IoT Security

Dr Priyanka Bagade, IITK

CS698T, Lecture 13

Content Copyrights

- The instructor owns the copyright of the CS698T: introduction to internet of things and its industrial applications course material. It includes lectures, presentations, exams and assignments. It should not be distributed in print or through electronic media without the consent of the instructor. Students can take notes or make their own copies of the content.

Security Challenges in IoT systems [3,4]

- Resource constrained systems
- Deployment in hostile environment
- Unattended operations
- Large number of tiny devices
- Current security algorithms may not be directly applicable
  - Mainly developed for stationary systems. IoT systems can be mobile
  - IoT engineers focus on adding new features/functionality and not on the risk assessment
  - Internet application developers solved the M2M communication issue. It seems that the same technique can be applicable to IoT systems. However, transport security is just one of the many risks in IoT devices.
  - For web applications on internet, there are few stationary publishers and a small number of consumers which are behind the safe firewalls and guarded by antivirus and operating systems. They get updated automatically for every new threat
    - However, IoT systems have number of mobile publishers and consumers which are not protected by antivirus and don't get updated periodically

Types of attack for IoT systems [4] -1

- **Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack**
  - Aimed to crash a service or make the system unresponsive
  - Makes repetitive requests to a server until its resources gets exhausted
  - Sends multiple requests to multiple clients in case of the distributed systems
  - Possible solution
    - Develop a distributed system than a centralized system to reduce the worth of each target
- **Guessing the credentials**
  - Possible solutions
    - Long and unique password generated by the randomizer for each device. Never use factory setup default credentials
    - Set a limit on number of authenticated limits
    - Log the details of the failed attempts – location and entered credentials
      - Helps with detecting systematic attempts of intrusion

Types of attack for IoT systems [4] - 2

- **Getting access to stored credentials**
  - reuse credentials in different systems
  - Possible solutions
    - Have different credentials for every system which should not be easily memorized
    - Never store the authentication details centrally in plain format or even encrypted format
      - Store the hash values
      - Compute these hash values for every installation
- **Man in the middle**
  - Try to impersonate the sensor server
  - Pass the messages in clients and servers and learn confidential information in the messages
  - Possible solutions
    - Periodically check the authenticity of the server
      - Usually done using certificates
      - Make sure the certificates are not expired or self-signed
    - Never use less secure authentication
      - A compromised server might force clients to use less secure authentication methods

