Military grade wireless ad hoc networks

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

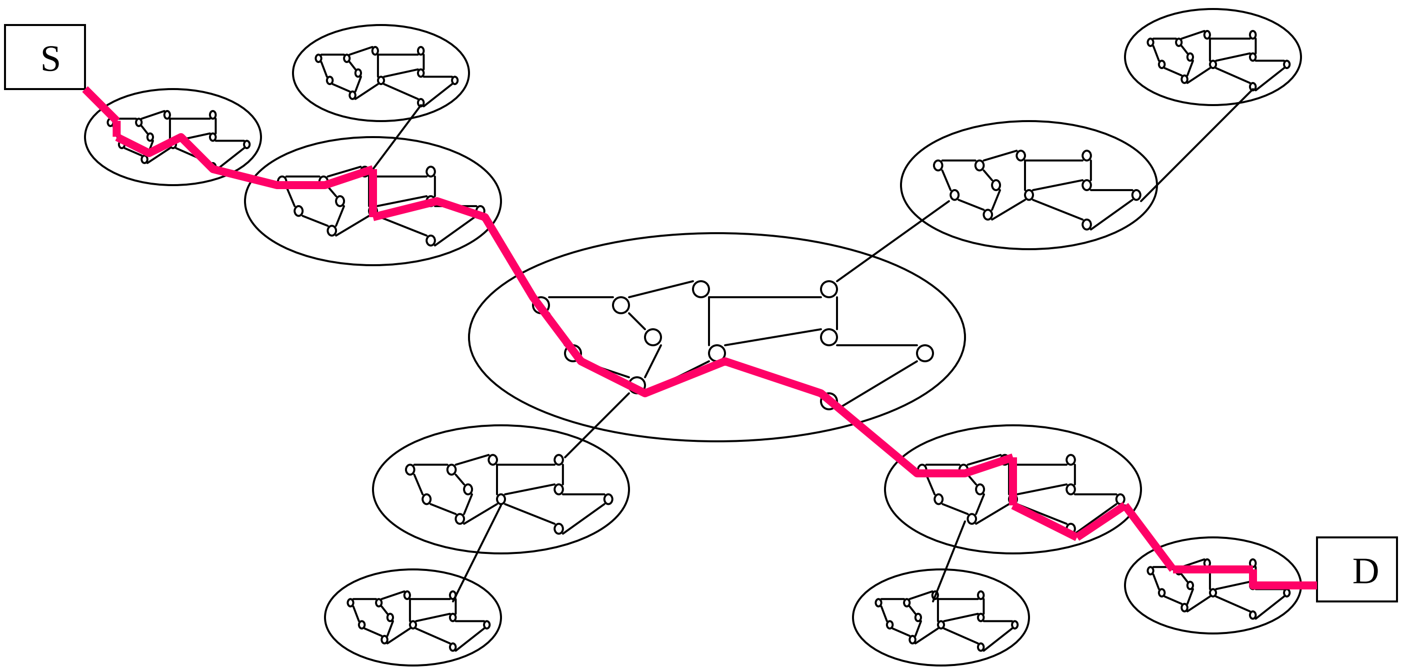
Agenda

- Internet
- Privacy
- Military and civilian networks
- Problem statement
- Requirements
- Security levels
- Current and new solutions
- Context Aware Management/Policy Manager (CAM/PM)
- Packet Level Authentication (PLA)
- Applications
- Performance
- Conclusions

