ENES489P FALL 2010

Wireless Sensor Networks: Perimeter Security

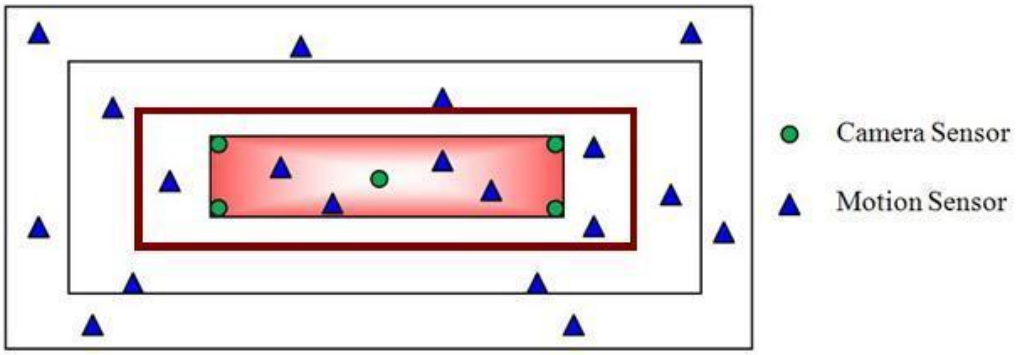
By Kaustubh Jain, Brad Klein, Jeremy Prince & Brian Wang

Contents

Abstract:

We will build a wireless sensor network to track intruders and monitor the security area, the filled in red square. Both camera sensors and motion sensors will be needed. Motion sensors are deployed in the whole area we are interested, and video/camera sensors are only deployed in the security area. The interested area is divided into layers for the sake of energy efficiency. Sensors in the outmost layer are always in the "ON" mode, while other sensors are in the low-power mode by default. When an intruder enters the outmost layer, sensors in this layer will begin to track him/her. Before the intruder enters the inner layer, sensors around his/her location in the inner layer will be notified to wake up by the sensors in the outer layer. Then sensors in the outer layer will enter the low-power mode. The case is similar if the intruder moves from a inner layer to an outer layer.

When the intruder enters the unauthorized area, everything inside the dark red square, the near by camera sensor will be woken up. The unauthorized area is determined by the distance the camera sensors can take a clear picture of the Person. The camera sensors are responsible for taking pictures of the Person. When the intruder moves to another sub-area, another camera sensor will be woken up and this one will enter the low-power mode.



Systems Requirements:

- The sensor network should always detect and track an intruder
- Cost of the system is low
- There is enough redundancy in sensing (both camera and motion) and to cope with failures of neighbors.
- The operator is able to identify malicious sensors.
- The system is resilient to attack on sensors / network.
- The energy consumption of the network is as small as possible to maximize the network lifetime without increasing the errors.

Preliminary Structure:

Sensor nodes:

1. Motion
    a. Detection thresholds – size of object, speed
    b. Response times – signal detection, processing and messaging
    c. Sensor Range
    d. Cost
2. Video/Camera
    a. Video and/or thermal
    b. Field of view – wide / narrow
    c. Night time performance
    d. Range/ zoom
    e. Resolution/ frames per second
    f. Cost
3. Network Configuration:
    a. Layers of motion sensors
    b. Camera at the centre
4. Network actions:
    a. Detect intruder
    b. Track intruder
    c. Photograph/Video intruder
5. Sensor modes:
    a. ON
    b. Transmit
    c. Receive
    d. OFF
    e. SLEEP (receive on/off signal only)
6. Antenna:
    a. Energy
        i. Transmit power
            1. Bit rate or range
        ii. Receive power
        iii. Loss model
            1. loss rate related to wireless channel/propagation loss and distance/packet loss
        iv. Sleep power (power consumed in sleep mode)
        v. Range
            1. Distance of sensors from each other (depends on propagation losses, and transmit power as well)
    b. Direction
        i. Omni
    c. Cost
7. CPU:
    a. Processor

i. Speed
ii. Energy/ Power

b. Memory
i. Size

c. Software
i. Algorithms for measurements and data processing
ii. Limit on data processing
iii. Messaging
iv. Algorithms for communication with other sensor nodes

d. Cost

8. Link
   a. Delay
      i. Transmission delay
      ii. Propagation delay
   b. Rx Power
      i. Tx Power
      ii. Distance
      iii. Pathloss model
      iv. Channel effects / fading
   c. Signal-to-interference-noise-ratio
      i. Rx power
      ii. Background noise
      iii. Interference
   d. Packet loss probability
      i. Tx bitrate, modulation
      ii. Bit-Error-Rate curve
      iii. Packet length
      iv. SINR
9. Alarm subsytem
   a.
10. Environment:
    a. Setting - Outdoors or Indoors
       i. roads and secure facility
       ii. area inside a building
    b. Condition
       i. Temperatures
       ii. Wind, rain, etc.
       iii. Lightings – night vision, etc.
    c. Wireless Channel
    d. Propagation losses – free-space model
11. Performance metrics:
    a. Cost (required)
       i. Balance cost and performance (?)
       ii. Fixed costs (sensors)

iii. Variable costs (energy used)
iv. Response to alarms

b. Energy (required)
   i. Efficiency
   ii. Lifetime
c. Quality (probability of detection)
   i. How well picture
   ii. False alarms
   iii. Missed alarms
d. Security
   i. Crypto – encryption or data authentication and measures against false data injection
   ii. Physical protection of exposed nodes
   iii. Authentication of sensors
   iv. Authentication of user/human controller
   v. Jamming?
e. Reliability and resilience to failure of a sensor node
   i. Performance degradation
   ii. Redundancy to avoid system wide failure

Problem Statement

Why is this work needed? Who will use it? And where?

- To gain a better understanding of wireless security networks and to improve the current security systems in place. Anyone one interested in wireless networks. Anywhere where a facility needs to be kept secure.

Who are the project stakeholders and, generally speaking, what are their concerns?

- The stakeholders ARL at Aberdeen. They want their wireless networks to be secure.

If successful, what are the potential benefits of this project?

- The benefits will be more secure data transfer.

What factors are likely to drive economics of development?

- Prices of sensors and importance/value of data that needs to be secure.

Use Case Development

Who are the stakeholders?

- Security agency, operator, authorized personnel, intruder

Who are the actors?

- Operator, intruder, authorize personnel, response team

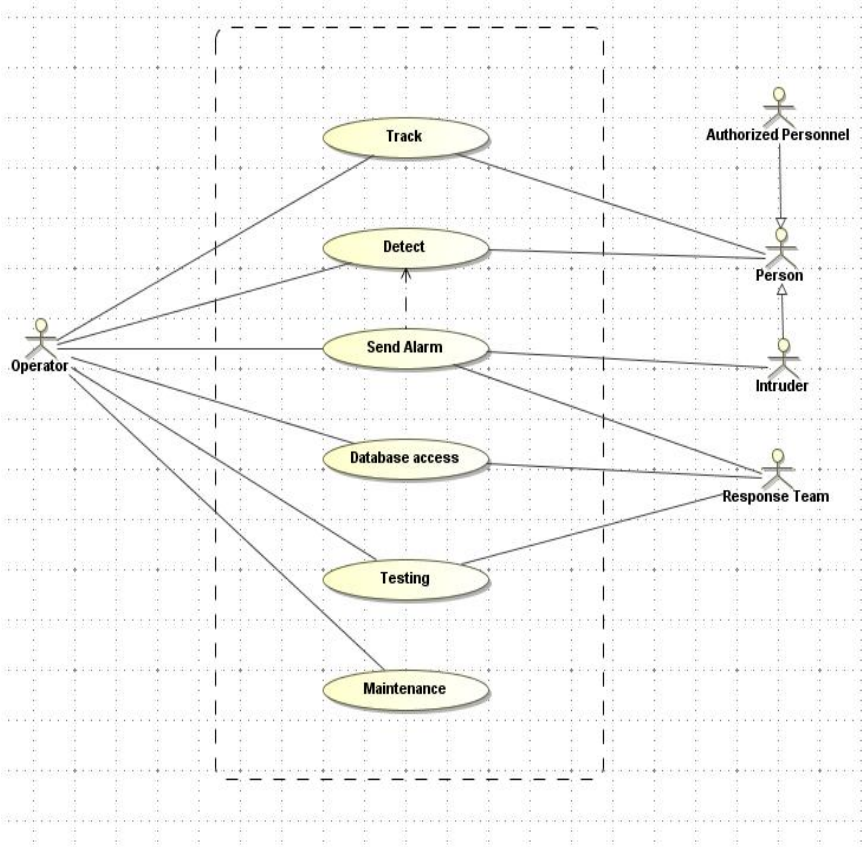
What are the individual functionalities (use cases) that the system will support?

