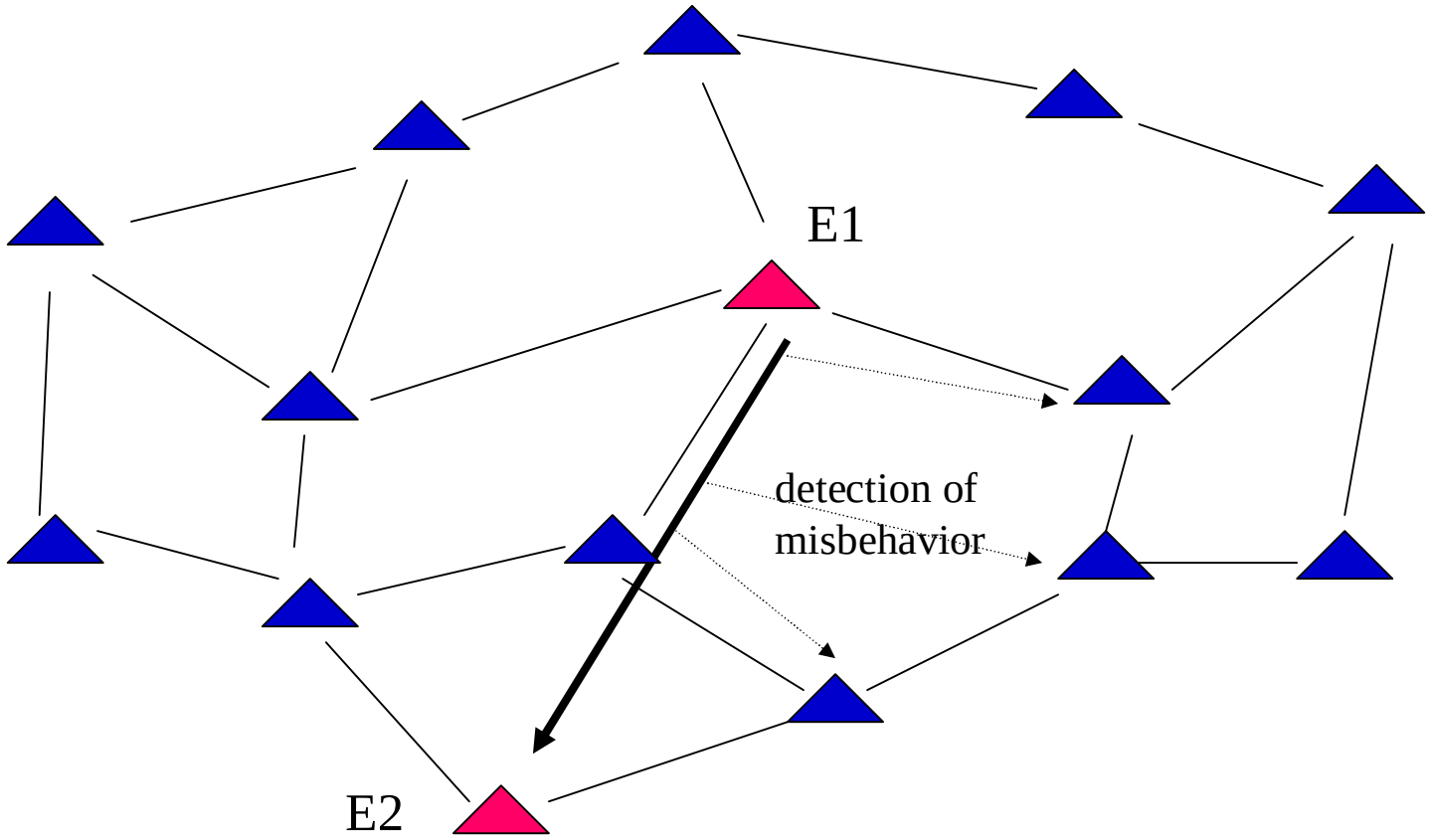
Application: Restricting DoS attack



Utilizing CAM/PM with PLA and adaptive trust model: Detecting malicious behavior and revocating nodes

