Corso Professionalizzante di Specializzazione (3 CFU)

Ingegneria delle Telecomunicazioni, Ingegneria Informatica, Ingegneria dei Sistemi di Controllo e dell'Automazione, Informatica

WSN and VANET Security

Course Intro

Ing. Marco Pugliese, Ph.D., SMIEEE
Senior Security Manager UNI 10459-2017 ICMQ cert. 25-00238
marco.pugliese@univaq.it

April 4th, 2025

About me

- Laurea degree in Electronic Engineering, University of Roma ”La Sapienza”
- Ph.D. degree in Electrical Engineering and Computer Science, University of L'Aquila
- Registered Civil and Industrial Engineer – Roma district
- Coordinator for Safety in Workplaces (CSP/CSE) according to D.lgs. 81/08.
- Master on Security Management at CE.S.INT.E.S. (CEntro Studi in INTelligence Economica e Security Management), University of Roma ”Tor Vergata”
- Certified UNI 10459:2017 “Senior Security Manager” cat. III
- Auditor for UNI 10459:2017 certification process
- Associated at the Center of Excellence EX-EMERGE, University of L’Aquila
- Member of the Board of Directors, Secretary at A.I.PRO.S. (Associazione Italiana Professionisti della Sicurezza), head of Department "Vehicular and Transport Network Security"
- Lecturer on “Wireless Sensor and Vehicular Networks Security”, Specialization Seminar, University of L’Aquila
- Lecturer on "Security Management applied to D.lgs. 231/01 and D.lgs. 81/08“, Course of Qualification in Security Management, Fondazione ICSA (Intelligence Culture and Strategic Analysis)
- IEEE Senior Member (SMIEEE)
- Over 25 years working on ICT and system security with leading industries and service operators, over 40 scientific contributions

See my website https://mpugliese.webnode.it

The Course

- **Recipients:** potential recipients are students of the “laurea magistrale” as well as students of the “laurea triennale” master’s degree courses regularly enrolled in the third year of the course, in Telecommunications Engineering, Computer Engineering, Control Systems and Automation Engineering, Computer Science . Participation in the course and the achievement of eligibility allow you to acquire 3 CFU in type F. Up to a maximum of 30 participants will be admitted, selected on the basis of the number of credits acquired. The seminar is also suitable for students of the PhD course in Engineering and Information Sciences. External auditors are also allowed.

- **Duration**: 28 hours (lessons of 4 hours a day for 7 days)

- **Lecturer**: Ing. Marco Pugliese, Ph. D., Sr. IEEE Member, Sr. Security Manager UNI 10459:2017

The Course

Part I. Security Analysis applied to WSN and VANET

- **Lecture I.1 The Framework of Security Management:** from Risk to Security Management: Security Management Process, Approaches for Risk Evaluation, Techniques for Risk Evaluation, P-I Matrix and isorisk curves, FTA – CVSS, NIST SP 800-30 Guide for Conducting a Risk Assessment. Security management in the automotive domain: ISO / SAE 21434, Threat Analysis and Risk Assessment (TARA), Cybersecurity Risk Quantification technique EVITA, Guide line for TARA execution using EVITA. Reference Cyber Security functions: Security metrics, Timing constraints, Cyber Risk Mitigation.
- **Lecture I.2 The case of WSN**: Definition of WSN. Applications, Design Issues, Reference WSN Architecture. IEEE 802.15.4.
- **Lecture I.3 The case of VANET**: Definition of VANET. VANET vs. MANET. VANET Applications. Inter-Vehicular Communications Systems. Intra-Vehicular Communications Systems
- **Lecture I.4 Threats and Attacks against WSN and VANET**: Classification of Cyber attackers, Classification of attacks, Cyber attacks against WSN, Cyber attacks against VANET, Cyber attacks against Intra-Vehicle Communications, Classification of the Security Functions

The Course

Part II. Mitigation Measures: Security Techniques applied to WSN and VANET

- **Lecture II.1 Passive Security Functions**: Mathematical background: Kerckhoff's Principle, the Shannon's lessons, Modular Arithmetic, Generating Prime Numbers, Generating Pseudo-random Numbers, Elliptic Curve (EC) Algebra, Discrete Logarithm Problem and its EC version, Pairings on Elliptic Curves, Zero Knowledge Proof. Techniques: Ciphering, Hash functions, Message authentication codes, Digital signatures. Key Establishment Protocols: Symmetric KEP, Asymmetric KEP, ID Based KEP, Hybrid KEP, Authentication of public key.