1. Detect a person entering the premises.
2. Track the movement on the person inside the premises.
3. Send alarm to the response team if detected an intruder.
4. Store photo of the intruder and allow response team to retrieve the images.
5. Allow operator to test and maintain the system against failures

Goals and scenarios

1. Test the working of the system
2. Authorize person entering the premises.
3. Detect single intruder via motion then video
4. Detect multiple intruders via motion then video
    a. Single direction
    b. Multiple directions
5. Track the movement of persons on the premises.
6. Send alarm to the response team
7. Check for sensor failures
8. Handle False Alarms
9. Handle Missed Detections
10. Handle sensor failures or compromised sensors

What is the relationship between each actor and the individual use cases?



Use Cases

1. Use Case: Track

1. **Description:** The operator/system analyzes the data collected from sensor nodes to find the location/image of the intruder.
2. **Primary Actors:** Operator
3. **Pre-Conditions:** A person is inside the network, the sensors detect him/her, and sensor node data is sent to the operator.
4. **Flow of Events:**
    a. The Operator analyzes the motion sensor data.
        i. Information about which sensors have detected the intruder
    b. Draw a live track of the person, and monitor where they move.
    c. Watch if the person leaves the network or moves toward the unauthorized area.
6. **Alternate Flow of Events:** None
7. **Post Conditions:** If the Person leaves the network without entering the unauthorized area, then the event is recorded but no actions are taken. If the Person enters the unauthorized area, then the picture is taken and sent to the Operator to be analyzed.

8. **Assumptions:**
    a. The sensor network is working properly.
        i. Sensors detect Person.
        ii. Sensors can send packet to Operator.
    b. The operator is effective at his/her job.
        i. Aware of motion sensor ID locations.
        ii. Aware of how to analyze data from the motion sensor.
9. **New Requirements:**
    a. Motion sensors are able to relay packets to the Operator.
    b. Sensor ID included in motion sensor packet sent to Operator.
    c. Time stamp included in motion sensor packet sent to Operator.

2. Use Case: Detect

1. **Description:** The motion sensors realize a person in within the network, or the camera sensors take picture
2. **Primary Actors:** Operator
3. **Pre-Conditions:** The sensor has been woken up by its neighbor, and the person is within its detection range. The threshold for motion sensors is pre-configured.
4. **Flow of Events:**
    a. The motion sensor receives the IR signal of the object
    b. The motion sensor processes the IR signal. If it exceeds the pre-defined threshold, then the object is considered to be a person.
    c. The motion sensor transitions to the Active Mode.
    d. The motion sensor notifies its neighbors.
    e. The motion sensor generates the packet with the location of the person and sends the packet to the inner sensor destined for Control Center/ Operator.
    f. Sensor receiving the packet destined for Control Center/Operator wakes up, sends packet and goes back to sleep. The sensor receiving both wakeup signal and packet, stays in standby.
    a. The camera sensor takes the picture
    b. The camera sensor generates the packet with the picture of the person and sends the packet to the Control Center/Operator.
6. **Alternate Flow of Events:** None
7. **Post Conditions:** The packet has been sent to the Control Center. The neighbors of the motion sensor have switched to the Standby Mode (motion sensor) or the Active Mode (camera sensor)
8. **Assumptions:**
    a. Quality of the picture will depend on the environment (time of day, air quality, etc.).
    b. Even if the intruder has moved out of the frame / field of view, a picture will be taken.
    c. The wake-up time for sensors should be short enough (negligible compared to the movement of the person).
    d. Waking up to send packet requires minimal power (negligible)

e. Each sensor knows who its neighbors are, and processes the packets accordingly.

9. **New Requirements:**
    a. The camera sensor has enough local memory to store the picture.
    b. The threshold results in low missed detections and low false detections.
    c. The sensor has an appropriate re-detection rate
    d. The location has lights for night time.

3. Use Case: Send Alarm

1. **Description:** The operator notifies the Response Team of an Intruder inside the unauthorized area.
2. **Primary Actors:** Operator, Response Team
3. **Pre-Conditions:** The Operator has received data from the sensors that a Person is in the unauthorized area.
4. **Flow of Events:**
    a. The Operator analyzes the data.
        i. Information about which sensors have detected the intruder
        ii. Image of the person sent from the camera sensor.
    b. The Operator compares the image of the Person against the database of Authorized Personnel.
    c. Determine the severity of the threat, Intruder or Authorized Personnel
    d. Alerts Response Team if the person is deemed an intruder.
        i. Response Team receives the camera sensor pictures with times and sensor IDs.
    e. The Response Team goes to the location determined by the camera sensor IDs.
5. **Alternate Flow of Events:** None
6. **Post Conditions:** The Response Team ascertains the Intruder.
7. **Assumptions:**
    a. The sensor network is working properly.
    b. The Operator is effective at his/her job.
        i. Aware of motion sensor ID locations.
        ii. Aware of authorized personnel.
        iii. Aware of how and when to notify Response Team.
    c. Response Team is effective at his/her job.
        i. Aware of camera sensor ID locations.
        ii. Quick at getting to location.
        iii. Able to ascertain Intruder.
8. **New Requirements:**
    a. Sensor ID included in camera sensor packet sent to Operator.
    b. Time stamp included in camera sensor packet sent to Operator.
    c. A list of authorized personnel is kept and it is kept up to date.

4. Use Case: Testing

1. **Description:** Before the network is made operation, checks are run to ensure everything is working properly.
2. **Primary Actors:** Operator, Response Team
3. **Pre-Conditions:** The network is being constructed.
4. **Flow of Events:**
    a. For each motion sensor placed, test it to see if it has full functionality.
        i. Send packet
        ii. Receive wake-up
        iii. Change states
        iv. Relay packets
    b. Once the network of motion sensors are placed, check to see if the sensor network has full functionality.
        i. Sensors can communicate with neighboring sensors.
    c. Adjust the threshold on the motion sensor to get the desired sensitivity.
    a. For each camera sensor placed, test to see if it has full functionality.
        i. Send
        ii. Receive
        iii. Change states
        iv. Picture has expected quality
    b. Find the range of the cameras and set the unauthorized area.
5. **Alternate Flow of Events:** None
6. **Post Conditions:** The network is now ready to be operational.
7. **Assumptions:**
    a. The testers are competent.
    b. Have test cases to test the functionality of the motion sensor, camera sensor, and entire sensor network.
    c. Have enough sensors to cover whole area with overlap.
8. **New Requirements:**
    a. none

5. Use Case: Maintenance

1. **Description:** After the network is constructed, checks are done to ensure everything continues to work properly.
2. **Primary Actors:** Operator
3. **Pre-Conditions:** The network is fully constructed.
4. **Flow of Events:**
    a. Receive signal that a sensor has problems.
    b. Fix the problem.
5. **Alternate Flow of Events:** None
6. **Post Conditions:** The network is working properly.
7. **Assumptions:**
    a. The testers are competent.
    b. A problem is fixed.

c. Operator can tell when a sensor has a problem.

8. **New Requirements:**
   a. A sensor can notify the Operator if it is having problems.
   b. A sensor can notify the Operator if a neighboring sensor is having problems.