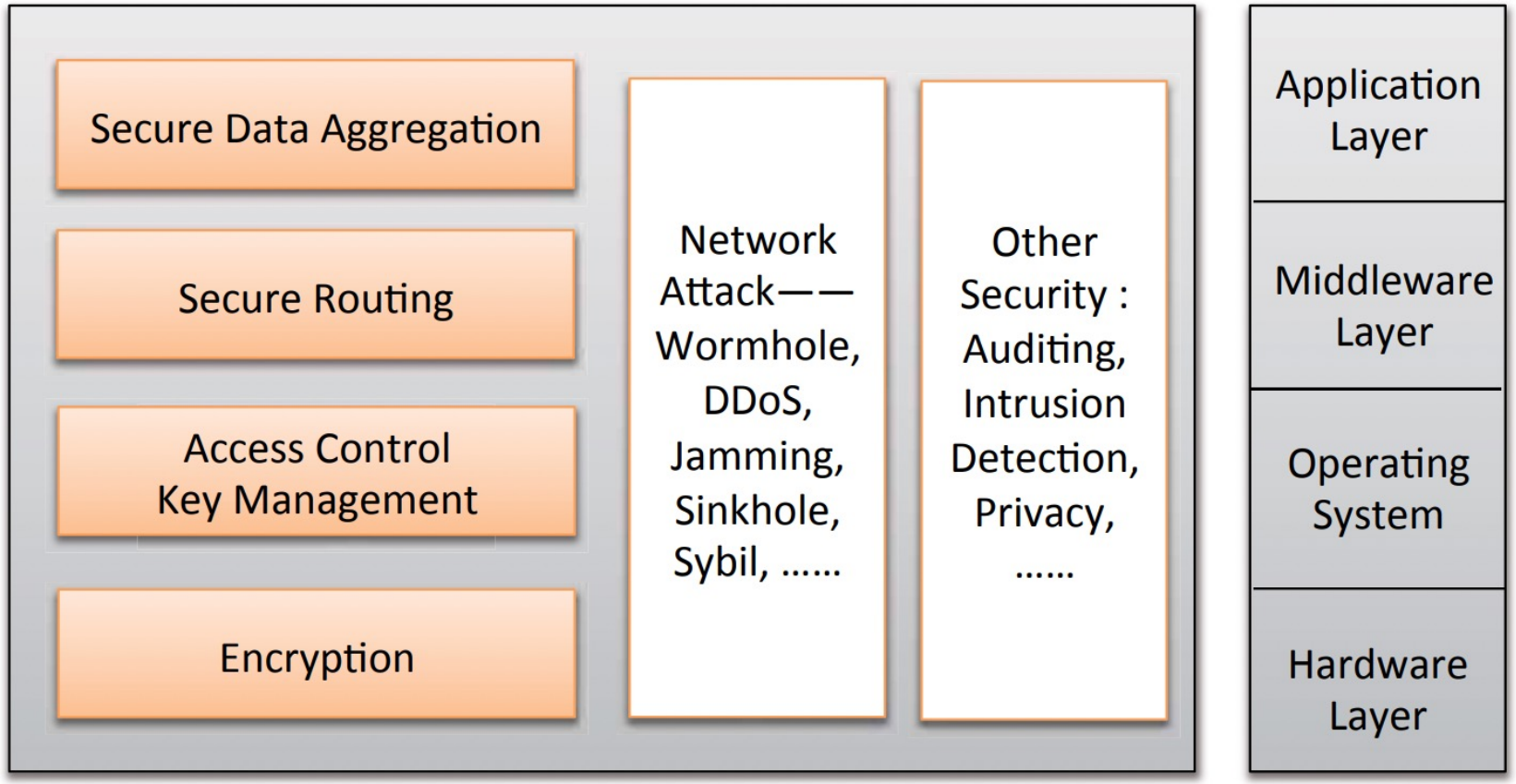
Types of attack for IoT systems [4] - 3

- **Sniffing network communication**
  - Anyone can listen to unencrypted messages using simple tools such as Wireshark
    - For the multicast messaging services such as CoAP, anybody within the range of the Time to live (TTL) parameter (maximum number of router hops) can eavesdrop
    - For point-to-point communication, the communication can be heard by any application on the sending machine, the receiving machine, or any of the bridges or routers in between.
  - Possible solutions
    - ALWAYS ENCRYPT YOUR DATA BEFORE TRANMISSION
    - For a smart home, a malicious entity can if someone is home or not by simply monitoring temperature sensors, water flow meters, electricity meters, or light switches

Types of attack for IoT systems [4] - 4

- **Port scanning and web crawling**
  - Systematically scans the ports to see which ports are open
  - Standard page names and web-crawling techniques can be used to try to figure out which web resources lie behind each HTTP server
  - Possible solutions
    - close all the incoming ports in firewalls
    - Use protocols that create the connections from inside the firewall.
    - Any resources published on the Internet should be authenticated so that any automatic attempt to get access to them fails.
- **Search features and wildcards**
  - Very easy to find devices communicate over a network
  - Possible solution
    - Always authenticate before data communication
  - XMPP protocol allows only authenticated clients to receive messages from the server
  - MQTT does not authenticate the end clients. Anyone can request the published data as long as the topic and the broker is known, since identities are stripped away by the protocol.
    - Solution: build a proprietary end-to-end encryption layer on top of the MQTT protocol
- **Breaking ciphers**
  - Using encryption does not solve the problem completely
  - Ciphers can be broken using known vulnerabilities in code
  - Possible solutions
    - Decentralize storage and control logic to reduce the value of each target .
      - mitigates the effects of attacks and decrease the interest in attacking a target.
      - But increasing the number of participants leads to increase in the number of actual attacks

Security Architecture for IoT network [1]



Node security [1]

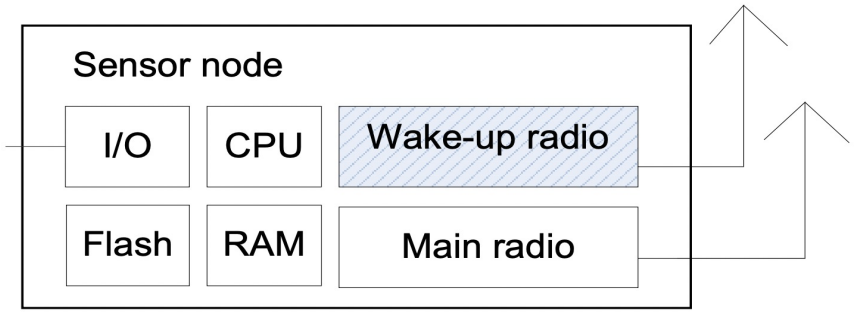
Tampered via logical interfaces or by direct physical attacks

- Gets relocated without authorization or gets stolen.

Sleep deprivation attack

- Special class of denial of service attack
- Does not allow system/node to go into power saving/sleep mode
- Results in fast depletion of battery
  - Message encryption is not useful to avoid this attack as the node needs to wake up to process the received message.
  - The attack gets noticed when the battery is already depleted.

- Solution: secure wake up time
  - Add additional ultra-low power wake-up radio
  - Listens on channel when the node is in sleep mode
  - Wakes up the node after receiving the encoded wake up message



