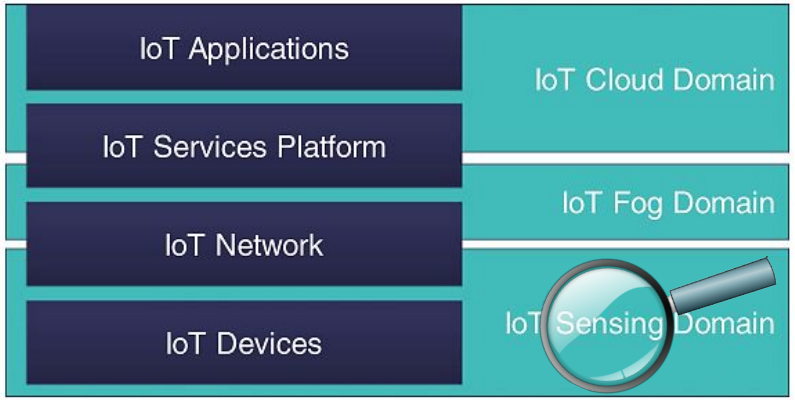
Ch. 14 - IoT Security and Privacy

Sec 4 – Sensing Domain

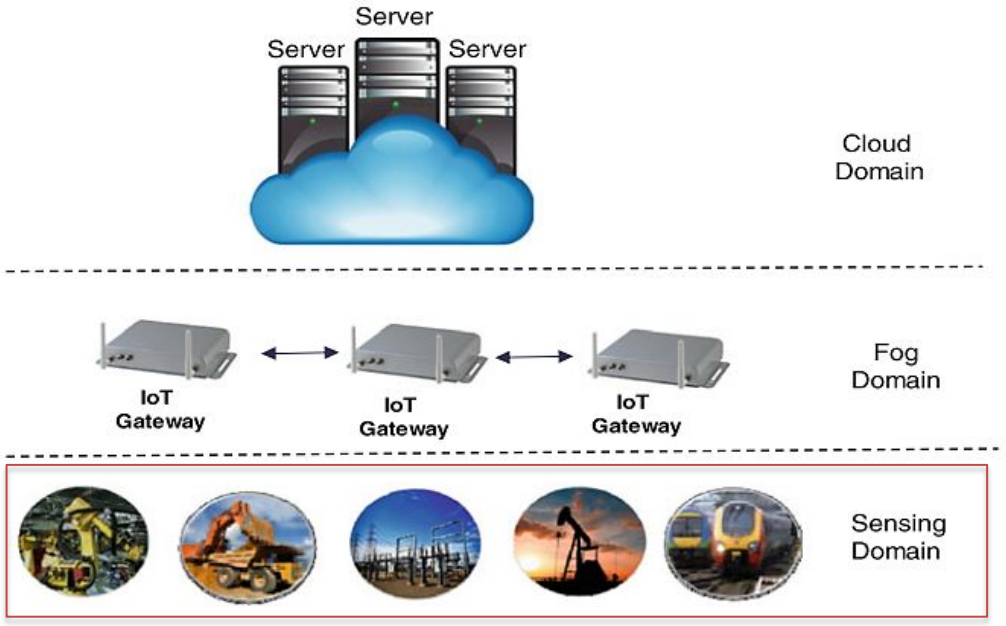
COMPSCI 244p

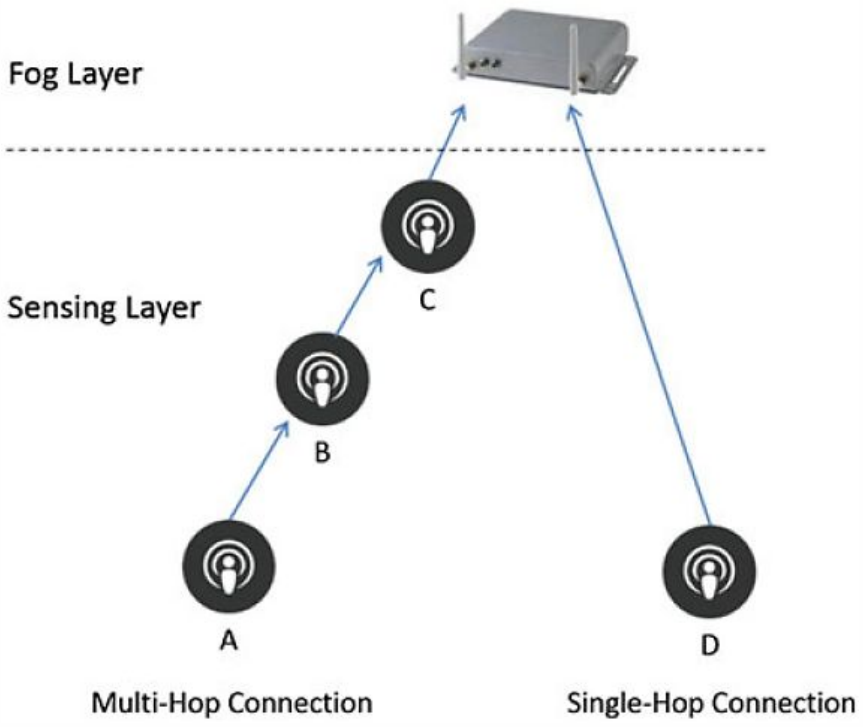
Internet-of-Things; Software and Systems



