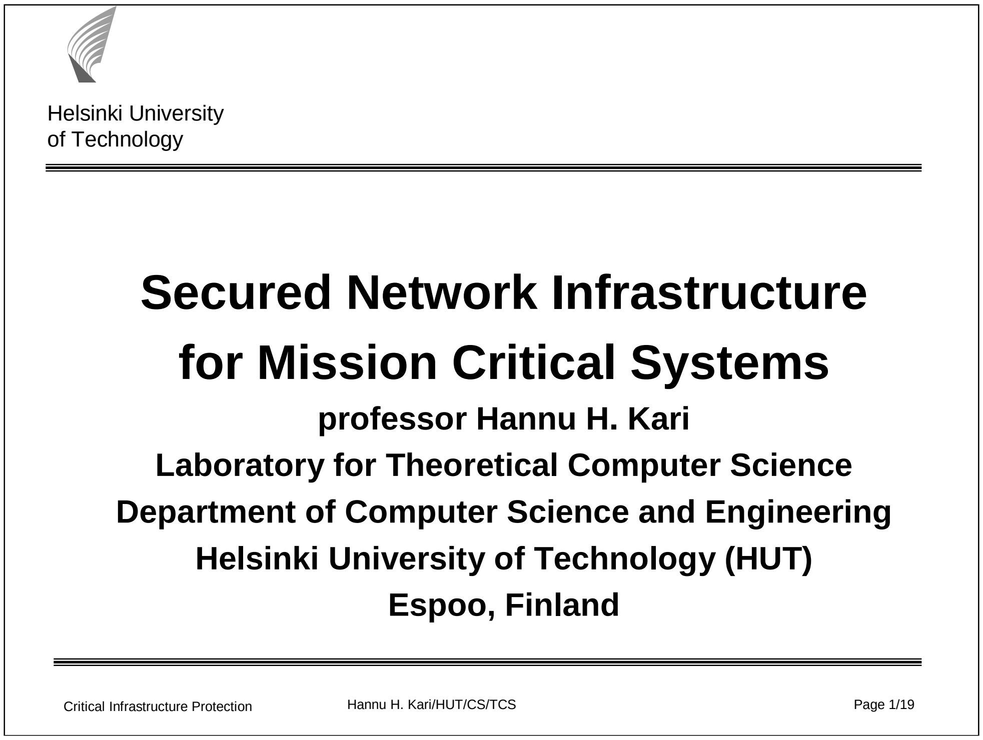
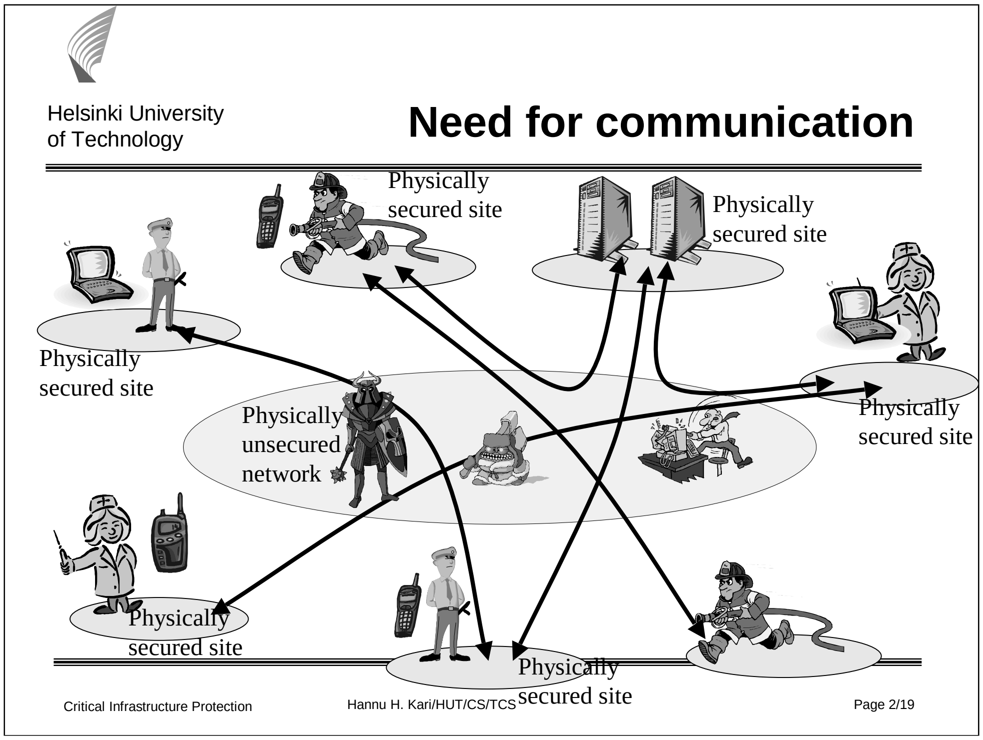


Secured Network Infrastructure for Mission Critical Systems

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

A short introduction how to help decision making by ensuring communication between authorities that are using any arbitrary communication network to carry critical information between authorities.

