International Doctorate School in
Information and Communication Technologies

Università degli Studi di Modena e Reggio Emilia

System Architecture and Security Issues In Emergency Networks

Alessandro Paganelli

Curriculum: Electronics and Telecommunications

Tutor: Prof. M. Casoni

Presentation outline

- Part I: System architecture for Emergency Networks
  - Design principles
  - Proposed architecture
- Part II: Security issues in Emergency Networks
  - Security properties for an emergency network
  - Proposed solutions
- Part III: Future work and conclusions

Part I:
System Architecture for Emergency Networks

Design approach

- An **emergency network** is the communication infrastructure of a public safety system. It is used by the **first responders** (FRs) to improve the emergency response and to communicate with the command & control centers (EOC and MEOCs).

- Some of its **design requirements** are:

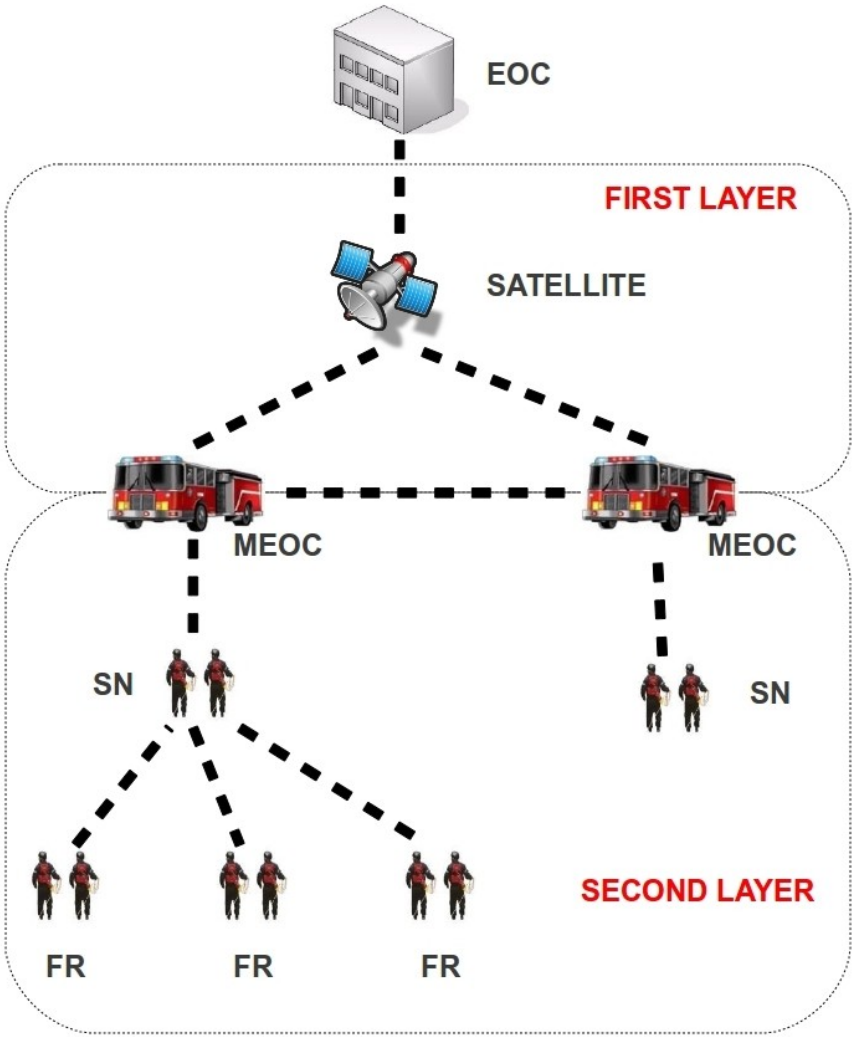
  - Reliability, availability and robustness
  - Scalability
  - Interoperability
  - It should support many different services (QoS requirement)

- In our vision, an emergency network should adopt **standard** and **widespread** technologies (both wireless and wired), in order to make the whole system **interoperable** and to take advantage of the economies of scale. Examples:

  - IP as the main internetworking protocol
  - IEEE 802.11, IEEE 802.16, DVB-RCS and 3G/LTE

