WK 01-02: COMP4337/9337
Securing Fixed and Wireless Networks

Never Stand Still

Professor Sanjay K. Jha

Topic: Network Architectures and Security

School of Computer Science and Engineering, UNSW

Today’s Agenda

- Security in Wireless Network
- Security in IP protocol stack
- Review of wired and wireless networks and security concerns

Course Coverage

- Introduction
- Internet Architecture
- Network Protocols and Vulnerabilities
- Application Layer Security
- Transport Layer Security
- Network Layer Security
- Link Layer Security
- Wireless LAN Security
- Network Defence Tools
- Advanced Network Security topics

NOTE: We may not take exactly the layered approach to accommodate for labs/assignments during a term

Introduction

- Internet connectivity is essential but is vulnerable to threats

- Our heavy reliance on networking technology, that provides unprecedented access to a whole range of applications and services anytime, anywhere, makes it an attractive target for malicious users
  - Malicious users attempt to compromise the security of our communications and/or cause disruption to services

- Certain original protocols are either designed without bearing security in mind, or with poor security design decisions
  - Not merely of historical interest: contemporary designs are often constrained by their predecessors for pragmatic reasons

Introduction

We explore

- The challenges in securing a networks under a variety of attacks
- Widely used security protocols
- Emerging security challenges and solutions

A basic understanding of networking protocol stack and TCP/IP suite is assumed from 3331/9331 or equivalent

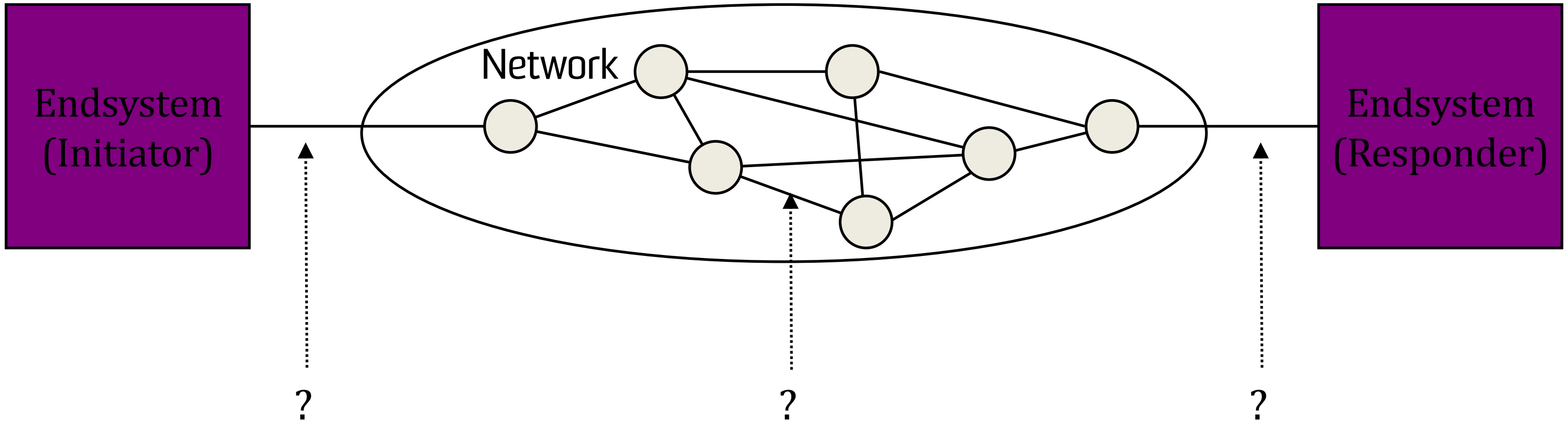
Internet Architecture

- A complex system such as distributed applications running over a range of networking technologies is best understood when viewed as layered architecture

- We will revise the 7-layer ISO OSI protocol stack and the interaction between various layers
  - TCP/IP protocol stack uses only five layers from OSI model i.e., layers 1- 4 and 7
  - Presentation and Session layers are optional and their functionality can be offloaded to the application layer