Helsinki University
of Technology

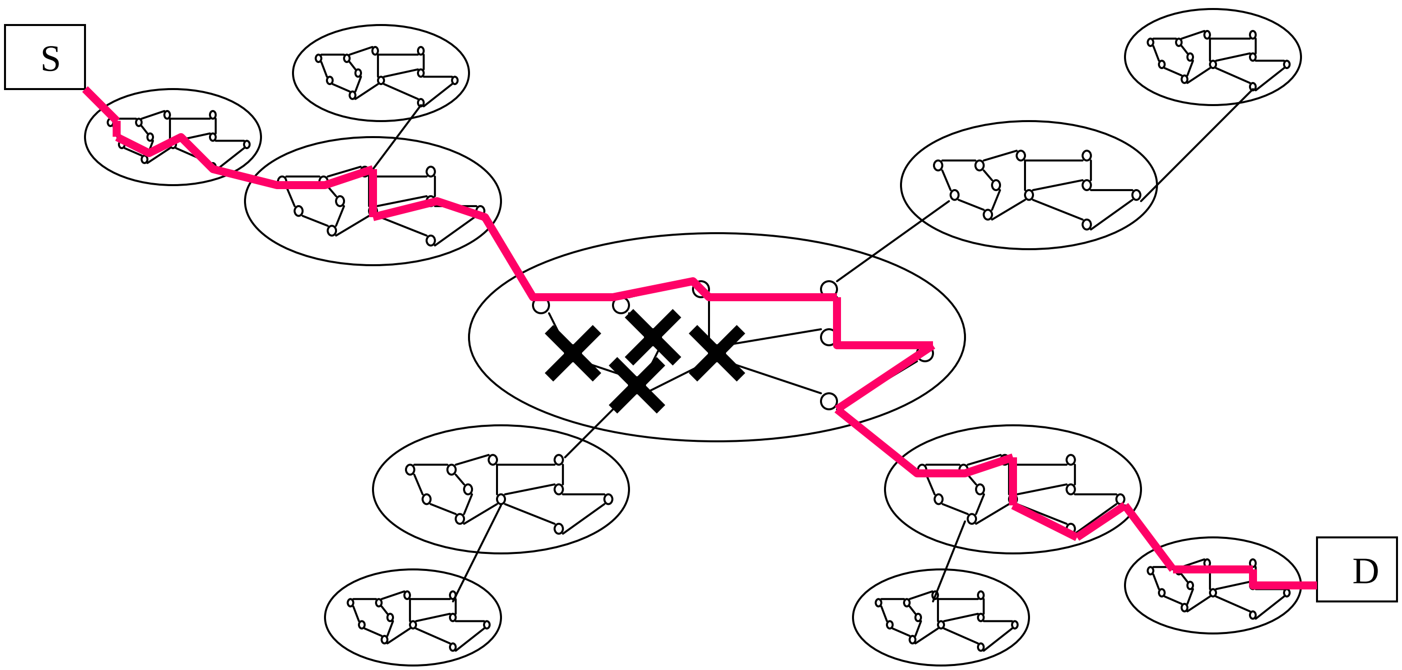
Internet

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



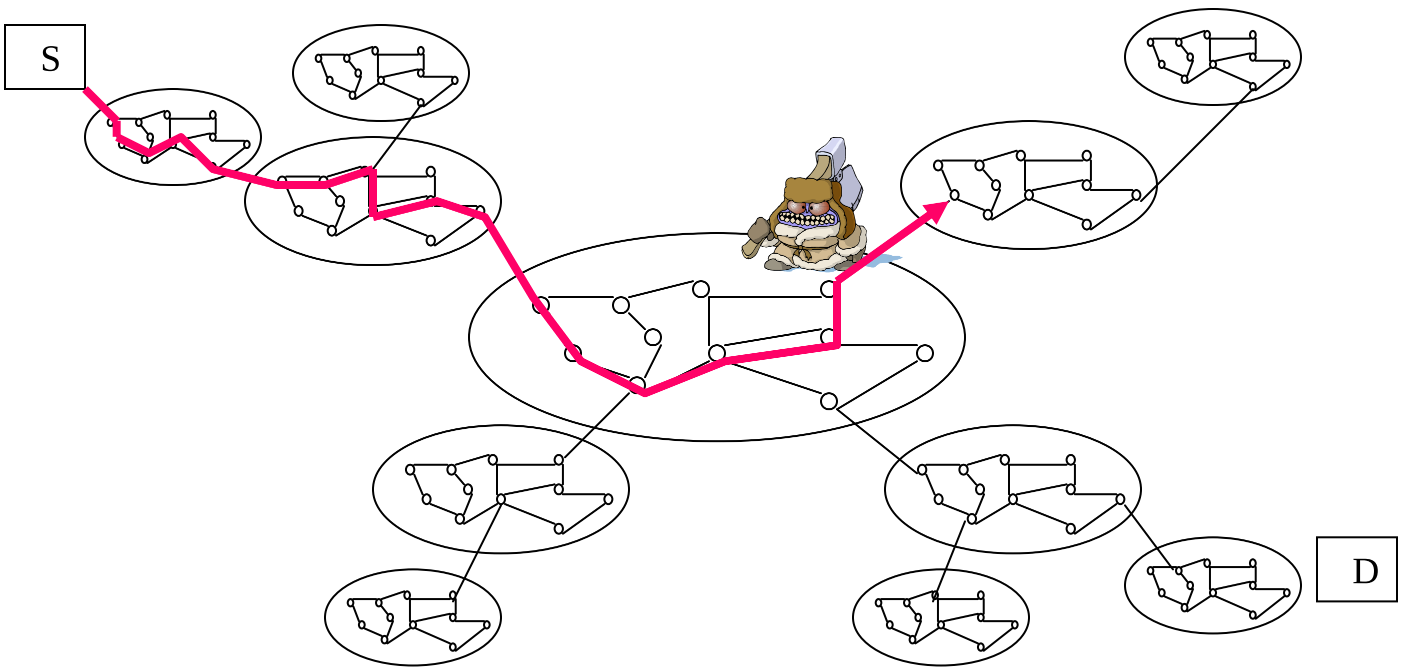
Internet

- **Packets can be rerouted quickly**



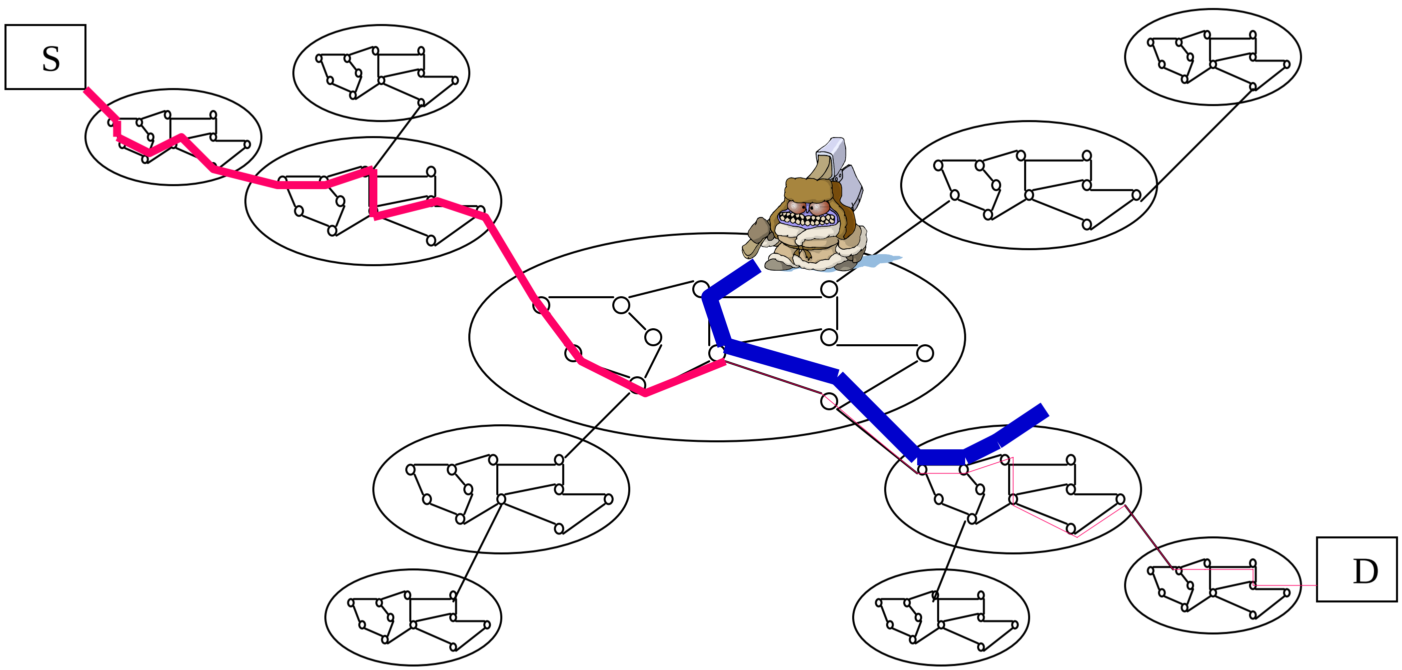
Internet

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



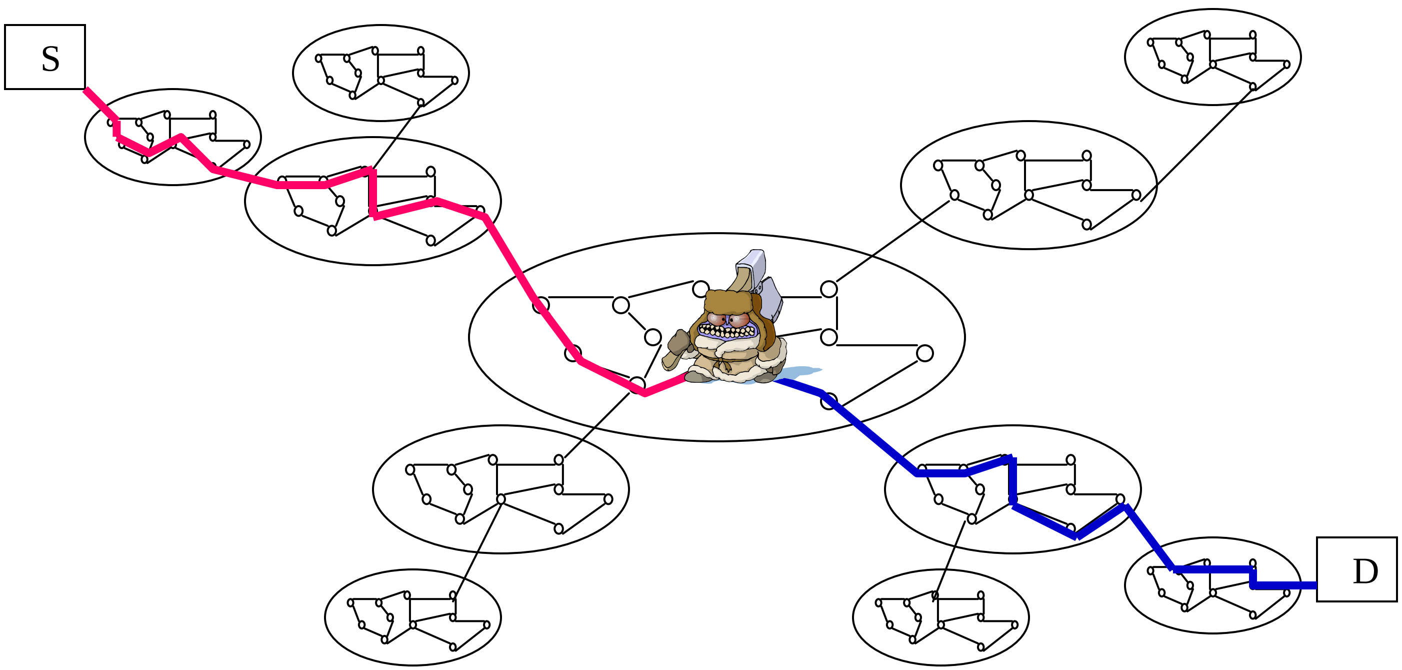
Internet

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



Internet

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



Internet

- **Problems are dramatically getting worse, when**
  - **wireless networks are used instead of wired links**
  - **dynamic network infrastructure is used instead of static**
  - **nodes are mobile**
  - **enemy is hostile**
  - **nodes may get compromised**
  - **strict Quality of Service requirements are needed**
  - **transmission channel has very limited capacity**

Privacy

- **Definition of Privacy**

Privacy is the claim of individuals, groups, and institutions to determine for themselves, when, how, and to what extent information about them is communicated to others.

Alan Westin 1967

5 categories of privacy

- **Data privacy (content)**
- **Identity privacy (source/destination)**
- **Location privacy (place)**
- **Time privacy (when)**
- **Privacy of existence (does it exist)**

Military and civilian networks

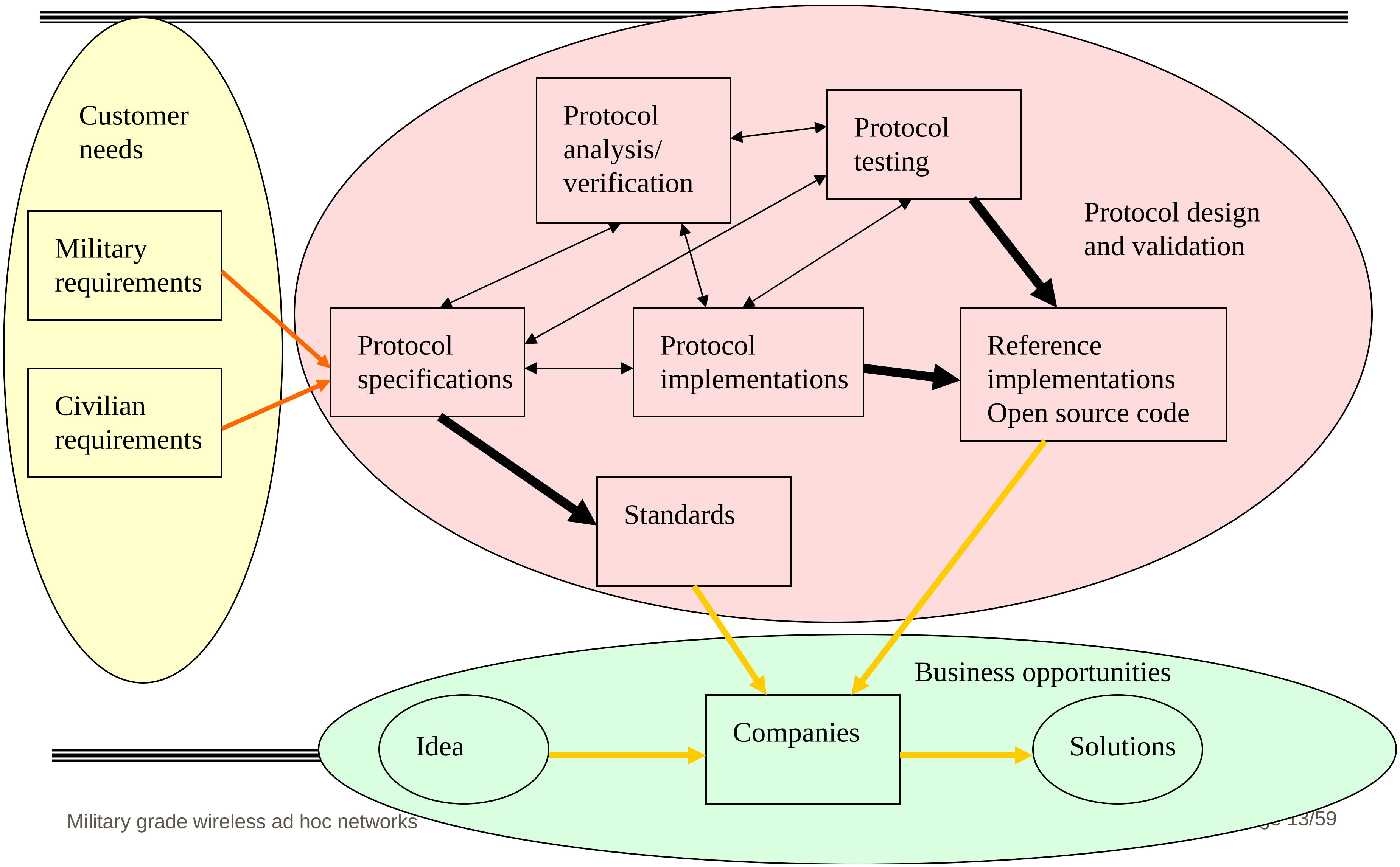
- **Military networks**
  - **Clearly hostile enemy, high casulty rate of nodes**
- **Governmental/resque**
  - **No clear enemy always present**
- **Civilian**
  - **Professional criminals, hackers, industrial espionage**

Problems in military grade wireless ad hoc networks

- **Hostile enemy**
- **Privacy**
- **Routing**
- **Security**
- **Quality of service**
- **Performance**
- **Compromised nodes**
- **Dynamicity**
- **Life time of nodes**
- **Reliability**
- **Costs**
- **Unequality of nodes**

Helsinki University of Technology

Operating model for open source research



Communication

- **Modes of communication**
  - **Human-human**
  - **Human-computer**
  - **Computer-computer**
- **What is communication?**
  - **Exchange/deliver of information**
    - **Fetch information**
    - **Send information**
    - **Send commands**
    - **Delegation of rights**
    - **Friend or Foe?**

Problem statement

- **How to ensure**
  - **the privacy**
    - **of communication**
  - **in military grade**
    - **wireless**
      - **ad hoc networks**

Problem statement

- **How to ensure**
  - **the privacy (data, indentity, location, time, existence)**
    - **of (reliable) communication**
  - **in military grade (hostile enemies, compromised nodes, high casulty rate)**
    - **wireless (eavesdropping, disturbance, unreliable links)**
      - **ad hoc networks (no static infrastructure, mobile nodes, dynamic routing)**

