WK 01: COMP4337/9337 Secure Wireless Networks

Topic: Security Challenges in Wireless Networks

Never Stand Still

Professor Sanjay K. Jha

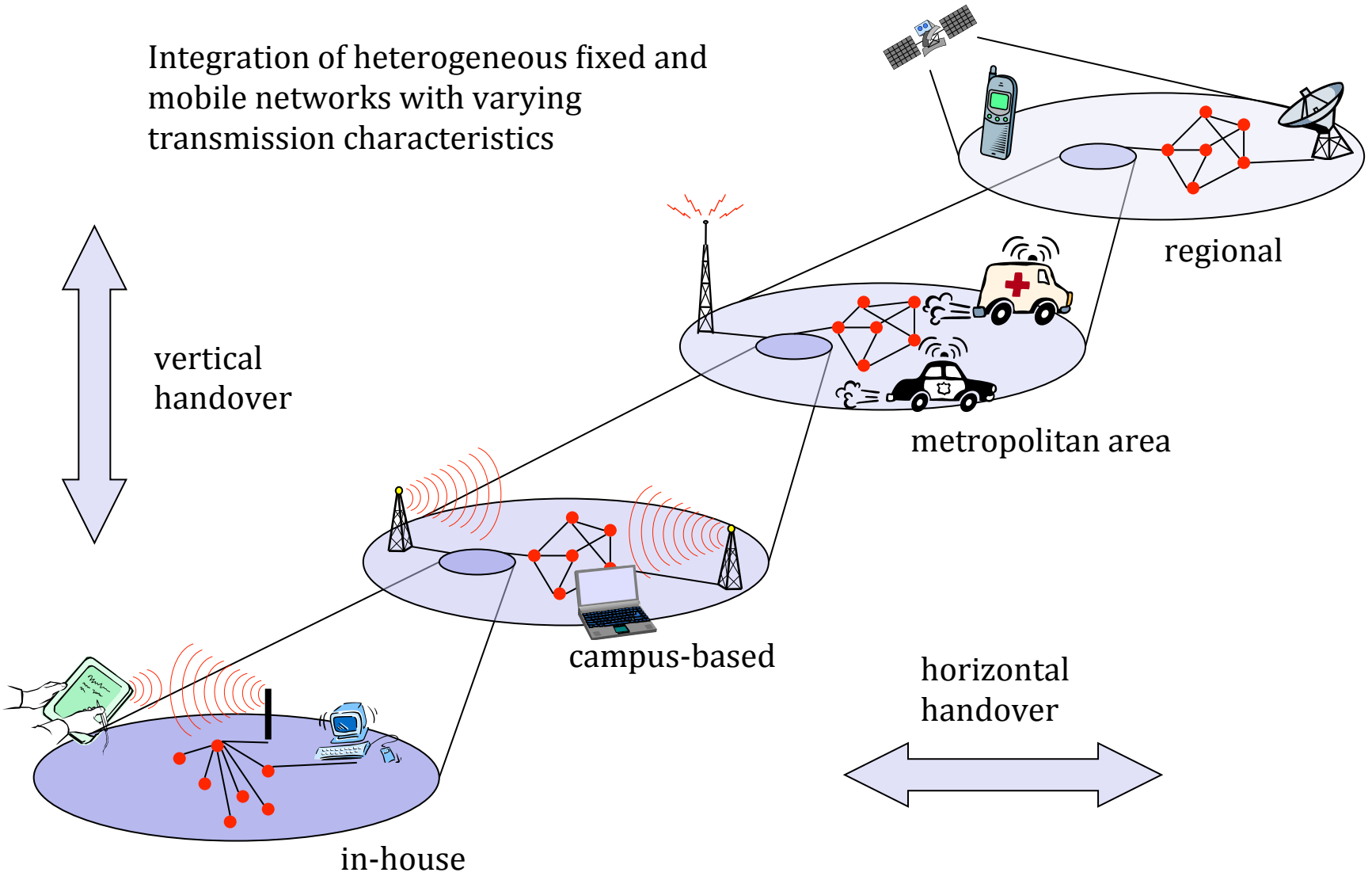
School of Computer Science and Engineering, UNSW

Today's Agenda

- Security in Wireless Network
- Wireless Architecture and Challenges
  - Cellular Networks
  - Wireless LAN (Wifi)
  - Wireless Mesh Networks
  - Wireless Sensor Networks
  - Vehicular Networks
  - Personal Area Networks

Emerging Network Trend

Integration of heterogeneous fixed and mobile networks with varying transmission characteristics



Security Services – Wireless Network

- *Authentication*
  - The most fundamental security service which ensures, that an entity has in fact the identity it claims to have
- *Integrity*
  - In some kind, the "small brother" of the authentication service, as it ensures, that data created by specific entities may not be modified without detection
- *Confidentiality*
  - The most popular security service, ensuring the secrecy of protected data
- *Access Control*
  - Controls that each identity accesses only those services and information it is entitled to
- *Non Repudiation*
  - Protects against that entities participating in a communication exchange can later falsely deny that the exchange occurred

Security Aspects of Wireless Networks

- *Wireless networks faces all threats that does its wired counterpart:*
  - *Masquerade, eavesdropping, authorization violation, loss or modification of transmitted information, repudiation of communication acts, forgery of information, sabotage*
  - *Thus, similar measures like in fixed networks have to be taken*