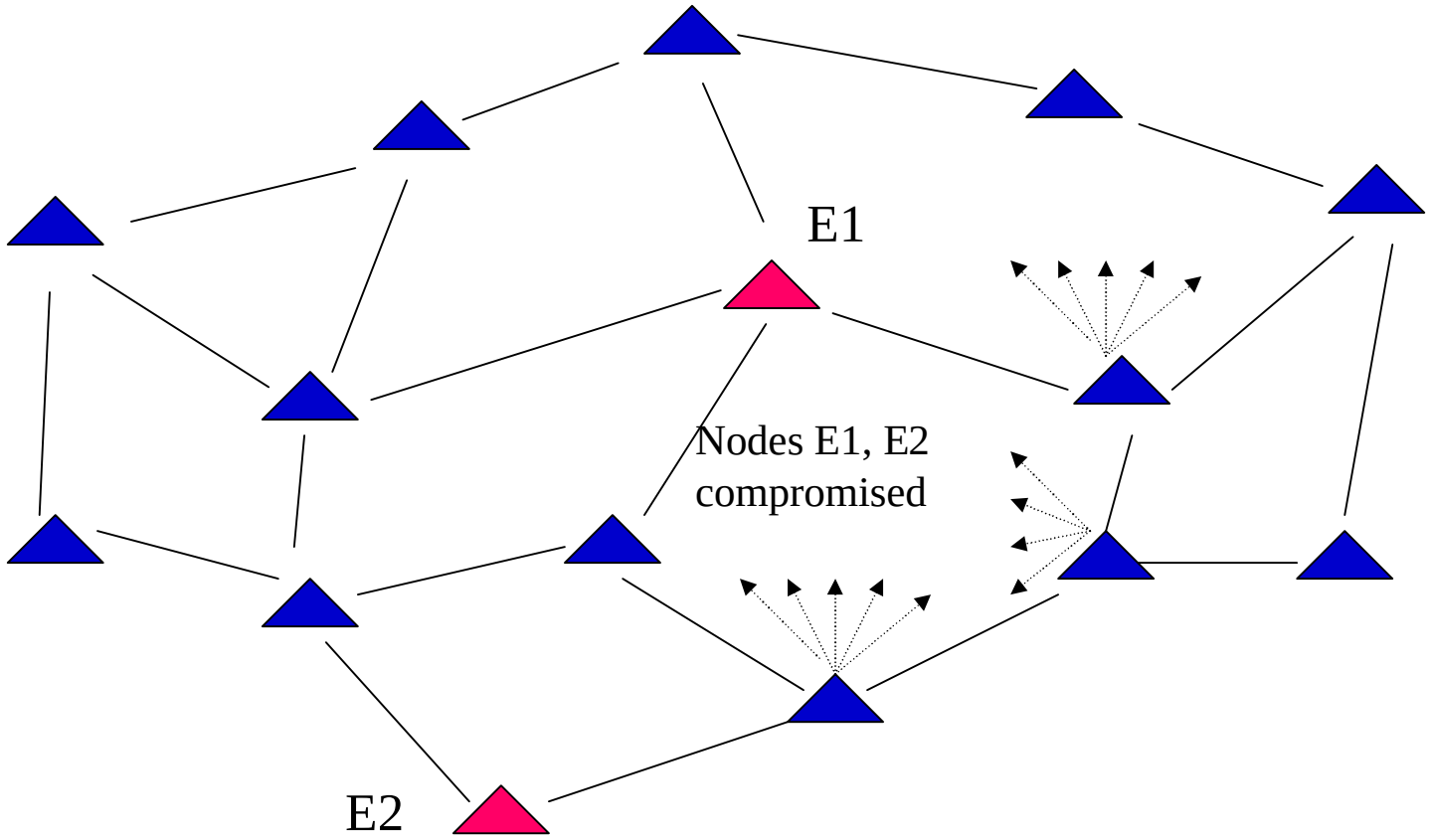
Helsinki University
of Technology

Application: Excluding compromised nodes



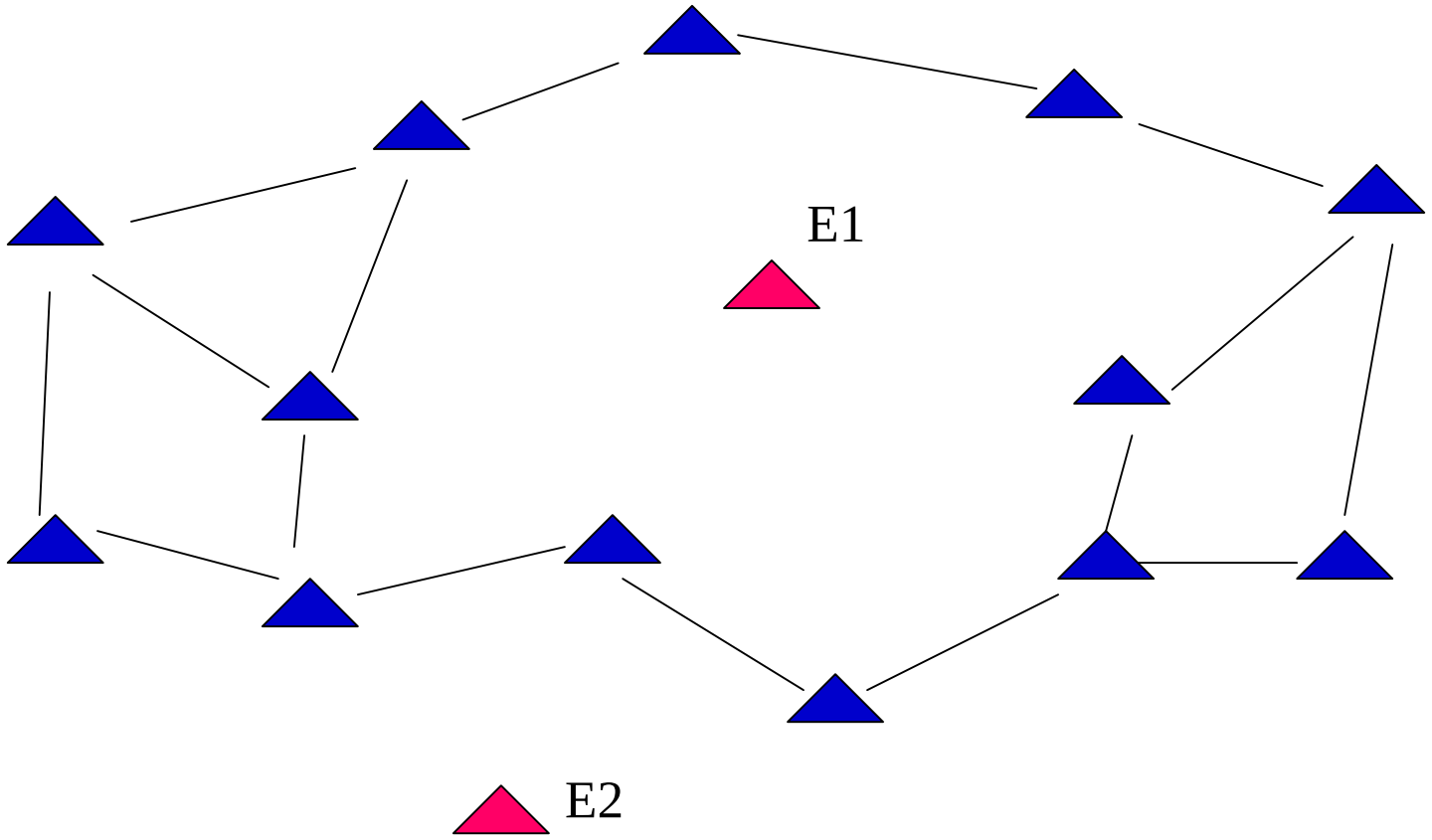
