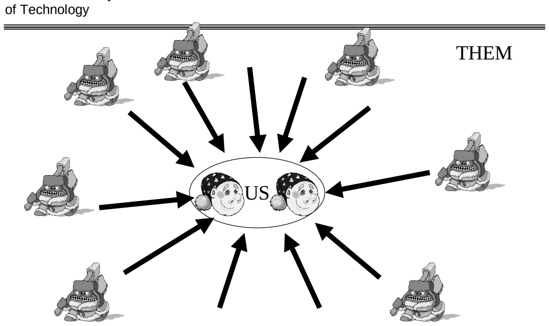
T-79.192 Special Course in Theoretical Computer Science

Military grade wireless ad hoc networks

Laboratory for Theoretical Computer Science
professor Hannu H. Kari
Helsinki University of Technology (HUT)

Topics

- **Problem statement**
- **Privacy issues**
- **Communication**
- **Trust**
- **Background information**
- **Sun Tzu**
- **Problems in military grade wireless ad hoc networks**
- **Requirements**
- **Security levels**
- **CAM/PM**
- **Military/Civilian networks**
- **Packet level authentication**



Problem statement

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

Helsinki University of Technology

What is privacy?

Helsinki University of Technology

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

Helsinki University of Technology

5 categories of privacy

- **Data privacy (Informaatio)**
- **Identity privacy (Kohde/lähde)**
- **Location privacy (Tapahtumapaikka)**
- **Time privacy (Tapahtuma-aika)**
- **Privacy of existence (Olemassaolo)**

Helsinki University of Technology

What is communication?

Helsinki University
of Technology

Communication

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

Helsinki University
of Technology

What is trust?

Helsinki University
of Technology

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

Trust

- A trusts B to perform operation X with probability 75%
  - T(A, B, X) = 0.75
- B trusts C to perform operation X with probability 50%
  - T(B, C, X) = 0.50
- A trusts C (via B)
  - T(A, C, X) = f (T(A, B, X), T(B, C, X))
    ≅ T(A, B, X) * T(B, C, X)

Helsinki University of Technology

Trust

- **A trusts C (via others)**
  - **$T(A, C, X) = \Sigma f(T(A, i, X), T(i, C, X)), i \neq A,C$**
- **Iterative trust of A to C**
  - **$T_{i+1}(A, C, X) = \alpha T_i(A, C, X)+(1- \alpha)\Sigma f(T(A, i, X), T(i, C, X)), i \neq A,C$**

Helsinki University of Technology

Trust

- **Normalizing trust**
  - **A learns that B tells the time always in 2 minutes later than others**
    - **B is trustworthy, but 2 minutes must be added to its time estimate**

Helsinki University of Technology

Background information

- **Wired and wireless networks**
  - **Multitude of access technologies**
- **IPv4 and IPv6**
- **Routing protocols**
- **Mobility management**
  - **Mobile IP and HIP**
  - **Ad hoc routing protocols**
  - **Hierarchical networks**
- **Security**
  - **Ipsec, Secure shell, SSL**
  - **PKI certificates**
- **Adaptive applications**

Helsinki University of Technology

Sun Tzu: The Art of War

- **Military action is important to the nation
it is the ground of death and life,
the path of survival and destruction.**
- **Five things are**
  - **Way**
  - **Weather**
  - **Terrain**
  - **Leadership**
  - **Discipline**

Sun Tzu: "The Art of War", 6th century BC

Helsinki University
of Technology

What are problems in military grade wireless ad hoc networks?

Helsinki University
of Technology

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

Difference between military & civilian networks?