Requirements and Traceability:

Traceability

Component	Use Case	Requirement	Structure/ Behavioral	Description
Sensor Requirements	1.a	1.1	Behavior	Motion sensors are able to relay packets to the Operator.
	2.a	1.2	Structure	The camera sensor has enough local memory to store the picture.
	2.b	1.3	Structure	The (detection) threshold results in low missed detections and low false detections.
	2.c	1.4	Behavior	The sensor has an appropriate re-detection rate.
	5.a	1.5	Behavior	A sensor can notify the Operator if it is having problems.
	5.b	1.6	Behavior	A sensor can notify the Operator if a neighboring sensor is having problems.
Packet Requirements	1.b	2.1	Structure	Sensor ID included in motion sensor packet sent to operator.
	1.c	2.2	Structure	Time stamp included in motion sensor packet sent to operator.
	3.a	2.3	Structure	Sensor ID included in camera sensor packet sent to operator.
	3.b	2.4	Structure	Time stamp included in camera sensor packet sent to operator.
Data Analysis Requirements	2.d	3.1	Structure	The location has lights for night time.
	3.c	3.2	Structure	List of authorized personnel is kept and it is up to date.
Performance Requirements	1.d	4.1	Behavior	The network should be able to track the movement of the intruder.
	1.e	4.2	Behavior	The delay for relaying information to the operator is smaller than deadline.
	1.f	4.3	Structure, Behavior	The percentage of packet losses is small
	2.e	4.4	Behavior	The sensor network should be able to detect all the intruders with negligible errors.
Miscellaneous Requirements	N/A	5.1	Structure	There is enough redundancy in sensing (both camera and motion) and to cope with failures of neighbors.
	N/A	5.2	Behavior	The operator is able to identify malicious sensors.
	N/A	5.3	Structure, Behavior	The system is resilient to attack on sensors / network
	N/A	5.4	Structure, Behavior	The energy consumption of the network is as small as possible to maximize the network lifetime without increasing the errors.
	N/A	5.5	Structure	The cost of the system is low.

Sensor Requirements

1.a Motion sensors are able to relay packets to the Operator.

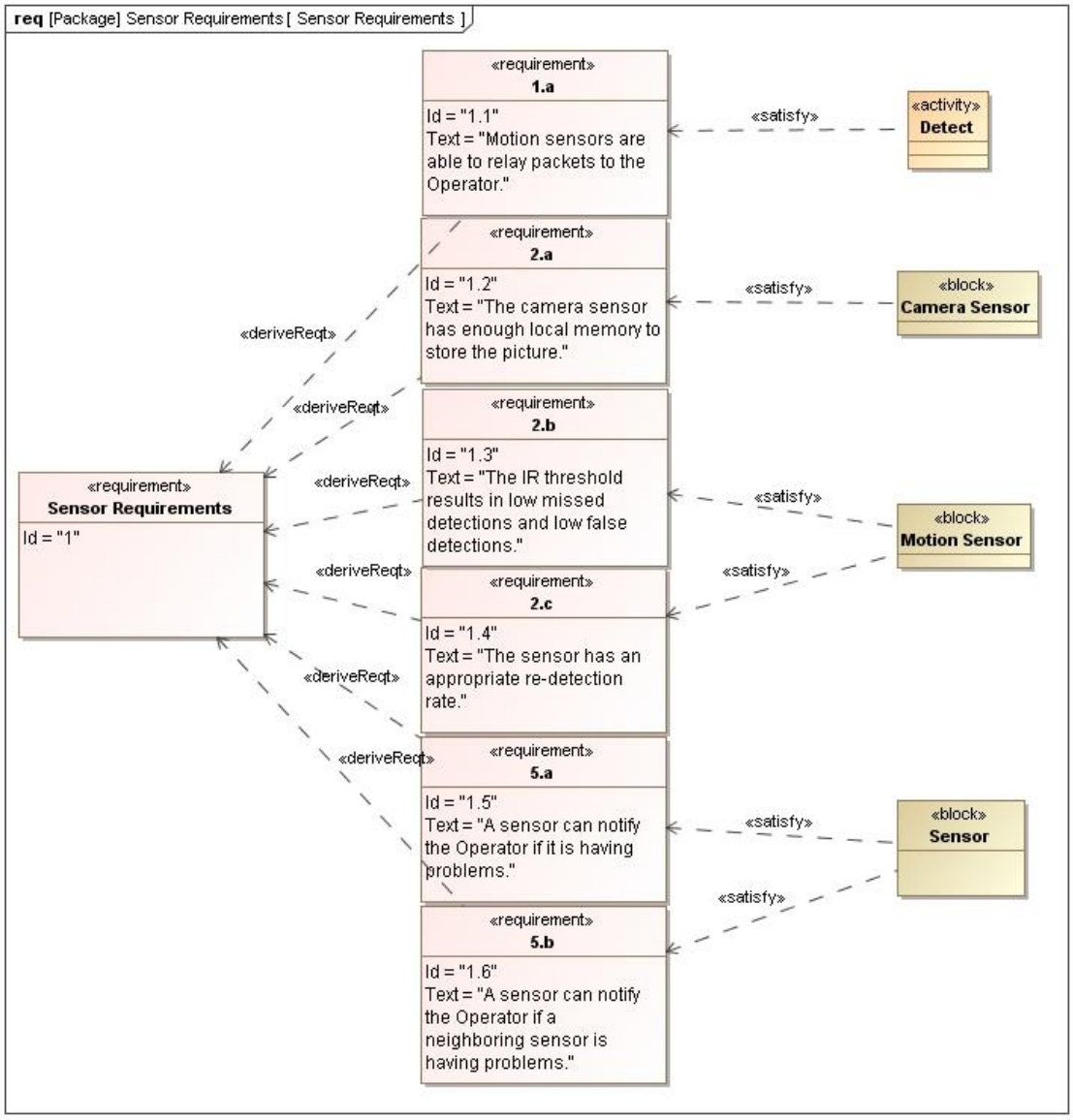
2.a The camera sensor has enough local memory to store the picture.

2.b The (detection) threshold results in low missed detections and low false detections.

2.c The sensor has an appropriate re-detection rate.

5.a A sensor can notify the Operator if it is having problems.

5.b A sensor can notify the Operator if a neighboring sensor is having problems.



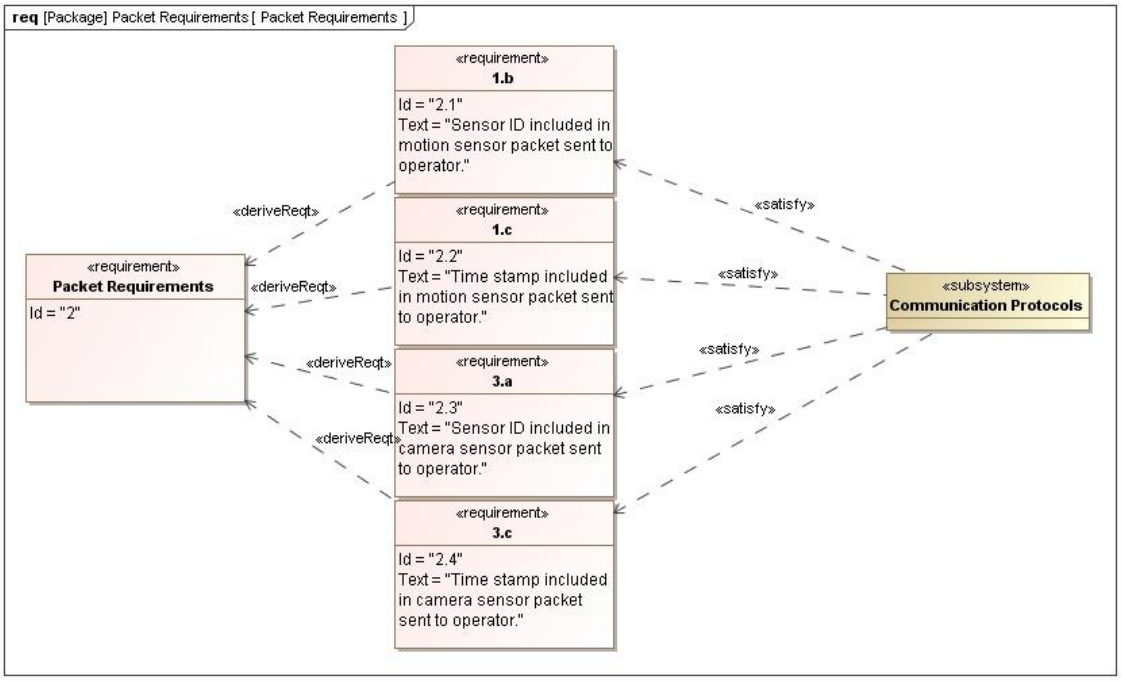
Packet Requirements

1.b Sensor ID included in motion sensor packet sent to operator.

1.c Time stamp included in motion sensor packet sent to operator.