Helsinki University
of Technology

Application: Excluding compromised nodes



Helsinki University
of Technology

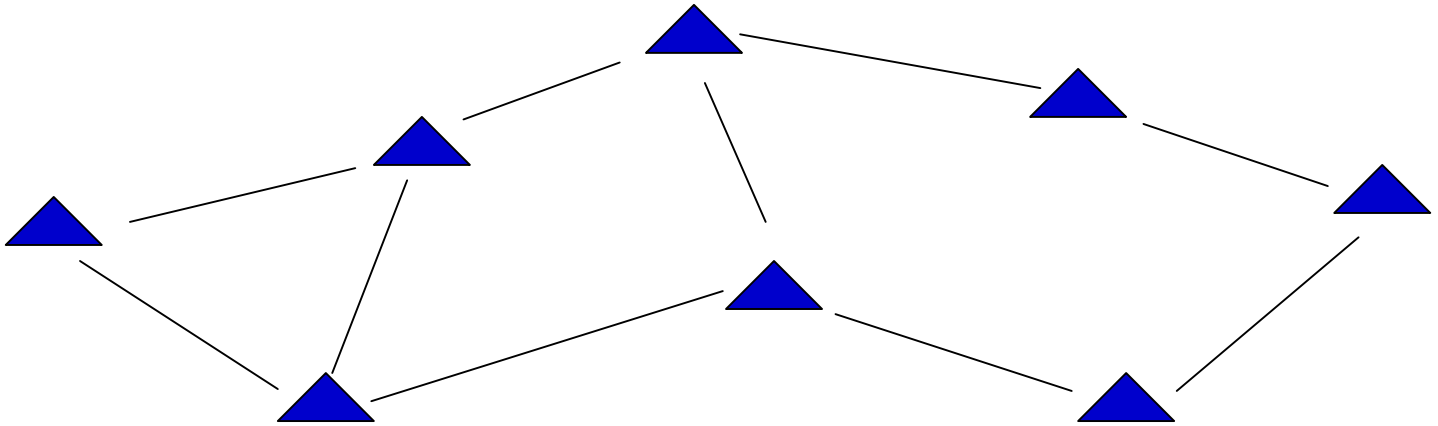
Application: Excluding compromised nodes



Utilizing CAM/PM with PLA and adaptive trust model: Combining two ad hoc network organizations