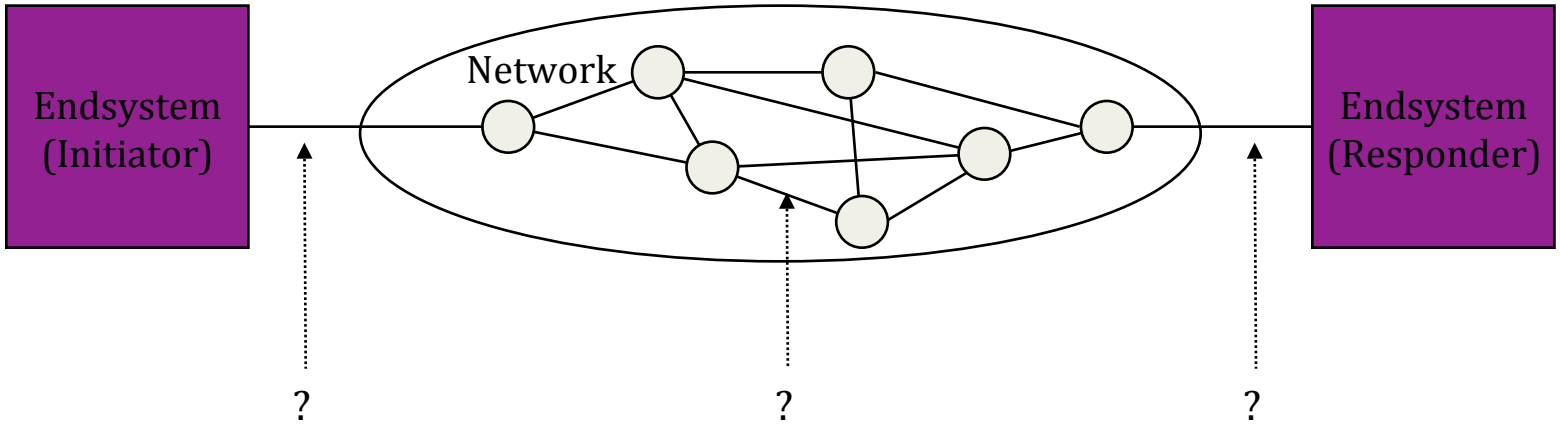
What is different?

- *Wireless Network is more accessible for eavesdropping*
- *The lack of a physical connection makes it easier to access services*
- *Authentication has to be re-established when the mobile device moves*
- *Key management gets harder as peer identities can not be pre-determined*
- *The location of a device / user becomes a more important information that is worthwhile to eavesdrop on and thus to protect*

What is different ? (contd)

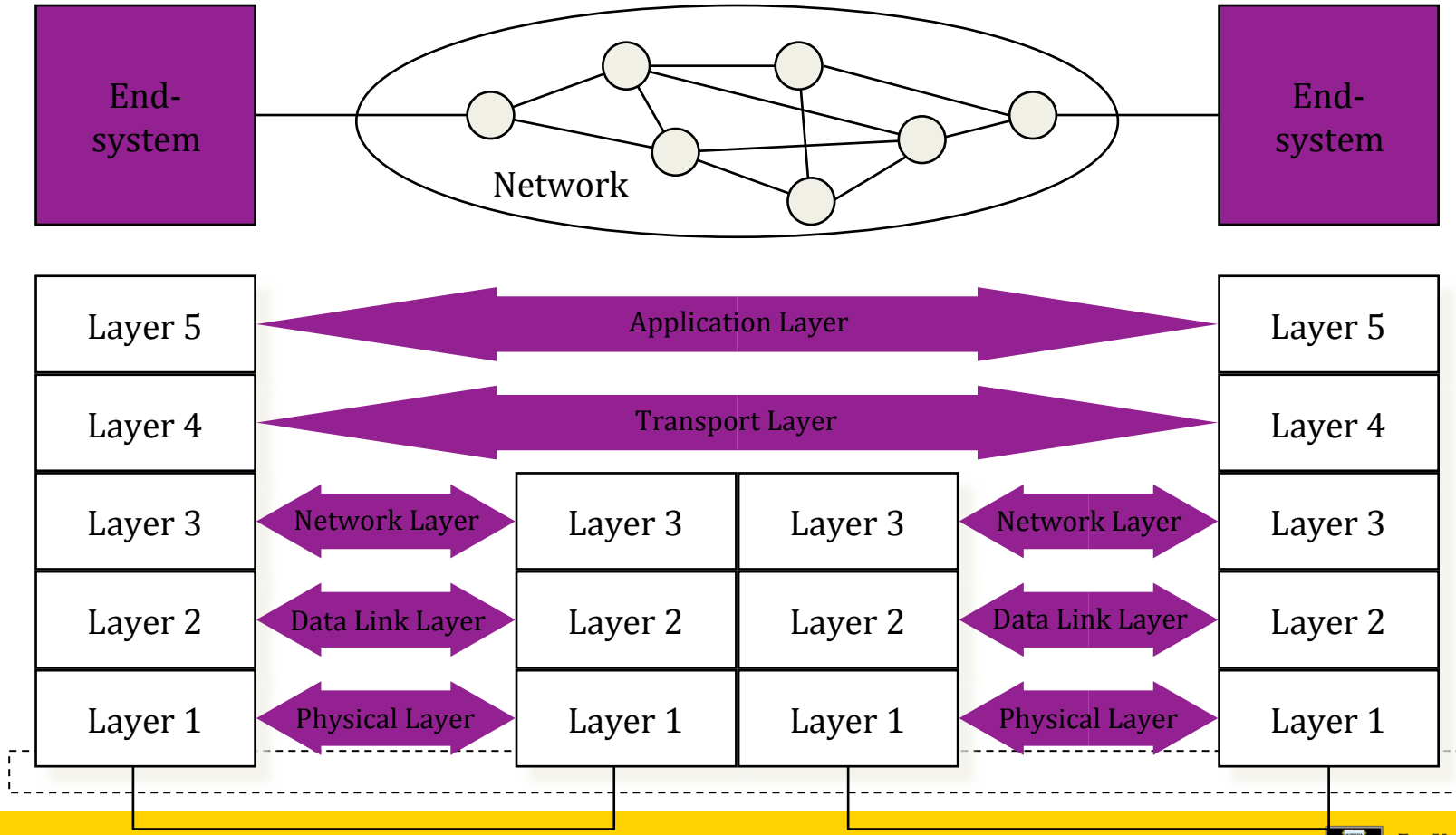
- *Injecting bogus messages into the network is easy*
- *Replaying previously recorded messages is easy*
- *Illegitimate access to the network and its services is easy*
- *Denial of service is easily achieved by jamming*