3.a Sensor ID included in camera sensor packet sent to operator.

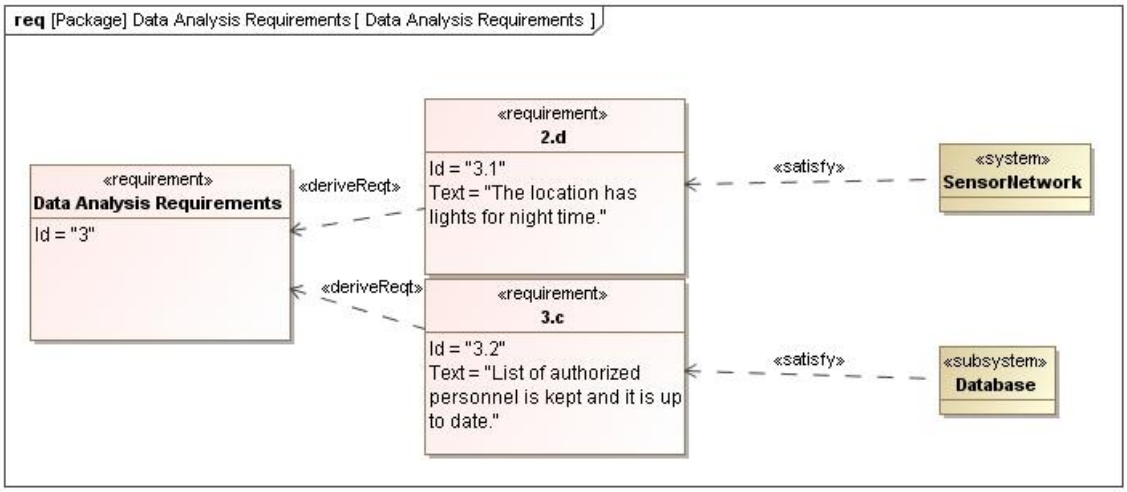
3.b Time stamp included in camera sensor packet sent to operator.



Data Analysis Requirements

2.d The location has lights for night time.

3.c List of authorized personnel is kept and it is up to date.



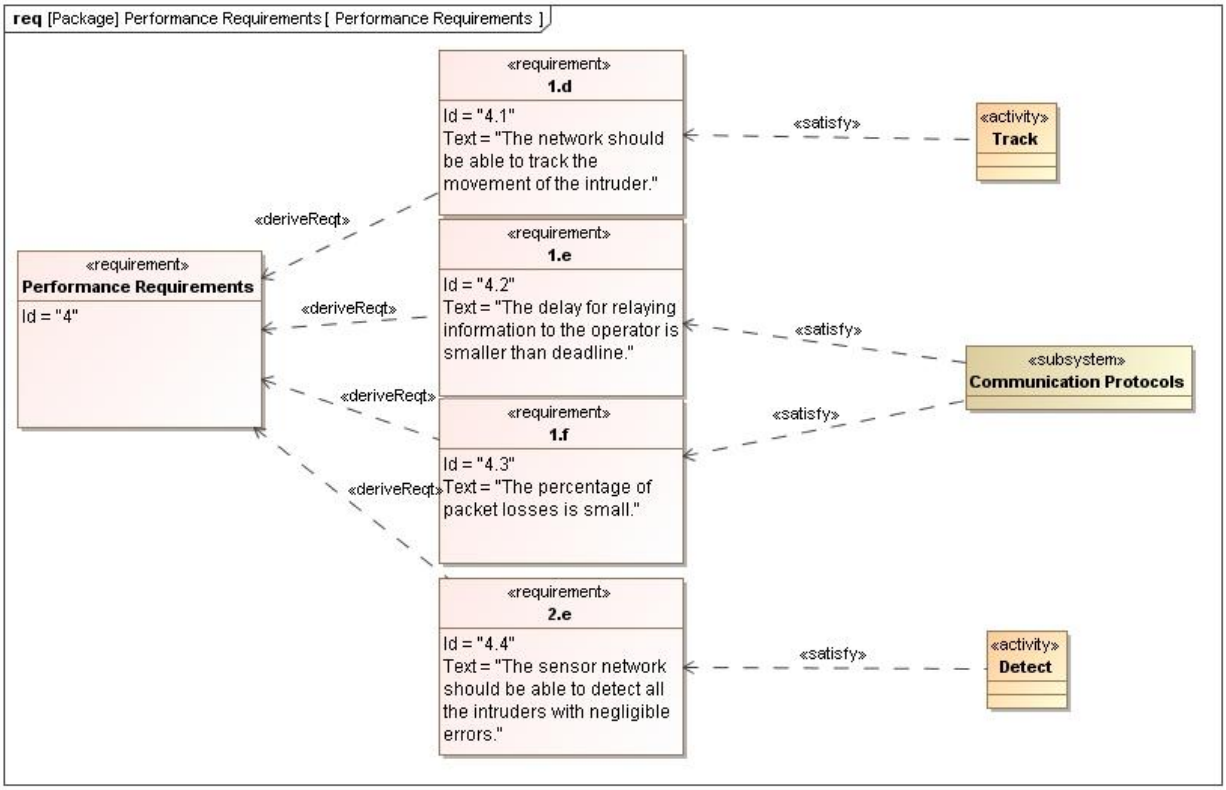
Performance Requirements

1.d. The network should be able to track the movement of the intruder.

1.e The delay for relaying information to the operator is smaller than deadline.

1.f The percentage of packet losses is small.

2.e. The sensor network should be able to detect all the intruders with negligible errors.



Miscellaneous Requirements

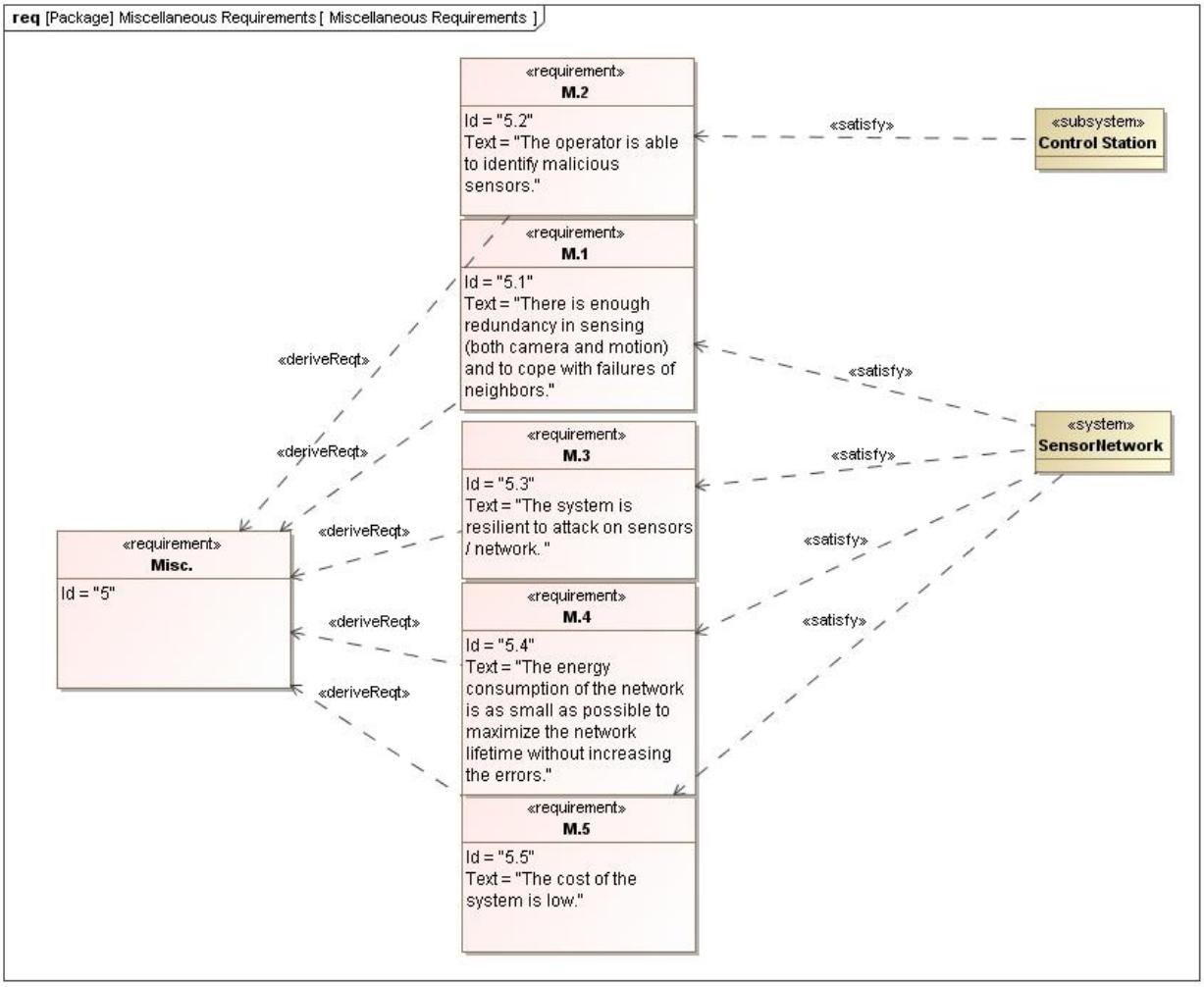
M1 There is enough redundancy in sensing (both camera and motion) and to cope with failures of neighbors.

