

Smart Health – CSE 40816

University of Notre Dame
Spring 2020



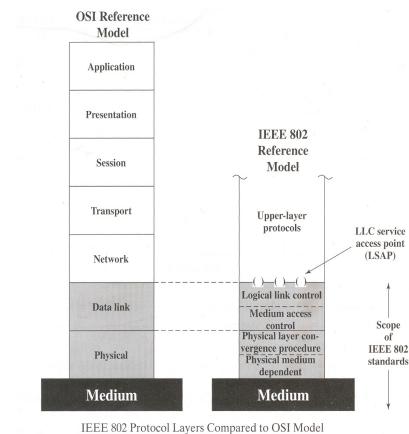
Computer Science and Engineering - University of Notre Dame

Wi-Fi

- Wi-Fi:
 - name is NOT an abbreviation
 - play on “Hi-Fi” (high fidelity)
- **Wireless Local Area Network (WLAN)** technology
- WLAN and Wi-Fi often used synonymous
- Typically in **2.4 and 5 GHz bands**
- Based on **IEEE 802.11** family of standards

IEEE 802.11 Standard

- 802.11 is primarily concerned with the **lower layers of the OSI model**
- **Data Link Layer**
 - Logical Link Control (LLC)
 - Medium Access Control (MAC)
- **Physical Layer**
 - Physical Layer Convergence Procedure
 - Physical Medium Dependent (PMD)



Wi-Fi Alliance Mission Statement

- Non-profit organization
- Certify the interoperability of products and services based on IEEE 802.11 technology
- Grow the global market for **Wi-Fi® CERTIFIED** products and services across all market segments, platforms, and applications
- Rigorous interoperability testing requirements

Certificate & Logo

Wi-Fi® Interoperability Certificate **Certification ID: 24567832AP**



This certificate represents the capabilities and features that have passed the interoperability testing governed by the Wi-Fi Alliance.
Detailed descriptions of these features can be found at www.wi-fi.org/certificate

Certification Date: February 14, 2004
Category: Access Point
Company: Name of Company
Product: Wireless LAN Access Point/Router Model#EX1010
Model/SKU #: EX1010





This product has passed Wi-Fi certification testing for the following standards:

IEEE Standard	Security	Quality of Service	Public Access
802.11a	WPA - Personal	WMM (802.11e EDCF profile)	
802.11b	WPA - Enterprise	WMM (802.11e HCCA profile)	
802.11g	WPA2 - Personal (802.11i)		
802.11n	WPA2 - Enterprise (802.11i)		
Regulatory	Supplicant		
802.11d	EAP-TLS		
802.11h	EAP-TLS/MSCHAPv2		
	EAP-TLS/PP		
	PEAPv0/EAP-MSCHAPv2		
	PEAPv0/EAP-GTC		
	PEAPv0/EAP-MD5		
	EAP-SIM		
	Authentication Server		
	EAP-TLS		
	EAP-TLS/MSCHAPv2		
	EAP-TLS/PP		
	PEAPv0/EAP-MSCHAPv2		
	PEAPv0/EAP-GTC		
	PEAPv0/EAP-MD5		

For more information: www.wi-fi.org/certified_products



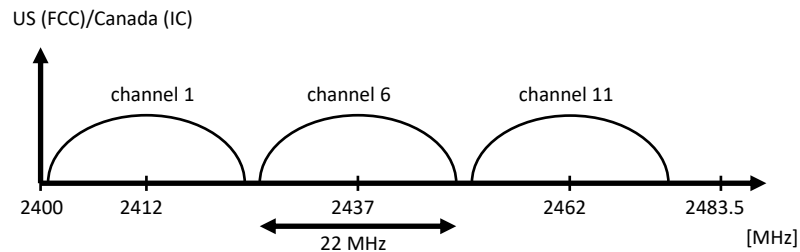
Certificate inside packaging (optional)

- Logo on product packaging (mandatory)
- Helps retailers and consumers

IEEE 802.11b (obsolete)

- **2.4 GHz range** (very “busy” part of spectrum)
- **ISM bands:** industrial, scientific and medical (now unlicensed use)
- Prone to **interference from other devices** (microwave ovens, cordless phones, etc.) and also has security disadvantages
- Limits the number of access points in range of each other to three
- Has **11 channels (3 non-overlapping)** and supports rates from **1 to 11 Mbps**, but realistically about 4-5 Mbps max
- Range: **100-300ft** (indoors/outdoors)

Channel Selection (Non-Overlapping)



- Width of band: 22MHz
- Channel 1 center: 2412MHz
- Channel center distance: 5MHz (2412, 2417, 2422, 2427, 2432, 2437, ...)