- **Lecture II.2 Active Security Functions**: Mathematical background: Dynamic Systems, Discrete Events Dynamical Systems (DEDS), The Intrusion Detection Problem: DEDS Modeling using Petri Nets, Mapping PN into a finite automaton (FA), Identification of observables and hidden states, State Sequence Estimation. Behavior Classifier. Information Theoretic Model of an Intrusion Detection System. Techniques: Machine Learning, Anomaly Detection System, Audit data, Representation Model: Rules Based Techniques, Statistics Based Techniques. Classification Model.

The Course

Part II. Mitigation Measures: Security Techniques applied to WSN and VANET

- **Lecture II.3 Security Functions made in Univaq. TAKS/ECTAKS/WIDS/MVET schemes:** TAKS / ECTAKS Scheme: TAKSx driving ideas & main features, Authenticated Network Topology. TAKS Definition: TAK Equations, Geometric Interpretation of TAK, TAKSx properties. From TAKS to ECC-based TAKS (ECTAKS): ECTAKS Local Configuration Data, ECTAKS vs. ECDHE. ECTAKS Encryption / Decryption Scheme, ECTAKS Sender Signature Scheme. Intro to ECTAKS Security Proof. Selective Secure Clusterwise Communications. TAKSx Release Chronology. WIDS (WPM based IDS) Driving Ideas & Main Features, WIDS Reference Architecture, WIDS Technique: Basic Network Threats, Examples of Anomaly Rules, WPM-based Threats Models, Aggregated Threats Models, Security Analysis. WIDS for IEEE 802.15.4 systems. MVET (Mean Variance Estimation Technique), Driving Ideas & Main Features, MVET Reference Architecture, MVET Technique, Performance Analysis.
- **Lecture II.4 VANET Privacy Functions:** V2X Communications Security: Architecture, Analysis, Privacy preserving solutions. Intra-Vehicle Communications Security: Vulnerabilities, Countermeasures.

Risk Based Thinking

- **Risk** is defined as the "***effect of uncertainty on objectives***" (ISO 31000:2018).
  - **uncertainty** deals with the intrinsic stochastic nature of any organization / system with some complexity.
  - **objectives** can have different aspects (financial, health, safety, environmental) and can apply at different levels (strategic, organization-wide, project, product, process).

- Therefore **uncertainty infers risks.**

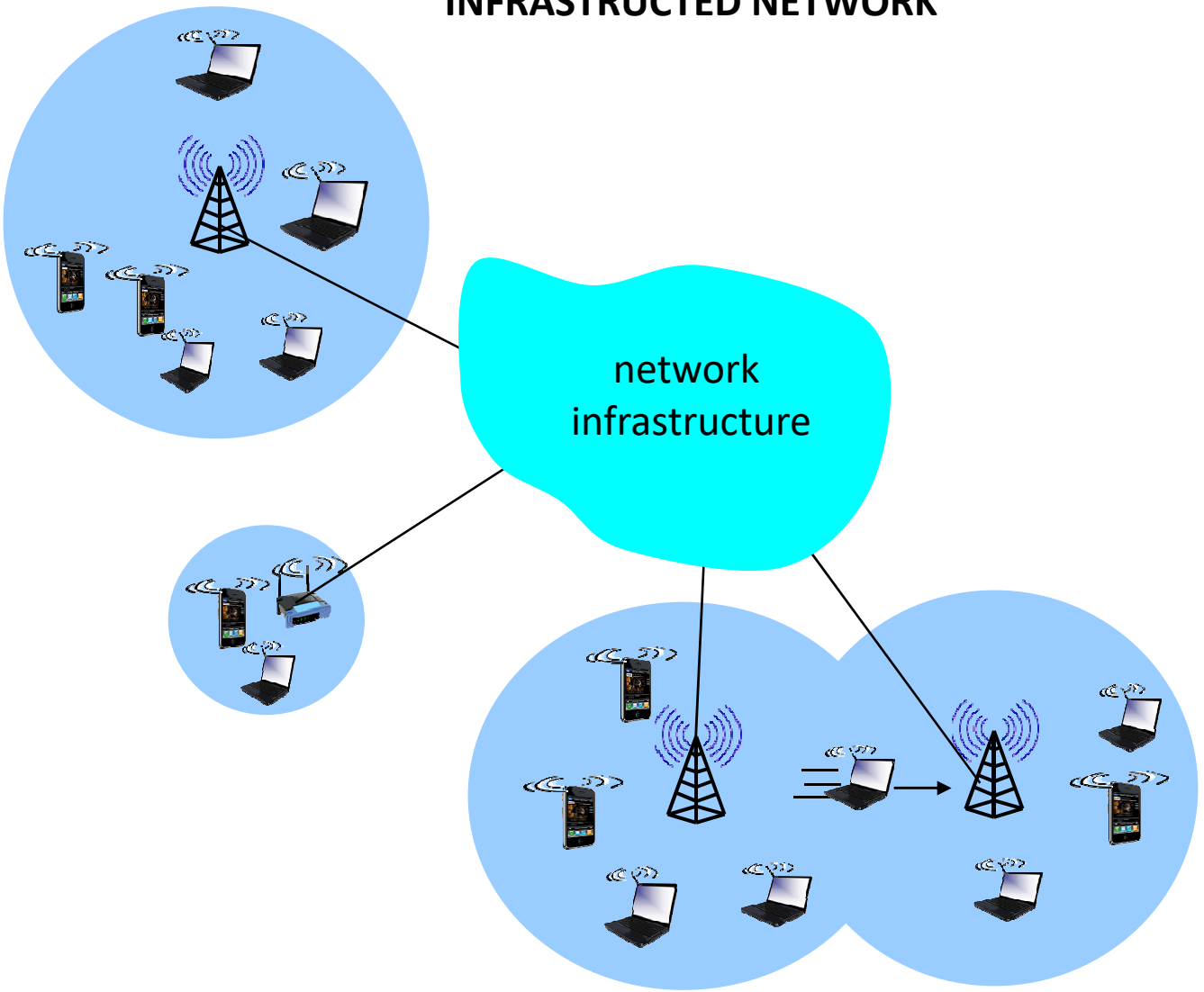
- **Risk Management** are the "*coordinated activities to direct and control an organization with regard to risk*" (ISO 31000:2018).