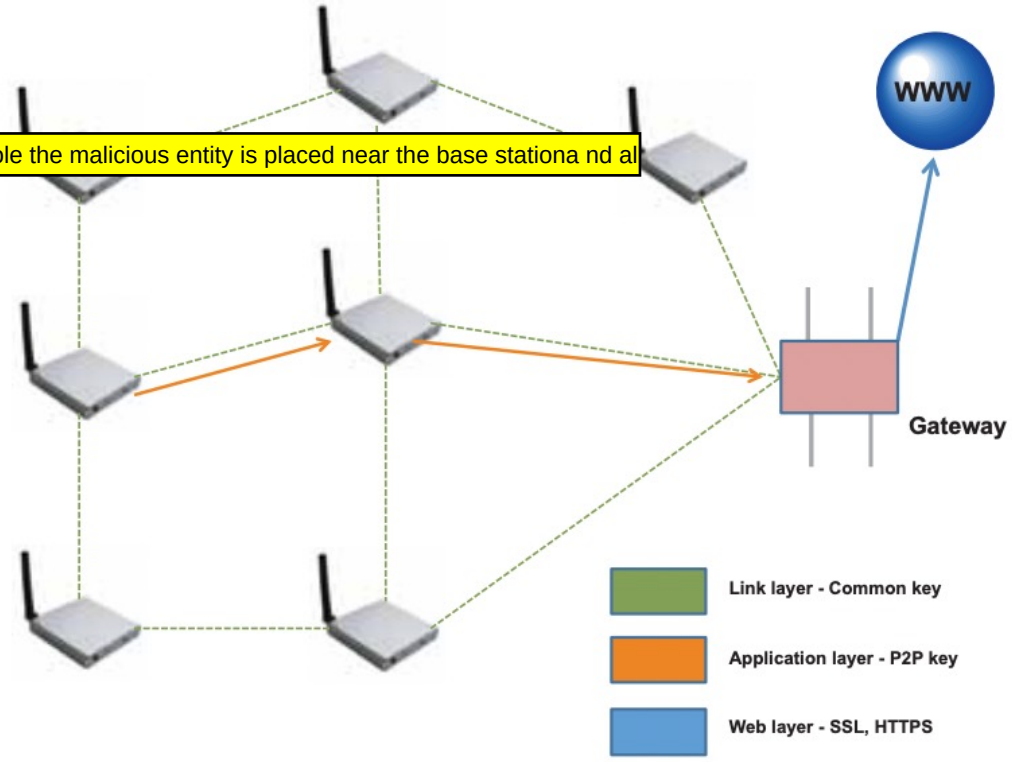
Node Security – Secure Bootstrapping [2]

- *"Bootstrapping in the context of Internet of Things (IoT) is a process by which the state of a device, a subsystem, a network, or an application changes from not operational to operational"* [2]
- IoT secure bootstrapping methods classification
  - Managed methods
    - Use authentication credentials to get access to the centralized server
    - Centralized server authorizes the IOT device for the network access
  - Peer-to-Peer (P2P) and Ad-hoc methods
    - Does not consider pre-established credentials
    - Establishes credentials for subsequent secure communication
    - Exchanges a Diffie-Hellman key over the insecure network for authentication. For example, Bluetooth pairing uses the OOB (out-of-band) channel to ask the user to compare pins and approve the completed exchange.
  - Opportunistic and leap-of-faith methods
    - Does not verify initial authentication, but focuses on the continuity of the initial identity
    - E.g. Gmail or Facebook allows users to create new accounts and only verifies the continuity of the same identity
  - Hybrid methods
    - Uses both managed and ad-hoc methods
    - E.g. Use ad-hoc methods to register the IoT devices. Then use a central server to authenticate these clients

Crypto algorithms [1]

- Unauthorized users can not understand the encrypted messages
- Link layer attacks
  - Sinkhole
  - Dos (Denial of Service)
  - Jamming
- Application layer attacks
  - distributed denial-of-service attacks (DDoS)
  - HTTP floods
  - SQL injections
  - cross-site scripting
  - parameter tampering

All are focussed on exhaustion of resources. In sinkhole the malicious entity is placed near the base stationa nd al

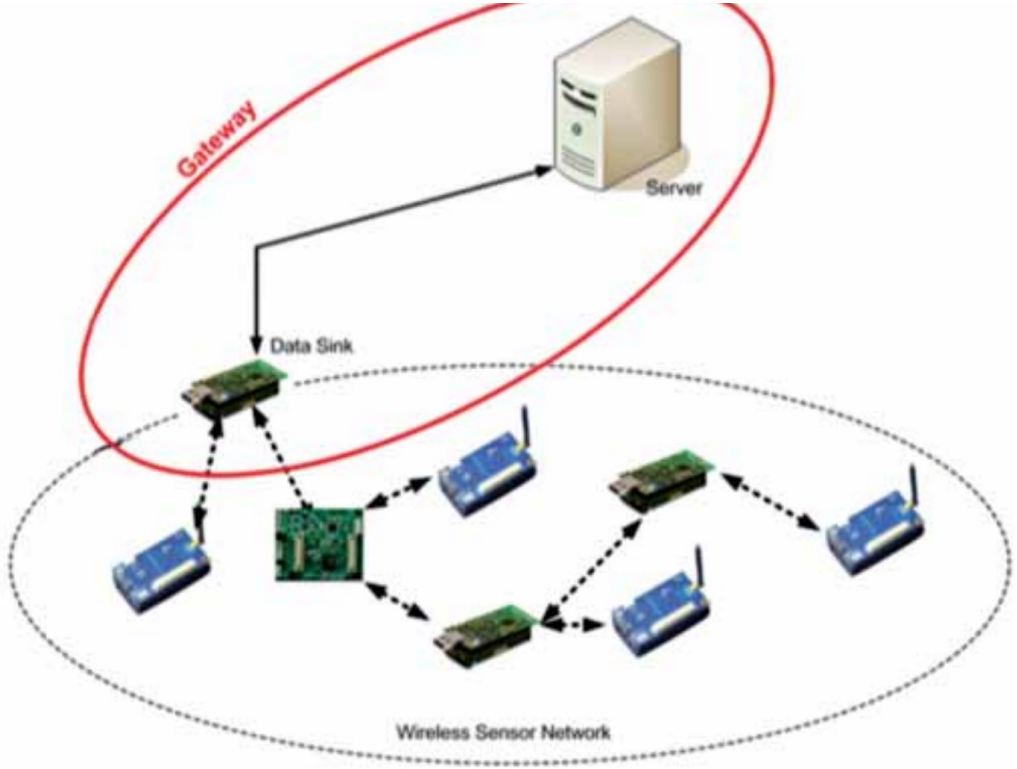


Secure Routing [1]