802.11g Standard

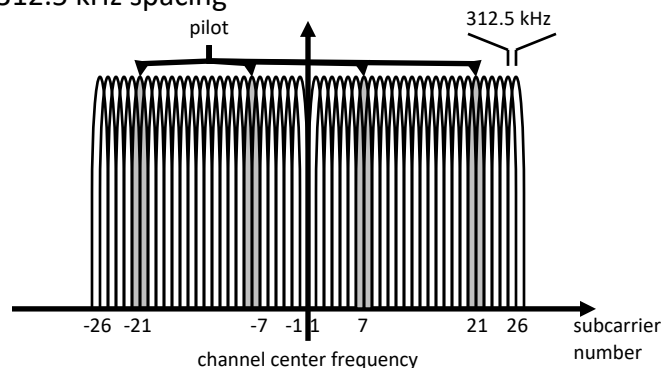
- Extension of 802.11b, with the same disadvantages (security and interference)
- Has a shorter range than 802.11b
- Is backwards compatible with 802.11b so it allows for a smooth transition from 11b to 11g
- Flexible because multiple channels can be combined for faster throughput
- Runs at **54 Mbps**, but realistically about 20-25 Mbps and about 14 Mbps when b associated
- Uses frequency division multiplexing

IEEE 802.11a

- Completely different from 11b (& 11g)
- Flexible because multiple channels can be combined for faster throughput and more access points can be co-located
- Shorter range than 11b
- Runs in the **5 GHz range**, so less interference from other devices
- Has 12 channels (8 non-overlapping)
- Rates from **6 to 54 Mbps** (realistically ~27 Mbps max)
- Uses frequency division multiplexing

OFDM = Orthogonal Frequency Division Multiplexing

- 52 subcarriers (64 in total)
 - 48 data + 4 pilot
 - (plus 12 virtual subcarriers)
 - 312.5 kHz spacing



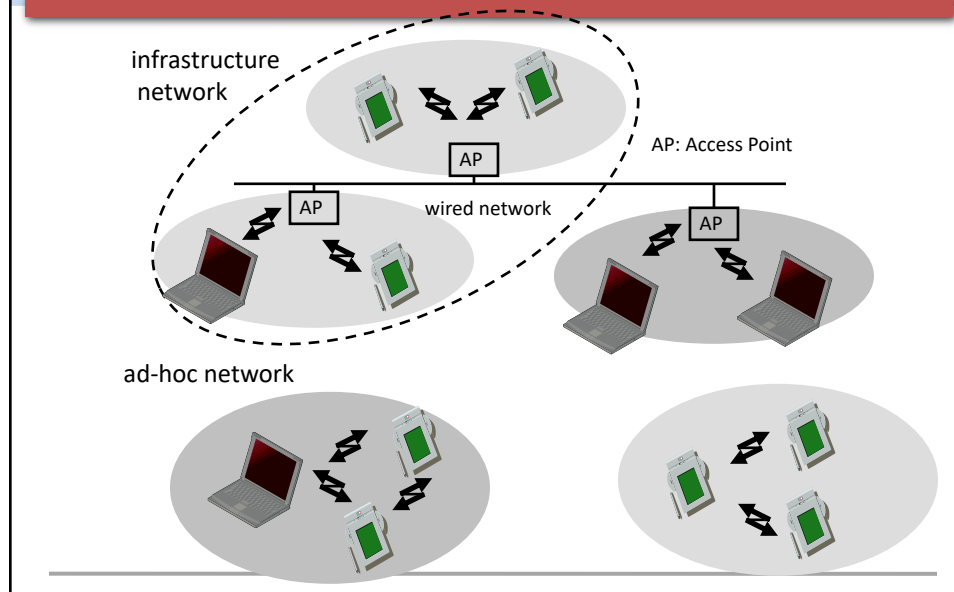
IEEE 802.11n & ac

- **IEEE 802.11n:**
 - **MIMO:** Multiple Input Multiple Output (multiple antennas)
 - 2.4 & 5GHz
 - Data rates up to 150Mbps (single antenna)
 - Range: 230-820 ft (indoor/outdoor)
- **IEEE 802.11ac:**
 - 5GHz
 - Data rates of 150 (2.4GHz) – 433 (5GHz) Mbps (single antenna)
 - Range: 115 ft indoor