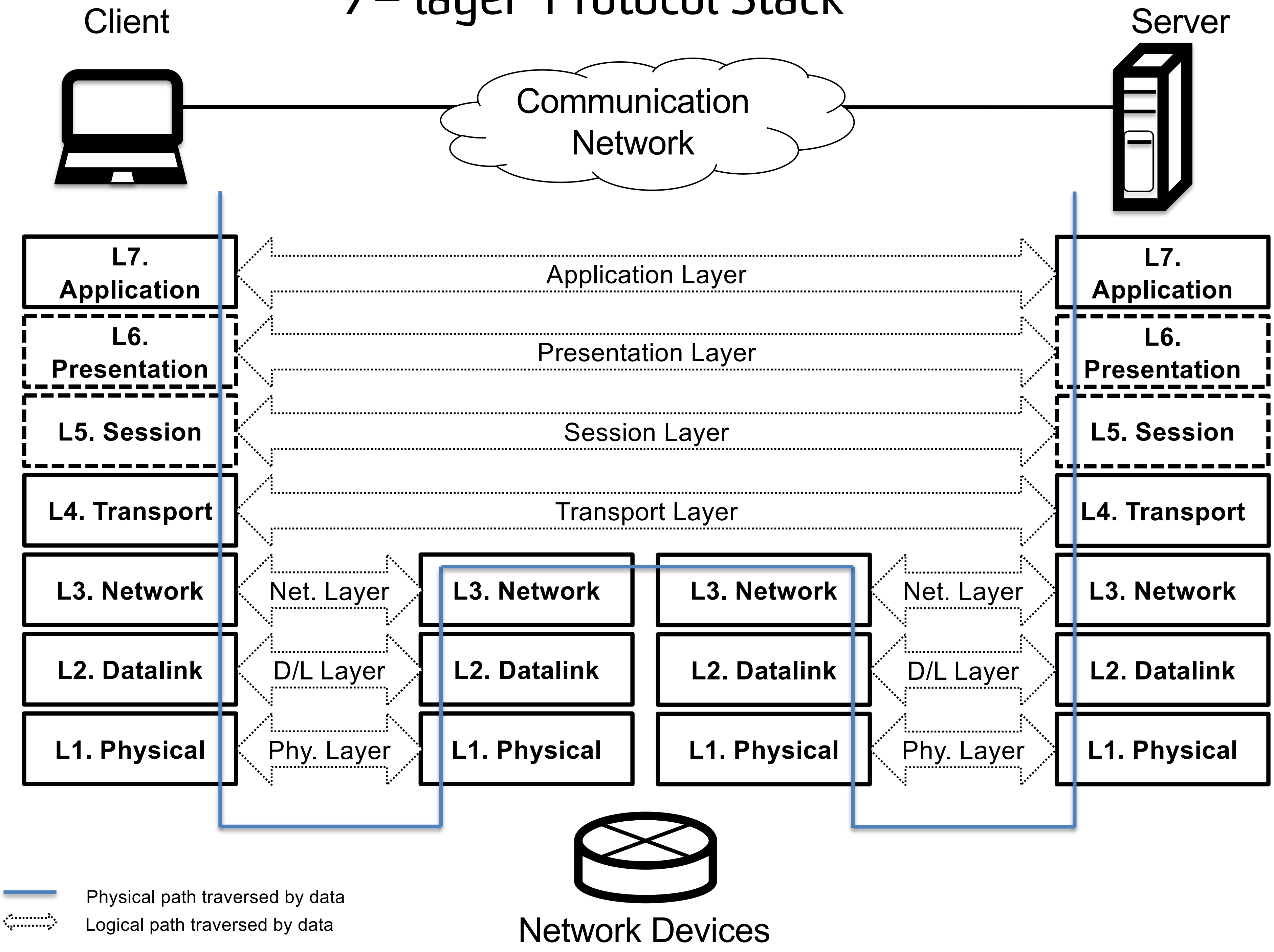
- The model also allows us to understand the security issues on each layer and the interplay between them.

Security Analysis of Layered Protocol Architectures



At which interface does the attack take place?

7– layer Protocol Stack



Client

Communication Network

Server

L7. Application

Application Layer

L7. Application

L6. Presentation

Presentation Layer

L6. Presentation

L5. Session

Session Layer

L5. Session

L4. Transport

Transport Layer

L4. Transport

L3. Network

Net. Layer

L3. Network

L3. Network

Net. Layer

L3. Network

L2. Datalink

D/L Layer

L2. Datalink

L2. Datalink

D/L Layer

L2. Datalink

L1. Physical

Phy. Layer

L1. Physical

L1. Physical

Phy. Layer

L1. Physical

Network Devices

Physical path traversed by data

Logical path traversed by data

Network Vulnerabilities

- Security research literature use Dolev-Yao (DY) adversarial formal model for formal analysis of security protocols
  - DY model describes the worst possible adversary that has complete control over the entire network allowing it to read any message, prevent delivery of any message, duplicate any message or otherwise synthesize any message for which the adversary has the relevant cryptographic keys (if any).
  - Real adversaries may have limited capabilities

Network Security Attacks

- Network security characters Alice, Bob, Eve and Mallory back again
- Alice and Bob want to exchange messages securely while Eve (an eavesdropper) and Mallory (a malicious attacker) are waiting to compromise their communications
  - In real world Alice and Bob ->   Webservers and clients, two email clients, DNS servers etc.
- Eve can capture (eavesdrop) the traffic and extract confidential information such as passwords, credit card details etc. , while Mallory can launch a man in the middle (MiTM) attack by placing itself between Alice and Bob
  - Real world Eve and Mallory -> compromised gateways/routers/access-points, or malware

Network Security Attacks

- Denial of Service (DoS) : attacker sends an avalanche of bogus packets to a server to keep the server constantly busy or clog up the access link

- Distributed DoS (DDoS): attack a large number of compromised devices (bots)
  - Mirai is an example of DDoS in 2016, compromised Linux-based IP cameras, utility meters, home routers and others
  - Done by exploiting weak authentication configurations including use of default passwords