Security Analysis of Layered Protocol Architectures 1

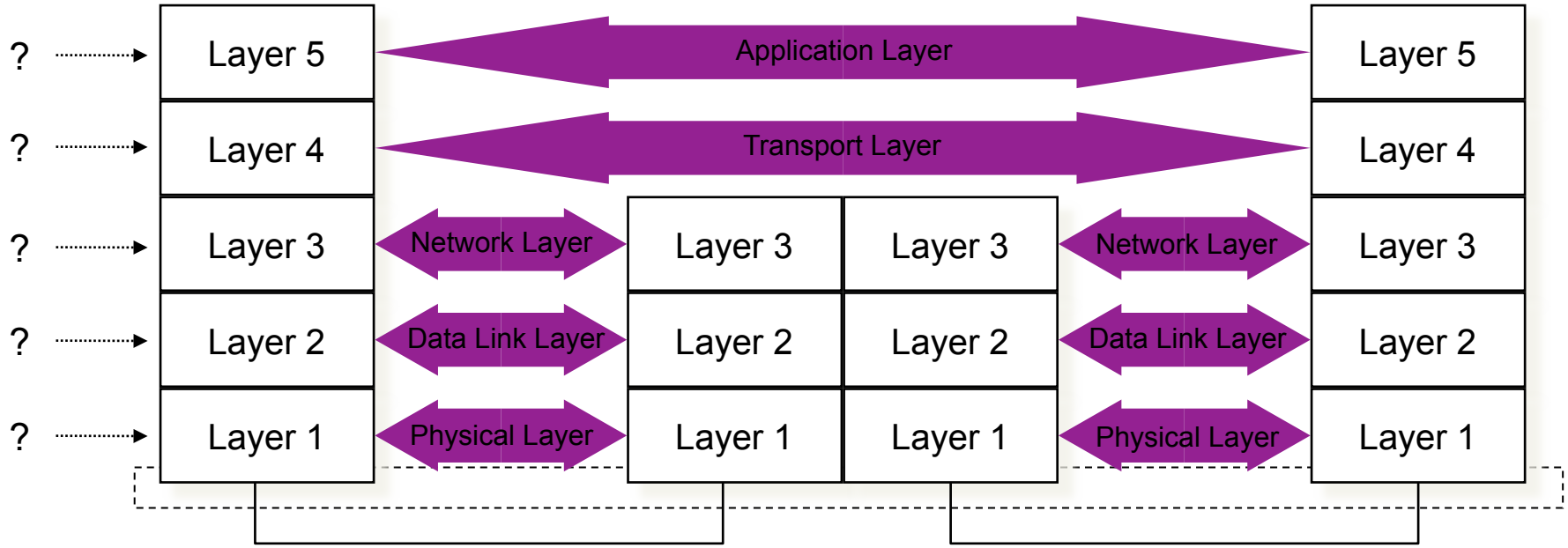


Dimension 1: At which interface does the attack take place?

Communication in Layered Protocol Architectures



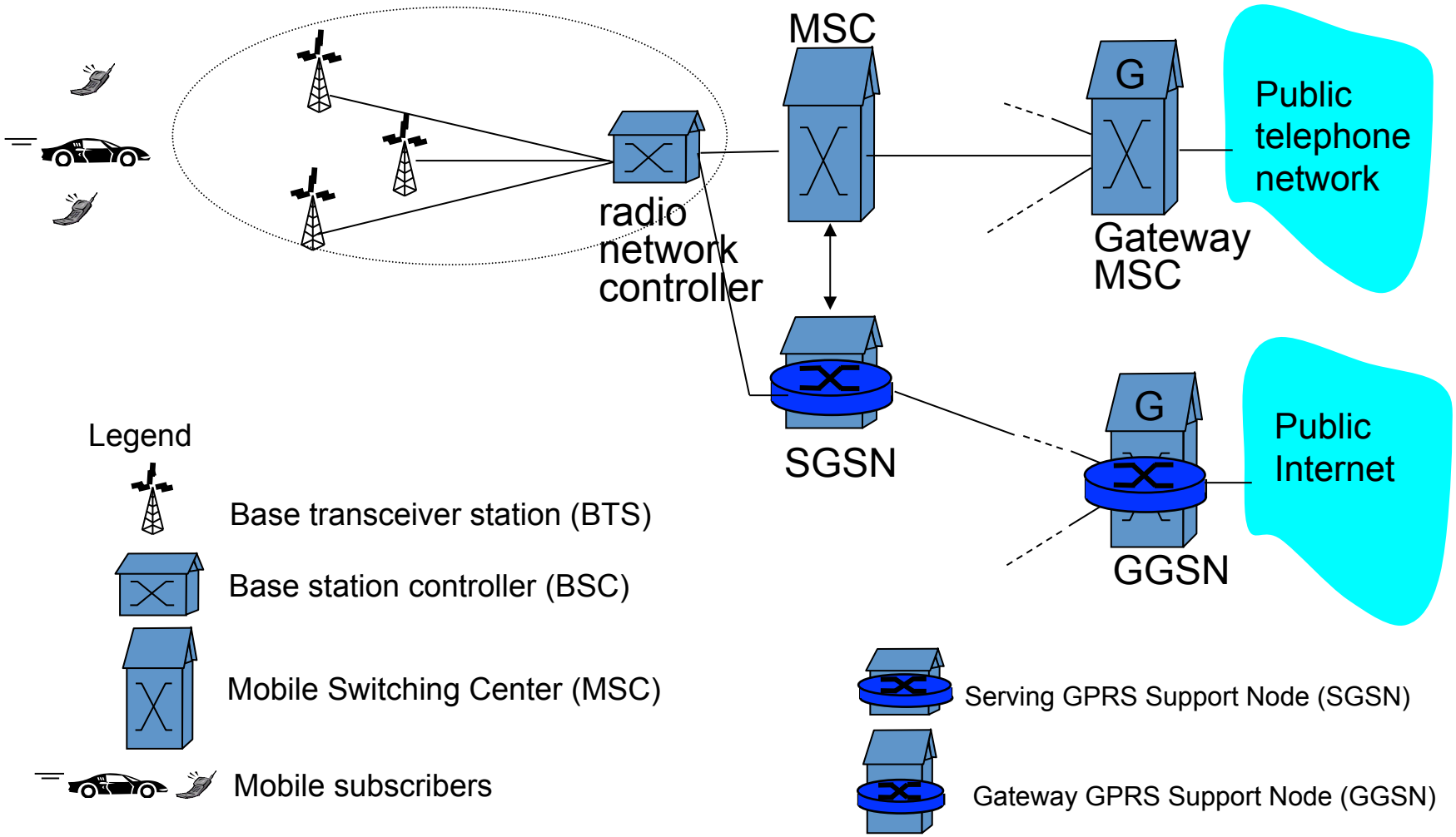
Security Analysis of Layered Protocol Architectures 2