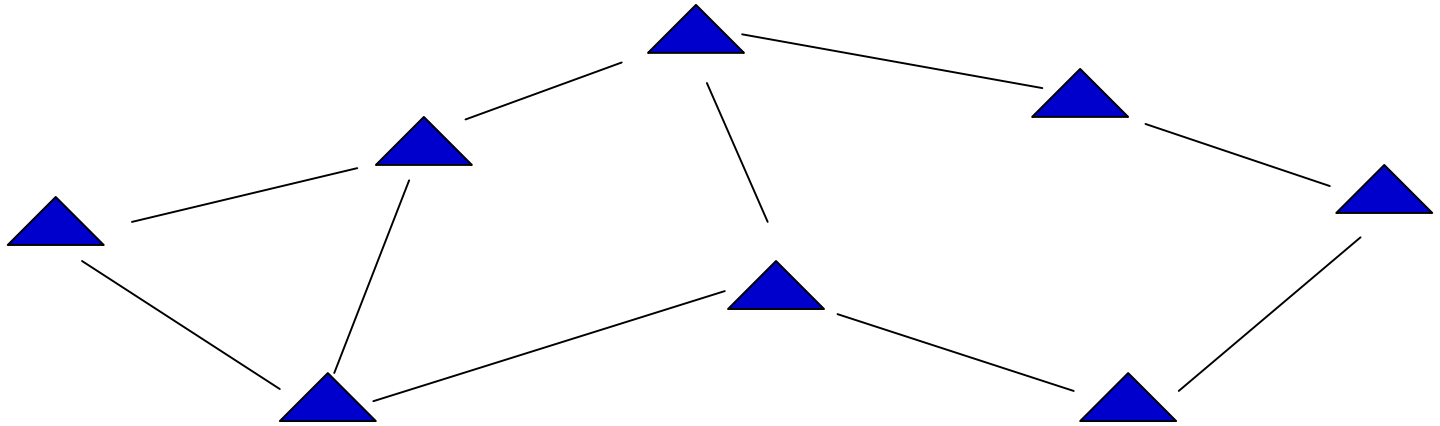
Helsinki University
of Technology

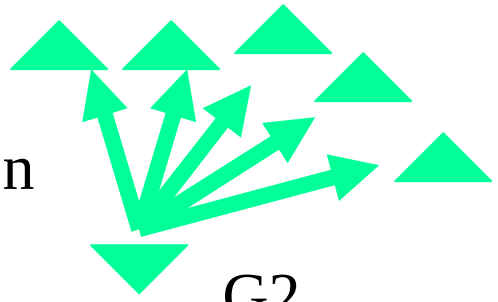
Application: Delegation of command chain



Helsinki University
of Technology

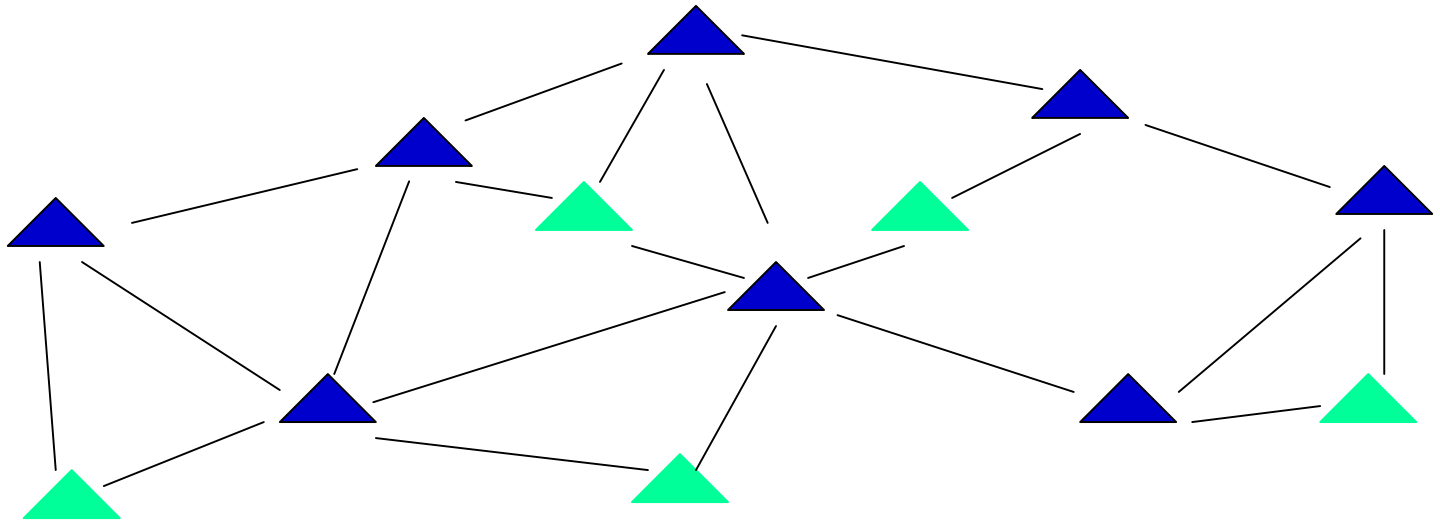
Application: Delegation of command chain