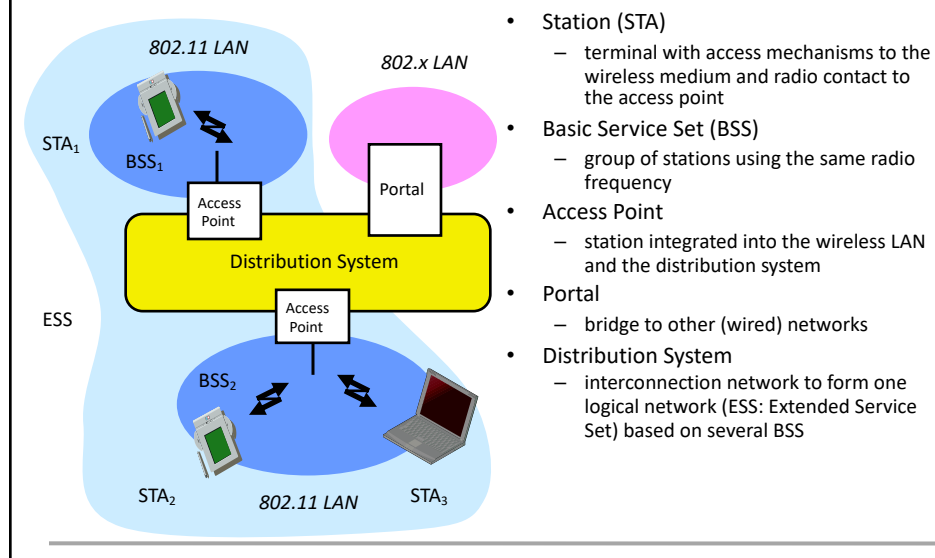
IEEE 802.11ax (Wi-Fi 6)



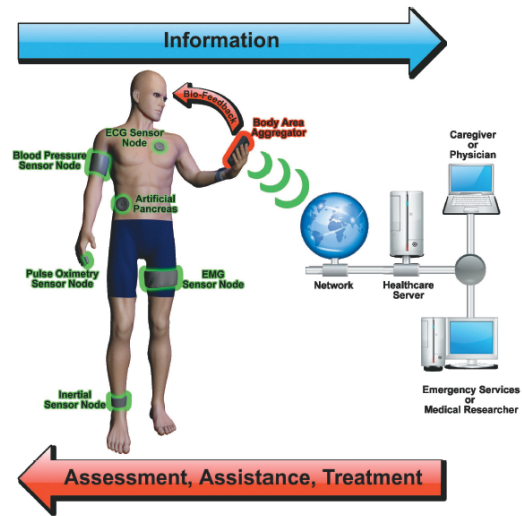
Infrastructure vs. Ad-Hoc Networks



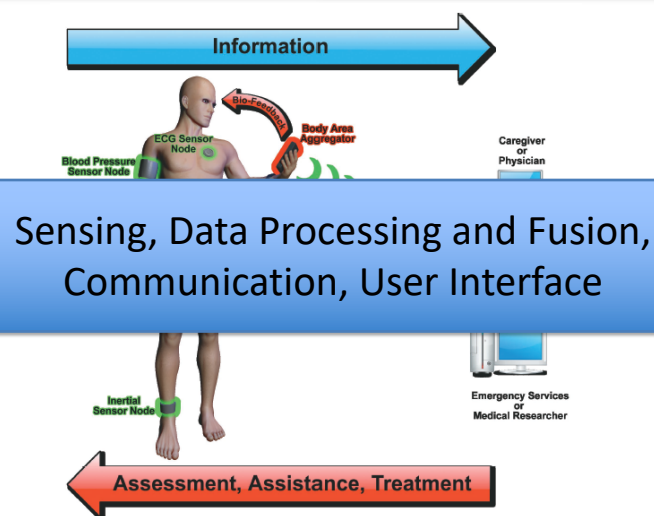
802.11 - Architecture of an Infrastructure Network



Body Area Sensor Network (BASN)



Key Components of BASN?