Dimension 2: In which layer does the attack take place?

Types of Wireless Networks and Associated Security Challenges

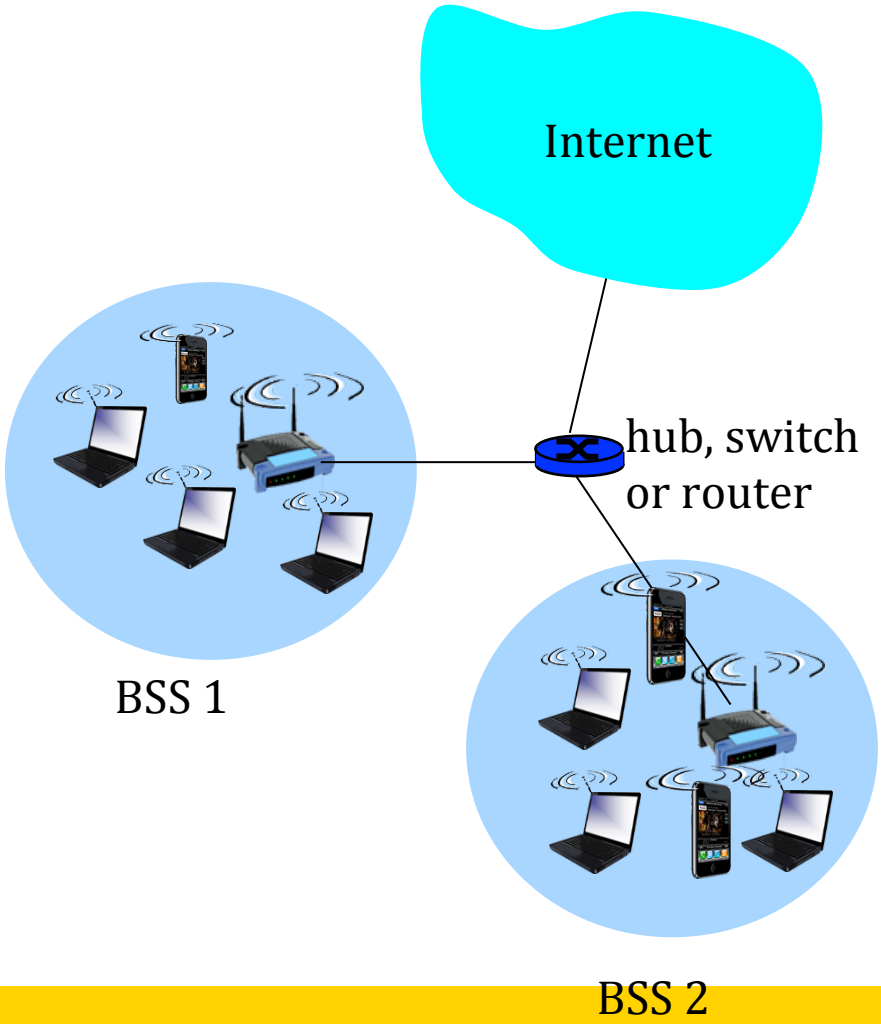
Cellular network architecture



Cellular Network Security

- *2G had weak security*
  - Possible attacks from a faked base station
  - Cipher keys and authentication data transmitted in clear between and within networks
  - Encryption not used in some networks ➔ open to fraud
  - Data integrity not provided
- *Some improvement with respect to 2nd generation*
  - Cryptographic algorithms are published
  - Integrity of the signalling messages is protected
- *Cellular Security not a focus but may explore a bit more*