M2 The operator is able to identify malicious sensors.

M3 The system is resilient to attack on sensors / network.

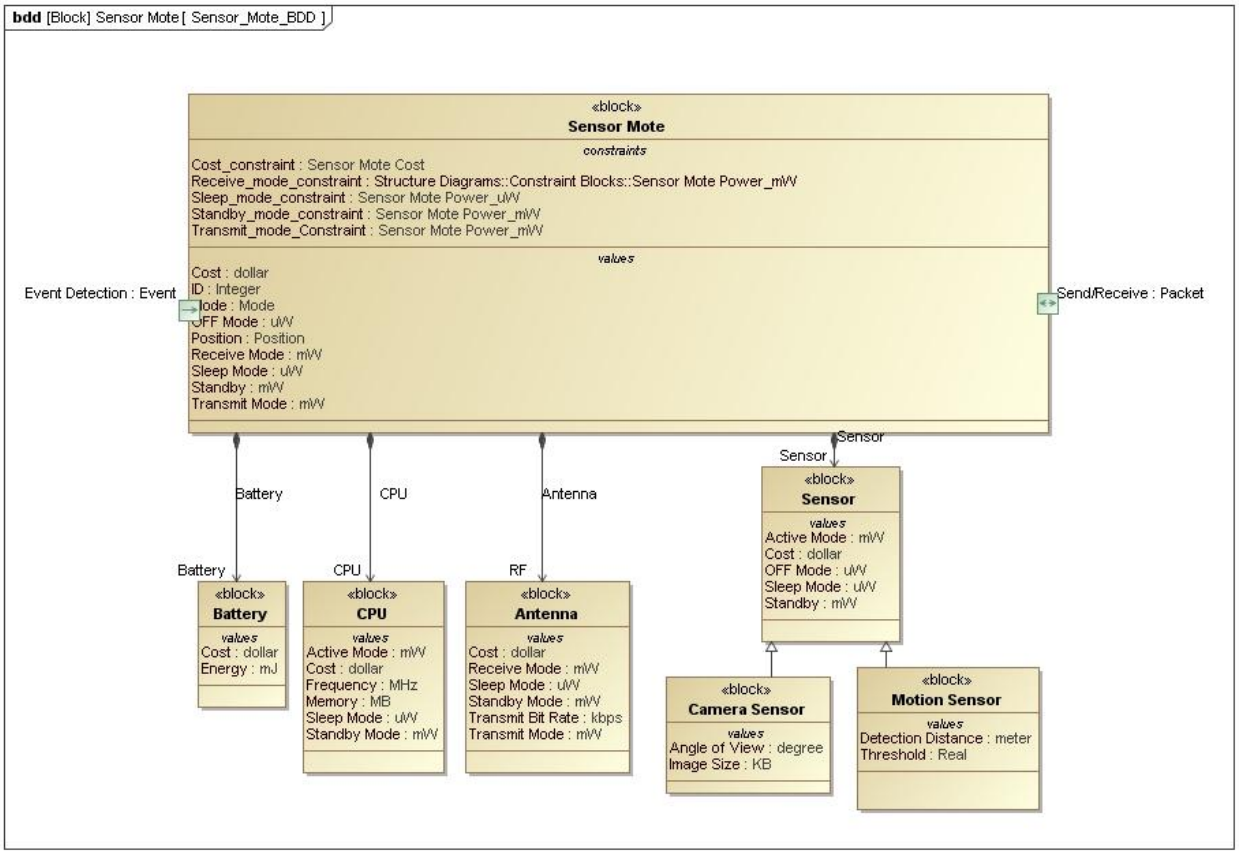
M4 The energy consumption of the network is as small as possible to maximize the network lifetime without increasing the errors.

M5 The cost of the system is low.