Helsinki University
of Technology

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

Helsinki University of Technology

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**

Helsinki University of Technology

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**

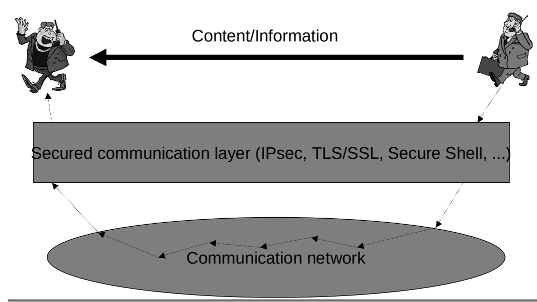
Helsinki University of Technology

3 levels of security

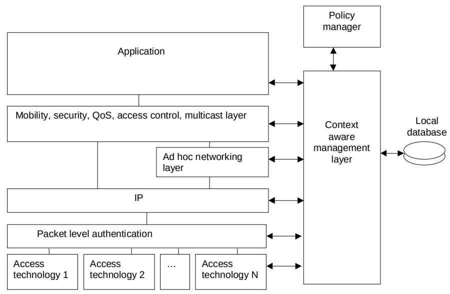
- **Content level security**
- **Transmission security**
- **Network security**

Helsinki University of Technology

3 levels of security



Context Aware Management/ Policy Manager



CAM/PM

- 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)

Packet level authentication

- Communication shall be based on strong security
  - 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

- Packet level authentication (PLA)
  - Every packet can be checked for authenticity, integrity, non-repudiation, timeliness, ...
    - Just like in IPsec
  - Any node in the network can do the PLA checking
    - IPsec requires security association
  - PLA checking requires no previous negotiation or exchange of security parameters between the sender and verifier
    - IPsec can't do this!

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**
- **Disadvantages**
  - **Increased packet size (~60-100 bytes)**
  - **Requires strong crypto algorithms**
    - **Elliptic curves, digital signatures, ...**
  - **More computation per packet**