Wifi - WLAN



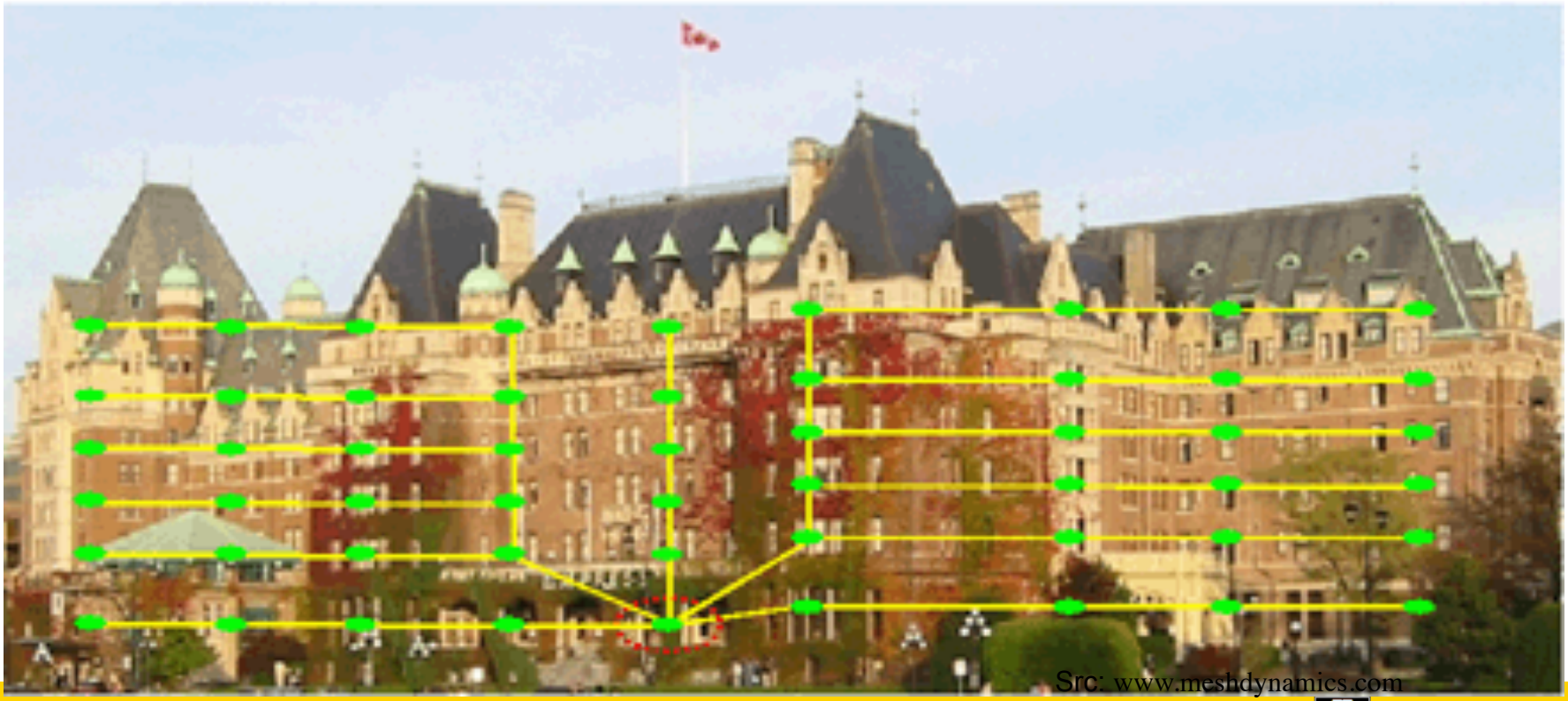
- *wireless host communicates with base station*
  - *base station = access point (AP)*
- *Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:*
  - *wireless hosts*
  - *access point (AP): base station*
  - *ad hoc mode: hosts only*

Security in WLAN

- *Some basic issues covered in COMP3331/9331*

- *We will treat this topic in detail in later week*
  - *WEP, Why failed, what lesson did we learn*
  - *802.11i, Temporal Key Integrity Protocol (TKIP)*
  - *.....*

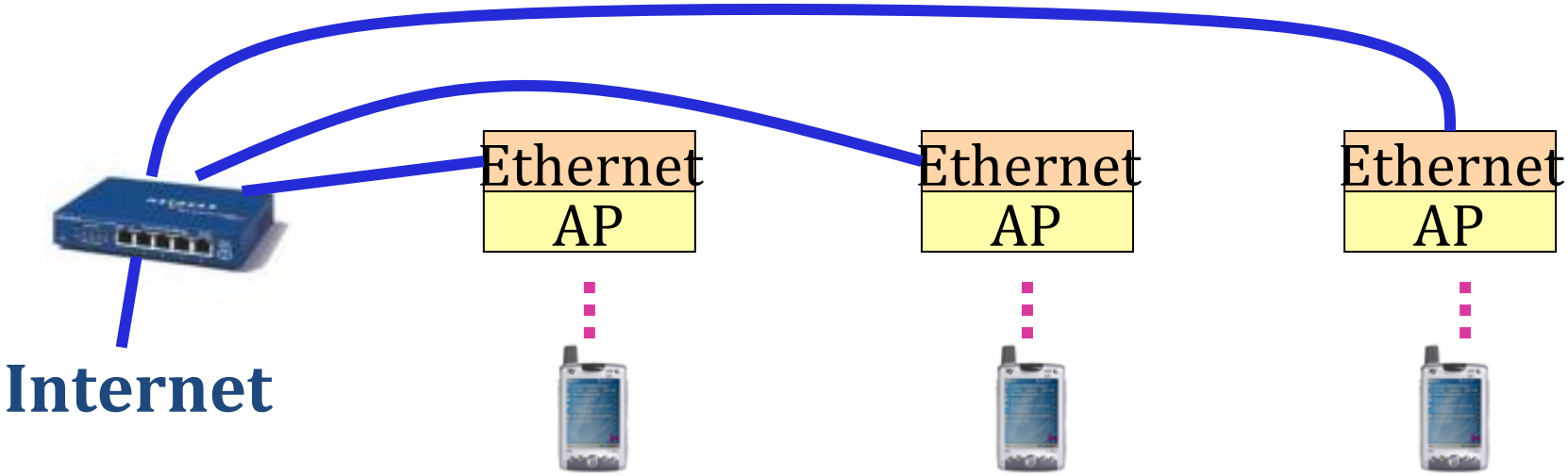
Wireless Mesh Networks: Extended WLAN coverage