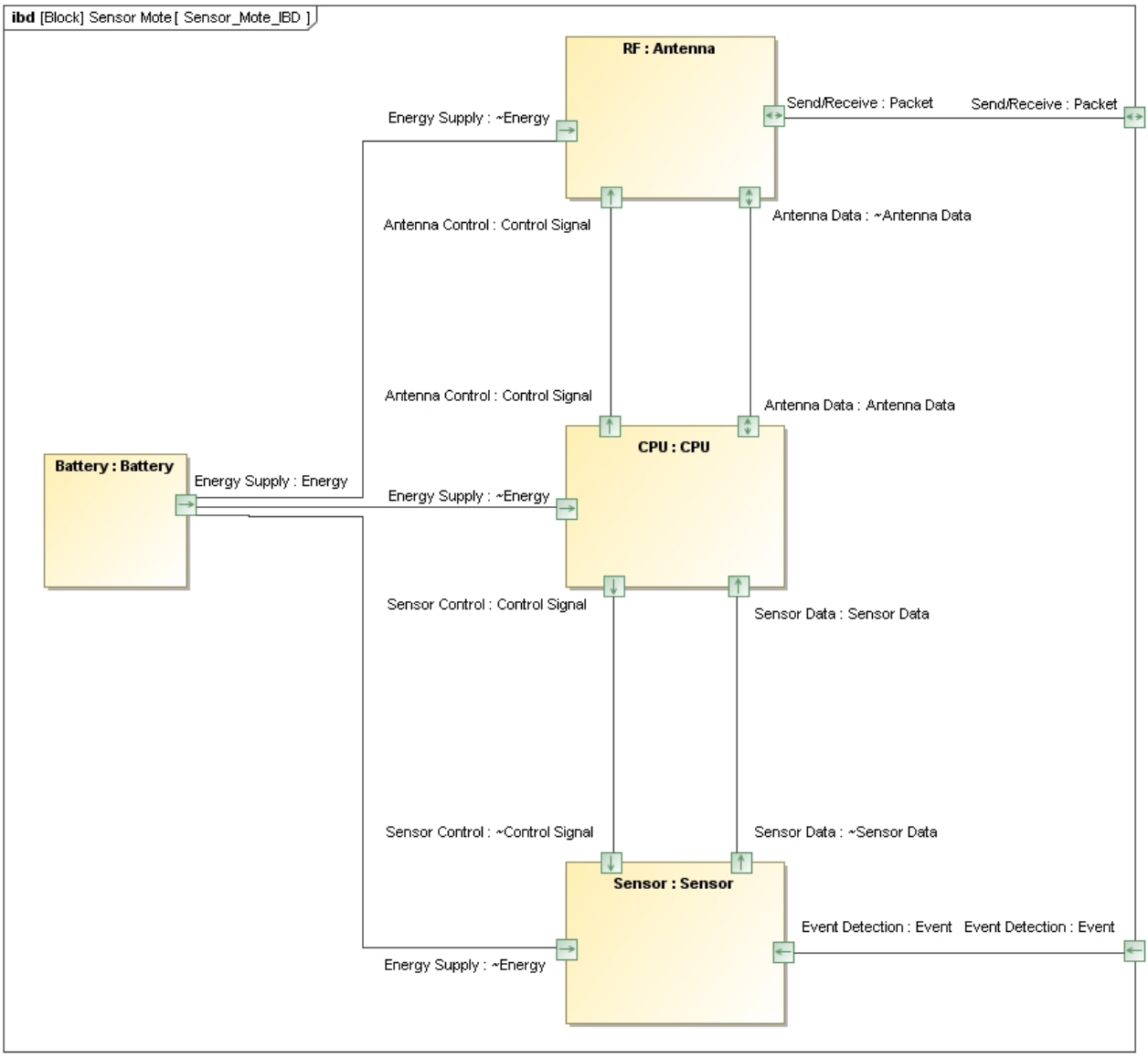


Structure Diagrams

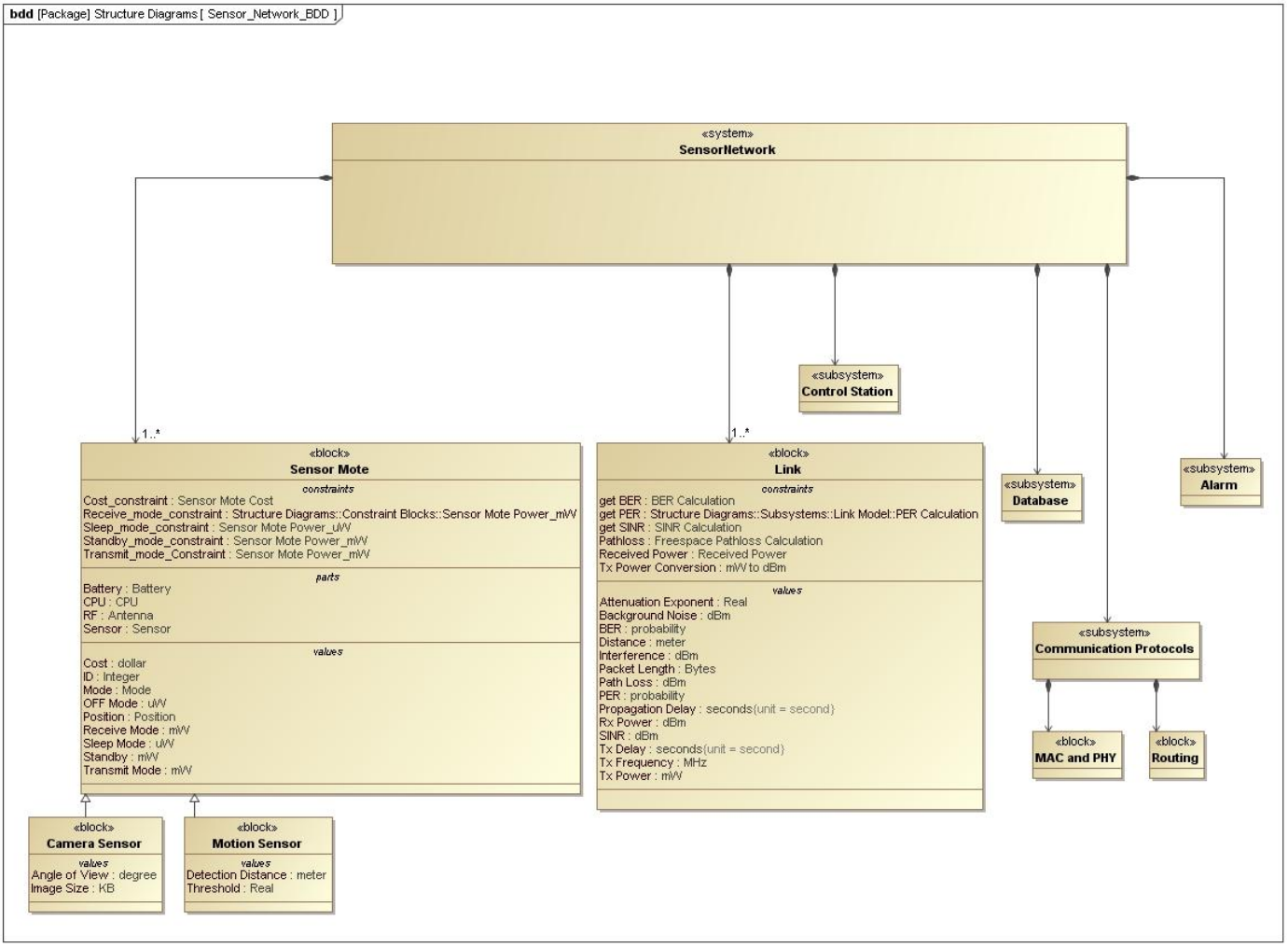
Block Diagram for Sensor Mote



Block Diagram for Sensor Mote

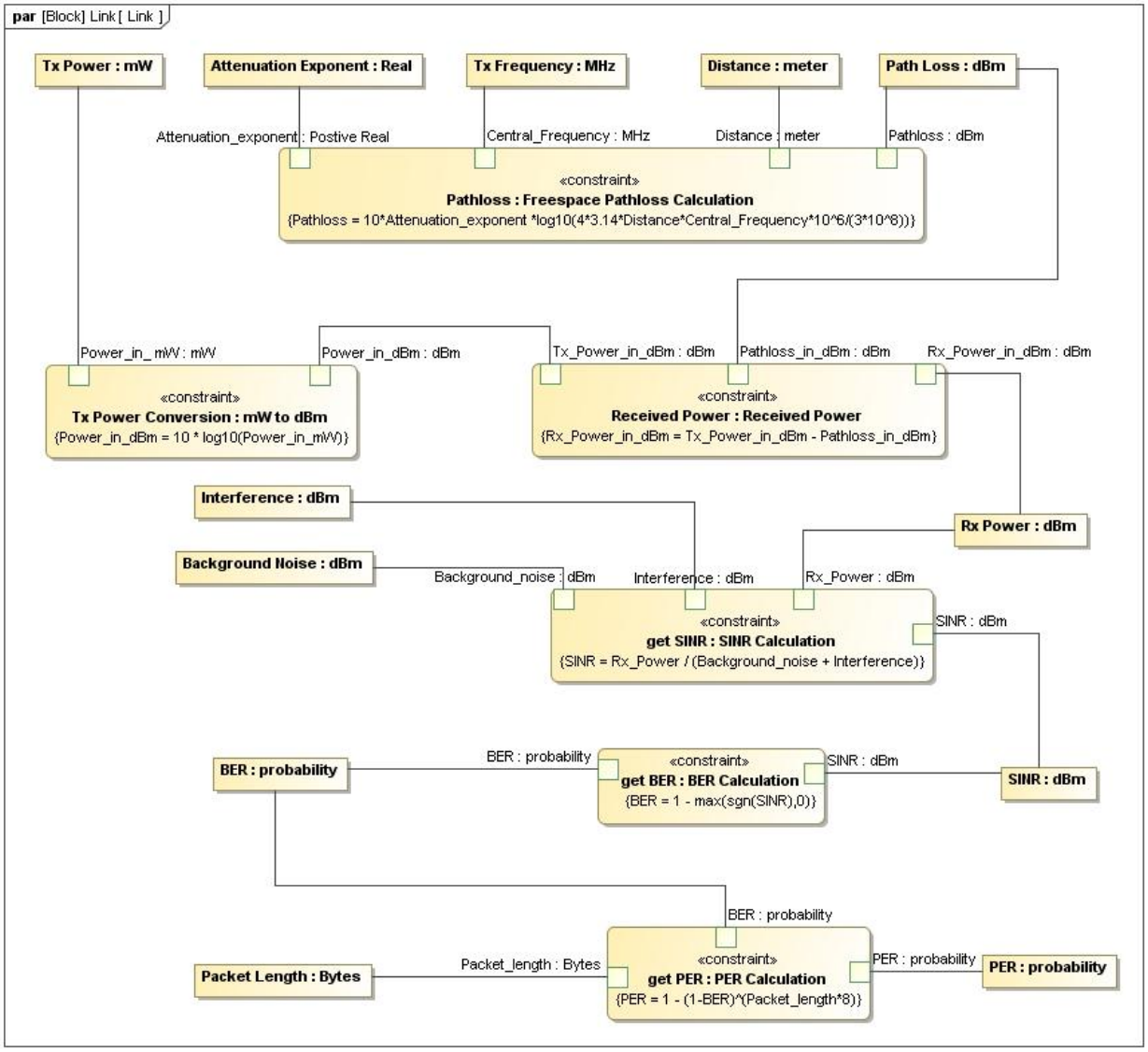


Block Diagram for Sensor Network