Helsinki University
of Technology

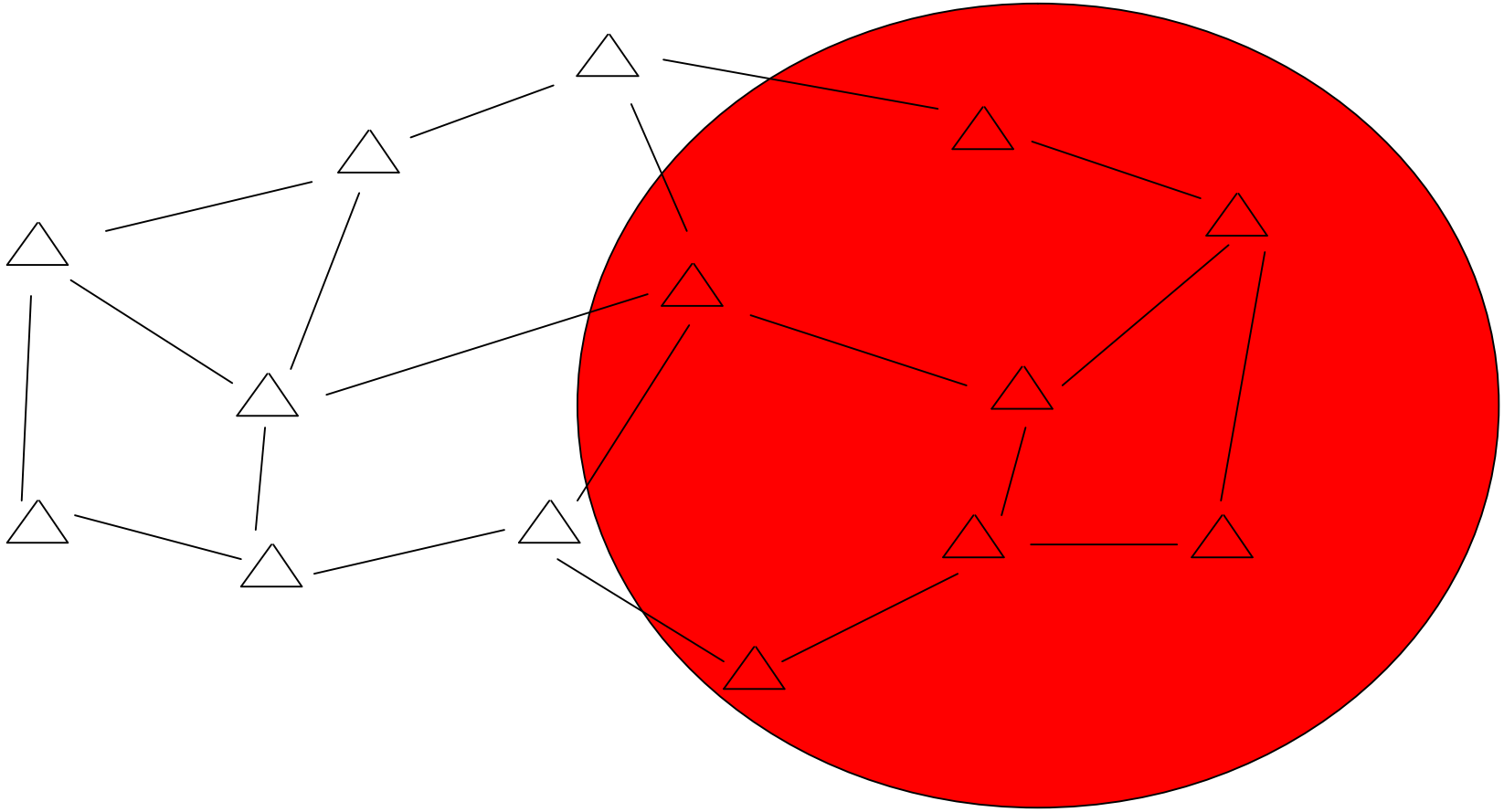
Application: Delegation of command chain