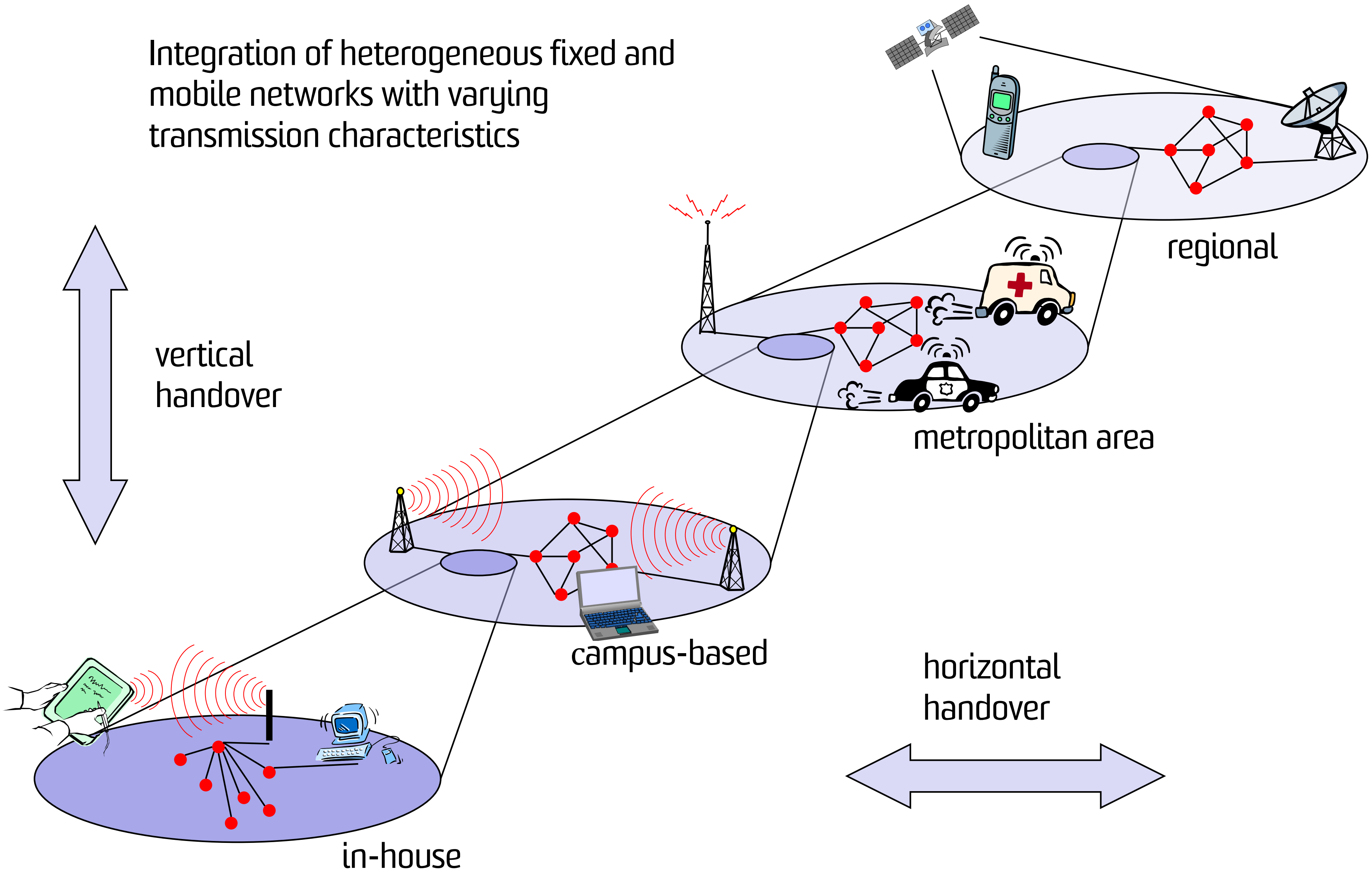
- In IP spoofing attacks: impersonate as an authorised user by crafting a packet with forged IP address and adjusting certain other fields to make it look legitimate

Desirable properties of secure communication

- *confidentiality*: only sender, intended receiver should "understand" message contents
- *authentication:* sender, receiver want to confirm identity of each other
- *message integrity:* sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
- *non-repudiation: no one (including the sender) can deny that message was sent by the sender*
- *access and availability*: services must be accessible and available to users

Emerging Network Trend

Integration of heterogeneous fixed and mobile networks with varying transmission characteristics



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
    - *We need to learn fixed network techniques to be able to protect wireless networks .*

What is different?

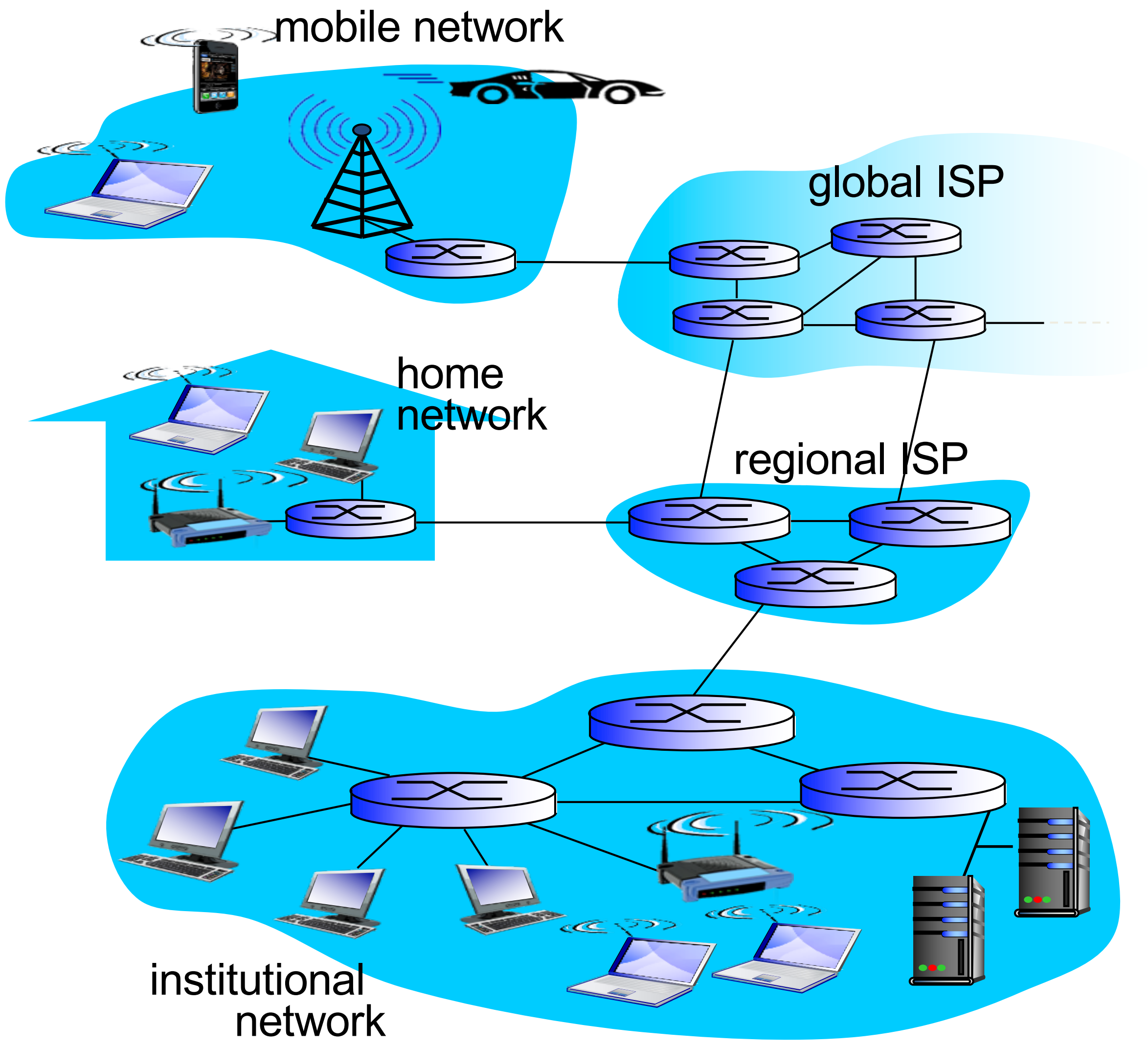
- Wireless Network is more accessible for eavesdropping
- The lack of a physical connection makes it easier to access services
- Authentication has to be re-established when the mobile device moves
- Key management gets harder as peer identities can not be pre-determined
- The location of a device / 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