- **Security Management is a specific instance of Risk Management** when effect is a deviation from the expected positive.

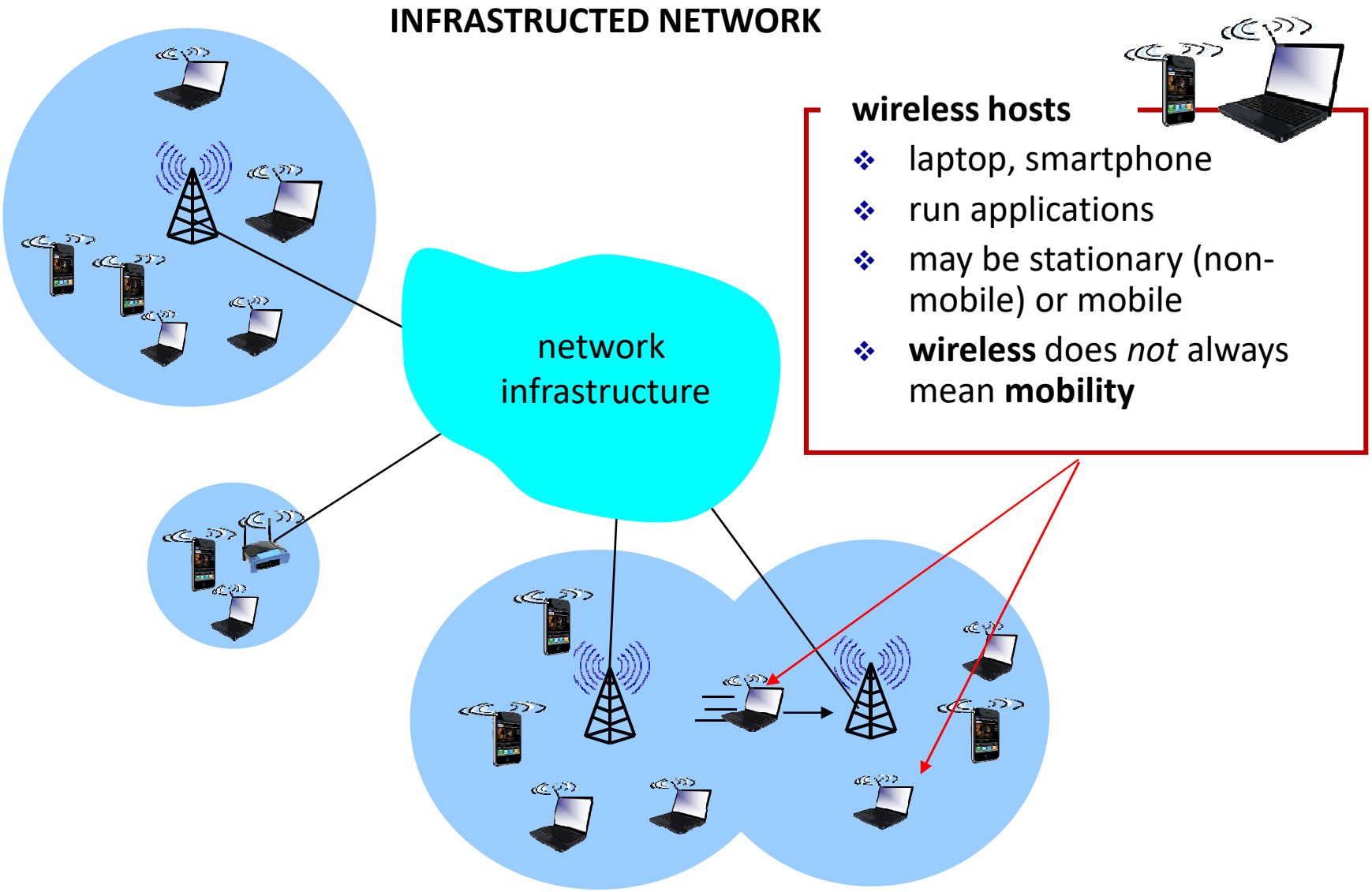
- **"Risk Based Thinking" defines a risk-oriented approach for any phase in the life cycle of organizations and systems.**