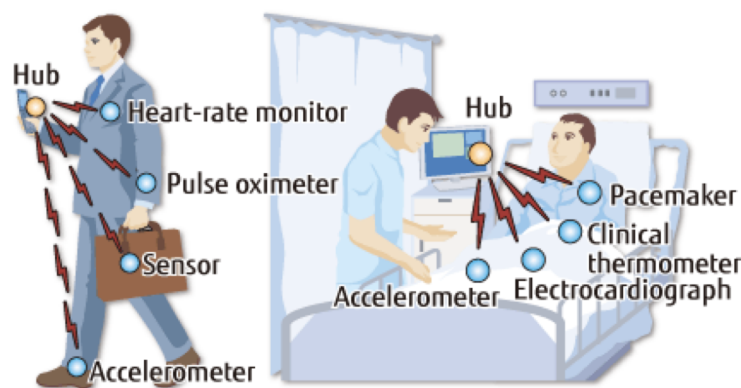


BASN Features

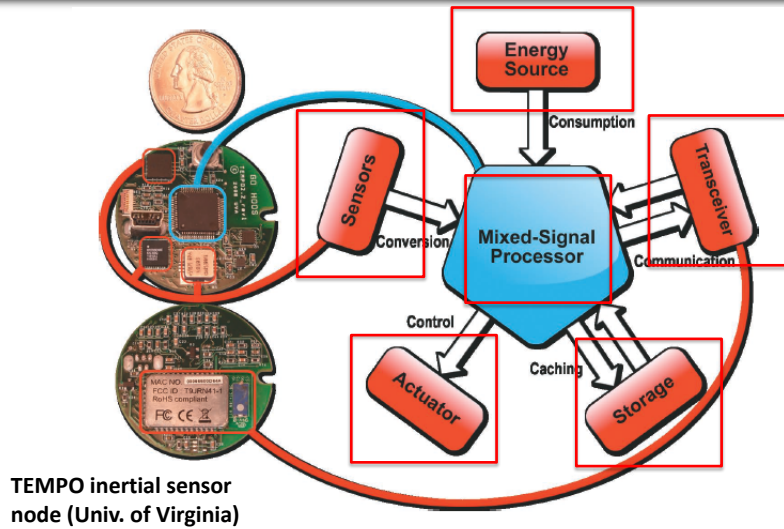
- **Ideally noninvasive (or minimally invasive)**
 - Social acceptance
- **Tiny in size**
 - Small battery, limited resources, tradeoffs between energy and data quality
- **Packaging and placement**
 - Neither prominent nor uncomfortable
- **Amortize nonrecurring costs**
 - Either significant volume in a single app or aggregate volume across apps
- **Emphasis on “value to user”**
 - Useful apps that deliver valuable information to users