This proposal does not discuss the information confidentiality, that should be handled with end-to-end secured communication, such as IPsec. Instead, this proposes a new method that provides high reachability (i.e., very high probability that legitimate data transmission reaches the destination in every situation).



Helsinki University
of Technology

Need for communication

Physically
secured site

Physically
secured site

Physically
secured site

Physically
secured site

Physically
unsecured
network

Physically
secured site

Physically
secured site

Critical Infrastructure Protection Hannu H. Kari/HUT/CS/TCS Page 2/19

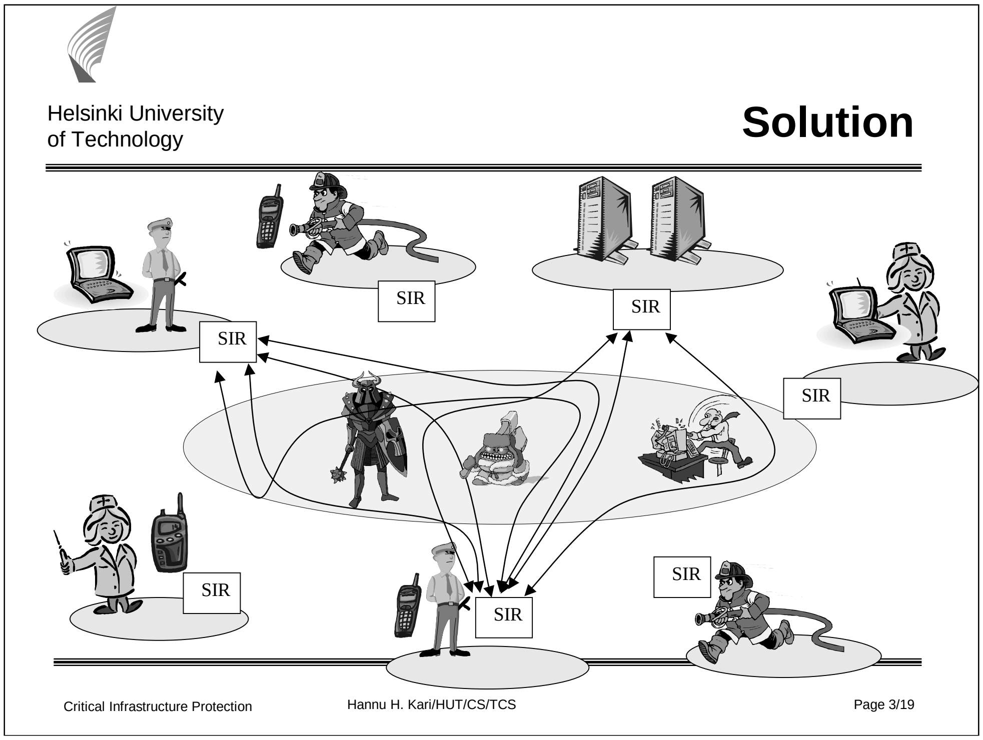
Problem of modern networks:

Various authorities - such as police, fire departments, medicare, or political decision makers - need operational communication systems in all situations. Communication networks are needed to enable prompt decision making based on actual and correct information. Also, commands must be delivered promptly.

One approach is to use dedicated networks, such as VIRVE, for this. Such networks are still vulnerable against attacks on the physical networks and very costly, especially, if high level of redundancy is needed. Even if the communication is end-to-end secured, it is very simple to paralyze the communication by physically attacking the network and cut the communication.

More sophisticated attacks includes manipulation of the data flow thus causing difficulties in detecting the location of the attacker. Physical sites, such as computer centers, can be protected with reasonable level of physical access control methods, but it is infeasible to physically protect thousands of kilometers (optical) cables around the country.

Additionally, we have needs to share information between authority groups and distribute information also to civilians.



