Wireless Computer Networks

Course code: 0790322
Dr. Firas Najjar
Office : 7318
Email:fnajjar@philadelphia.edu.jo

Course Information (cont.)

- **Textbook & references:**

  This is the required textbook:

  Security in Wireless Communication Networks - by Yi Qian, Feng Ye, Hsiao-Hwa Chen, Wiley-IEEE Press, December 2021 (ISBN: 978-1-119-24436-3).

  .

Wireless Network Introduction

Objectives

- List different wireless data applications
- Explain the advantages and disadvantages of wireless technologies
- Explain the roles of the different standards organizations

Wireless Applications

- Wireless communications are very common in all areas
- Several sectors use wireless more extensively than others:
  - Education
  - Business
  - Industry
  - Travel
  - Public safety
  - Health care

Education

- Educational institutions were among the first to adopt wireless technology
  - Teachers can create presentations on a laptop and carry them into any classroom where it will connect automatically to the campus network
  - Students can easily connect wirelessly to a campus network
- WLAN technology translates into cost savings for schools
  - Reduces need for wiring and infrastructure
  - Fewer computer labs necessary

Business

- The introduction of wireless access in conference rooms provides all employees with a mobile office
- Employees no longer have to compete for an available wired connection or carry cables with them
- A Cisco study showed that wireless communications increased productivity by 86 minutes per day per user
- Small office/home office (SOHO) business can also benefit from wireless data communications

Industry

- Examples of wireless data transmission can be found in the fields of construction, warehouse management, and manufacturing
- Construction examples:
  - Construction equipment (bulldozers and earth graders) have wireless devices that turn them into smart machines capable of precise positioning using a **global positioning system (GPS)**

Figure 1-2 GPS on bulldozer

Industry

- Warehouse Management examples:
  - Forklift trucks can be outfitted with wireless equipment and employees can wear portable wireless inventory devices to scan bar codes
  - **Warehouse management system (WMS)** software manages all warehouse activities
    - WMS is tied into network so managers have ready access to up-to-the-minute statistics
  - **Radio frequency identification (RFID)** tags emit a wireless data signal containing an ID number
    - Works with WMS to track inventory

Industry

- Manufacturing examples:
  - RFID tags are often used
  - RFID Used for inventory and security

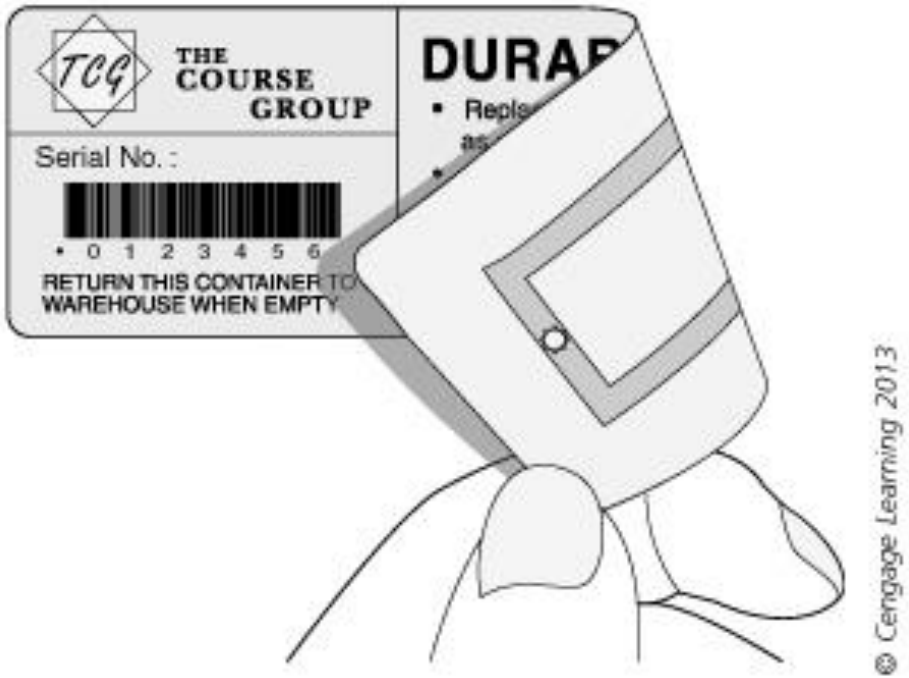

Figure 1-4 RFID tag

Travel

- Airlines, commuter rail lines and even ferry boats are now offering wireless data access
- Airlines use wireless technology for communication with aircraft and even for flight maintenance
- *Vehicle-to-vehicle (V2V)* communications uses both GPS and wireless to create a network that allows cars to communicate with one another
  - Can alert drivers of accidents or traffic hazards ahead of them
  - Can also be used to control traffic jams