Problem statement

- **When the above problem is solved in this most difficult environment, the solution can be scaled down into other environments**
  - **Fixed networks**
  - **Static networks**
  - **Civilian networks**
  - **...**

Military network requirements

- **Military environment is the most difficult for the mobile communication and mobility management**
  - **Hostile enemy**
  - **Radio power usage restrictions**
    - **battery, reveal location, time, and importance of the node**
  - **Trust models**
    - **Handling of compromised nodes**
  - **Quality of service control**
    - **Not all nodes or packets are equal**
  - **Need for robustness**
    - **Fault resilience, automatic repair after failure, redundant routes**
  - **Need for performance**

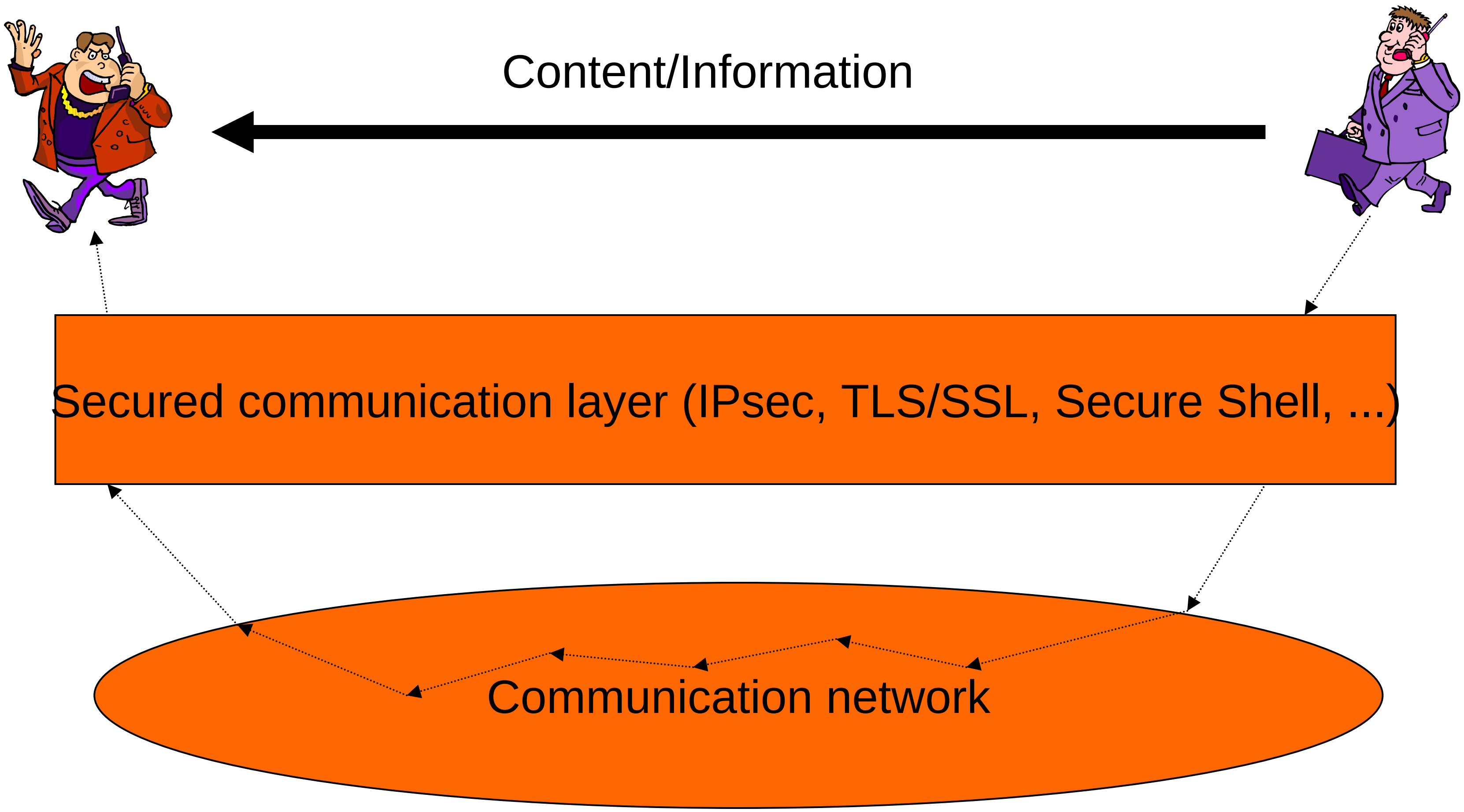
Military network requirements

- **Design goal to handle:**
  - **Two fast moving mobile nodes communicating in a military-grade network using partially ad hoc -formed wireless access networks**
- **Properties**
  - **Ultra frequent mobility (10 times/s), multipath routing**
  - **Mobility management is tightly coupled with security**
  - **QoS provided with security**
  - **Access control coupled with security**
  - **Ad hoc network needs to have security and mobility combined to route data packets**
  - **Ad hoc network provides connection to fixed network**

Civilian networks

- What military networks are missing?
- In governmental and civilian networks we have
  - Cost issue
    - Protocols and equipment may not be too expensive
  - No black/white relation between nodes
    - Not just friend/foe separation
    - Own/allies/neutral/enemy
  - Limited radio spectrum
    - Commercial radio licences
  - No predefined trust between nodes
    - In military trust is easy to establish but difficult to keep
    - In commercial networks trust is difficult to establish but easy to keep

3 levels of security



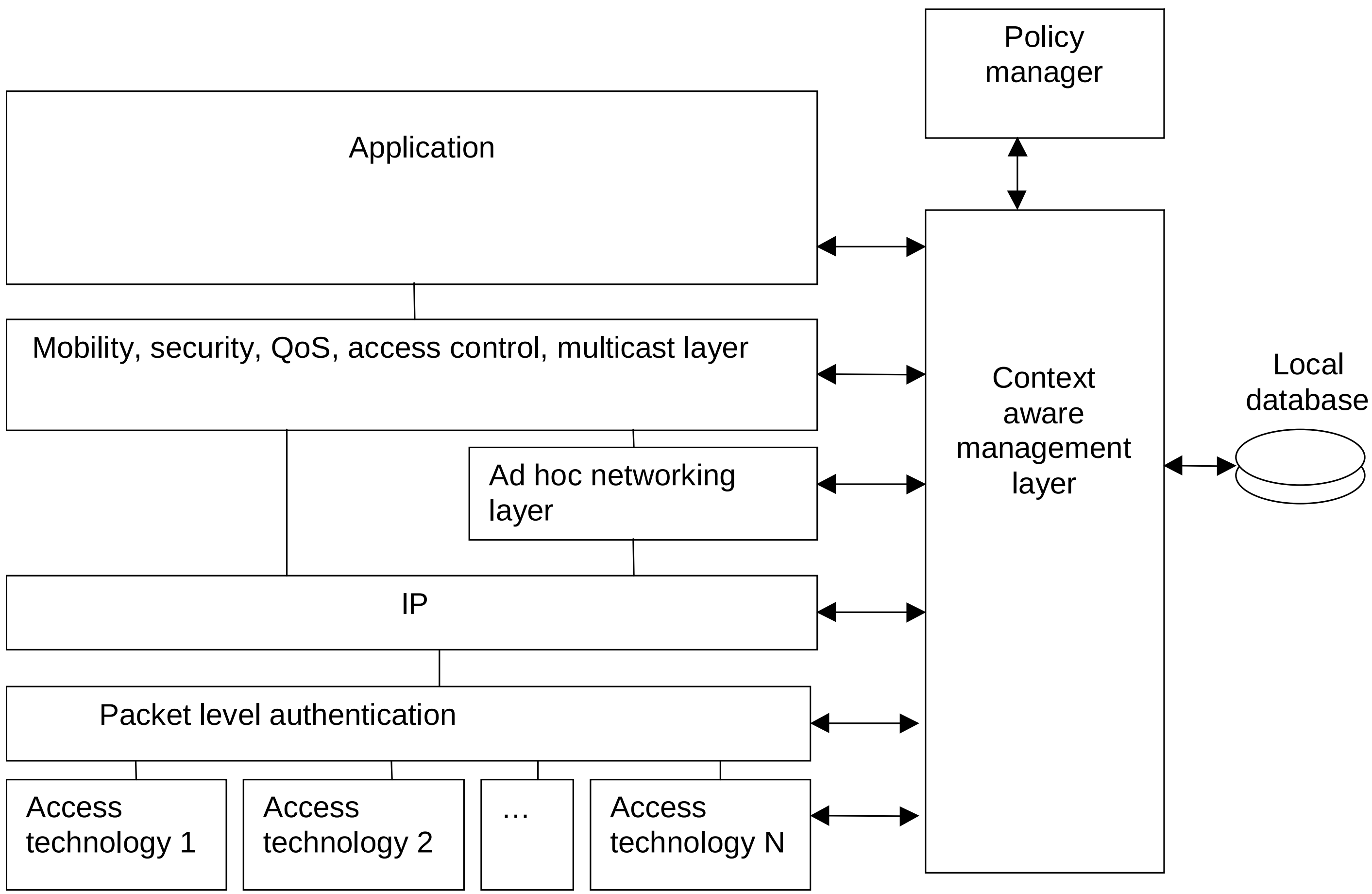
Current solutions

- **Application level security**
  - **PGP, Secure Shell, ...**
- **Network level security**
  - **IPsec**
- **Link level Security**
  - **WEP, A5,...**

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**

Context Aware Management/ Policy Manager



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)**

Trust

- **What is trust?**
  - **Belief that other party acts as agreed**
- **Form of trust**
  - **Trust on**
    - **Indentity**
    - **Information**
    - **Timeliness**
- **Transitivity of trust**
- **Concept of incomplete trust**

Helsinki University
of Technology

Packet level authentication

- **Analogy:**
- **Security measures on notes**
  - **Holograms**
  - **Microprint**
  - **Watermarks**
  - **UV-light**
  - **...**
- **Receiver of notes can verify the authenticity of each note without consultation with banks or other authorities**

Packet level authentication

- How about IP world?
- Each IP packet should have similar security measures
    - Receiver of a packet must be capable of verifying the authenticity of the IP packet without prior security association with the sender
        - 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

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**

Packet level authentication

- **Why not IPsec?**
  - **Benefits of IPsec**
    - **Fast cryptoalgorithms 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**