Helsinki University
of Technology

Solution

Critical Infrastructure Protection Hannu H. Kari/HUT/CS/TCS Page 3/19

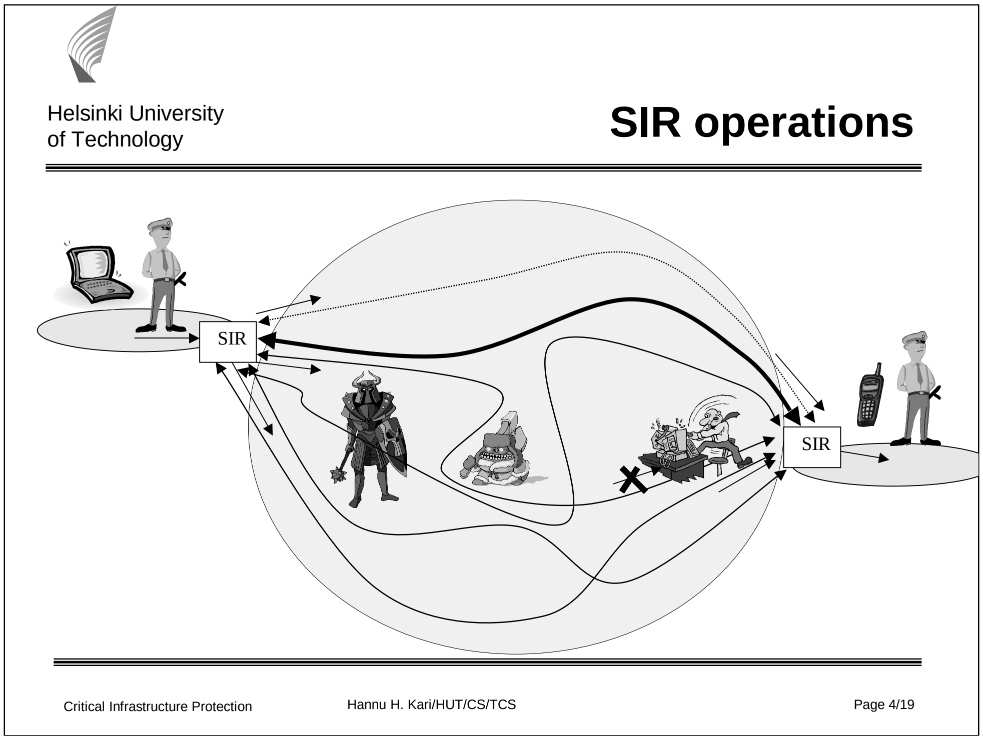
Solution principles:

To overcome these above mentioned problems, we propose here to use several, alternative communication networks in parallel with the principle that at least one of those networks should be operational. In order to paralyze our communication, the attacker must disable every alternative communication channel. In this picture, only one organization’s alternative routes are illustrated.

It is much easier to increase availability of a set of alternative networks than build highly reliable single network. Here, we can utilize also alternative network technologies (such as wired and wireless) and different owners (such as operators’, own, rental/leased, ...).

With a Secured Infrastructure Router (SIR), we can fulfill the needs. A SIR has several alternative networks to reach its counter parties at the other side. Each alternative network is attached to a SIR with separate network interface. This means that attackers that are in one network may either disable the communication or flood the interface with garbage, but problems do not impact on the other network interfaces.

SIRs establish a virtual private network (VPN) on top of physical networks so that they can learn alternative routes to other sites and guarantee reliable communication between sites.