Elements of a wireless network

INFRASTRUCTED NETWORK

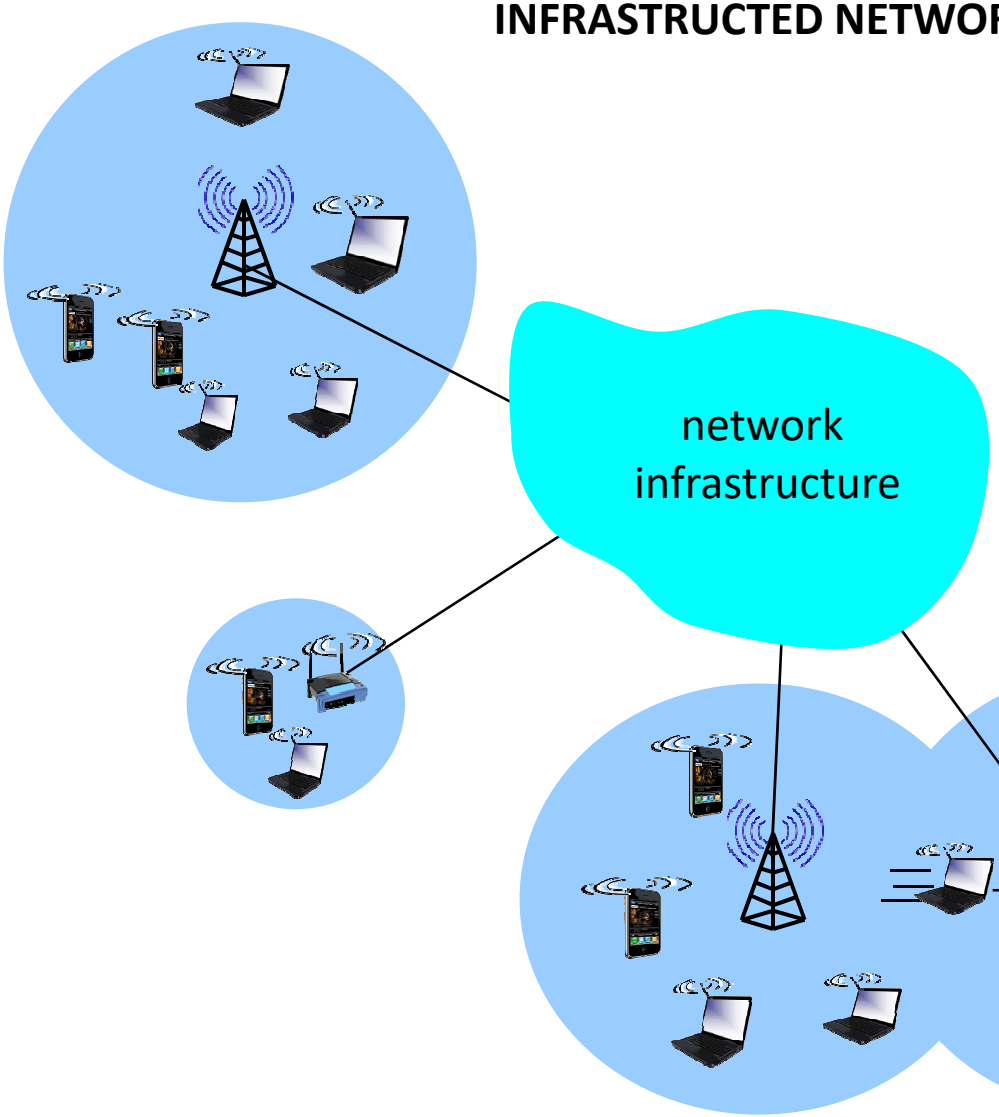


Elements of a wireless network



Elements of a wireless network

INFRASTRUCTED NETWORK