Packet level authentication

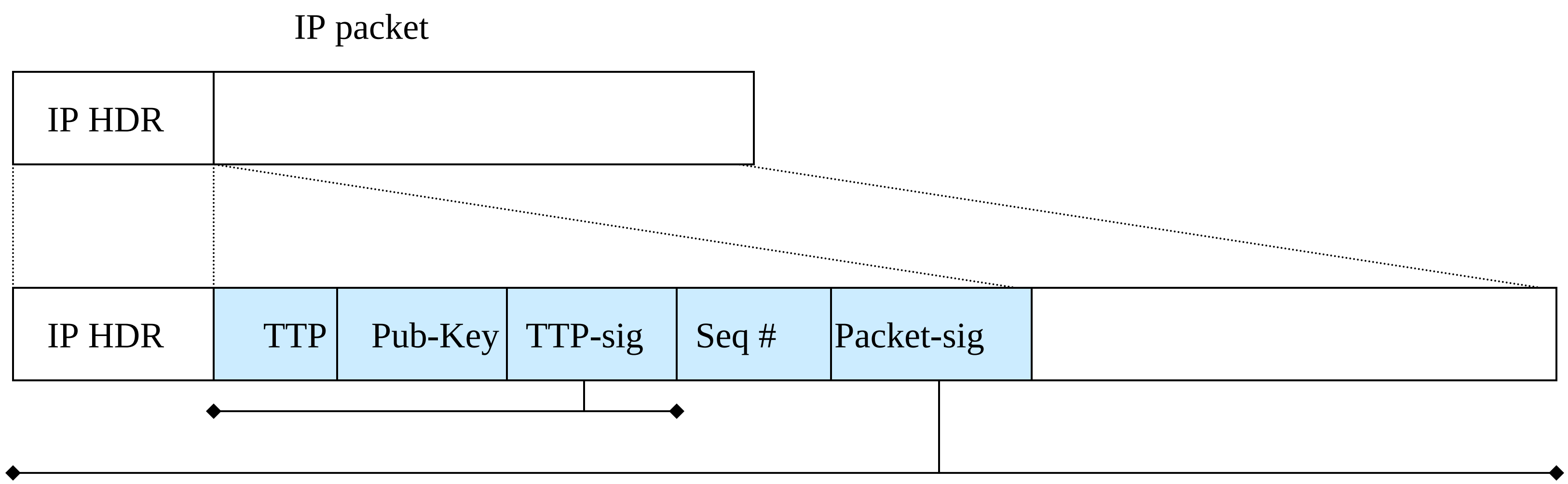
- **Basic operating principles**
  - **Sender digitally signs every packet**
  - **Extra header contains enough information for the receiver to check the packet authenticity**
    - **Header is handled the same way as MobileIP -header**
  - **A chain of trust can be used**
  - **Authenticity of every packet must be verified before using it**
  - **Impacts of hostile nodes shall be minimized, especially in the radio network**
  - **Decisions can be based on the trust level of the information and/or sending node**

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



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
  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

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 (+sequnce number)**
     - **Update per packet**
  5. **Signature of the sender of this packet**
     - **Caclulate per packet**

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**

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**

Packet level authentication: Implementation

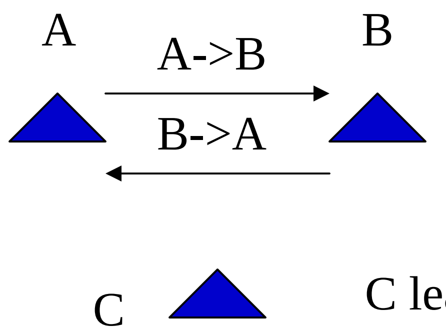
- **Routers in the network**
  - **To authenticate a packet, we need a trust on the authority that has authorized the sender**
    - **directly (same authority as ours)**
    - **indirectly (a chain of trust)**
  - **Routers may operate memoryless**
    - **no need for cache memory**
    - **needs more computing power**
    - **saves memory**
    - **possibility to optimize**

Applications for PLA

- Securing wireless ad hoc networks
- Restricting DoS and DDoS attacks
- Reestablishing core network after military strike
- Handling compromised nodes
- Delegation of command chain
- ...
- Handling access control
- Replacing firewalls
- Handle charging/accounting