- Methods of secure routing protocols based on
  - feedback information - information of delay, trust, location, excess capacity in acknowledgment frame of the media access control (MAC) layer
  - location information
  - encryption algorithm
  - multipath selection method
  - hierarchical structures
- Most of the currently available security protocols are developed for stationary sensor node.
  - Need to develop secure routing protocols for mobile nodes

Secure Data Aggregation [1]

- Transmit reliable data from sensor node securely to gateway or base station
- Base station or aggregator node checks the received data for creditability
- Aggregation node to select the next safe and reliable hop, transmit data to the central node or the base station



Security Attack on an IoT enabled healthcare system

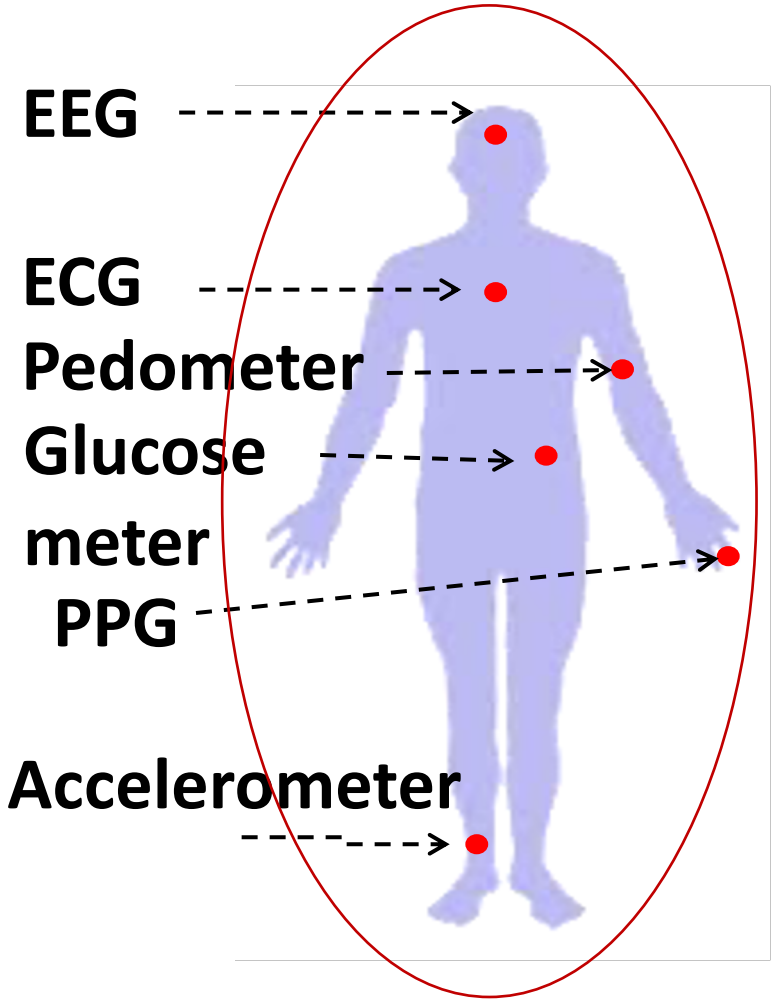
IoT enabled healthcare system

- Network of sensors on body
- Smart phone base station
- Cloud processing

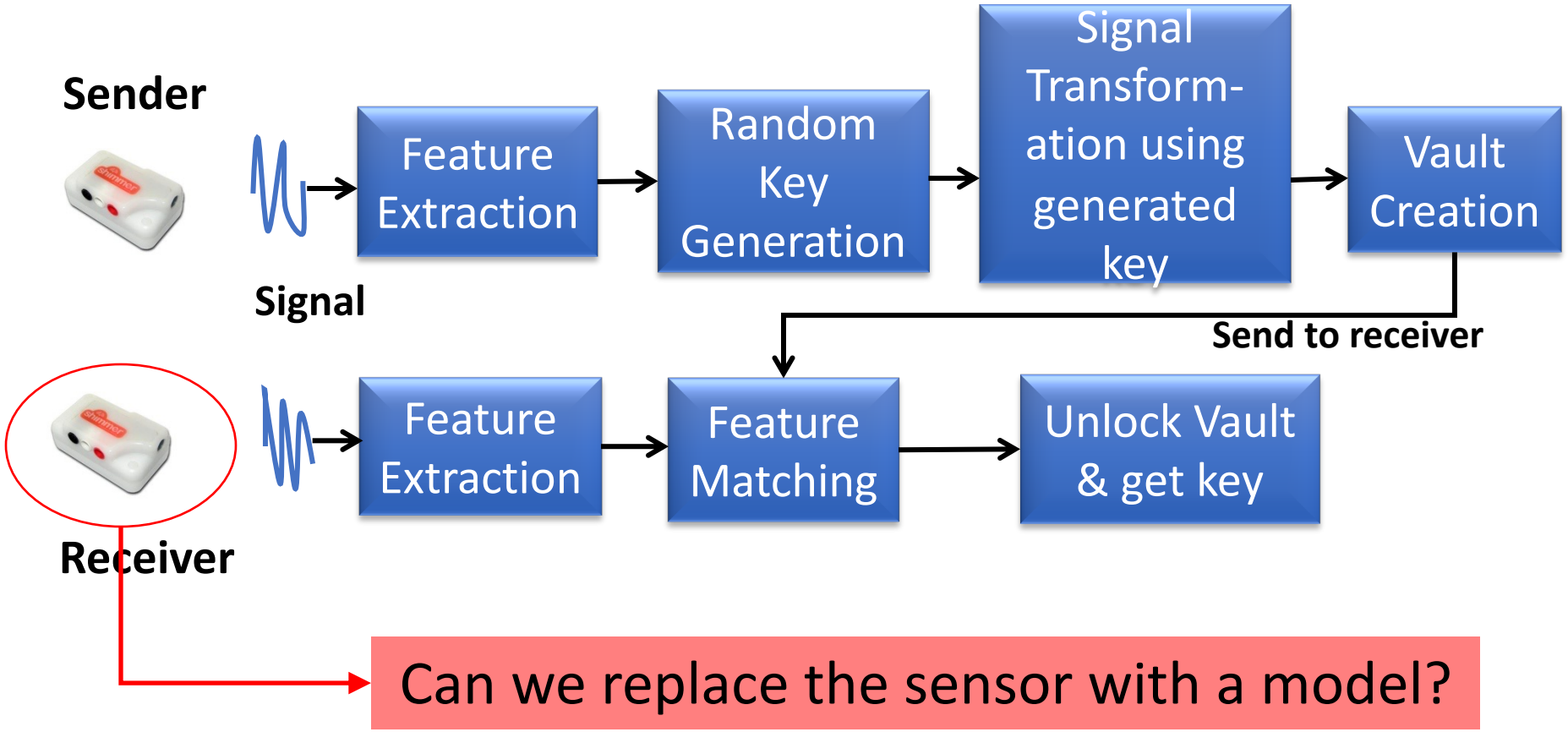
Focus: Inter-sensor communication security

Solution: Physiological signal based security

Plug-n-play & Light weight



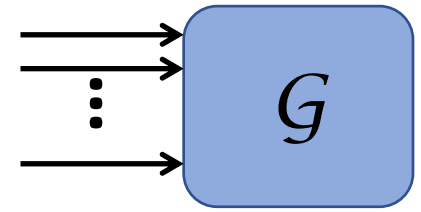
Physiological signal based security[1]

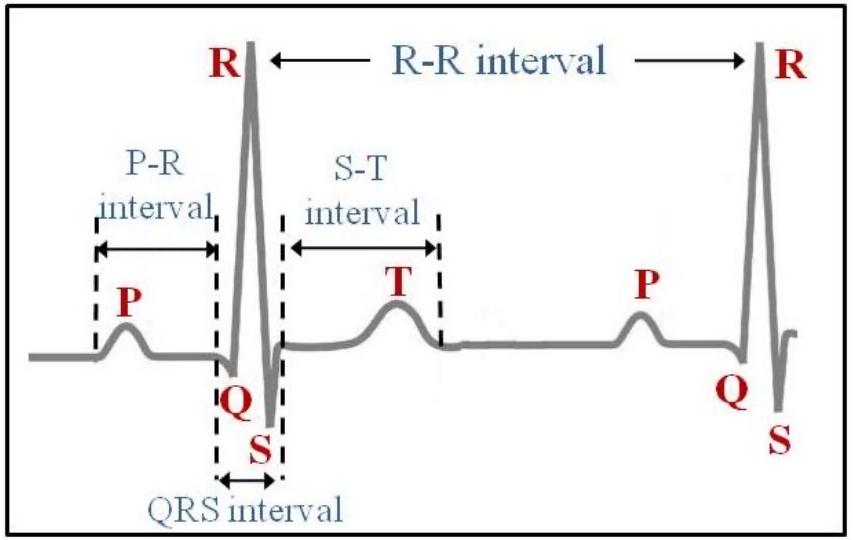


[1]K. K. Venkatasubramanian, A. Banerjee and S. K. S. Gupta, **PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks** (2010), in: Information Technology in Biomedicine, IEEE Transactions on, 14:1(60 -68)