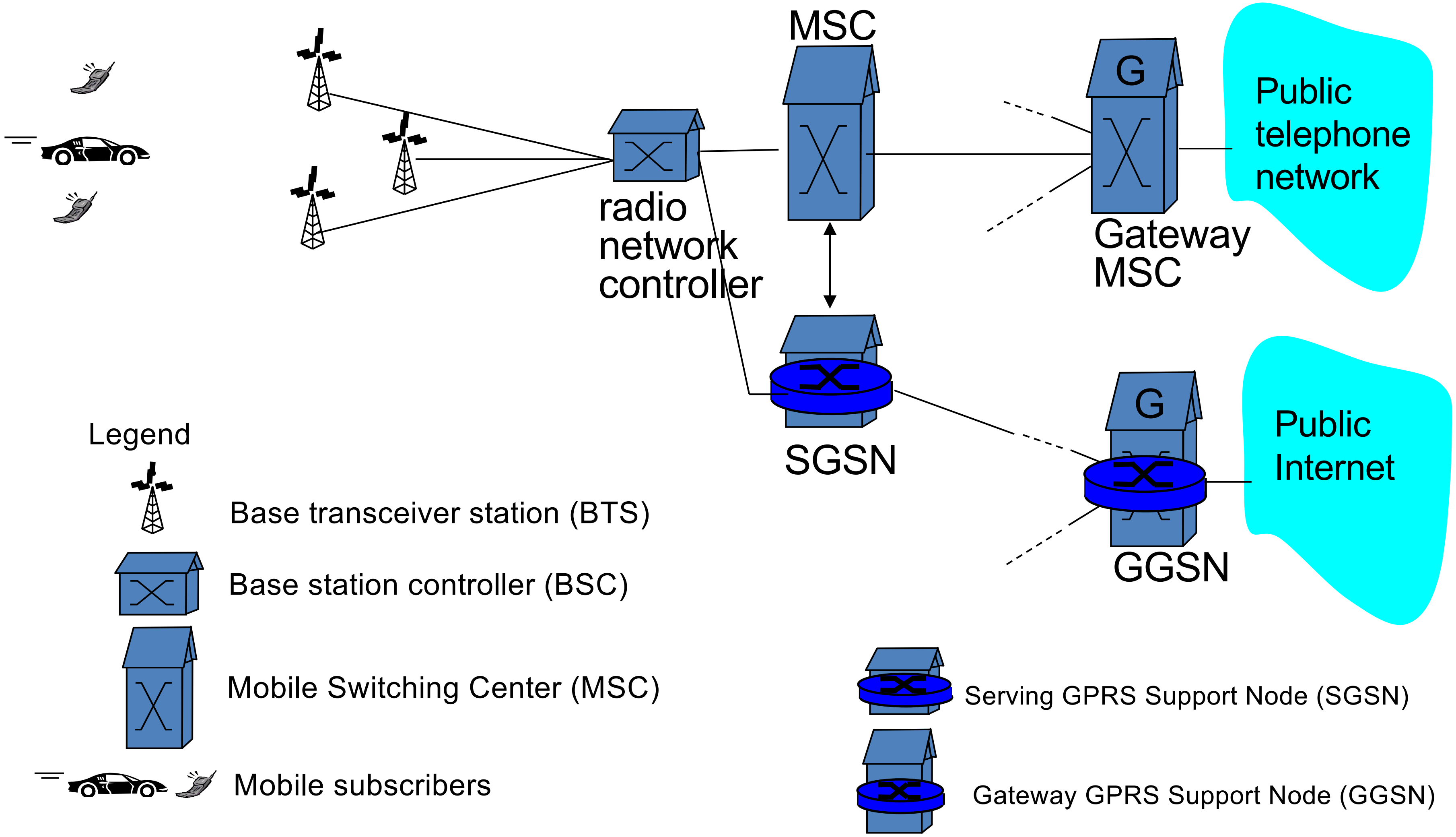
Review of Network Architecture and Associated Security Challenges

Internet architecture



déjà vu; 3331/9331

Cellular network architecture



MSC

G

Public telephone network

radio network controller

Gateway MSC

G

Public Internet

SGSN

GGSN

Legend

Base transceiver station (BTS)

Base station controller (BSC)

Mobile Switching Center (MSC)