Application: Quick secured communication in battle field

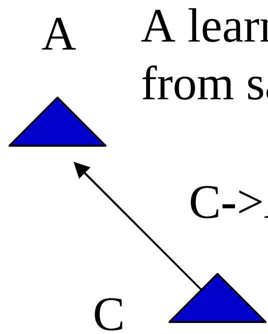
Any communication



C learns that both A and B are from same group

First message from C to A

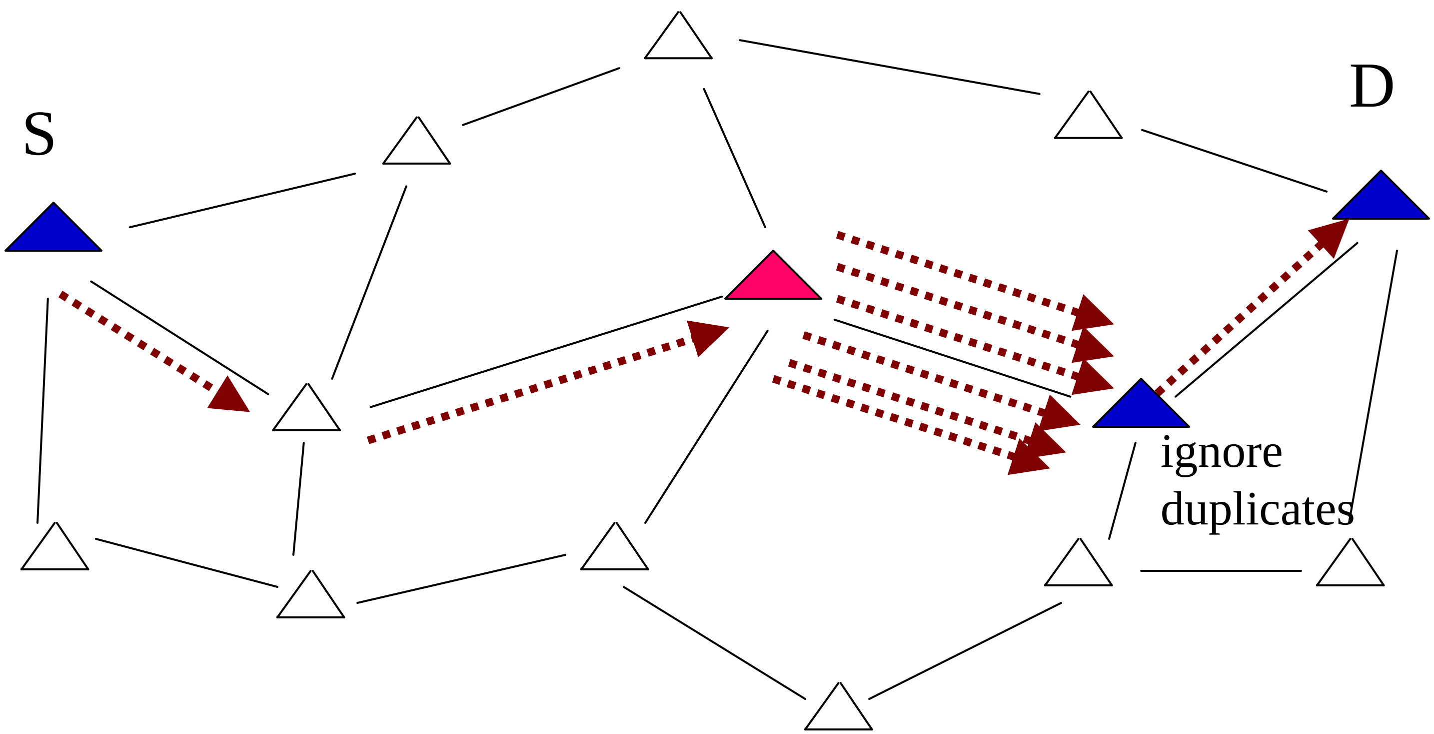
A learns that C is from same group



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

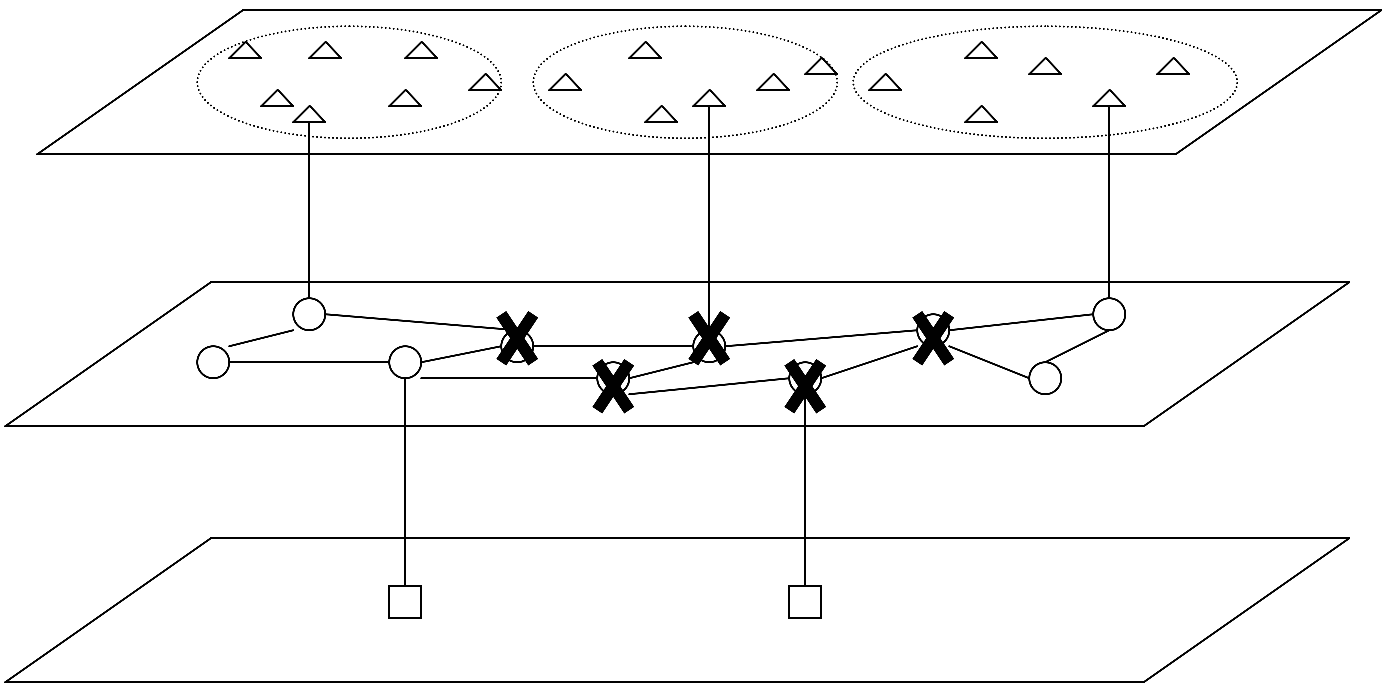
Helsinki University
of Technology

Application: Restricting DoS attack



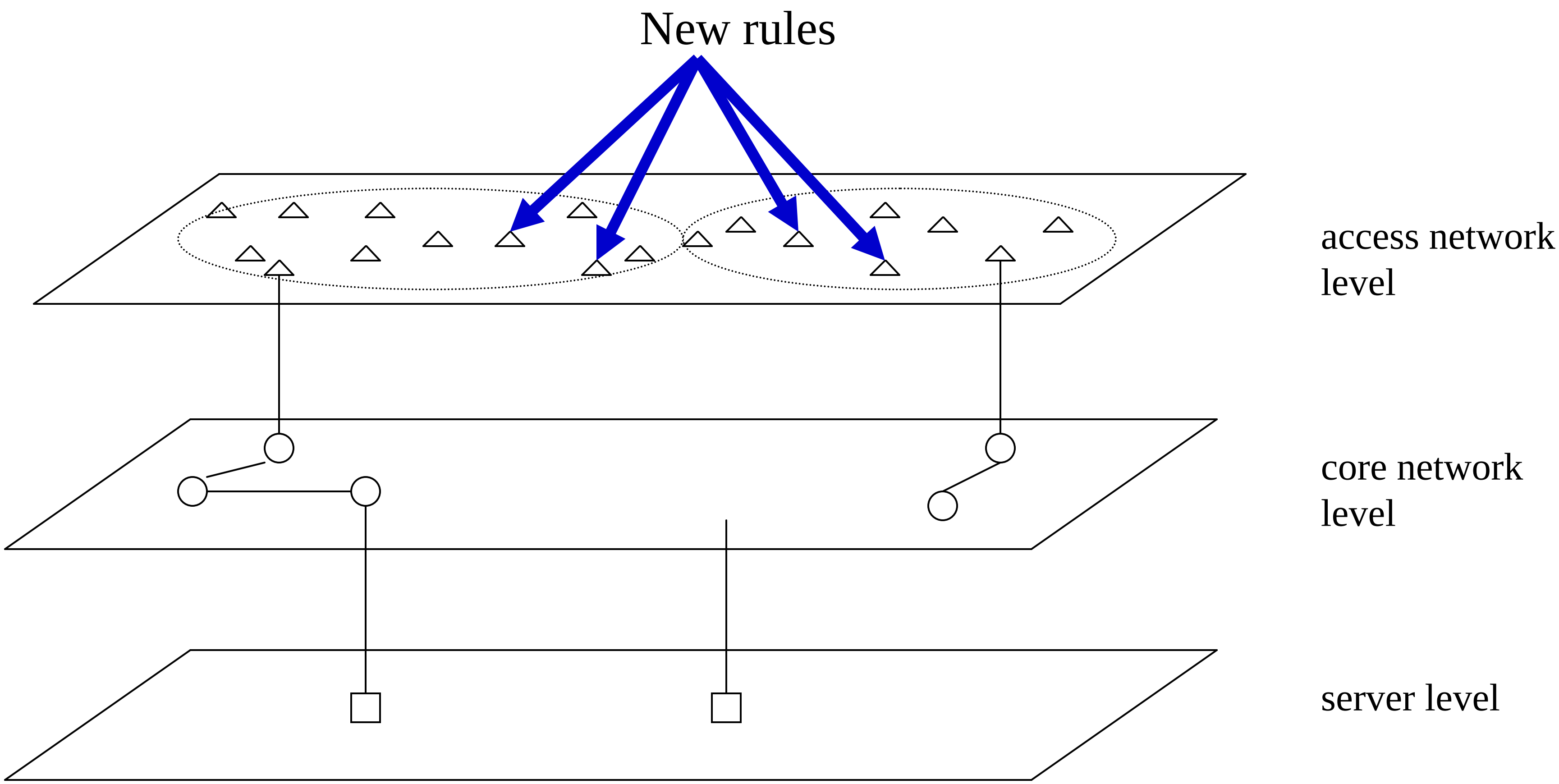
Helsinki University
of Technology

Application: New core network: Military strike



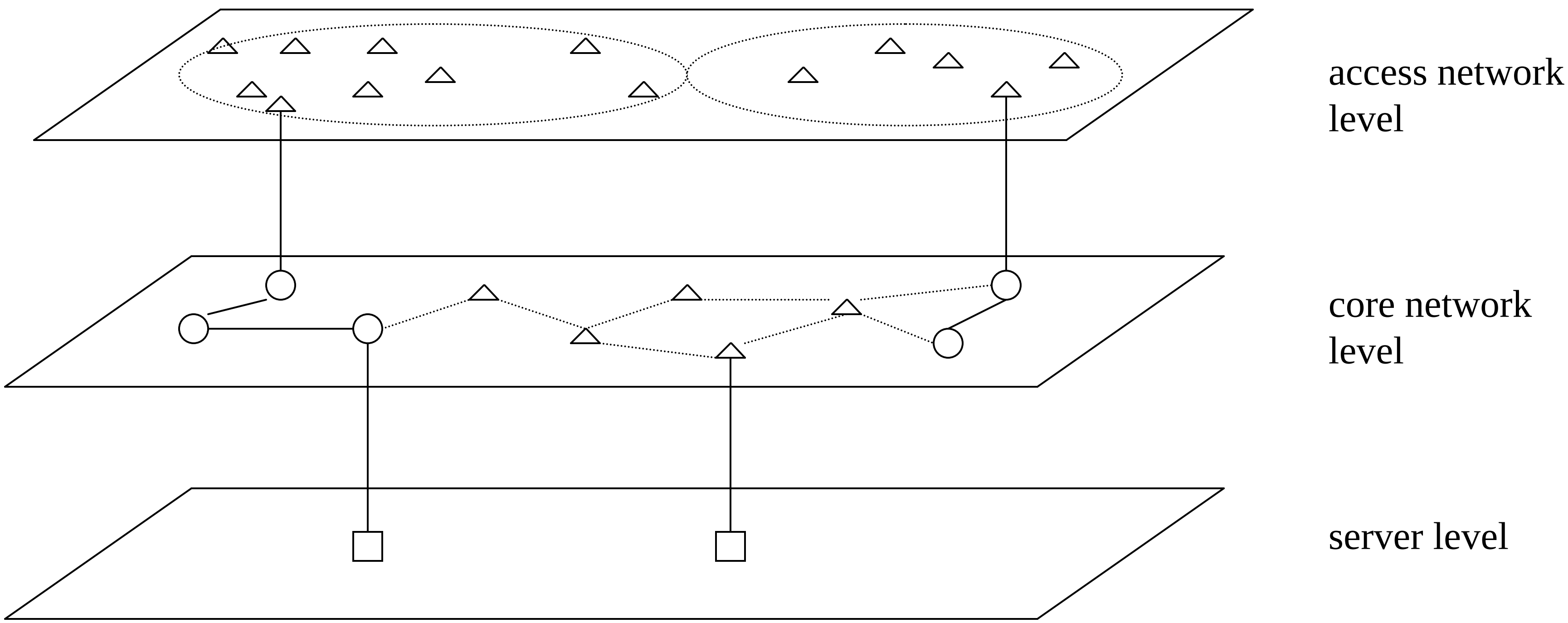
Helsinki University
of Technology

Application: New core network: Reconfiguration

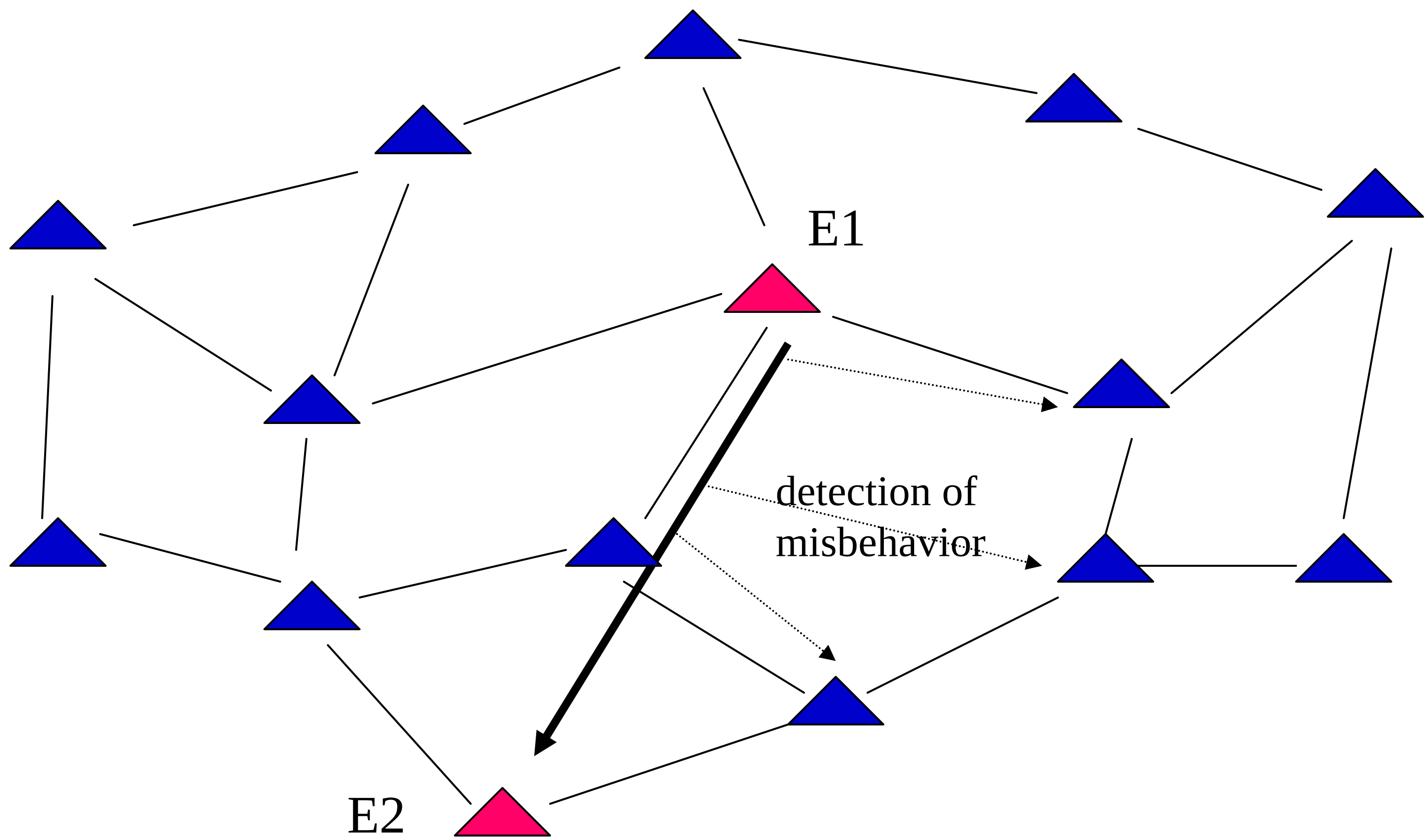


Helsinki University
of Technology

Application: New core network: After military strike