Public Safety

- Public safety departments using WLANs to communicate information with public safety vehicles
  - Large volumes of data can be quickly downloaded to vehicles
    - e.g., building floor plans, photographs of criminal suspects, and maps

Health Care

- Wireless LAN point-of-care computer systems allow medical staff to access and update patient records immediately
  - Document patient's medication administration immediately
  - Extensive use of RFID tags
    - Identify healthcare professionals, patients, medications
  - System verifies that medication being administered to correct patient in correct dosage
    - Eliminates potential errors and documentation inefficiencies

Health Care

- Documentation process takes place at bedside where care delivered
  - Improves accuracy
- Hospital personnel have real-time access to latest medication and patient status information
- Wireless technology also used in other medical areas:
  - e.g., video pills

Figure 1-6 Video pill

Wireless Advantages and Disadvantages: Advantages

- **Mobility:** Primary advantage of wireless technology
  - Enables individuals to use devices no matter where users roam within range of network
  - Increasingly mobile workforce is characteristic of today's business world
  - WLANs give mobile workers freedom while allowing them to access network resources
  - "Flatter" organizations: WLANs give team-based workers ability to access network resources needed while collaborating in team environment

Wireless Advantages and Disadvantages: Advantages

- **Access**: wireless can provide network access to areas where previously none existed
  - **hotspot**: Locations where wireless data services are available
  - **Municipal networks**: hotspots typically found in downtown areas, parks and recreation areas and other high-traffic areas
  - Advantages of municipal networks:
    - More attractive to businesses
    - Local police, fire, and municipal workers can use them
    - Provide high speed Internet access for free or low cost

Wireless Advantages and Disadvantages: Advantages

- **Connectivity**: Wireless technologies can provide improved service, extend the reach of networks, and provide a less expensive alternative to wired technologies
  - **Wireless ISP**: provides wireless data access directly to the home instead of a cable or DSL provider
  - **Backhaul connection**: an organization's internal infrastructure connection between two or more remote locations
    - Wireless networks can be used eliminating the costs associated with leasing lines or installing fiber optic cables

Wireless Advantages and Disadvantages: Advantages

- **Deployment:** Installing network cabling in older buildings difficult and costly
  - Wireless LAN is ideal solution
  - Eliminating need for cabling results in cost savings
    - Significant time savings as well
  - Allows offices to reorganize easily
  - Wireless LAN technology eliminates certain types of cable failures and increases overall network reliability

Advantages of wireless data network

Advantage	Example
Mobility	Worker can read e-mail while traveling
Access	User can access Internet at a restaurant
Connectivity	Building-to-building network can be created at significant cost savings
Deployment	Older building can easily have network capacity created without major renovation

Wireless Advantages and Disadvantages: Disadvantages

- **Security:** Wireless signals broadcast in open air
  - Security for wireless LANs is prime concern
    - Unauthorized users might access network
      - Can often pick up signal outside the building
    - Attackers might view transmitted data
    - Employees could compromise network security
      - could install rogue access points
    - Attackers could easily crack existing wireless security
      - Older wireless products have very weak security features

Wireless Advantages and Disadvantages: Disadvantages

- **Radio Signal Interference:** Signals from other devices can disrupt wireless transmissions
  - e.g., Microwave ovens, elevator motors, photocopying machines, theft protection devices, cordless telephones
- **Range of Coverage:** Some wireless signals only have a range of 10 feet while others extend to over 350 feet
- **Slow Speed:** a packet moving through a wireless network is slower than it would be on a wired network

Disadvantages of wireless data network

Disadvantage	Example
Security	Attacker can read sensitive information by picking up wireless signal outside of building
Radio signal interference	Intermittent errors occur on wireless network due to interference
Range of coverage	User cannot access network outside of home
Slow speed	Wireless device times out while trying to download large e-mail attachment

Wireless Network Risks

- Internet-connected devices may be used by nefarious entities to collect personal information, steal identities, compromise financial data, and silently listen to— or watch— users.
- Taking a few precautions in the configuration and use of your devices can help prevent this type of activity

Piggybacking

- Failure to secure your wireless network could open your internet connection to many unintended users.
- These users may be able to conduct illegal activity, monitor and capture your web traffic, or steal personal files

Wardriving

- Wardriving is a specific kind of piggybacking

- In this risk, the attacker drive through cities and neighbourhoods with a wireless-equipped computer— sometimes with a powerful antenna— searching for unsecured wireless

Evil Twin Attacks

- In this attack, an adversary gathers information about a public network access point, then sets up their system to impersonate it.