Generative models of physiology

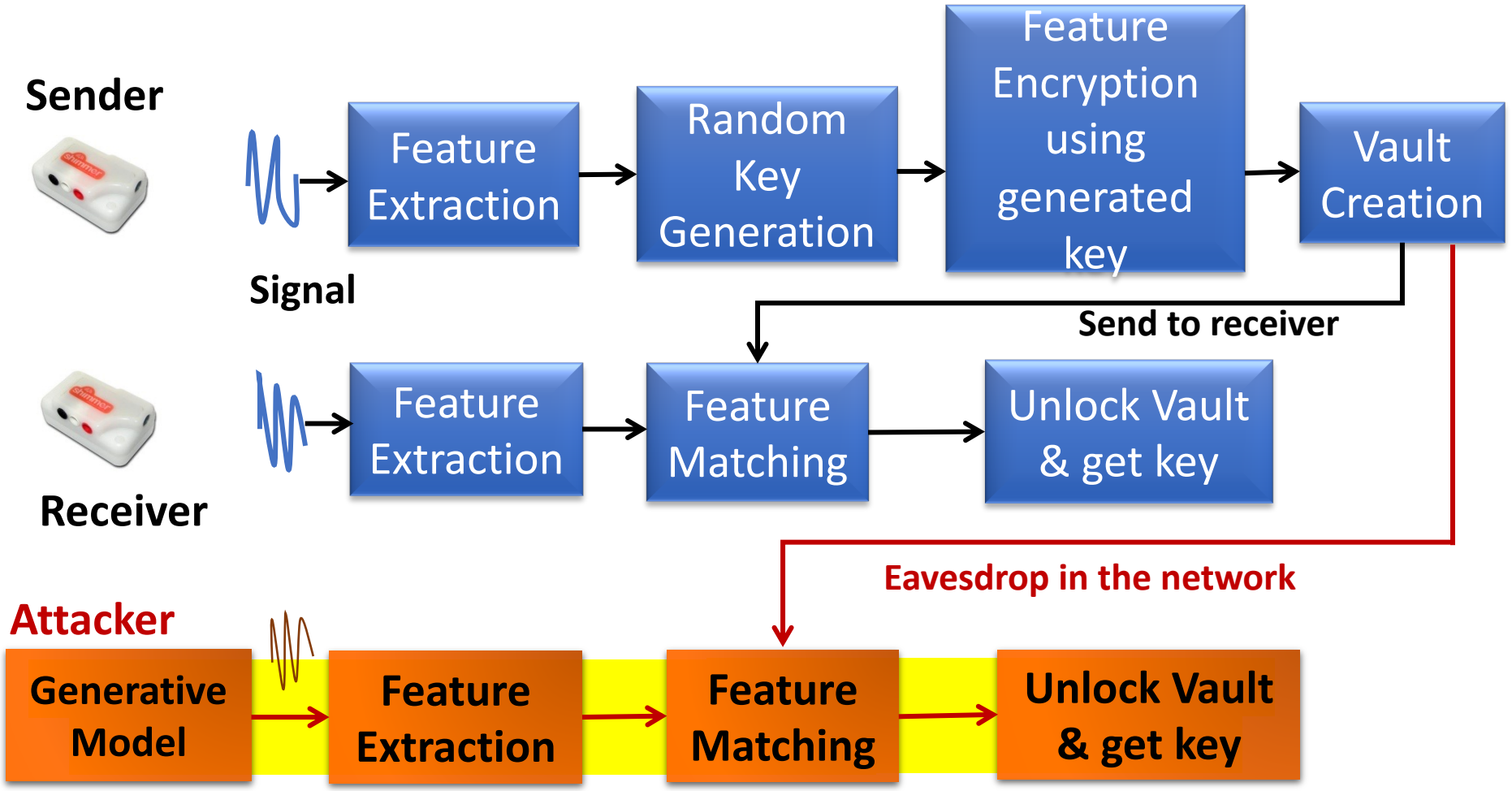
Input Parameters





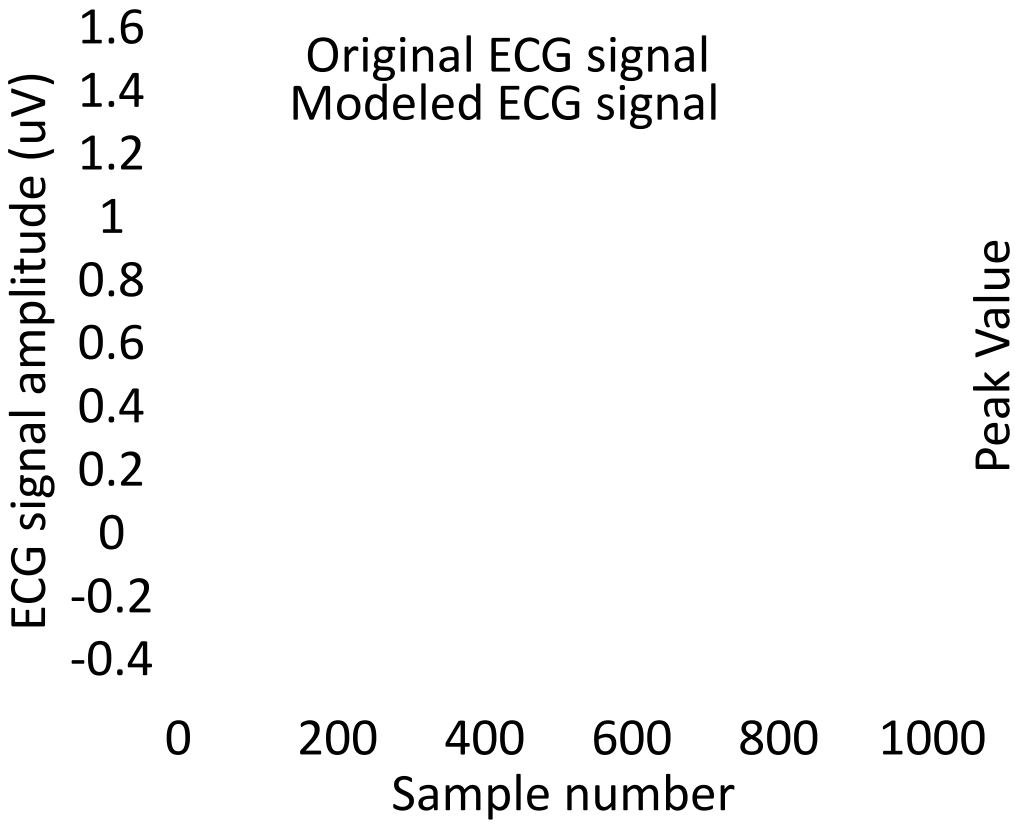
- Time domain features
  - -Highly time varying information
  - -Example: heart rate variability
- Morphological features
  - -Does not vary much over time
  - -Example: shape of a waveform