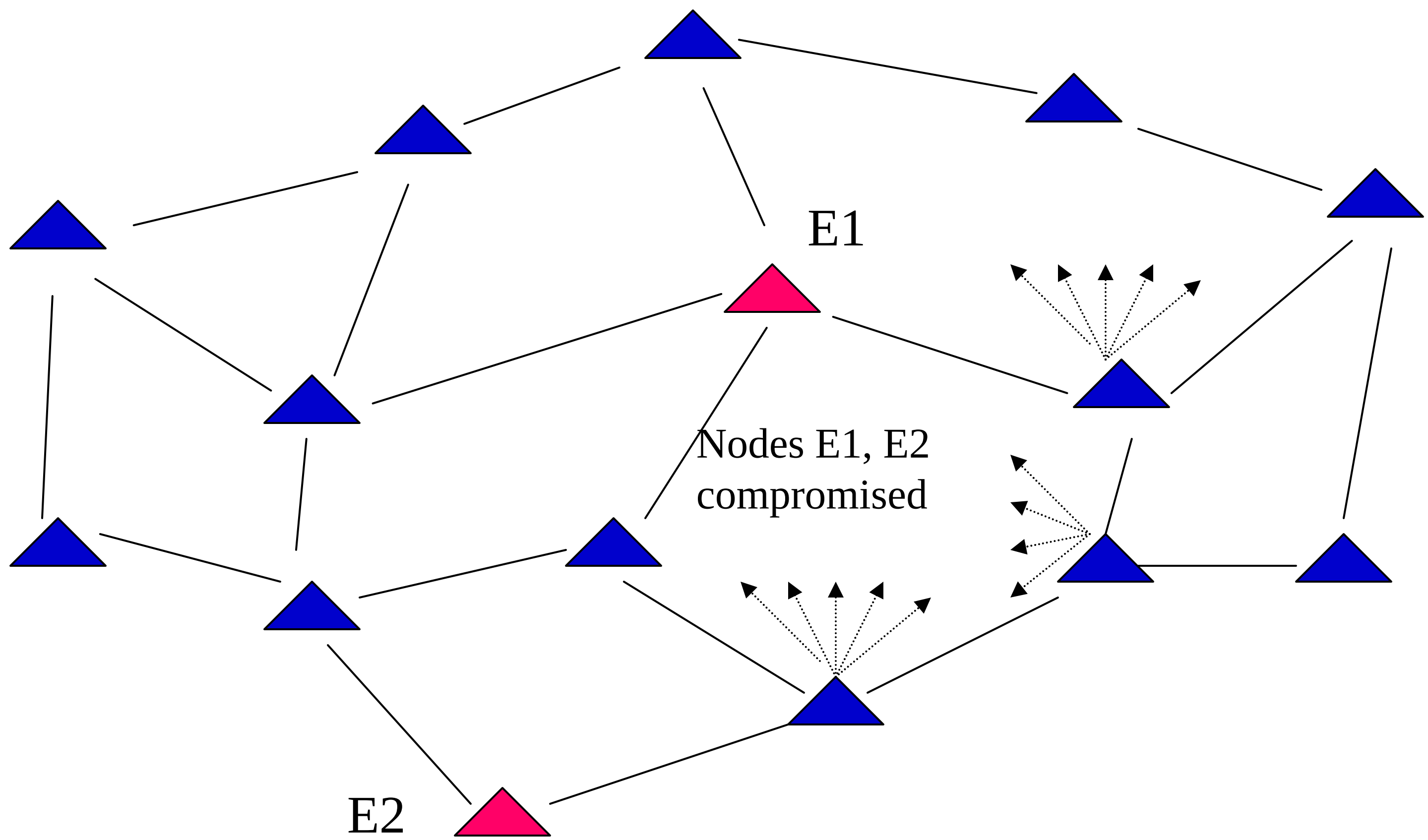


Application: Excluding compromised nodes



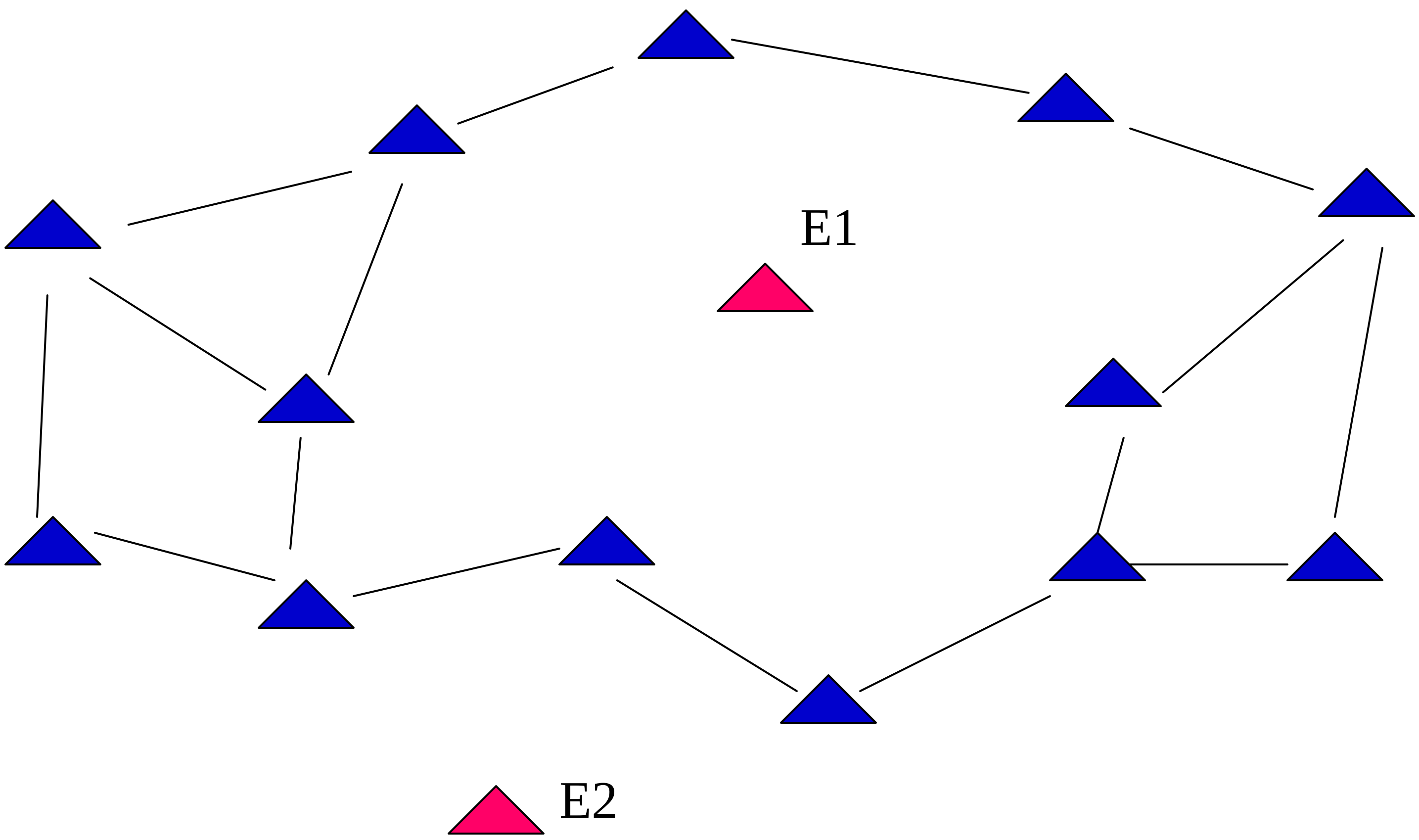
Helsinki University
of Technology

Application: Excluding compromised nodes



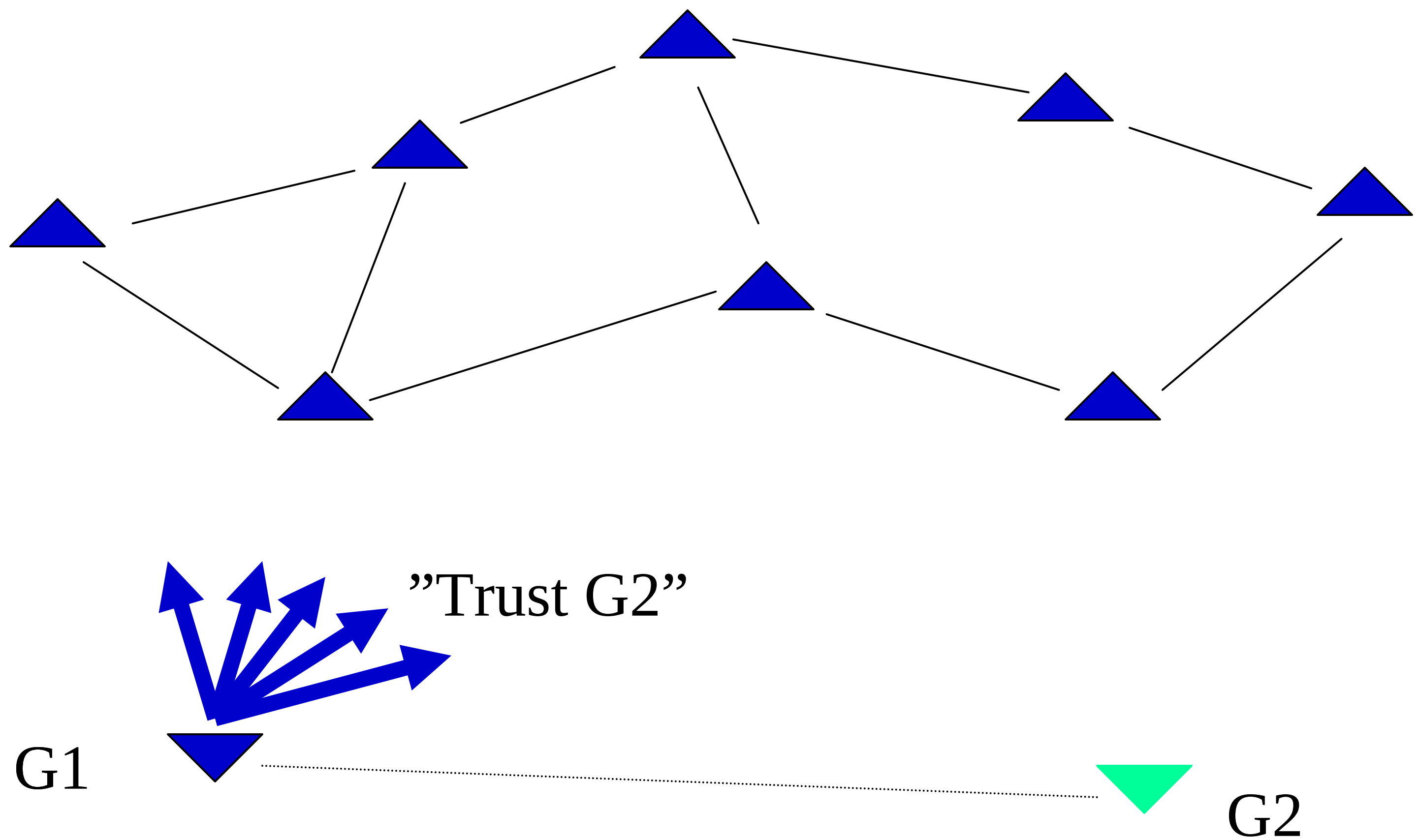
Helsinki University
of Technology

Application: Excluding compromised nodes



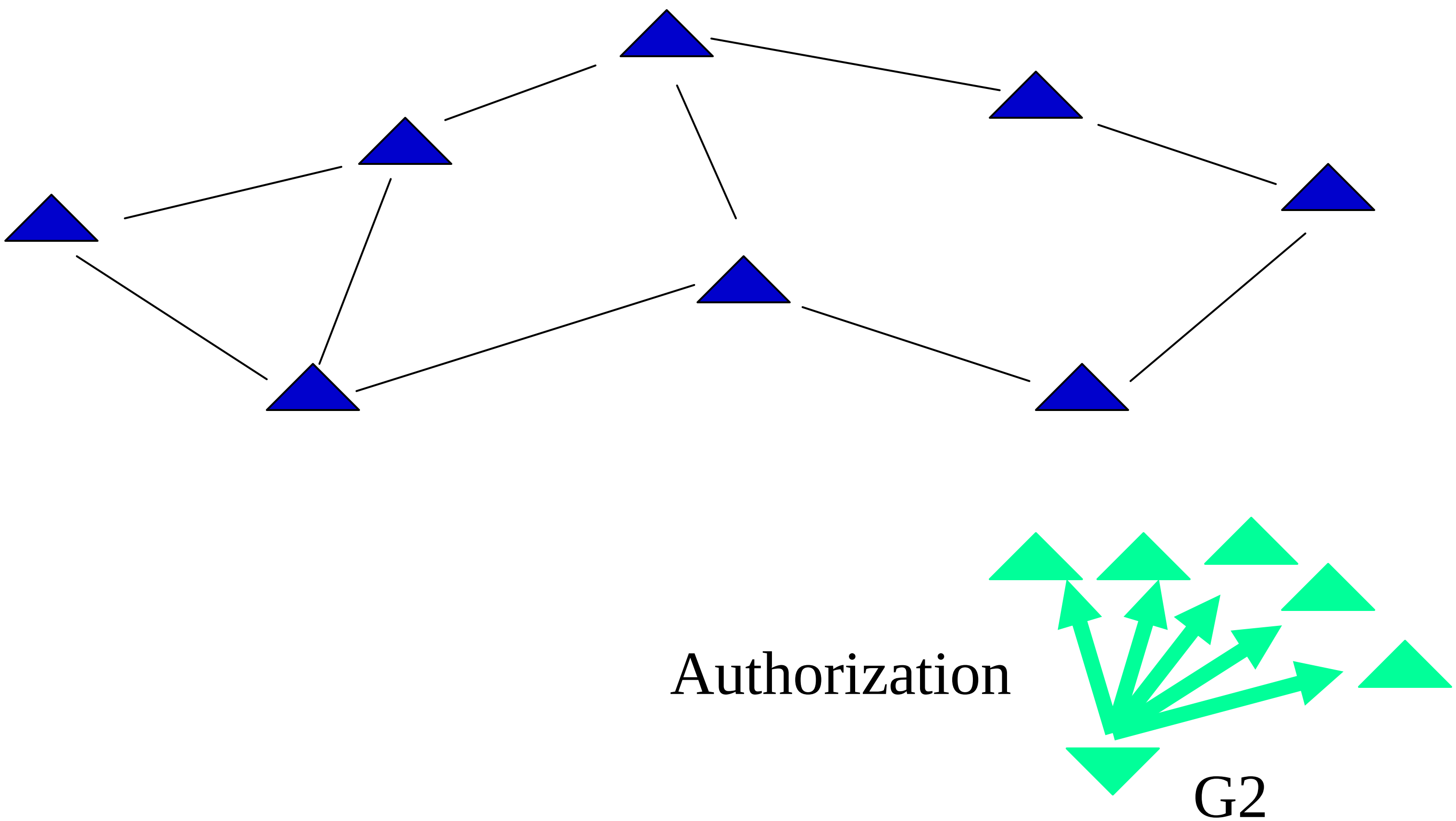
Helsinki University
of Technology

Application: Delegation of command chain



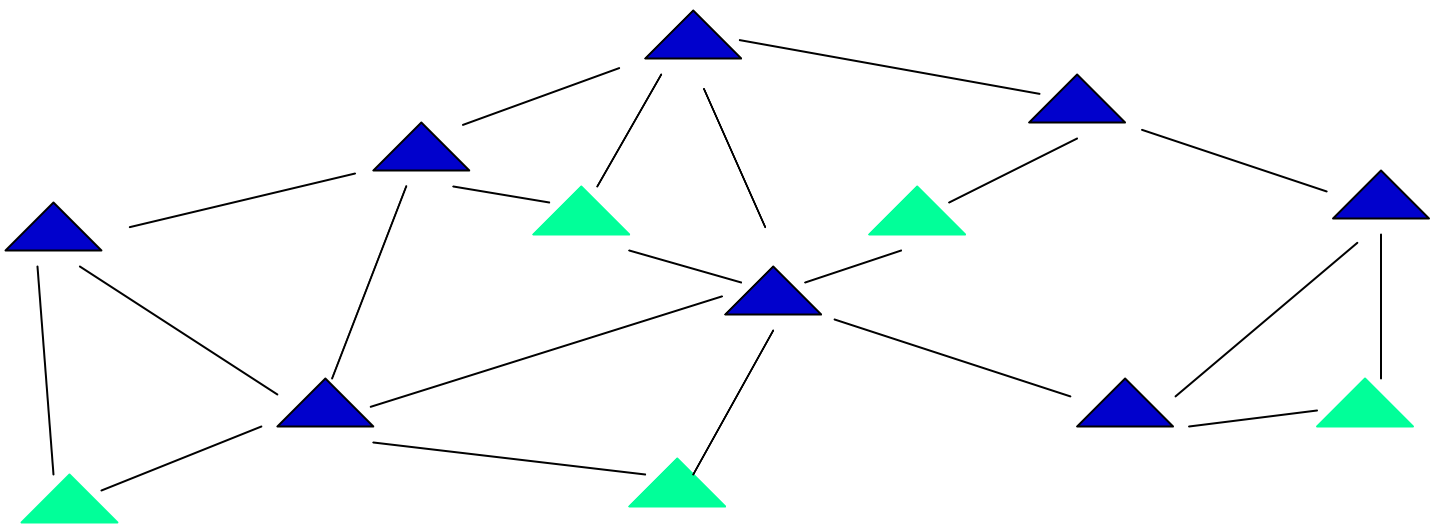
Helsinki University of Technology

Application: Delegation of command chain



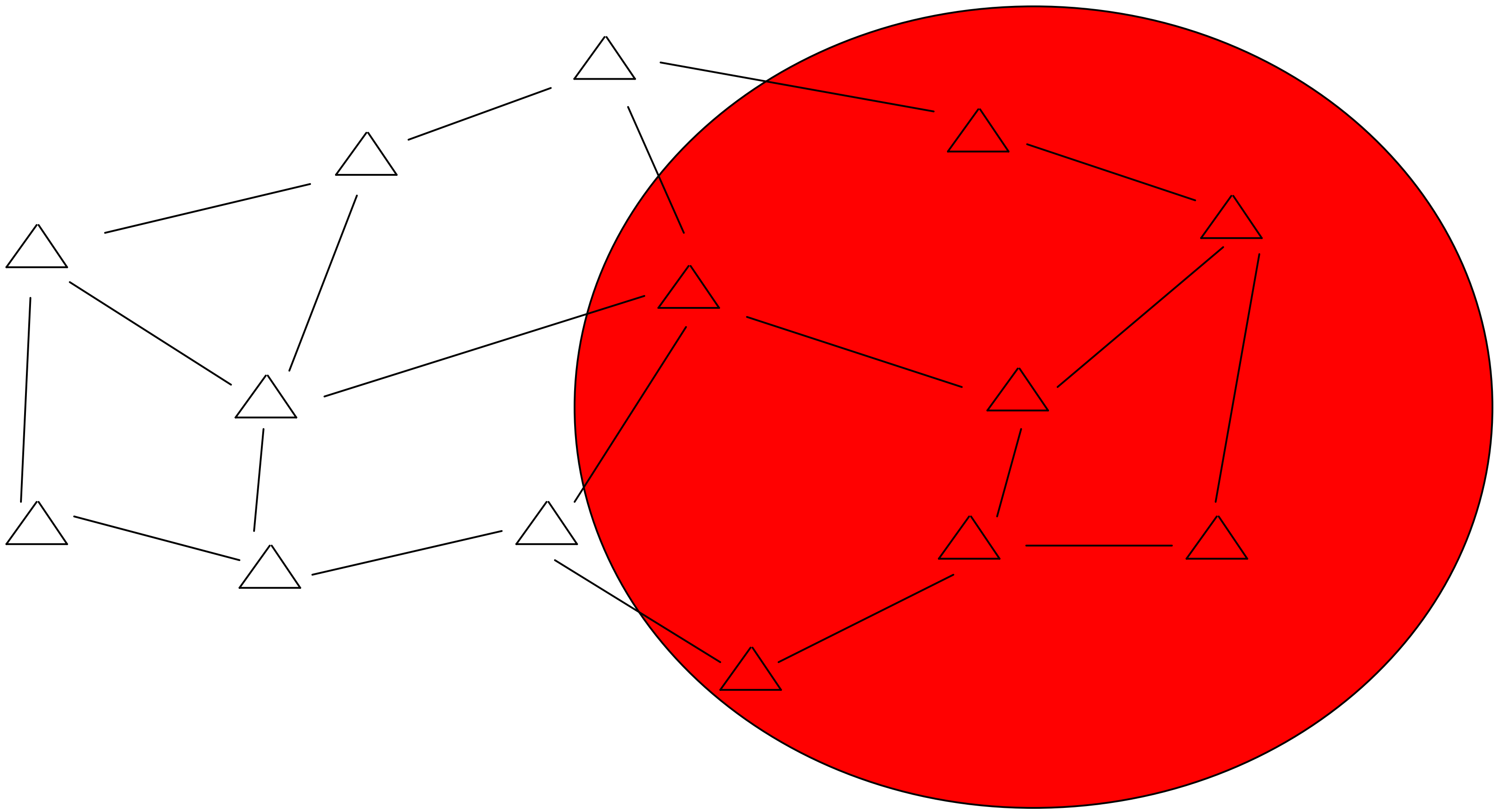
Helsinki University
of Technology

Application: Delegation of command chain



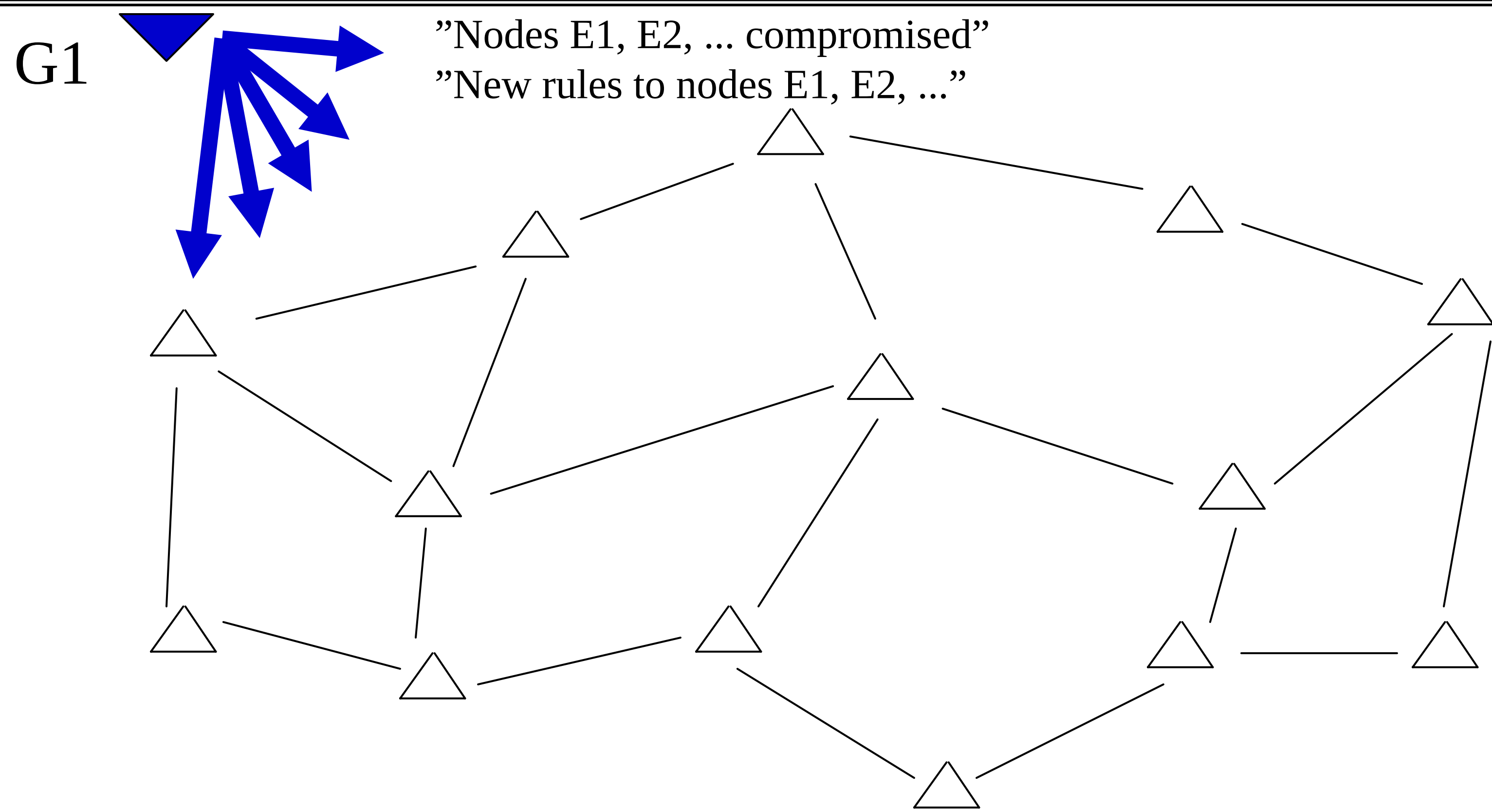
Helsinki University of Technology

Application: Revocation of large quantity of nodes