- The adversary uses a broadcast signal stronger than the one generated by the legitimate access point; then, unsuspecting users connect using the stronger signal.

Evil Twin Attacks Cont.

- it’s easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, and other personal information.
- To avoid this attack Always confirm the name and password of a public Wi-Fi hotspot prior to use. This will ensure you are connecting to a trusted access point.

Wireless Sniffing

- Many public access points are not secured and the traffic they carry is not encrypted.
- This can put your sensitive communications or transactions at risk. Because your connection is being transmitted “in the clear,”
- Special tools can obtain sensitive information such as passwords or credit card numbers.
- To minimize sniffing attack, all the access points you connect to use at least WPA2 encryption.

Unauthorized Computer Access

- An unsecured public wireless network combined with unsecured file sharing could allow a malicious user to access any directories and files you have unintentionally made available for sharing.
- Ensure that when you connect your devices to public networks, you deny sharing files and folders.

Theft of Mobile Devices

- Physically stealing your device, attackers could have unrestricted access to all of its data, as well as any connected cloud accounts.
- To secure you data, use encryptions tools to encrypt your sensitive data
- also it is advisable to configure your device's applications to request login information before allowing access to any cloud-based information.

Internet of Things

- Cars, lighting, healthcare, and home security all contain sensing devices that can talk to other machines and trigger additional actions and other tools that track your eating, sleeping, and exercise habits.
- This technology provides a level of convenience to our lives but the security of these devices is not always guaranteed

Wireless Standards Organizations and Regulatory Agencies

- Several organizations provide direction, standards, and accountability in wireless technology
  - International Telecommunication Union Radio Communication Sector (ITU-R)
  - US Federal Communications Commission (FCC)
  - International Organization for Standardization (ISO)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - Wi-Fi Alliance

International Telecommunication Union Radio Communication Sector (ITU-R)

- ITU-R: responsible for global management of the radio frequency spectrum
- Develops standards for wireless communications systems
  - To ensure most effective use of the radio spectrum

Federal Communications Commission (FCC)

- FCC: serves as the primary regulatory agency for wireless communications in the US
  - Includes communications by radio, television, wire, satellite, and cable
- Other responsibilities include:
  - Processing applications for licenses and other filings
  - Analyzing complaints
  - Conducting investigations
  - Taking part in congressional hearings
  - Representing the US in negotiations with other nations regarding telecommunications issues

International Organization for Standardization (ISO)

- ISO: international body that sets industrial and commercial standards
  - Officially not a government entity
- ISO identifies needs in business and develops standards to address needs
- Goal: make development, manufacturing, and supply of products and services more efficient, safer, and cleaner
- ISO works to make trade between countries easier and fairer

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE: most widely know and influential organization in computer networking and wireless communications field
- Currently involved in revising over 800 standards
- Developers of standards in energy, biomedical, health care, and transportation industries
- IEEE standard for WLANs is typically referred to as IEEE 802.11
  - Variations of the standard: 802.11g, 802.11n, 802.1af

Wi-Fi Alliance

- Initially known as the Wireless Ethernet Compatibility Alliance (WECA) – formed in 1999
- Had three goals:
  - Encourage wireless manufacturers to use the IEEE WLAN technologies
  - Promote and market these technologies
  - Test and certify that wireless products adhere to the IEEE standards to ensure interoperability

Wi-Fi Alliance

- In Oct. 2002 – WECA changed name to Wi-Fi (Wireless Fidelity) Alliance
- Only devices that have passed Wi-Fi Alliance testing are allowed to refer to their products as Wi-Fi Certified (registered trademark)

Summary

- Wireless data communications are in all sectors of the economy and is ideal for reducing operating costs of educational institutions and businesses
- The construction, warehouse management, and manufacturing industries rely heavily on wireless data technologies for scheduling employees, managing inventory, and in the manufacturing process itself
- The travel industry offers Internet access to passengers, installs software updates on planes, and accesses latest maintenance information using wireless communications

Summary

- Advantages to wireless technology include user mobility, providing access to a network where previously none existed, improved connectivity, cost effectiveness, and ease of installation
- Disadvantages to wireless technology include not being as secure as cabled networks, radio signal interference, limited coverage, and slower data transmission speeds
- Four basic types of wireless networks: WPAN, WLAN, WMAN, and WWAN

Summary

- Several different organizations provide direction, standards, and accountability in wireless technology: ITU-R, FCC, ISO, IEEE, and the Wi-Fi Alliance