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**

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**

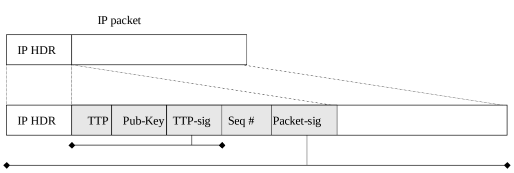
Helsinki University
of Technology

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**

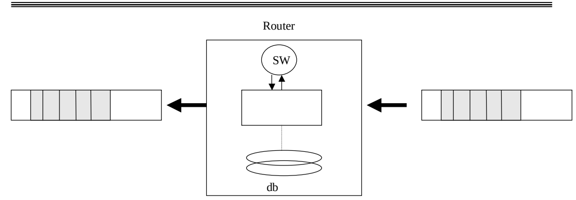
Helsinki University
of Technology

HW implementation



Helsinki University
of Technology

HW implementation



Helsinki University
of Technology

HW implementation

IP HDR	TTP	Pub-Key	TTP-sig	Seq #	Packet-sig	

1. Check sending time
2. Calculate hash

no-hash

3. Validate TTP
4. Store Pub-Key
5. Verify TTP-sig
6. Verify Packet-sig
7. Store Seq #

Helsinki University
of Technology

HW implementation

IP HDR	TTP	Pub-Key	TTP-sig	Seq #	Packet-sig	

1. Check sending time
2. Calculate hash

in-hash

3. Validate Seq #
4. Check validity time

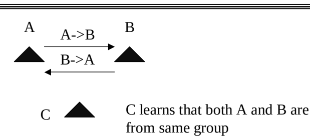
5. Verify Packet-sig
6. Store Seq #

Helsinki University
of Technology

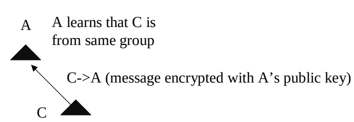
Helsinki University
of Technology

Application: Quick secured communication in battle field

Any communication

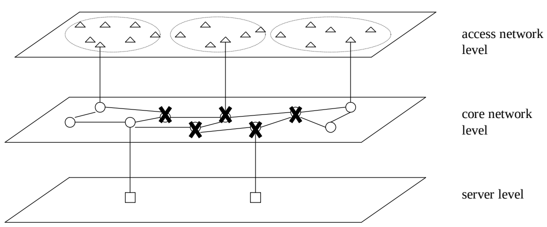


First message from C to A



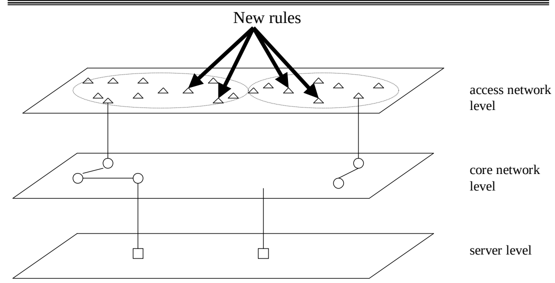
Helsinki University of Technology

Application: New core network: Military strike



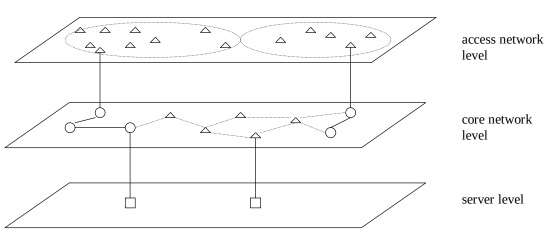
Helsinki University of Technology

Application: New core network: Reconfiguration



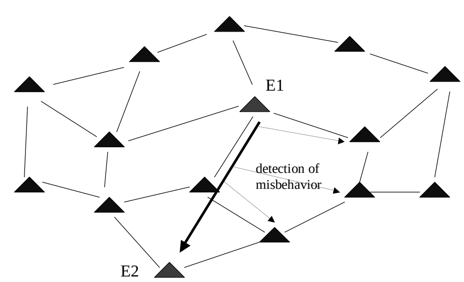
Helsinki University of Technology

Application: New core network: After military strike



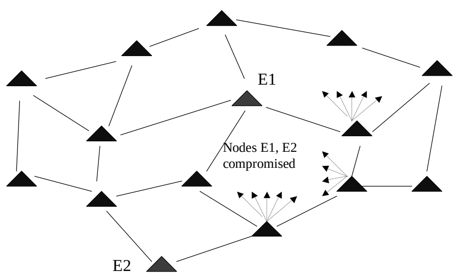
Helsinki University of Technology

Application: Excluding compromised nodes



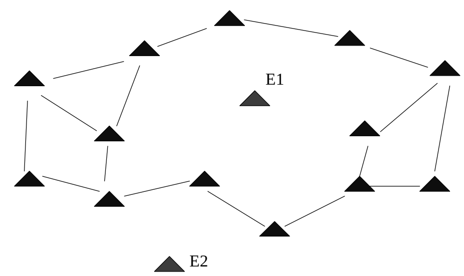
Helsinki University of Technology

Application: Excluding compromised nodes



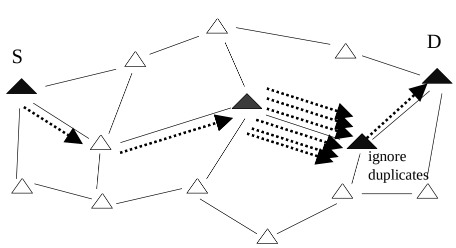
Helsinki University of Technology

Application: Excluding compromised nodes



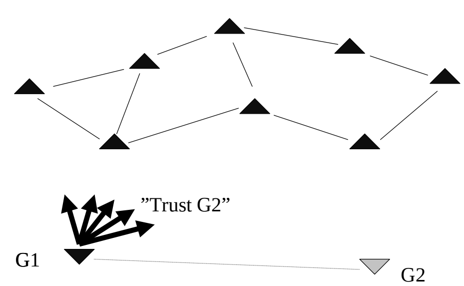
Helsinki University of Technology

Application: Restricting DoS attack



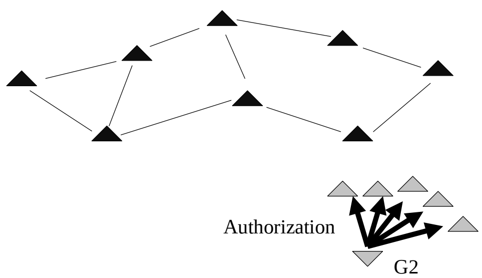
Helsinki University of Technology

Application: Delegation of command chain



Helsinki University of Technology

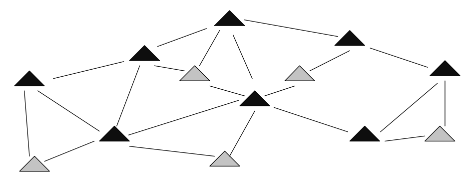
Application: Delegation of command chain