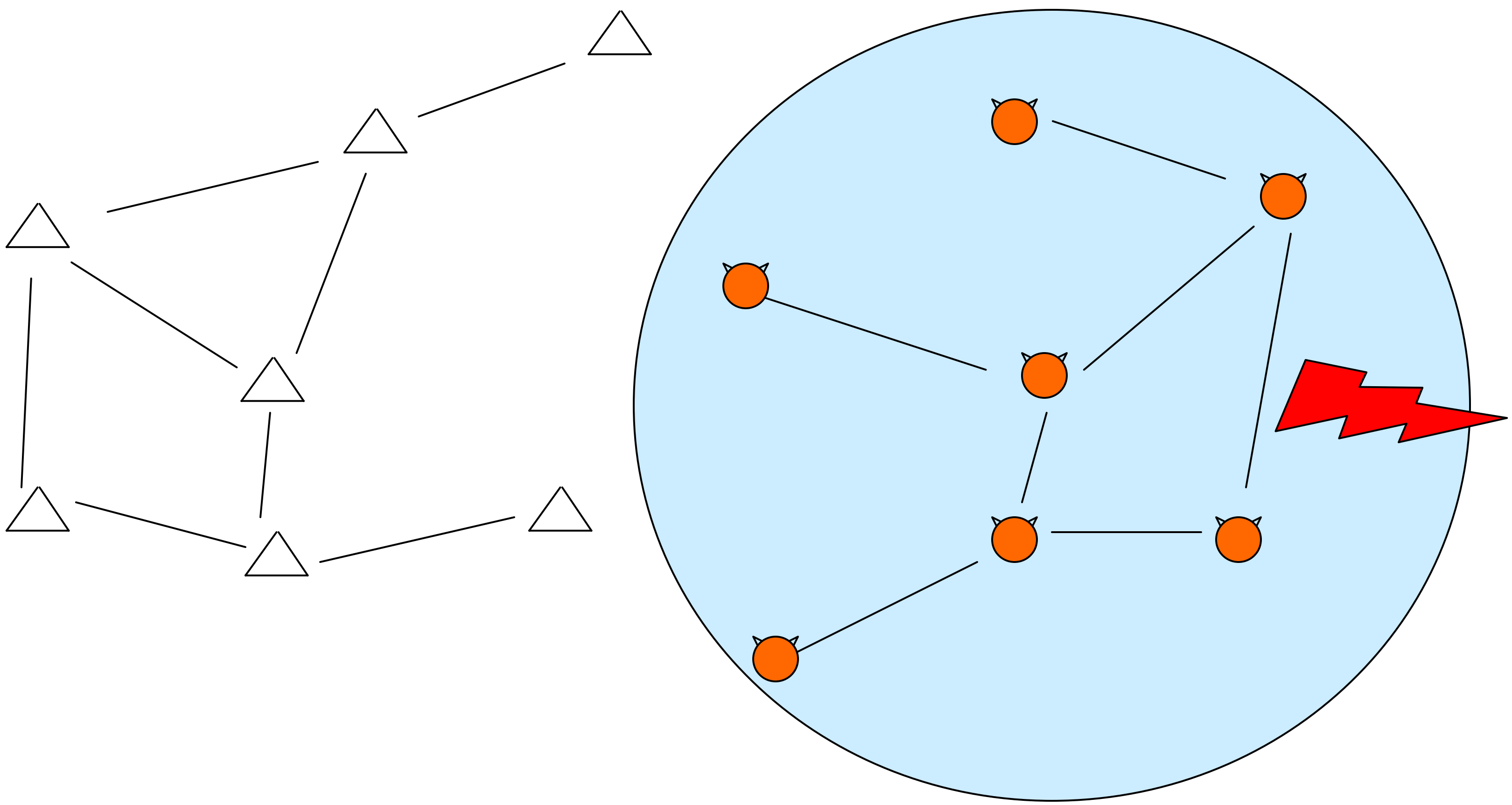
Helsinki University of Technology

Application: Revocation of large quantity of nodes



Helsinki University
of Technology

Application: Revocation of large quantity of nodes



Performance

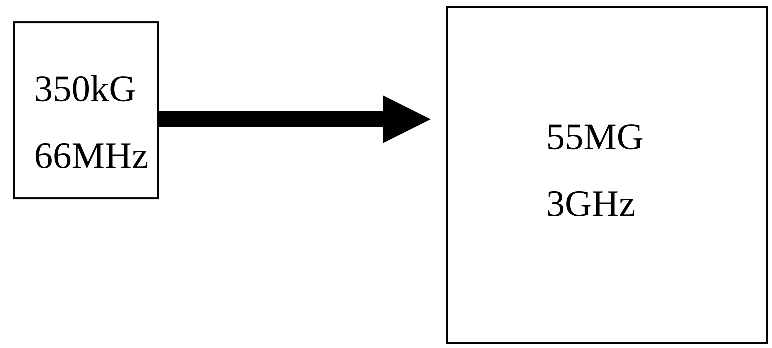
- **Sending node**
  - **One digital signature per packet**
- **Verifying node/Receiving node**
  - **First packet:**
    - **One certificate validation & One digital signature verification**
  - **Next packets:**
    - **One digital signature verification per packet**
- **Digital signature requires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

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**
  - **one signature in less than 1 ms**
- **Performace 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)**



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

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			

Methods to improve performance

- Parallel HW (multiple chips)
- Sending node
  - Include PLA only in every Nth packet
    - $\Rightarrow$ Potential security problem
  - Include forward credentials in PLA field
    - "I'm going to send X packets in next Y seconds"
- 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

Conclusions

- **Context Aware Management/Policy Manager (CAM/PM) -architecture is rule based system that adapts node's behavior according to its surrounding**
- **Concept of incomplete trust allows us to handle trust levels other than 0 and 100%**
- **Packet level authentication (PLA) provides scalable method to eliminate most of the faulty, forged, duplicated, and otherwise unwanted packets**