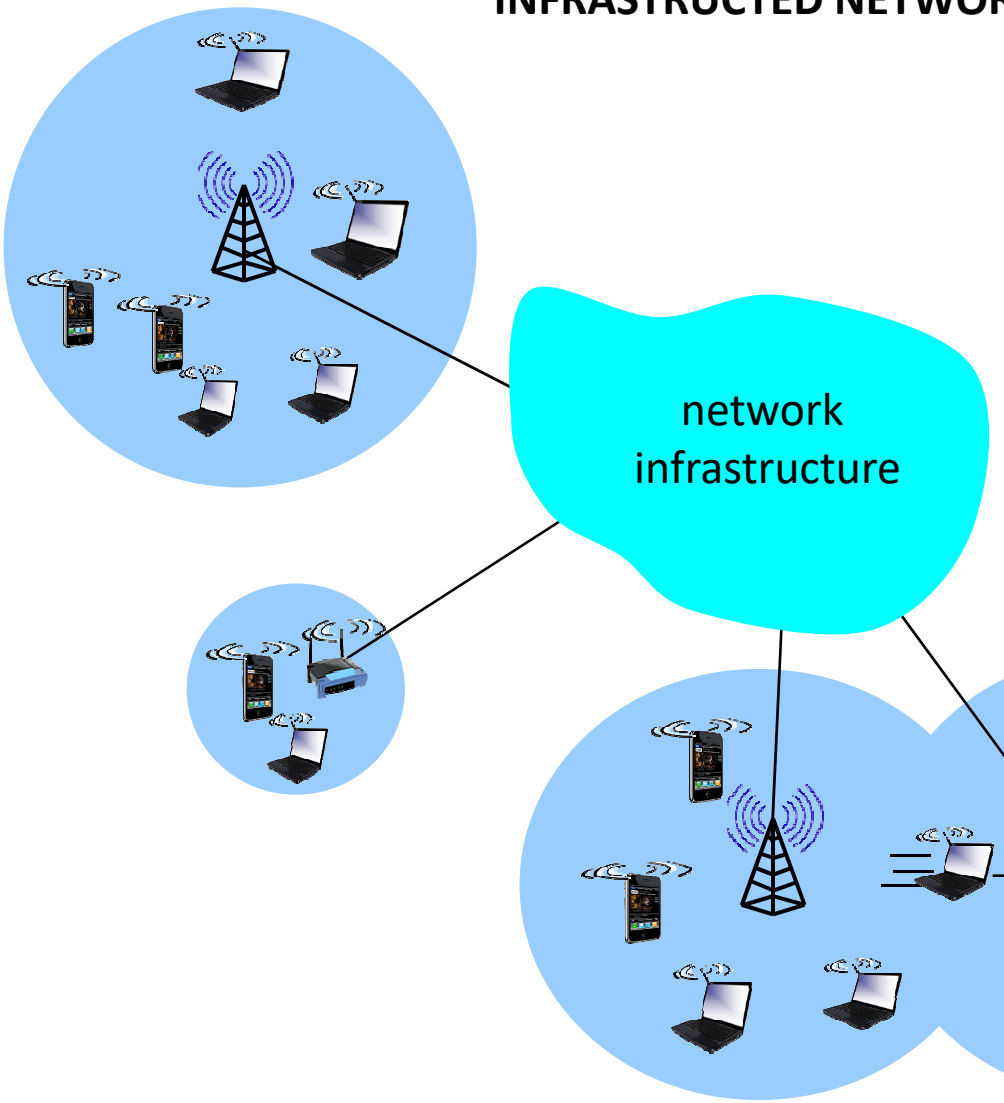


base station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless hosts) in its "area"
  - e.g., cell towers, 802.11 access points