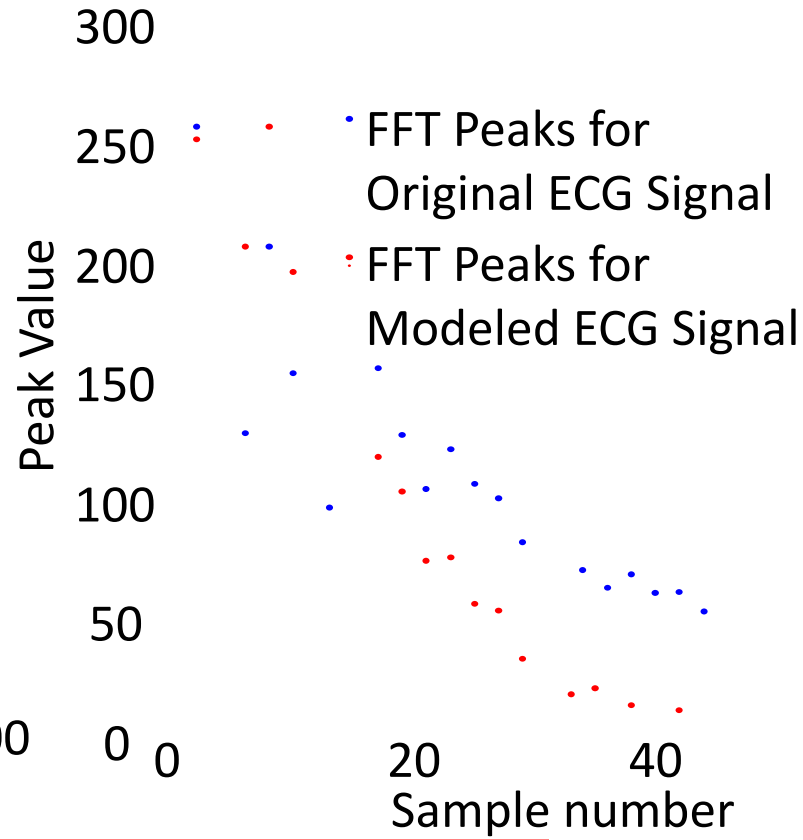
Model Based Attack [5]



Feasibility

- **Tested on MIT database and IMPACT lab database**



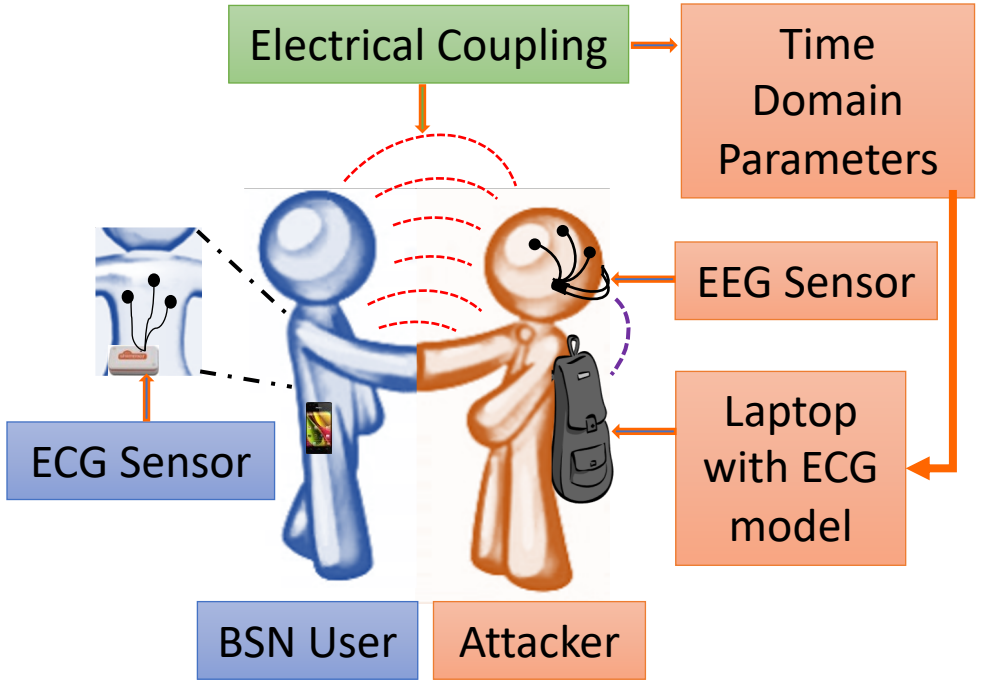


How to get ***morphology features***?

How to get ***time domain features***?