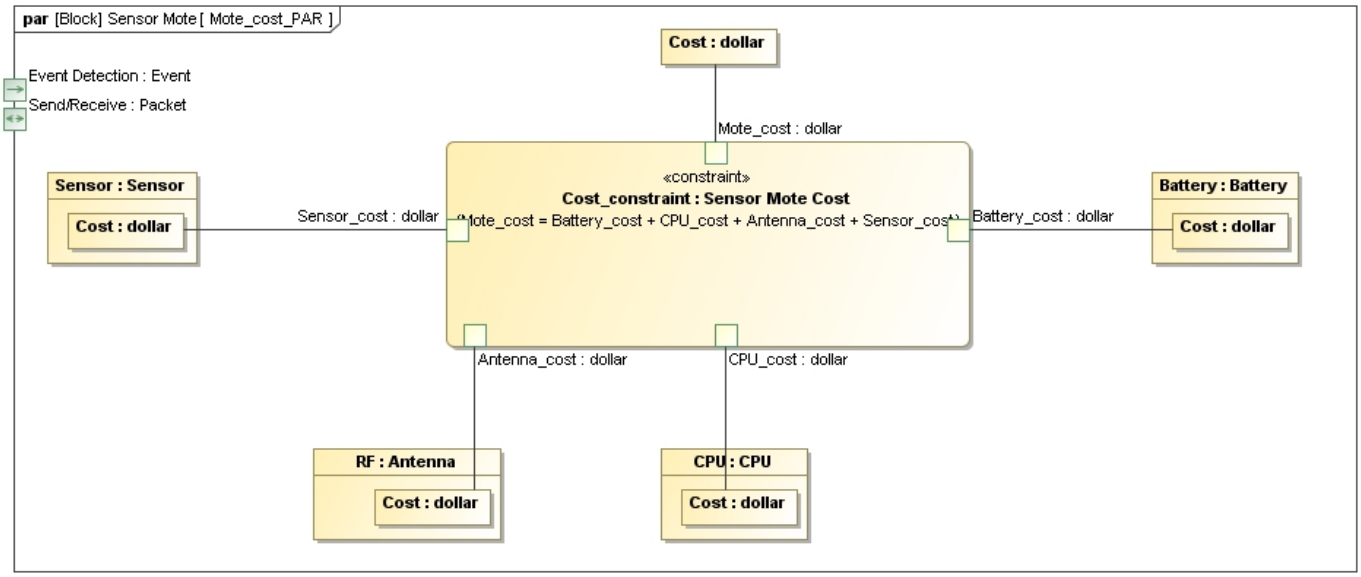


Parametric Diagrams

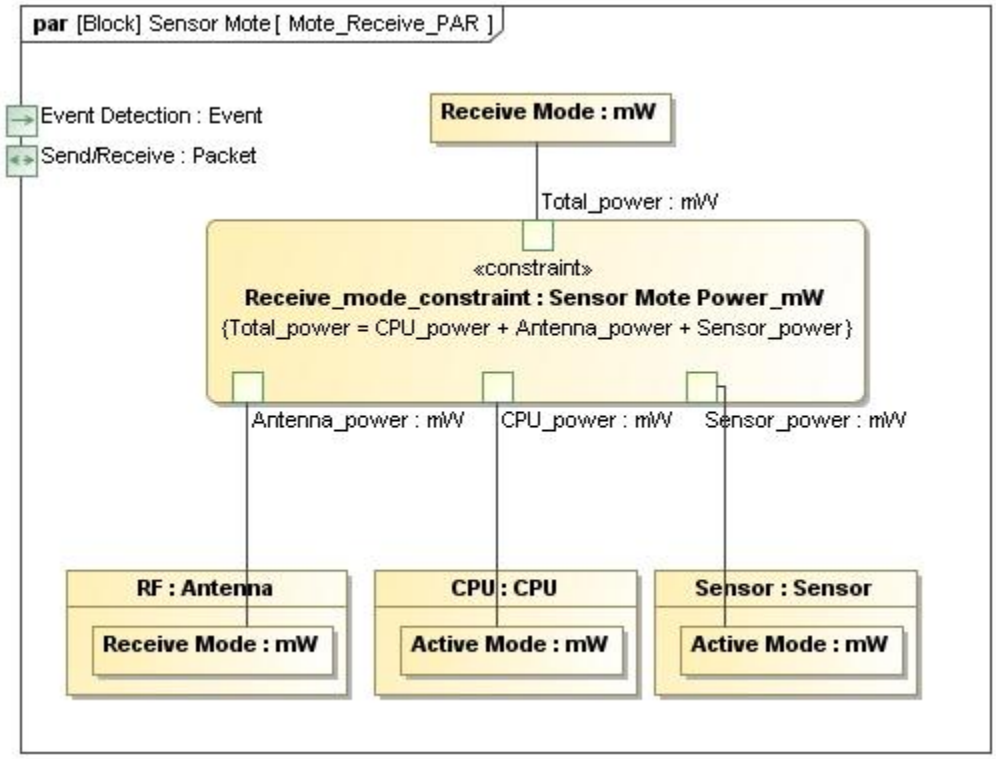
Parametric Diagram for Link



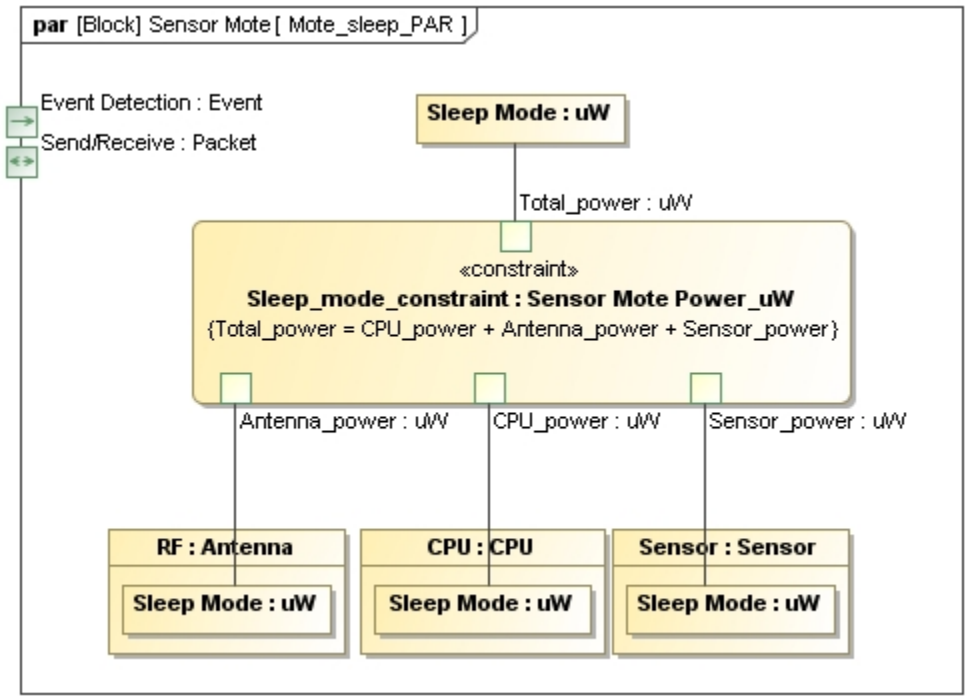
Parametric Diagram for Sensor Cost



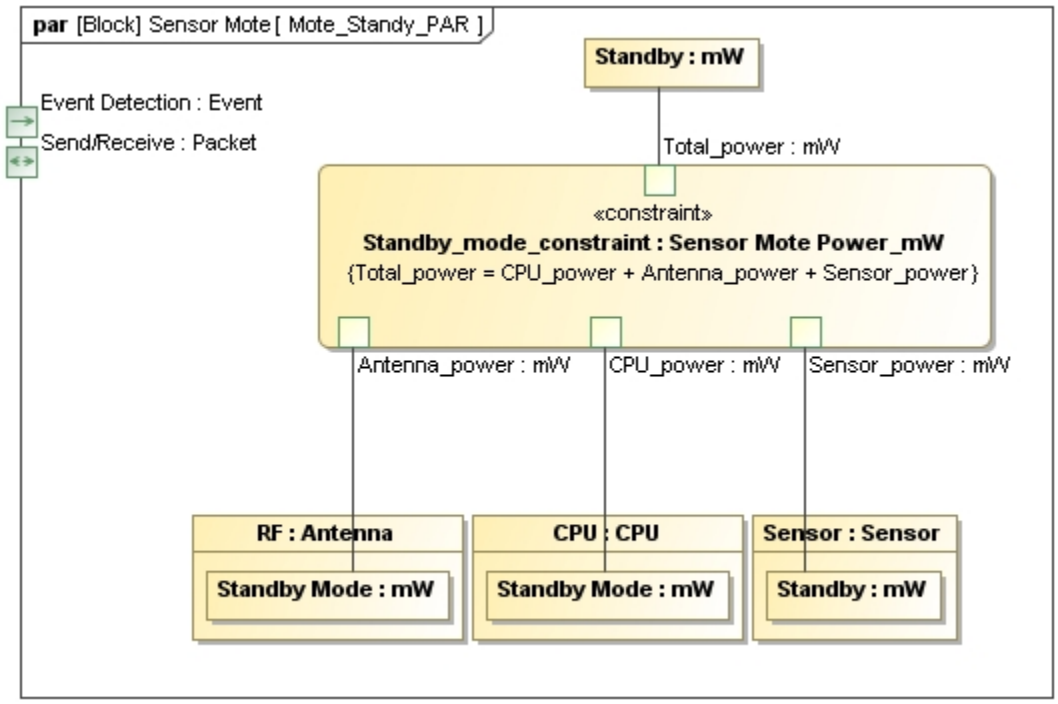