Mobile subscribers

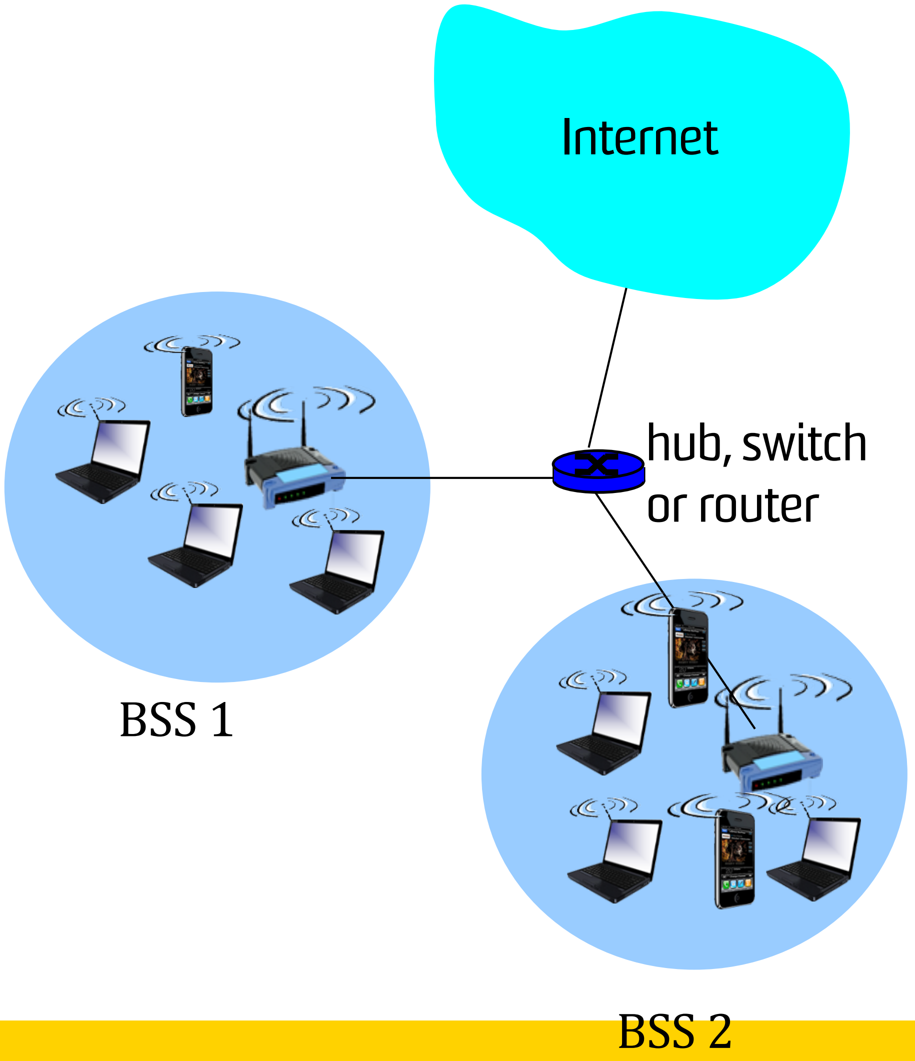
Serving GPRS Support Node (SGSN)

Gateway GPRS Support Node (GGSN)

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



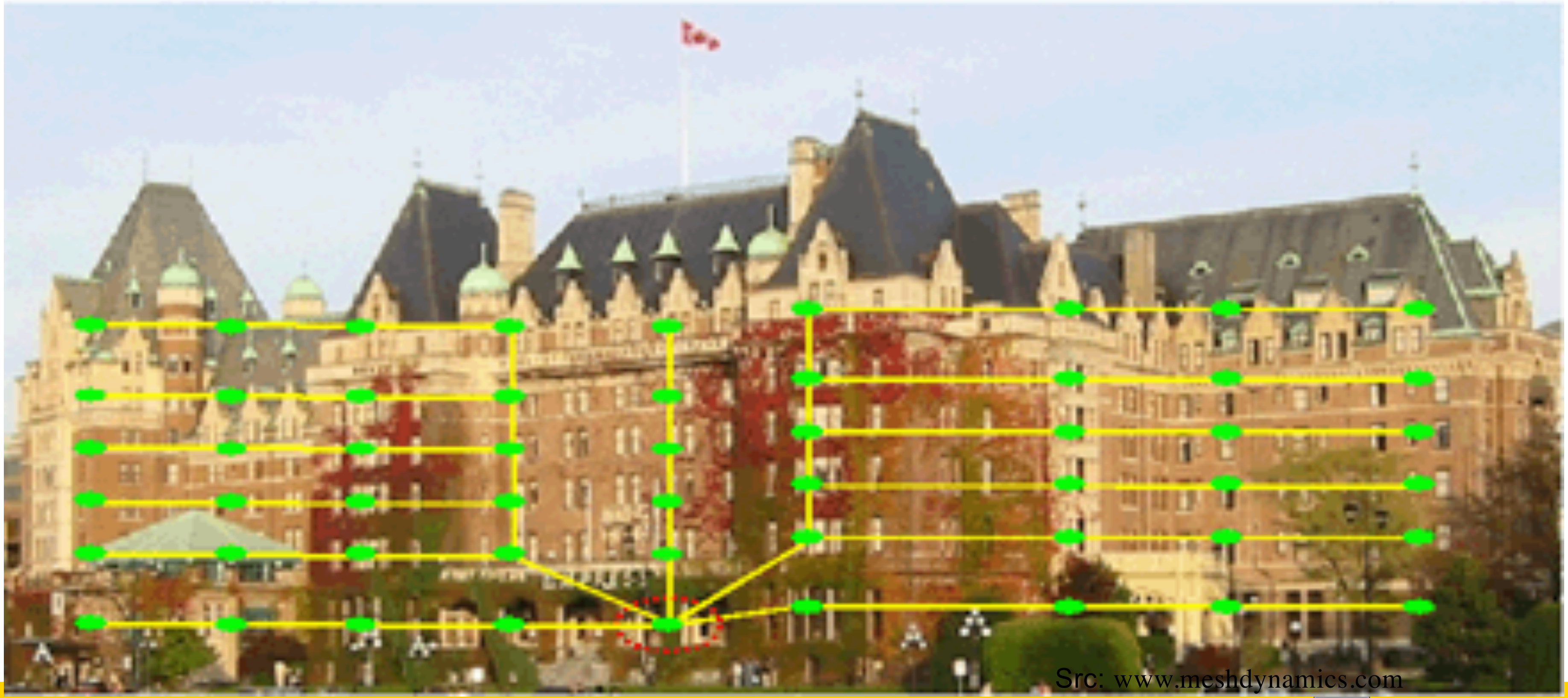
- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka “cell”) in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