Sensing Domain Attacks and Countermeasures

- **Challenges of sensing networks:**
  - **Multi-hop** versus **direct** connection between the smart object and the fog device
  - **Wired** versus **wireless** connection





Sensing Domain
1. Jamming Attack

- **To cause a service disruption**
  - Jamming the Receiver
    - Targets the **physical** layer of the receiver.
    - The jammer emits a signal that **interferes** with the **legitimate** signals.
    - Causing packet loss and retransmission.
  - Jamming the Sender
    - Targets the **data link** layer of the sender
    - The jammer sends a jamming signal preventing the neighboring objects from transmitting
    - The neighbors sense the wireless channel to be **busy** and back off **waiting** for the channel to become idle

Sensing Domain

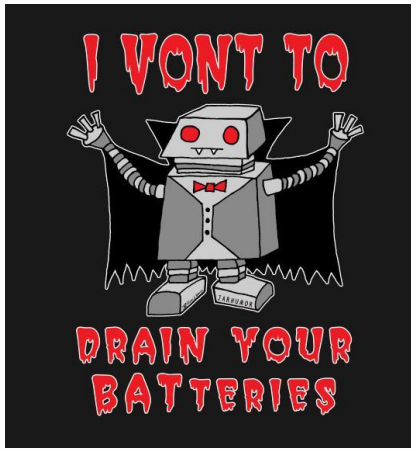
1. Jamming Attack strategies

- **Constant Jamming**
  - Continuously transmits a **random** jamming signal
  - Easy to detect
    - The jamming signal do not follow the MAC protocol pattern
- **Deceptive Jamming**
  - Similar to constant jamming
  - Jamming packets follow the structure of the MAC protocol
- **Reactive Jamming**
  - The jammer **listens** to the medium
  - Attacks only after it senses that a signal is being transmitted
  - Suitable for battery-powered jammers
- **Random Jamming**
  - To **hide** the malicious activity

Sensing Domain
1. Jamming Attack Countermeasures

- **Frequency Hopping**
  - Based on a generated random **sequence** that is **known** only by the sender and receiver.
- **Spread Spectrum**
  - Converts the narrow band signal into a signal with a wide band.
  - Harder to detect and jam by the attacker.
- **Directional Antennas**
  - Less **sensitivity** to the noise coming from the random directions.
- **Jamming Detection**
  - Collecting **features** such as the received signal strength (RSS) and the ratio of corrupted received packets.
  - Using **machine learning** technique to differentiate jamming attacks.

Sensing Domain
2. Vampire Attack



- **Goal: To exploit the limited battery lifetime of IoT devices**
  - Makes IoT devices consume **extra** amounts of **power**

1. Denial of Sleep

- Preventing objects from switching to sleep mode by sending control signals that change their duty cycles
- Effective even when control messages are **encrypted**!
  - Capture and replay encrypted control messages

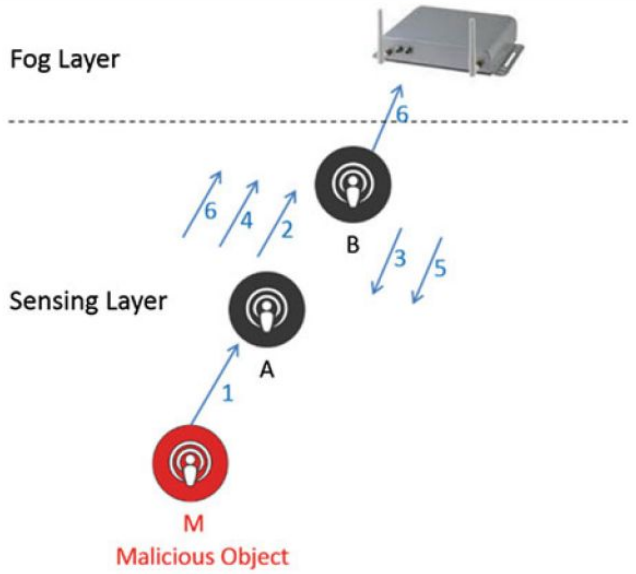
2. Flooding Attack

- Flood the neighboring nodes with dummy packets and request them to deliver those packets to the fog/next device