Proposed system architecture 1/2

- **Mesh-based** at the first layer
- "**Quasi star**"-based at the second layer
  - A **special node** (e.g. the FRs chief) acts as a hub, as in a star topology
  - It communicates with the MEOC via a back-haul link
- Technologies:
  - DVB-RCS and DVB-RCS NG for the main back-haul link at the first layer
  - IEEE 802.16 for terrestrial inter-MEOC links
  - IEEE 802.16/11 for the SN-MEOC link
  - IEEE 802.11 for inter-FR links



Proposed Architecture 2/2

- Pros:
  - **Simple** QoS management
  - **Simple** access control and AAA procedures
  - **Simple** traffic-shaping and filtering
  - FRs local connectivity is possible regardless of the SN-MEOC link
  - It conforms to the FRs' group **mobility model**

- Cons:
  - The **SN is a SPOF**

- Comments:
  - It is possible to introduce redundant links with the use of other technologies (e.g. 3G/LTE)
  - It is possible to **extend** this approach with the use of redundant and semi-fixed SNs (i.e. not human-equipped)
    - **No-more SPOF**

Part II:
Security Issues in Emergency Networks

Security Properties for an Emergency Network

- The main security properties for a “classical” computer network are:

1. Simple and mutual authentication
2. Data confidentiality and secrecy
3. Data / origin authentication
4. Authorization / access control and accountability
5. Data integrity
6. Non repudiation
7. Availability

- The main properties that affect the design of the system architecture for an emergency network are **authentication**, **data confidentiality** and **availability**

Authentication

- Requirements:
  - **Quick** and **simple**
  - Viable even in the case of **network disconnection** (i.e. it should not rely on a centralized node available all time)
    - In the worst case, two nodes should be capable of authenticate each other **without the involvement of other systems**
  - Should allow inter-jurisdiction cooperation

- Our proposal:
  - **Identity-based cryptography** (requires a certification authority at the setup)
  - **Self organization** model and **trusted sub-group model**
  - **Simultaneous authentication of equals** (SAE)

Data confidentiality and secrecy

- Implemented via cryptographic techniques
- The actual choice depends on:
  - The transmission standards adopted
    - In fact, every transmission standard provide its own crypto solutions
  - The **scope** required for confidentiality (i.e. end-to-end or local)
  - The presence of **additional requirements** (e.g. QoS)
    - QoS traffic differentiation needs packet “in clear” for inspection!
- Our proposal:
  - Cryptography implemented at data-link layer, with local scope for each network segment.
    - QoS classification made possible because the IP layer works with plain text packets, instead of encrypted ones.

Availability

- Can be enhanced by adopting **redundant solutions**, thus enhancing the number of alternatives that can be used to serve each incoming request.

- Our proposal:
  - As regards computer systems: implement **replicas** (i.e. redundant systems) and **caching**.
    - It can be done for those systems that are vital for the network
  - As regards the network: implement **redundant links** (i.e. more paths) and **redundant technologies** (which also increases interoperability)

- Open issues:
  - Different technologies → different logical networks
    - How to perform **path selection** among different logical networks?
    - **Authentication issues** among different networks
    - **Confidentiality issues** among different networks
    - **Access control**/**traffic shaping issues**

Part III:
Future Work

Future work

- Develop an **assessment tool** to evaluate the proposed architecture and the security solutions
  - In terms of throughput, delay, jitter, packet loss
  - We are considering **NS-3** as the main tool

Questions?

Conference publications:

1) D. Vassiliadis, A. Garbi, G. Calarco, M. Casoni, **A. Paganelli**, R. Morera, C. M. Chen, M. Wodczak, "*Wireless Networks at the Service of effective First Response Work: the E- SPONDER Vision*", presented at the 5th International Symposium on Wireless Pervasive Computing (ISWPC), 5-7 of May, Modena 2010.
2) G. Calarco, M. Casoni, **A. Paganelli**, D. Vassiliadis, M. Wodczak, "*A Satellite based System for Managing Crisis Scenarios: the E-SPONDER Perspective*", presented at the 5th Advanced Satellite Multimedia Systems Conference (ASMS), 13-15 of September, Cagliari 2010.

Submitted papers:

M. Casoni and **A. Paganelli**, "*Security Issues in Emergency Networks*", submitted to the 3rd International Workshop on "Emergency Management: Communication and Computing Platforms" Co-Located with the 7th International Wireless Communications and Mobile Computing Conference (IWCMC 2011).