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

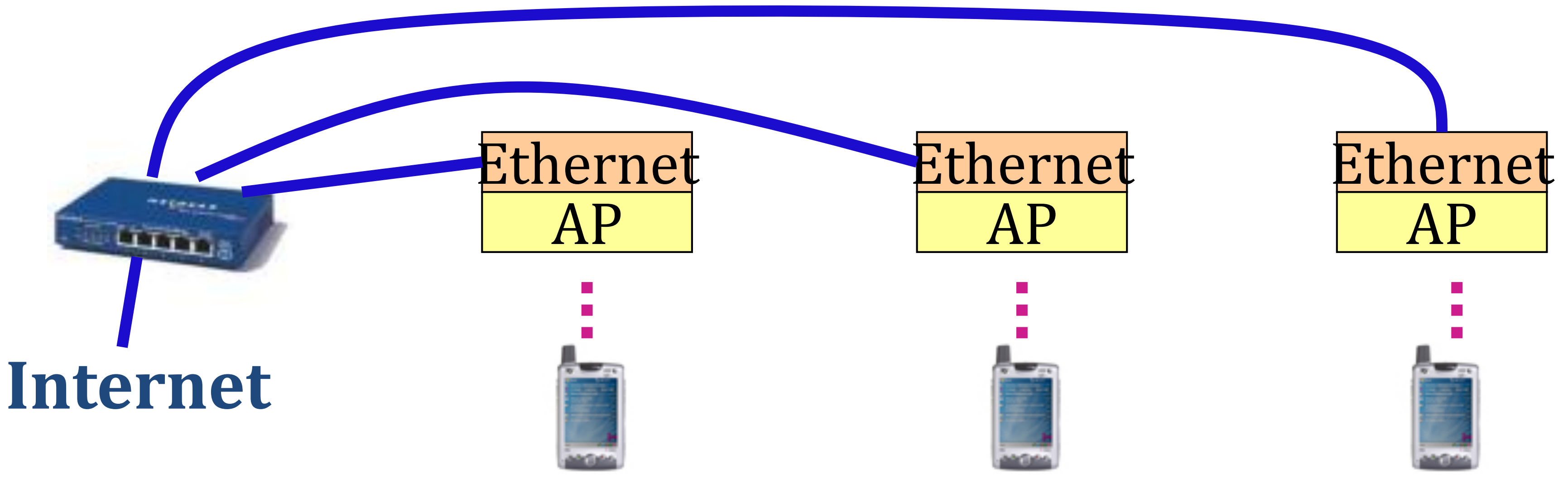
Hotel HotZone with MeshDynamics All Wireless Switch Stacks



Src: www.meshdynamics.com

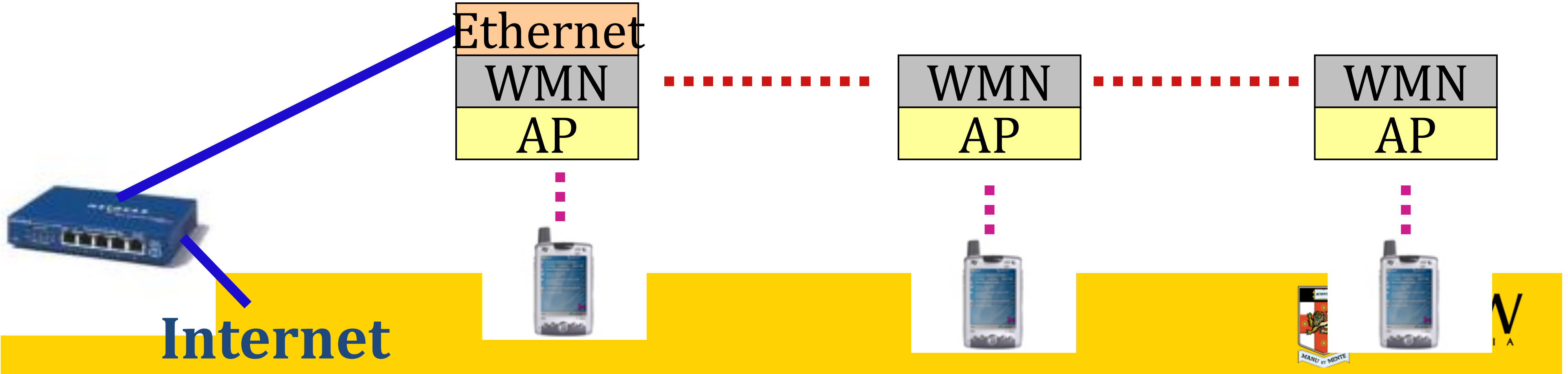
WLAN:

(AP = access point)