Src: www.meshdynamics.com

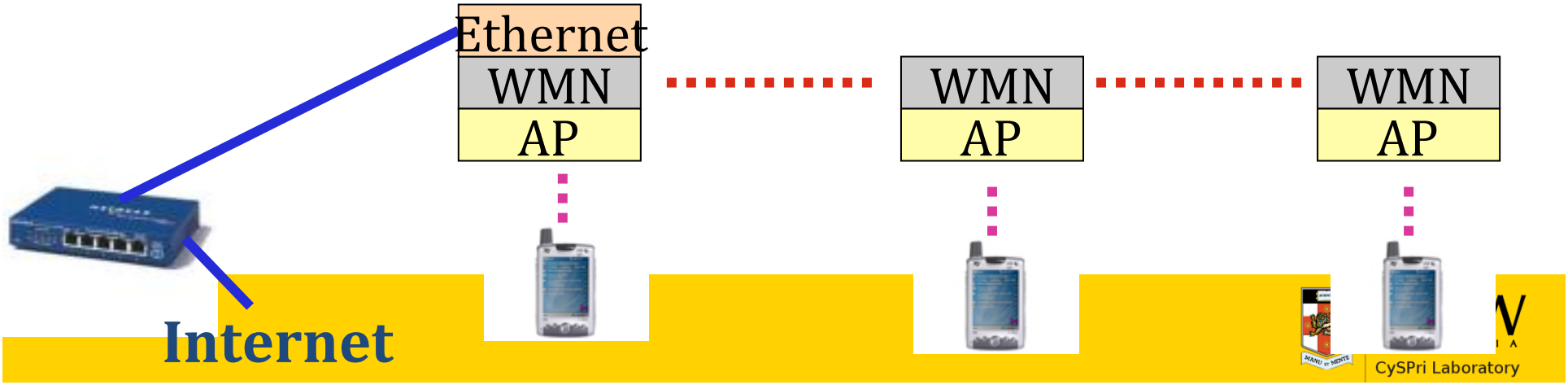
WLAN:

(AP = access point)



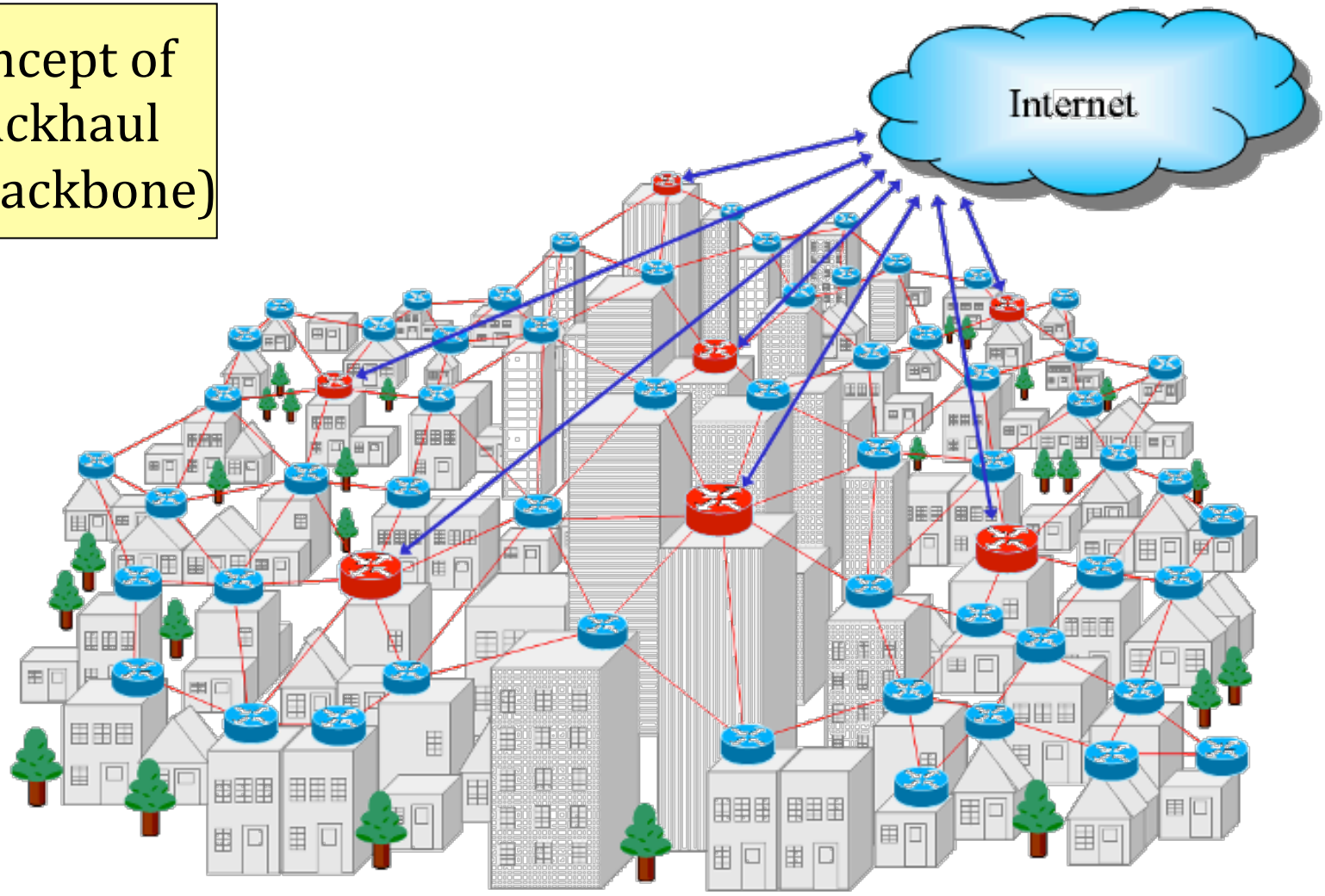
Wireless mesh network (WMN):