Helsinki University
of Technology

SIR operations

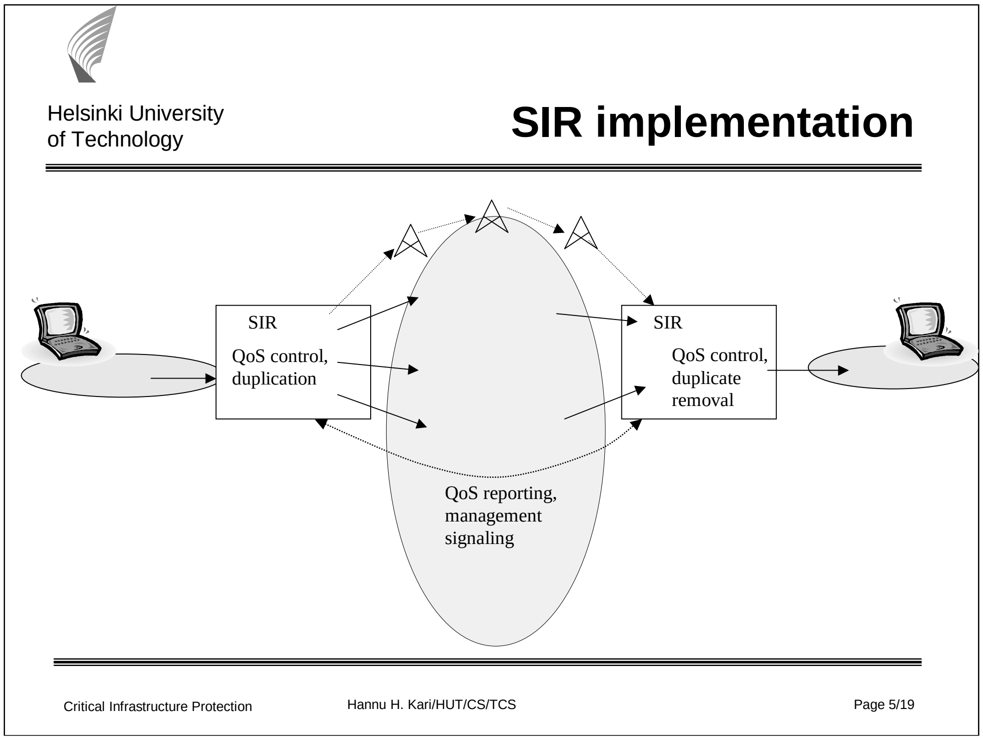
Critical Infrastructure Protection Hannu H. Kari/HUT/CS/TCS Page 4/19

SIR operations:

When two SIRs have established a logical connections between themselves, they may use one or several alternative networks to carry each packet reliably over the networks. Each SIR gathers statistical information of alternative networks. When a SIR gets a packet from its own local network, it makes one or several copies of that packet and sends them via alternative networks to the destination site. The number of copies depends, for example, on the importance of the packet (e.g., more copies if the packet is VoIP) or the quality of used networks (i.e., if networks are unreliable, then more copies are made). Each packet sent between SIRs contain management information so that the receiving SIR can remove duplicates and also monitor each networks quality. This is needed to learn each networks quality. Also, heartbeat messages can be used to do monitoring even in the case when no other traffic is available.

Since the SIRs are actively monitoring each networks quality, they can quickly adapt theit operation on the changing quality (i.e., attacks) on different networks. With the additional header information used between SIRs, it is possible to monitor quality of networks, negotiate policies and also adjust routing priorities between the networks. E.g., prioritize VoIP traffic over WWW-traffic.

SIRs are independent of network technologies. This means that we can use wired and wireless networks as well as dedicated connections or public networks.



Helsinki University
of Technology

SIR implementation

SIR

QoS control,
duplication

SIR

QoS control,
duplicate
removal

QoS reporting,
management
signaling

Critical Infrastructure Protection

Hannu H. Kari/HUT/CS/TCS

Page 5/19

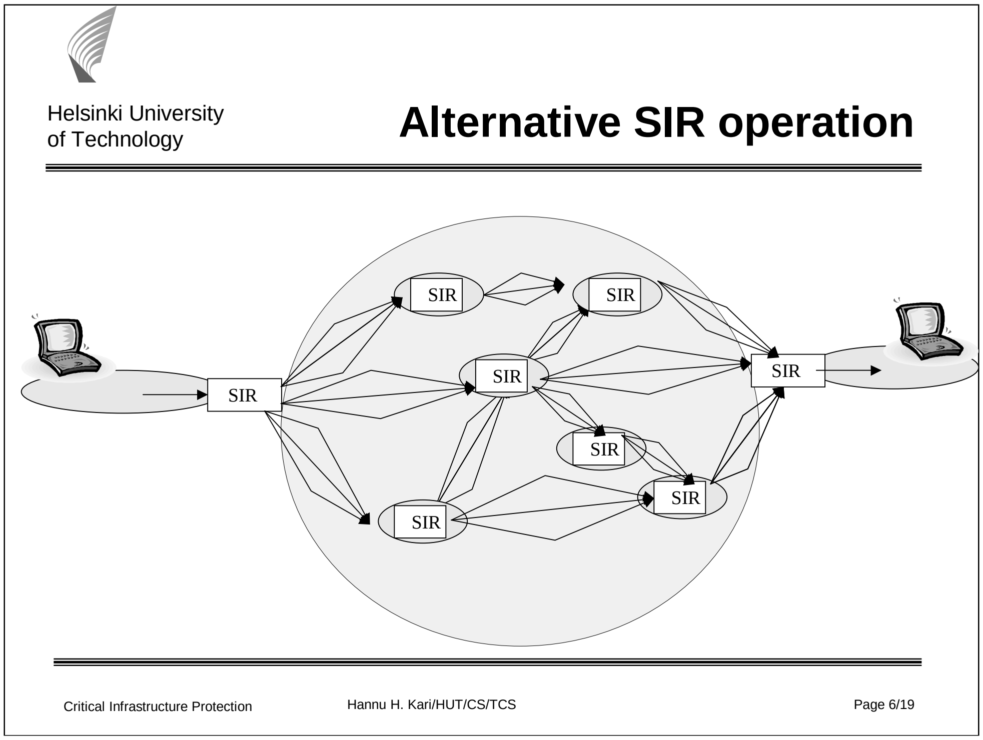
SIR implementation:

Implementation of a SIR box is very close to a standard router. It is possible to implement a SIR using standard PC HW and Linux operating system, with some SW enhancements

Additional SW that is needed is related with

- handling duplication of packet (and removal of received duplicates)
- SIR management system (monitoring alternative networks and handling routing with several routes)
- quality of service control to prioritize traffic (standard Linux features could most likely be used)

Since the performace requirements of SIRs is in the order of hundreds of megabits/s or gigabits/s, it is possible to implement SIRs with PC HW instead of special dedicated router HW. However, to support high level of reliability, we must have possibility to use redundant components as one logical SIR. Here, StoneGate –technology (http://www.stonesoft.com/products/VPN/) could be used as a main building block.



Helsinki University
of Technology

Alternative SIR operation

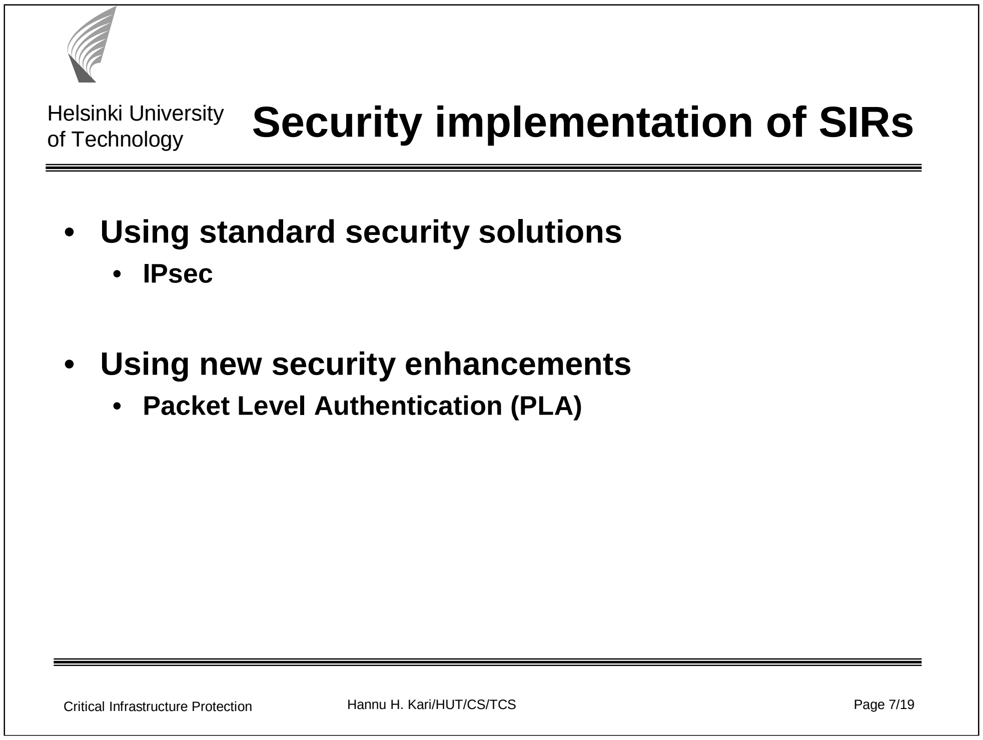
Critical Infrastructure Protection   Hannu H. Kari/HUT/CS/TCS   Page 6/19

Alternative SIR implementation:

It is not always possible to make direct connections between two SIRs that need to communicate. Hence, we can utilize similar methods as in ad hoc networks. Here, instead of individual mobile nodes that want to find alternative (best) routes from one node to another, we manage traffic between SIRs (and sites behind them).