BASN Application Areas

- Healthcare Applications

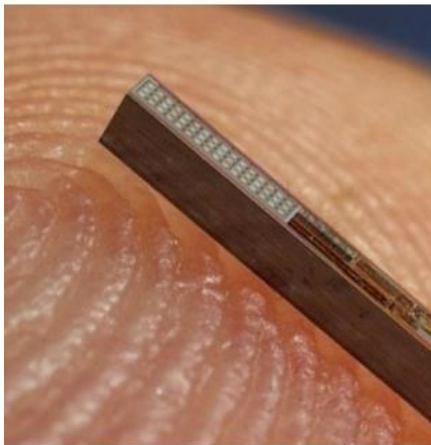


BASN Components: Sensors

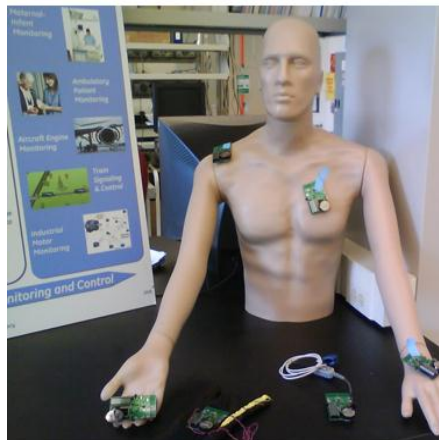


WBAN Sensors

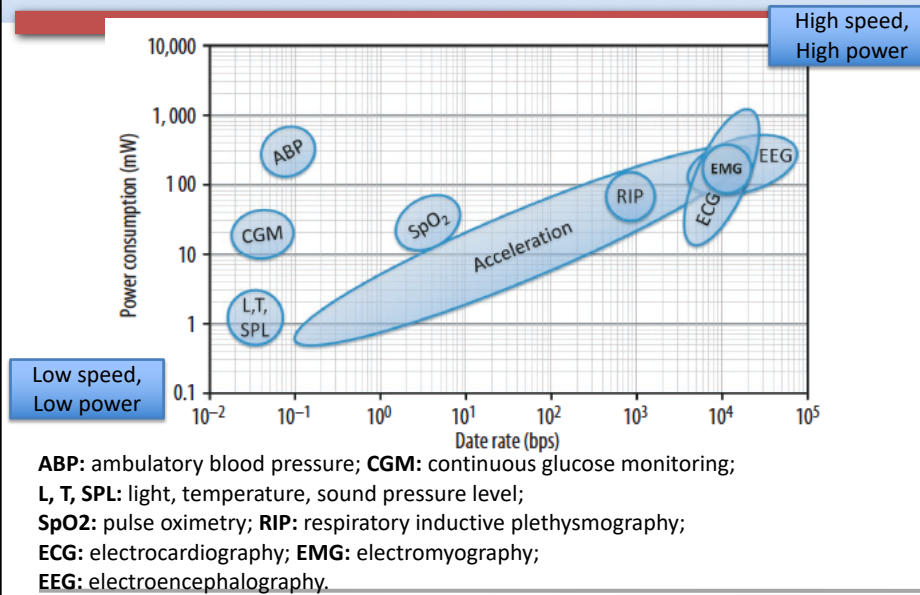
In-Body Sensors



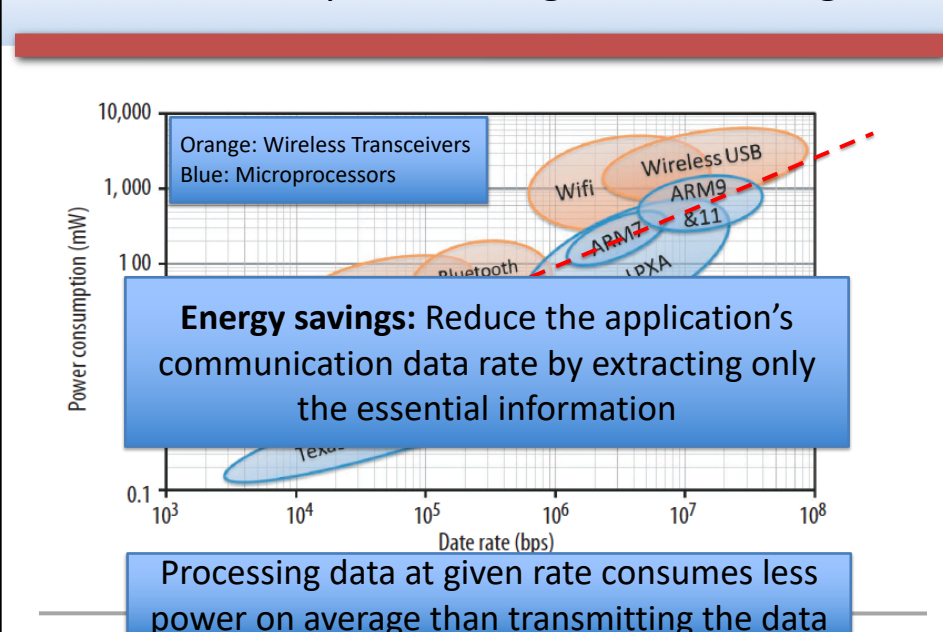
On-Body Sensors



BASN Components: Sensors



BASN Components: Signal Processing

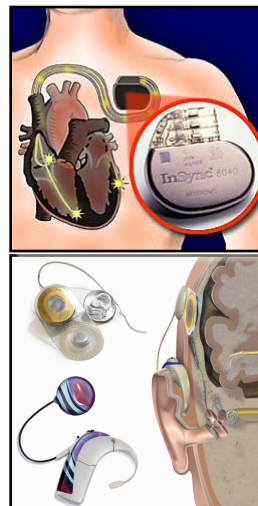


BASN Components: Communication

- Essential for node coordination
- Restrict the communication radius to the body's periphery
- RF channels: 850 MHz-2.4 GHz
- Big problem of **“body shadowing”**
 - Body's line of sight absorption of RF energy
 - Movements cause highly variable path

MICS

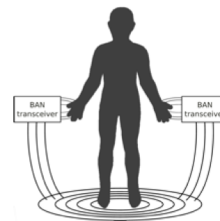
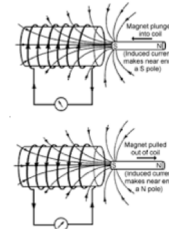
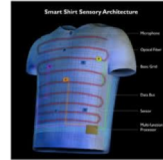
- Medical Implant Communication Service
 - 402-405MHz
 - Low power ($25\mu\text{W}$): reduce interference with other users
 - Low data rate
 - Couple of meters range (transceiver doesn't have to touch skin)