Features: Mesh routers;
Multi-hop routing



City-wide WiFi

Concept of Backhaul (or backbone)



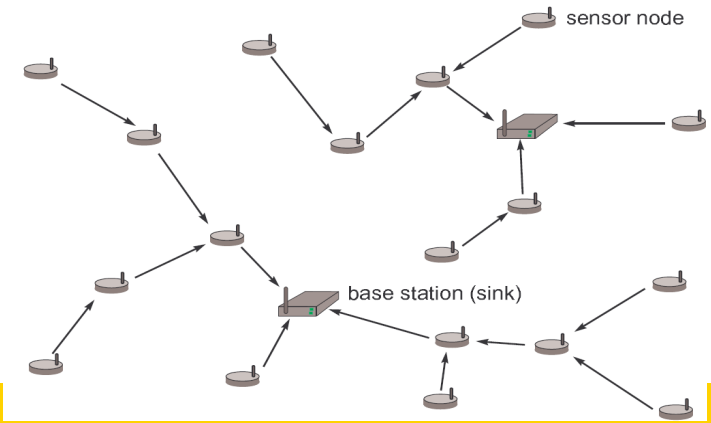
Source: M. Sichitiu

WMN Security

- *Several verifications need to be performed:*
  - *WAP (connected to internet) has to authenticate the user terminal.*
  - *Each user has also to authenticate the next hop mesh router*
  - *Each mesh router has to authenticate the other mesh routers in the WMN*
  - *The data sent or received by user has to be protected (e.g., to ensure data integrity, non-repudiation and/or confidentiality).*
  - *Denial of service attack possible*
- *Performing these verifications has to be efficient and lightweight, especially for the user terminal.*

Sensor Networks

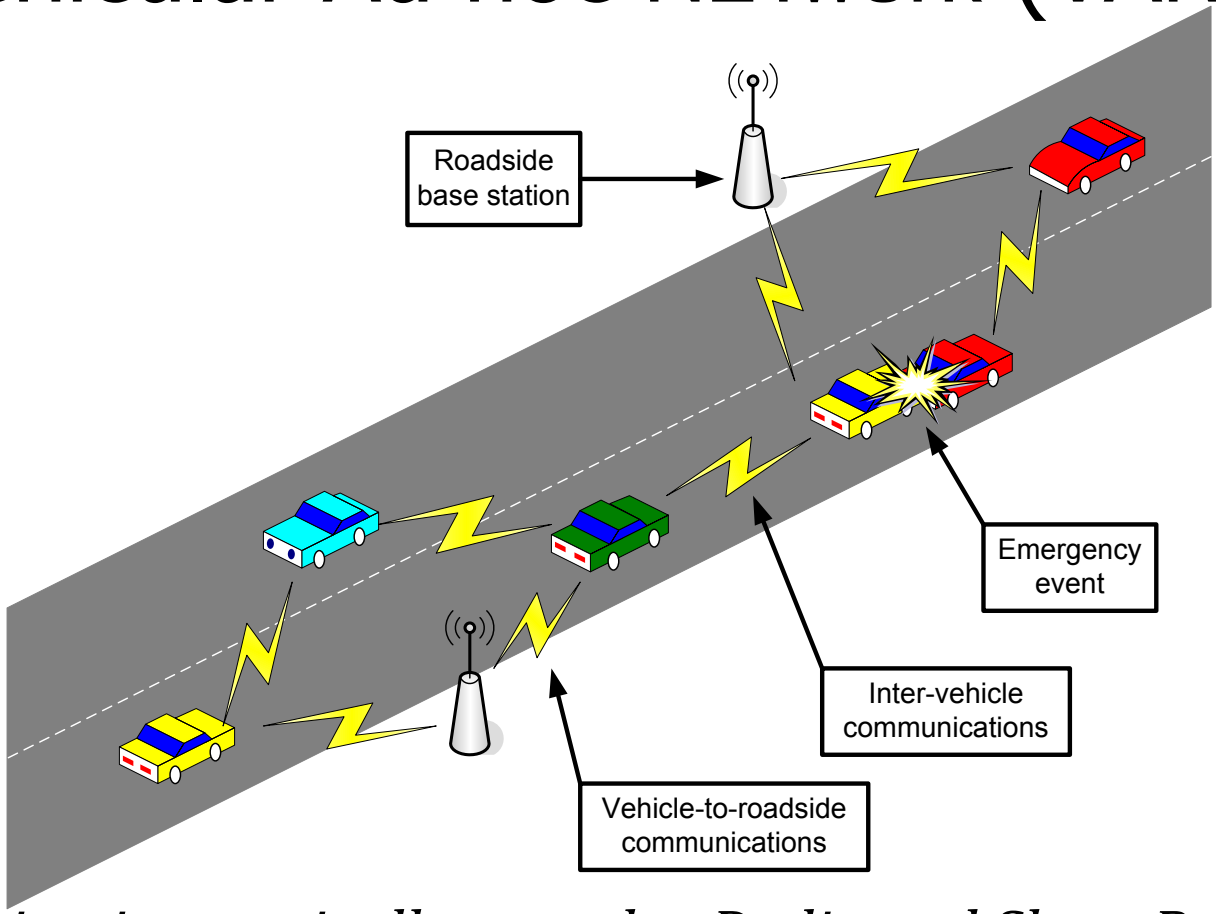
- *Large number of sensor nodes, a few base stations*
- *Sensors are usually battery powered:*
  - *Main design criteria: reduce the energy consumption*
- *Multi-hop communication reduces energy consumption:*
  - *Overall energy consumption can be reduced, if packets are sent in several smaller hops instead of one long hop*
  - *Fewer re-transmissions are needed due to collisions*