Elements of a wireless network

INFRASTRUCTED NETWORK

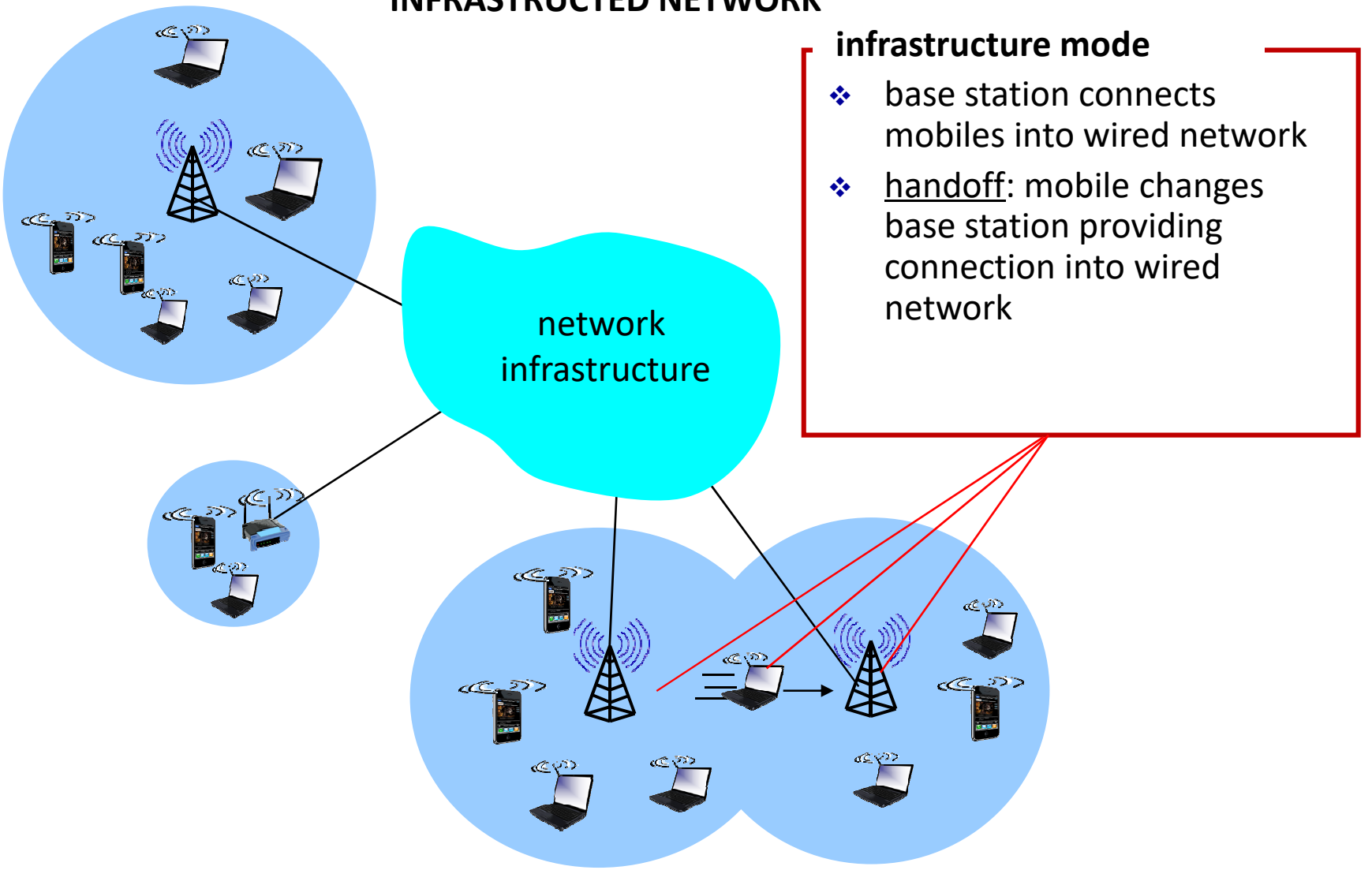


wireless link

- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access control (MAC) protocol coordinates link access
- various data rates, transmission distance