Sensing Domain
2. Vampire Attack

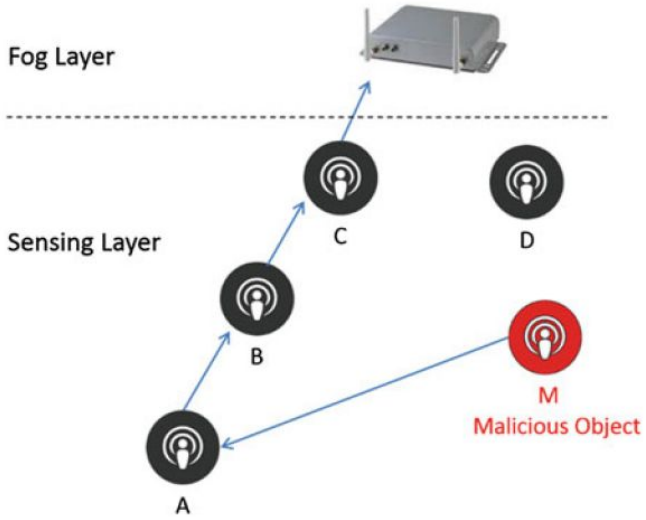
3. Carrousel Attack

- Attacks the **network layer** using ***source routing***
- Specifies routing paths that include **loops**



4. Stretch Attack

- Attacks the **network layer** using ***source routing***
- Choosing very **long** paths rather than the direct and short ones
  - Select a next hop not having the shortest path for ***non-source routing***

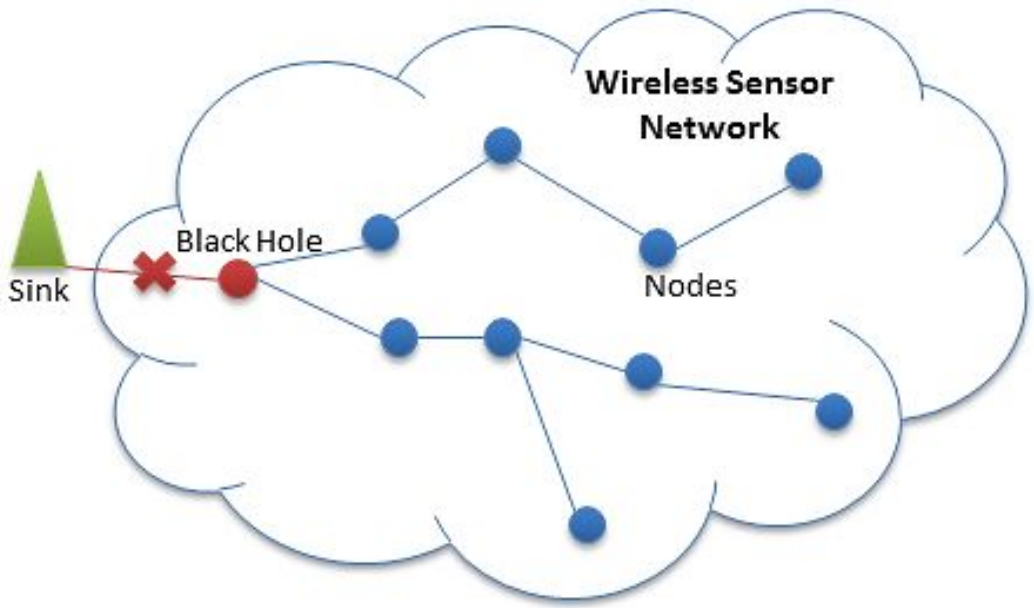


Sensing Domain
2. Vampire Attack Countermeasures

- Denial-of-sleep attacks => **encrypting the control message** + **including a timestamp**
- Flooding attacks => **limiting** the **rate** of the packets that each object may generate
- Carrousel attacks => making each forwarding object **check the specified path** or **disabling source routing**
- Stretch attacks => **disabling source routing or** making sure that the forwarded **packets** are **making progress**

Sensing Domain
3. Selective-Forwarding Attack

- Targeting multi-hoping (indirect) sensor-fog communication scenarios.
- A malicious object **does not forward** a **portion** of the packets that it receives from the neighboring objects.
- **Blackhole attack => dropping the entire packet.**



Unsal, Emre & Çebi, Yalçin. (2013). DENIAL OF SERVICE ATTACKS IN WSN. 10.13140/2.1.4040.9929.