BASN Components: Communication

New/future communication methods:

- **Smart textiles**
 - Embed wires in clothing
- **Magnetic induction**
 - Use near field effect to communicate
- **Body-coupled communication**
 - Use human body as a channel
 - Highly stable, low energy
 - Safety is critical



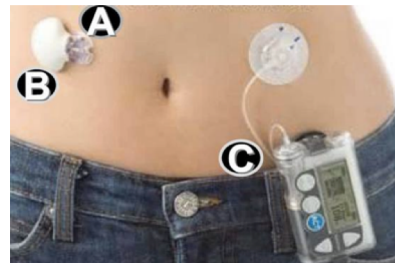
BASN Components: Storage

- **On-node storage:**
 - Low power nonvolatile storage
- **Cache data and wait for good channel conditions:**
 - Prolong battery life, decrease transmission error
- **Archive data for signal classification:**
 - Detect longitudinal trends (e.g., recovery from surgery)
 - Detect instantaneous events (e.g., falls)

BASN Components: Feedback Control



Prosthetics Devices



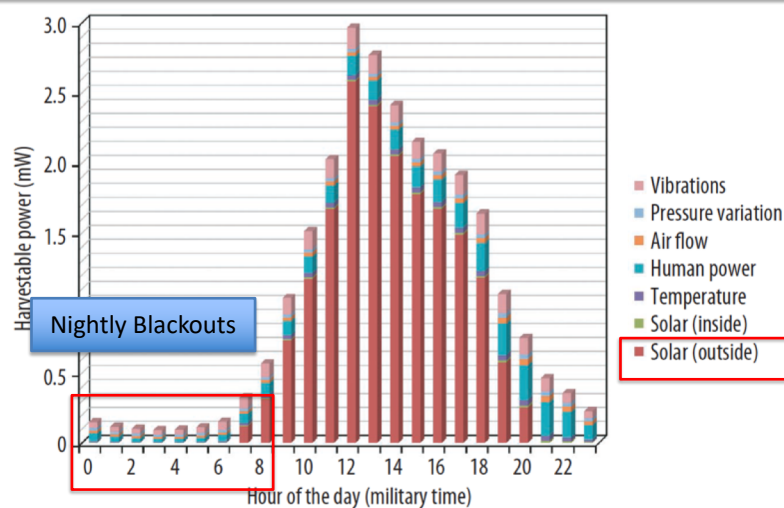
Diabetes Monitoring

EMG signals from the eyelid or jaw might be used to control prosthetics devices

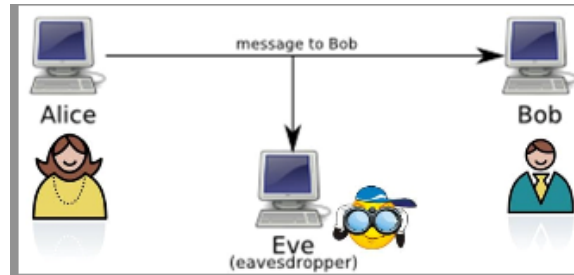
Use blood glucose measurements from biosensors to control insulin delivery

Energy Harvesting

Q: What can you observe from this figure?



Security in WBAN is CRUCIAL!



- “Shared” nature of wireless network; insecure channels
- Eve could break transmission
- More maliciously, Eve can modify the medical data
- Can lead to severe medical malpractice

Major security requirements	Description
Data storage security requirements	
Confidentiality	Patient-related data should be kept confidential during storage periods. Especially, its confidentiality should be robust against node compromise and user collusion.
Dynamical integrity assurance	Patient-related data must not be modified illegally during storage periods, which shall be checked and detected by a node dynamically.
Dependability	Patient-related data must be readily retrievable when node failure or data erasure happens.
Data access security requirements	
Access control (privacy)	A fine-grained data access policy shall be enforced to prevent unauthorized access to patient-related data generated by the WBAN.
Accountability	When a user of the WBAN abuses his/her privilege to carry out unauthorized actions on patient-related data, he/she should be identified and held accountable.
Revocability	The privileges of WBAN users or nodes should be deprived in time if they are identified as compromised or behave maliciously.
Non-repudiation	The origin of a piece of patient-related data cannot be denied by the source that generated it.
Other requirements	
Authentication	The sender of the patient-related data must be authenticated, and injection of data from outside the WBAN should be prevented.
Availability	The patient-related data should be accessible even under denial-of-service (DoS) attacks.