Sensor Network Security

- *Resource constraint*
  - *Limited CPU processing power*
  - *Limited Battery – attacker can deplete.*
  - *Need lightweight crypto protocols*
- *Physical Security*
  - *Capture, Cloning, and Tampering easy.*
- *Wireless Programming on Devices possible*
  - *Additional security risk*

Vehicular Ad hoc NETwork (VANET)



- *Communication: typically over the Dedicated Short Range Communications (DSRC) (5.9 GHz)*
- *Example of protocol: IEEE 802.11p*

Vehicular communications: why?

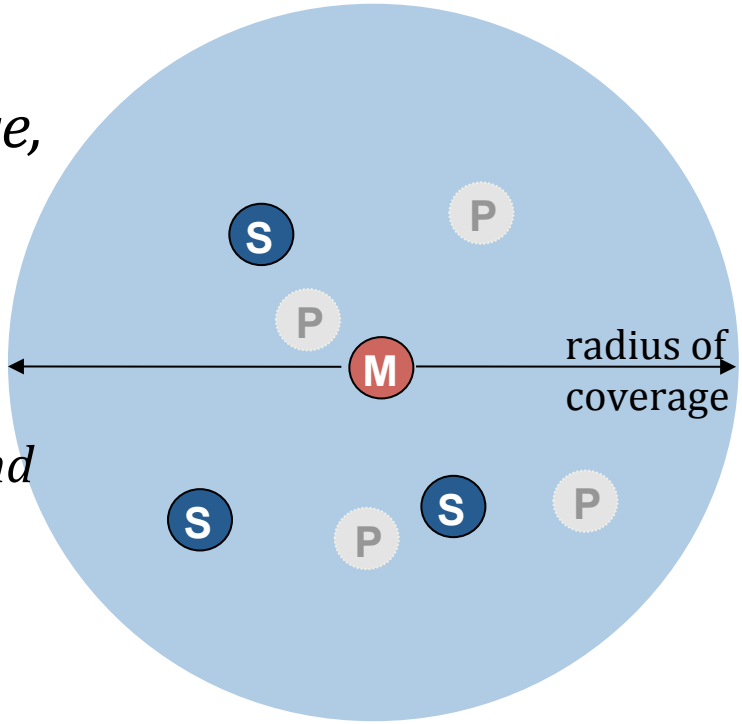
- *Combat the awful side-effects of road traffic*
  - *In the EU, around 40'000 people die yearly on the roads; more than 1.5 millions are injured*
  - *Traffic jams generate a tremendous waste of time and of fuel*
- *Most of these problems can be solved by providing appropriate **information** to the driver or to the vehicle*

Why Security important?

- *Bogus Traffic Information*
- *Disruption of road network/traffic movement*
- *Cheating with identity, speed, location*
- *Jamming*
- *Location/privacy issues*
- *Security requirements:*
  - Sender authentication, Verification of data consistency, Availability, Non-repudiation, Privacy, Real-time constraints

802.15: Personal Area Network

- *less than 10 m diameter*
- *replacement for cables (mouse, keyboard, headphones)*
- *ad hoc: no infrastructure*
- *master/slaves:*
  - *slaves request permission to send (to master)*
  - *master grants requests*
- *802.15: evolved from Bluetooth specification*
  - *2.4-2.5 GHz radio band*
  - *up to 721 kbps*



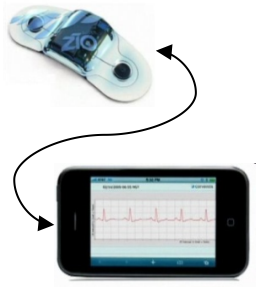
PAN Security

- *Short-range communications, master-slave principle*
- *Eavesdropping is difficult:*
  - Frequency hopping
  - Communication is over a few meters only
- *Security issues:*
  - Authentication of the devices to each other
  - Confidential channel
    - *Based on secret link key*

IoT Devices and Security

- The market for wearable wireless sensors is projected to grow to more than 420 million devices by 2014.

- Fundamental applications in patient monitoring, personalized healthcare, telemedicine, and athlete training.



1. Apple iPhone SensorStrip

2. Nike + iPod Sports Kit

3. Nokia Sports Tracker

4. Toumaz Life Pebble

- Security is critical because these devices generate medical data, and challenging given that they have low power and computation capabilities.

References

- *Chapter8, Kurose Ross*, **Computer Networking: A Top-Down Approach**, *for wireless network architecture overview*
- *Chapter 1 and 2, L. Buttyan and J. P. Hubaux,* **Security and Cooperation in Wireless Networks** *(note: the book leans towards game theory, restrict your reading to security. Cellular security is covered in detail – the book is slighlty old - missing 4G networks)*
- *Günter Schäfer,* **Security in Fixed and Wireless Networks**, *Wiley*

- *Acknowledgement: foils are adapted from Buttyan, Kurose-Ross, Schafer primarily. Special thanks to Prof Schafer for sharing foils in advance.*