The SIR on the left, finds (using standard ad hoc routing protocols), how to reach the SIR on the right with help of its trusted fellow SIRs. Communication between these two sites is possible, as long as there is a path between them with any of the alternative networks.

Since in this case, the used networks are divided into small hops, we can increase the reachability. For the first hop (from SIR1 to SIR2), we can use operator A’s network, from SIR2 to SIR3 operator B’s network, and so on.



Helsinki University
of Technology

Security implementation of SIRs

- **Using standard security solutions**
  - **IPsec**
- **Using new security enhancements**
  - **Packet Level Authentication (PLA)**

Critical Infrastructure Protection Hannu H. Kari/HUT/CS/TCS Page 7/19

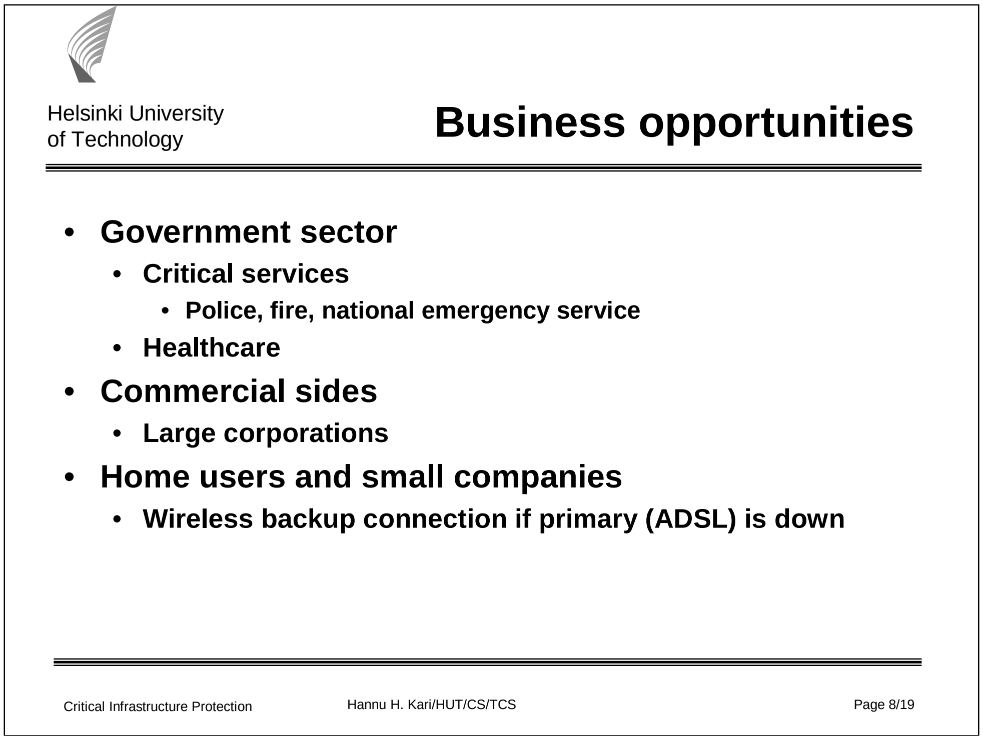
We have two alternative approaches how to handle information integrity between SIRs.

Traditional security approach:

> Here, we can use IPsec for integrity protection of packet. Additional SIR headers will be put first and then IPsec headers.

Enhanced security approach:

> In case stronger security solution is needed, a new PLA-approach can be used. The benefit of PLA is higher flexibility and possibility to detect erroneous packets already on the network level (not just at the final destination).



Helsinki University
of Technology

Business opportunities

- Government sector
  - Critical services
    - Police, fire, national emergency service
  - Healthcare
- Commercial sides
  - Large corporations
- Home users and small companies
  - Wireless backup connection if primary (ADSL) is down

Critical Infrastructure Protection Hannu H. Kari/HUT/CS/TCS Page 8/19

So, where’s the business?

At the beginning, such systems are needed to secure critical services, but we have envisioned to use the same approach also with corporate services and even with small companies and individuals.

Large corporations have nowadays 7/24 service requirement and much of their work is heavily networked. Hence, they require connectivity (or reachability) in all situations.

With small companies and individuals, it is not so critical to be reachable all the time, but it is still important to have backup system, for example, to be able to access Internet banking and send/receive emails. Here, wireless alternatives gives reasonably inexpensive backup.