Elements of a wireless network

INFRASTRUCTED NETWORK

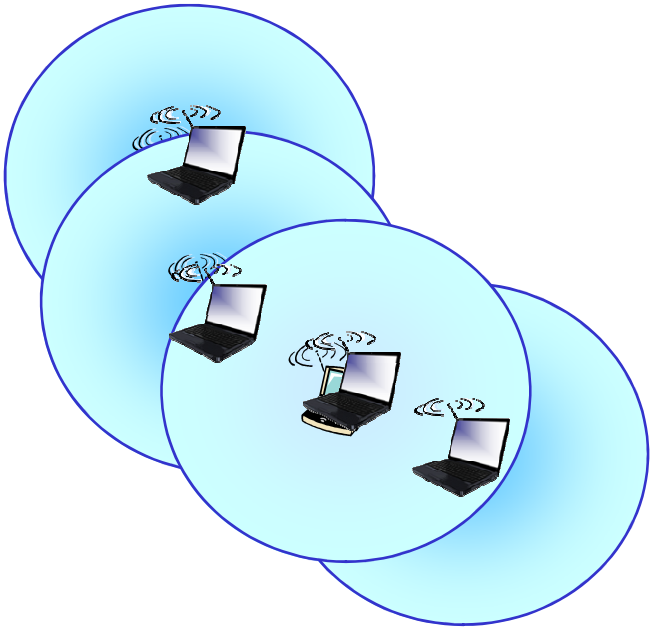


infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Elements of a wireless network

INFRASTRUCTERELESS NETWORK

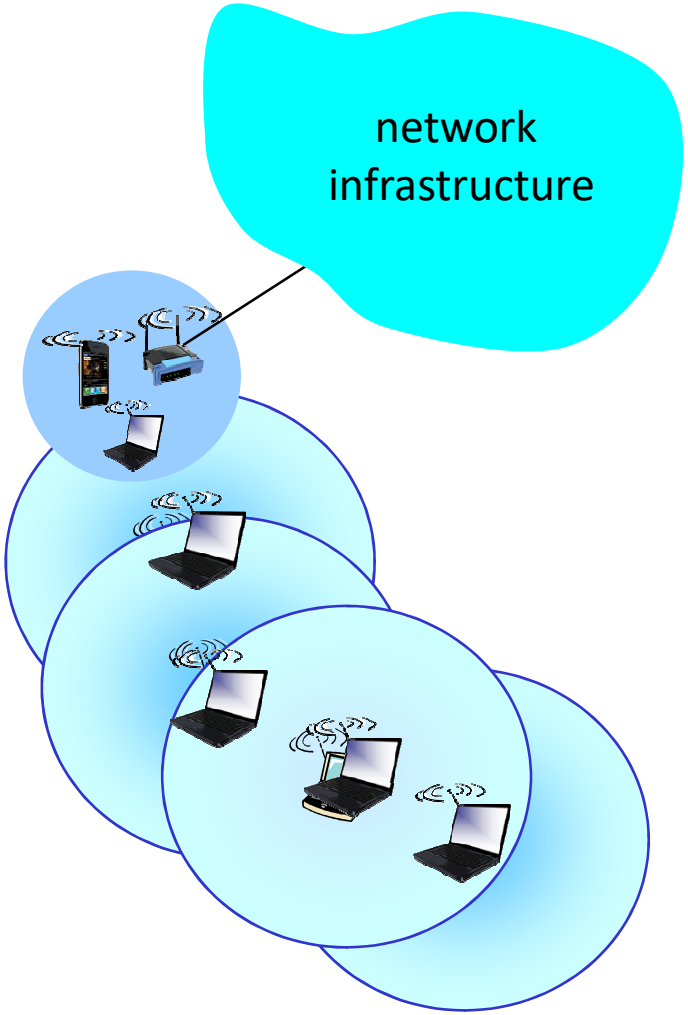


(pure) ad hoc mode

- **no base stations –only peer to peer communications**
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Elements of a wireless network