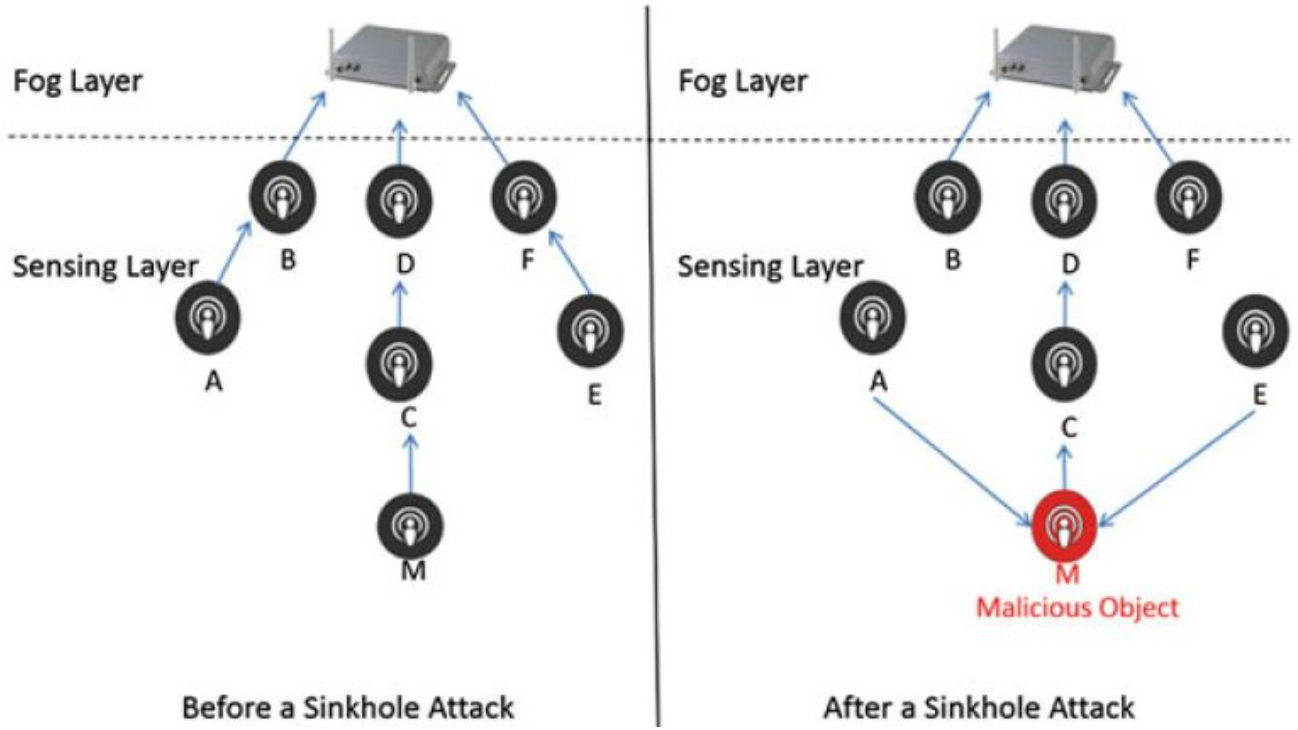
Sensing Domain

3. Selective-Forwarding Attack Countermeasures

- Increase the transmission capability of the objects to reach the fog device **directly, if possible**
  - i.e., Avoiding intermediate nodes
- Path redundancy
  - Generating multiple copies of the packets and forwarding to multiple neighbors
  - High energy and bandwidth overhead
- Detecting the attackers by selecting certain trusted objects as **checkpoints**
  - Checkpoints send **acknowledgements** to the sender

Sensing Domain
4. Sinkhole Attack

- Claiming to have **the shortest path** to the fog device to attract neighboring objects.
- The neighbors' data will go through the attacker
  - Uncover the content
  - Drop the packets



Sensing Domain
4. Sinkhole Attack Countermeasures

- Detect and isolate the malicious objects (**centralized intrusion detection)**
  - Collecting information from neighboring objects (distance to reach those objects)
  - Harder when multiple malicious nodes collude to hide each other