Utilizing CAM/PM with PLA and adaptive trust model: Handling compromized nodes

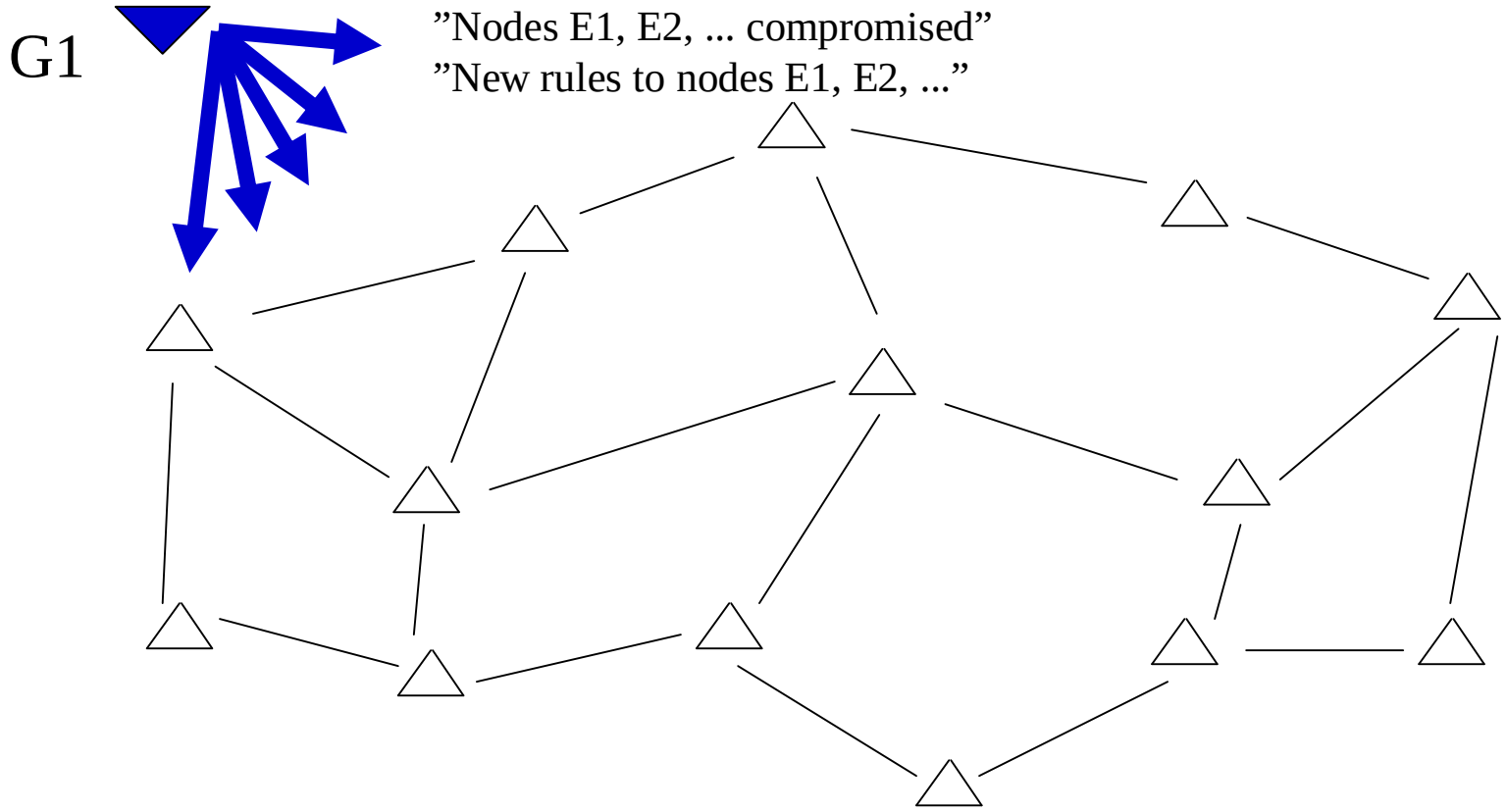
Helsinki University
of Technology

Application: Revocation of large quantity of nodes



Helsinki University
of Technology

Application: Revocation of large quantity of nodes



Helsinki University
of Technology

Application: Revocation of large quantity of nodes