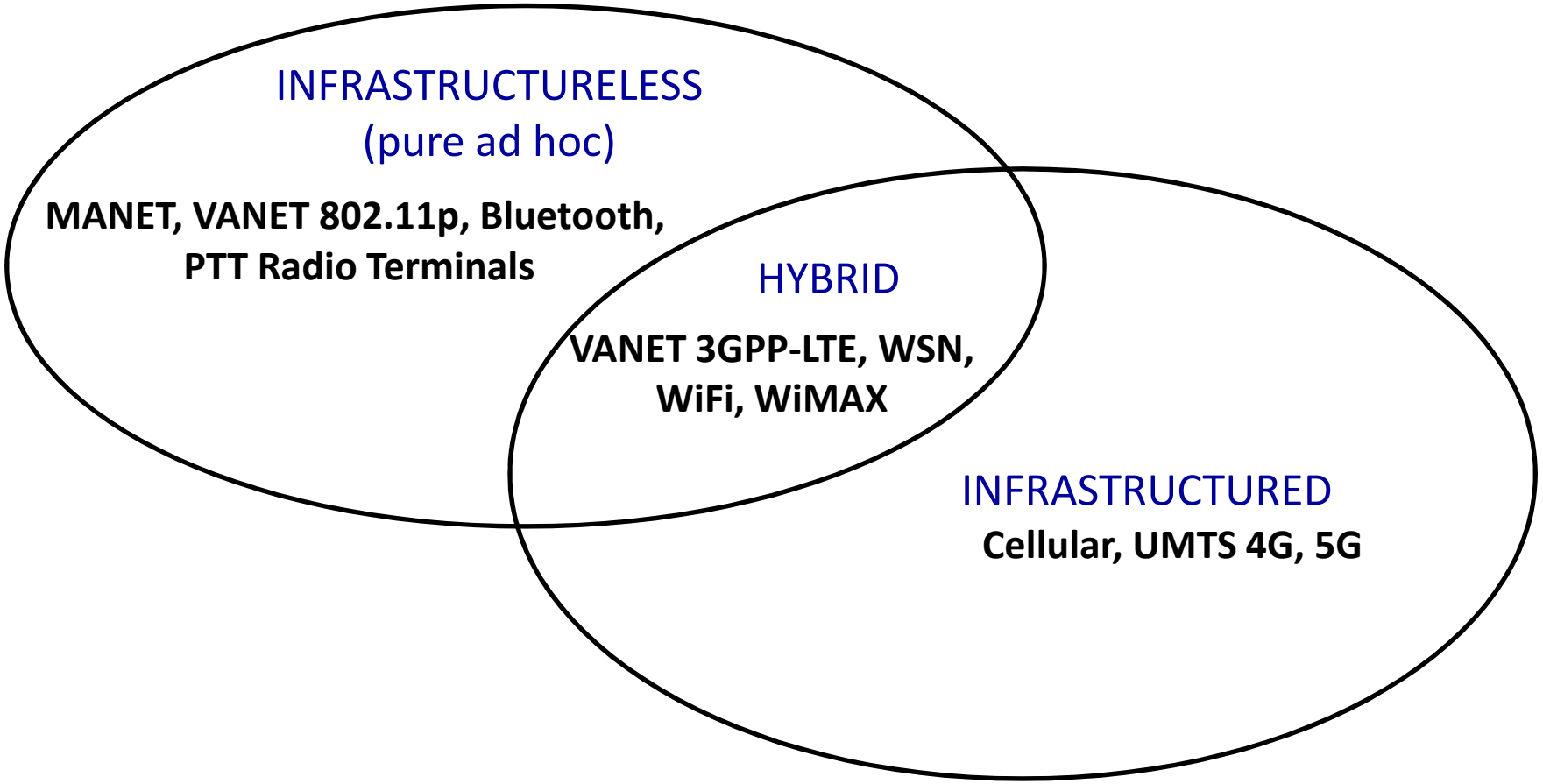
HYBRID NETWORK



(hybrid) ad hoc mode

- **An Access Point is foreseen**
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless network taxonomy



WSN vs. MANET vs. VANET

- **Ad hoc network (ANET):** continuously self-configuring, self-organizing, infrastructure-less network of radio connected devices (nodes). It is sometimes known as “on-the-fly” network or “spontaneous network”.
  - **Wireless Sensor Network (WSN):** nodes are fixed or nomadic sensor units with TX/RX and with energy-constrained processing and storage capabilities. Hierarchical network topology (clusterwise), convergecast data communication patterns.
  - **Mobile Ad hoc NETwork (MANET):** nodes are mobile not necessarily energy-constrained as sensor nodes. Mobile nodes are routers (multihop network) and hosts. Random topology changes rapidly and unpredictably. No hierarchies among nodes (peer-to-peer networks).
  - **Vehicular Ad hoc NETwork (VANET):** class of MANET where mobile nodes (i.e. vehicles) are constrained into predefined paths (roads). However VANET can be also considered infrastructured (3GPP approach to V2X through new V2V interfaces).

    V2I: communications nearby fixed equipment (Road Side Units, RSU).

    V2V: communications among vehicles for fast delivery of real time information (typically traffic, accident and in general alarm info).

    Intra-vehicle: communications among internal devices (ECU) and the edge device (On Board Unit, OBU).

    VANET security management include privacy preservation (GDPR in UE).