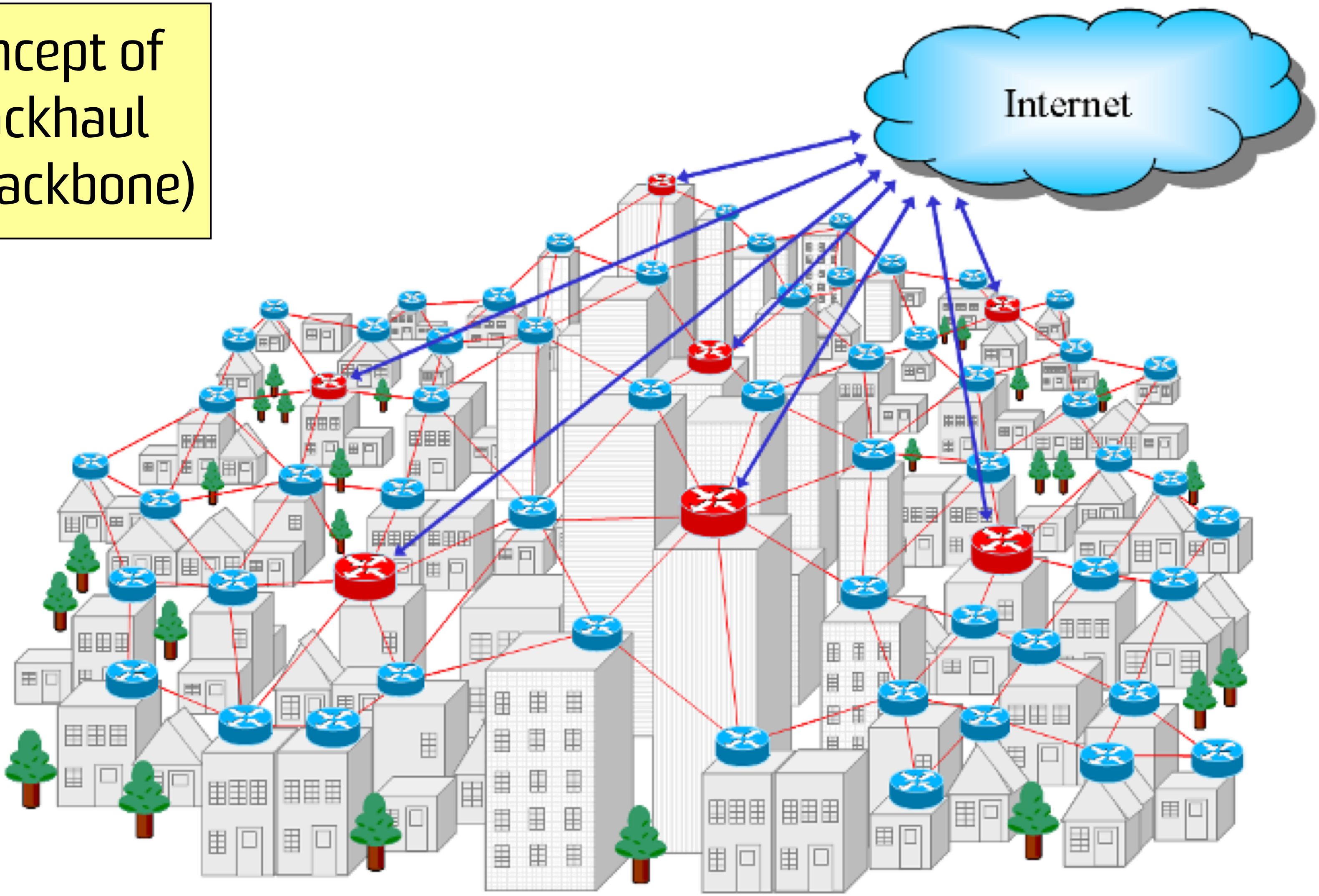
Wireless mesh network (WMN):

Features: Mesh routers; Multi-hop routing



City-wide WiFi

Concept of Backhaul (or backbone)



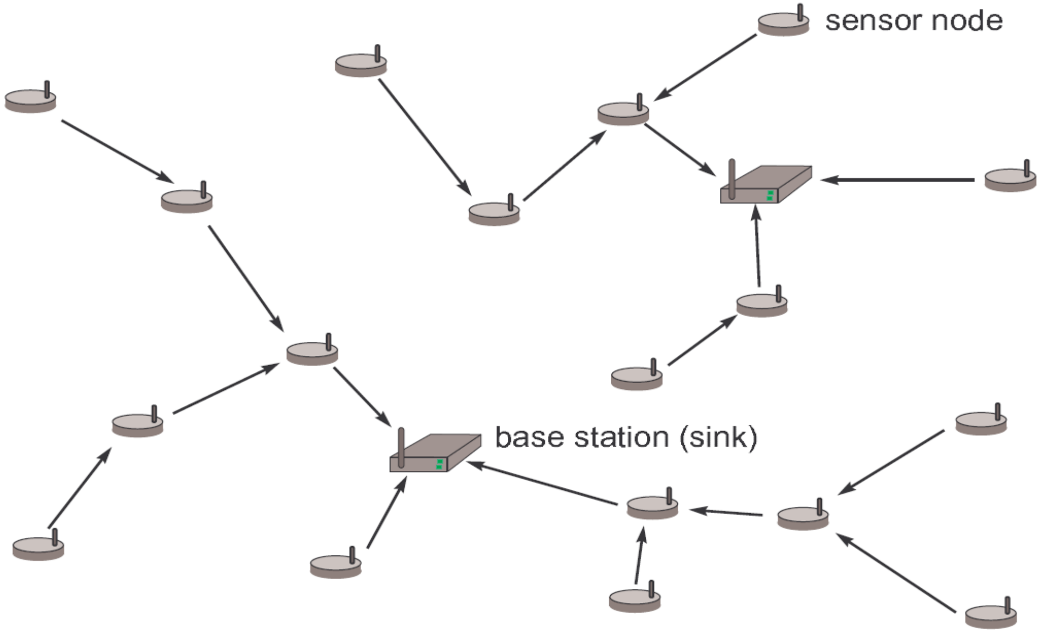
Source: M. Sichitiu

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.

Wireless 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:



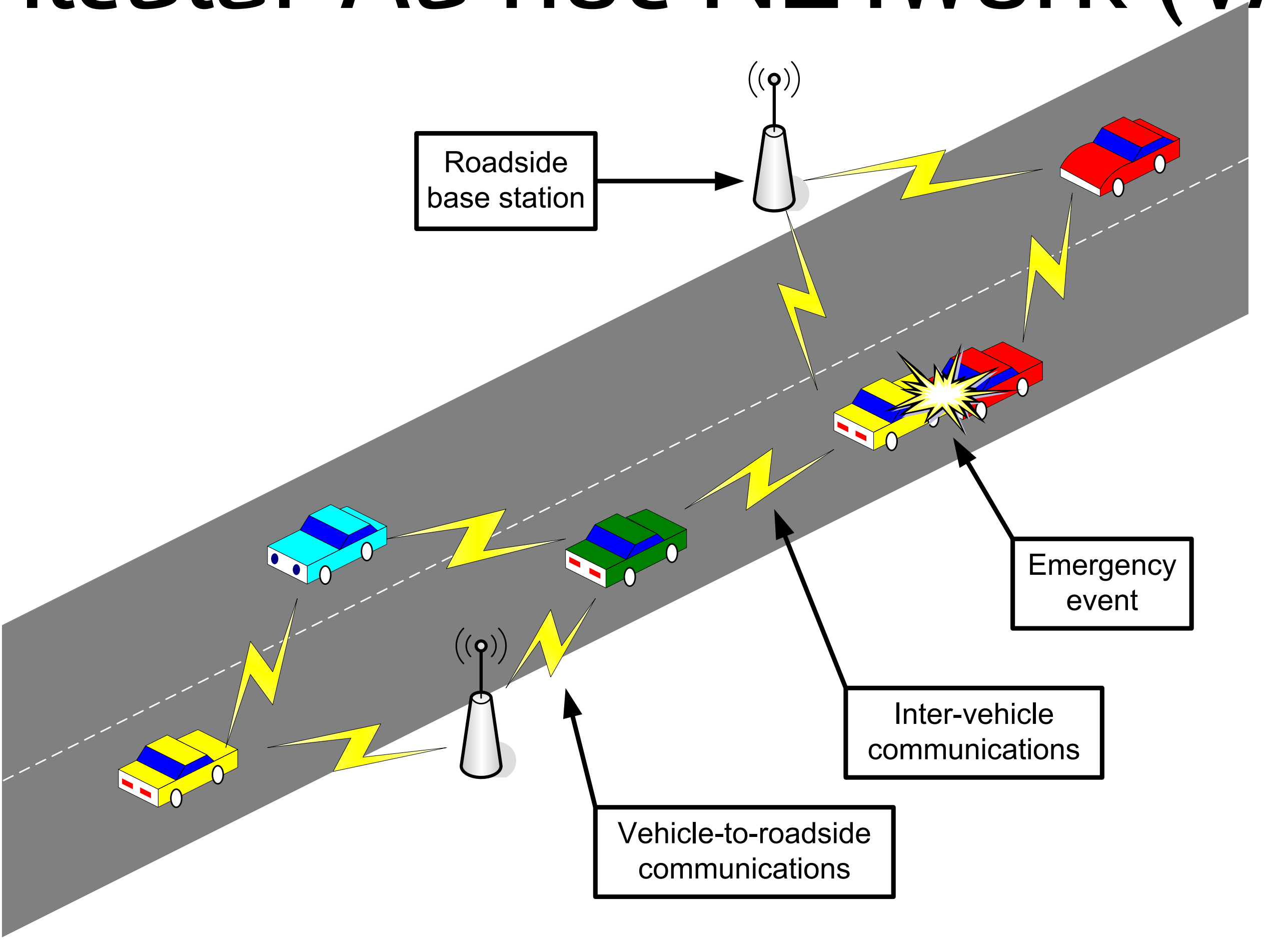
Sensor Network Security

- 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)


Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications

- Communication: typically over the Dedicated Short Range Communications (DSRC) (5.9 GHz)
- IEEE 802.11p: *applications such as toll collection, vehicle safety services, and commerce transactions via cars*

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

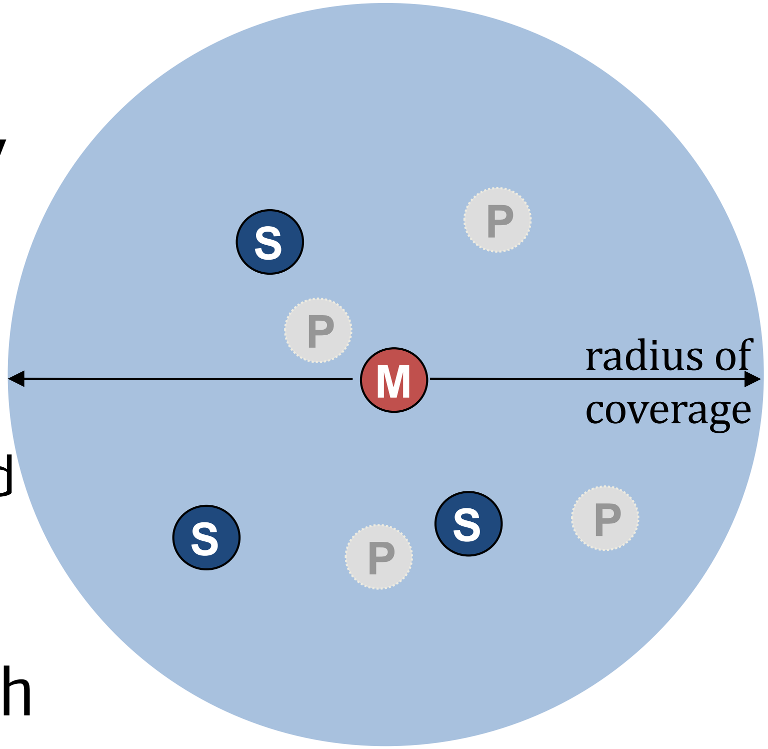
- Most of these problems can be solved by providing appropriate **information** to the driver or to the vehicle

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



M Master device

S Slave device

P Parked device (inactive)

PAN Security

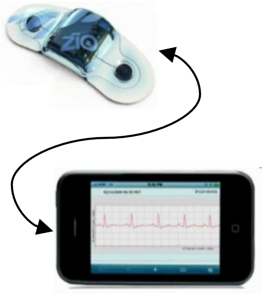
- Short-range communications, master-slave principle

- 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 IoT device projected to grow to more than 420 million devices by 2014.
- Security is critical because these devices generate medical data, and challenging given that they have low power and computation capabilities.



1. Apple iPhone SensorStrip

2. Nike + iPod Sports Kit

3. Nokia Sports Tracker

4. Toumaz Life Pebble

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.*