T-79.192
Military grade wireless ad hoc networks Hannu H. Kari/HUT/CS/TCS Page 49

Helsinki University of Technology

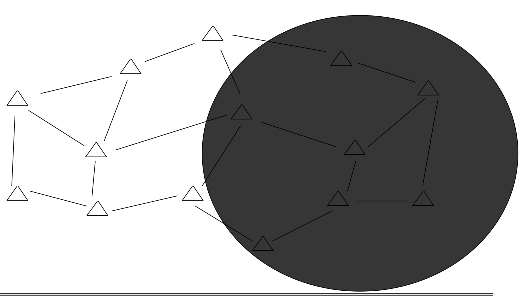
Application: Delegation of command chain



T-79.192
Military grade wireless ad hoc networks Hannu H. Kari/HUT/CS/TCS Page 50

Helsinki University of Technology

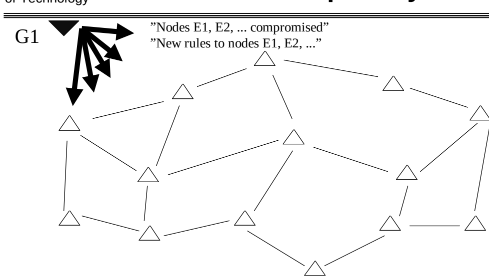
Application: Revocation of large quantity of nodes



T-79.192
Military grade wireless ad hoc networks Hannu H. Kari/HUT/CS/TCS Page 51

Helsinki University of Technology

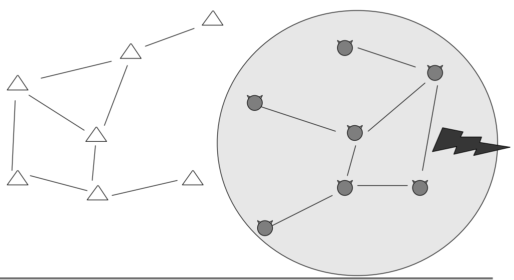
Application: Revocation of large quantity of nodes



T-79.192
Military grade wireless ad hoc networks Hannu H. Kari/HUT/CS/TCS Page 52

Helsinki University
of Technology

Application: Revocation of large quantity of nodes



Helsinki University
of Technology

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
  - HUT's HW implementation performs an ECC multiplication in around 100 microseconds
    - Isn't this enough for sending node?

Helsinki University
of Technology

Methods to improve performance

- Sending node
  - Include PLA only in every Nth packet
    - ⇒ 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

Helsinki University
of Technology

Time synchronization

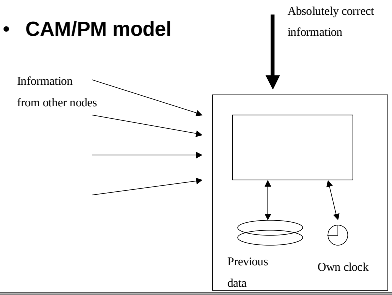
- Needs
  - Common understanding of the time
    - Perform operation at time T
    - Perform operation at T minutes from now
- Methods
  - Initial time synchronization
  - Global time beacon
  - Local time adjustment
    - Concept of incomplete trust and time adjustment

Time synchronization

- Problems
  - PLA and time consistency?
    - Packet rejection
    - Packet replay
  - Required accuracy of time?
  - Monotonically growing time
    - Clocks can't go backwards
    - Can clock stop for a while?
  - Clock inaccuracy
    - Typically in order of 1...10 ppm
  - Inconsistent clock
    - Time warps
  - Large time differences between neighbors

Time synchronization

- CAM/PM model



Location synchronization

- Needs
  - Knowledge of node's own position
  - Geographical operations
    - Routing, node activation, node movement
- Methods
  - GPS, manual configuration, physical attachment
  - radio signal measuments, laser/ultra sound,...
- Problems
  - Moving nodes
  - Accuracy

Securing communication for groups

- Common communication channel
  - For entiry army
- Channel for groups
  - Few nodes or hundreds of nodes
- Key change
  - Peer-to-peer keys, group keys
  - Periodic change
  - Change after compromising nodes