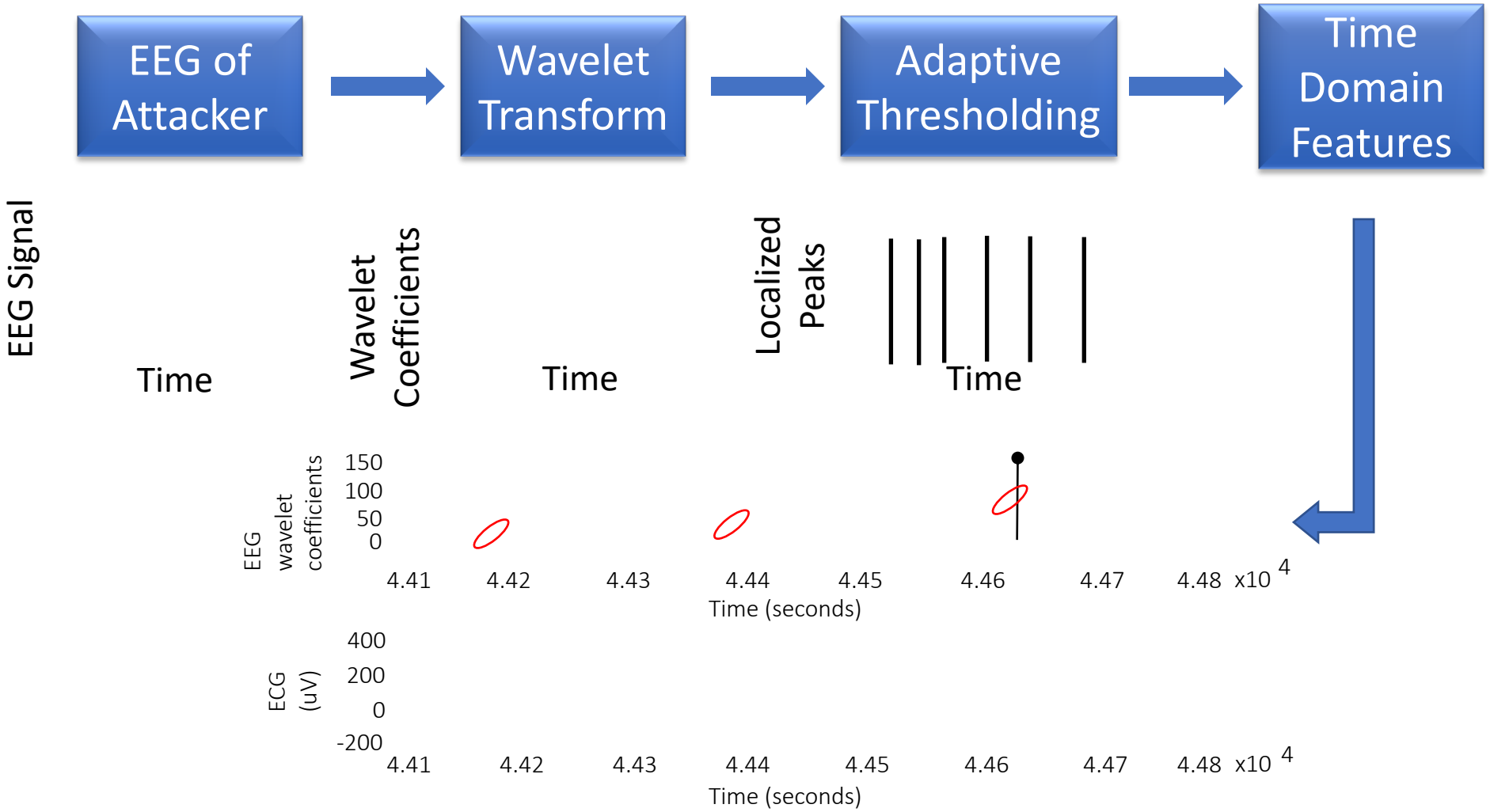
The Non-Invasive Attacker

- **Assumptions:**
  - Morphology parameters available to the attacker
- **Time domain parameters:**
  - Electricity of Touch[2]
  - ECG of BSN user coupled with EEG of attacker



[2] "The Electricity of Touch: Detection and measurement of cardiac energy exchange between people" by McCraty et al

Extraction Algorithm[6]



Summary

- Security Challenges in IoT systems
- Types of security attacks for IoT systems and possible solutions
- Security Architecture
- An example of breaching securing for an IoT system for health monitoring

Reading Material

1. https://storage-iecwebsite-prd-iec-ch.s3.eu-west-1.amazonaws.com/2019-09/content/media/files/iec_wp_internet_of_things_en.pdf
2. https://tools.ietf.org/id/draft-sarikaya-t2trg-sbootstrapping-05.html
3. A Comparison of Link Layer Attacks on Wireless Sensor Networks, https://www.scirp.org/html/4622.html
4. Waher, Peter. *Learning internet of things*. Vol. 3. Birmingham: Packt publishing, 2015.
5. Bagade, Priyanka, Ayan Banerjee, Joseph Milazzo, and Sandeep KS Gupta. "Protect your BSN: No handshakes, just namaste!." In *2013 IEEE International Conference on Body Sensor Networks*, pp. 1-6. IEEE, 2013.
6. *J.-A. Jiang, et.al,"An automatic analysis method for detecting and eliminating ECG artifacts in EEG," Computers in biology and medicine*

Questions?