Parametric Diagram for Sensor in Receive Mode



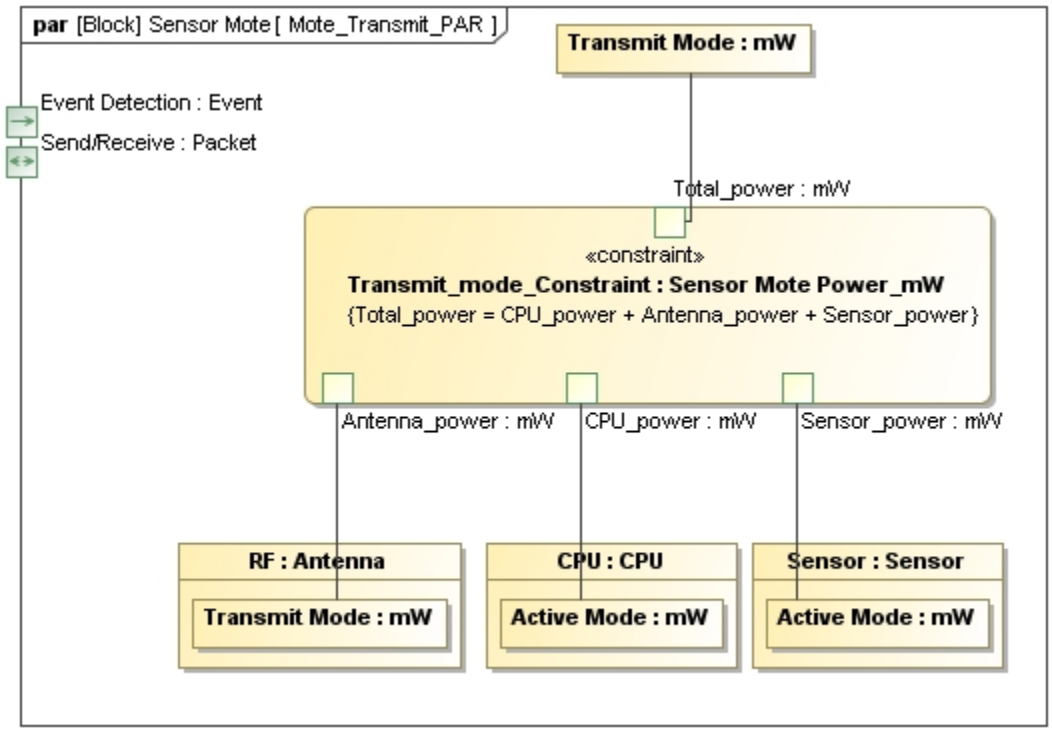
Parametric Diagram for Sensor in Sleep Mode



Parametric Diagram for Sensor in Standby Mode

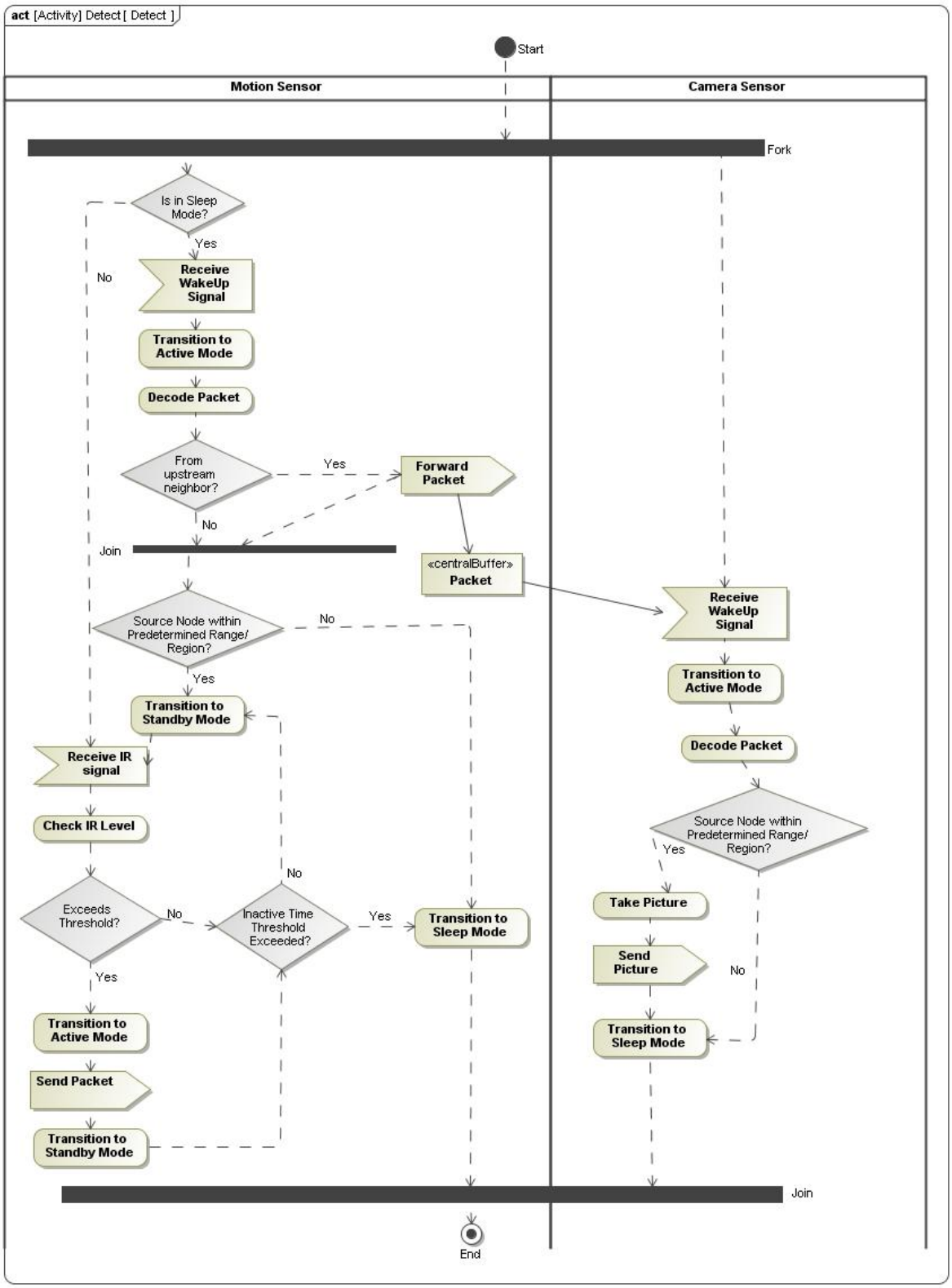


Parametric Diagram for Sensor in Transmit Mode

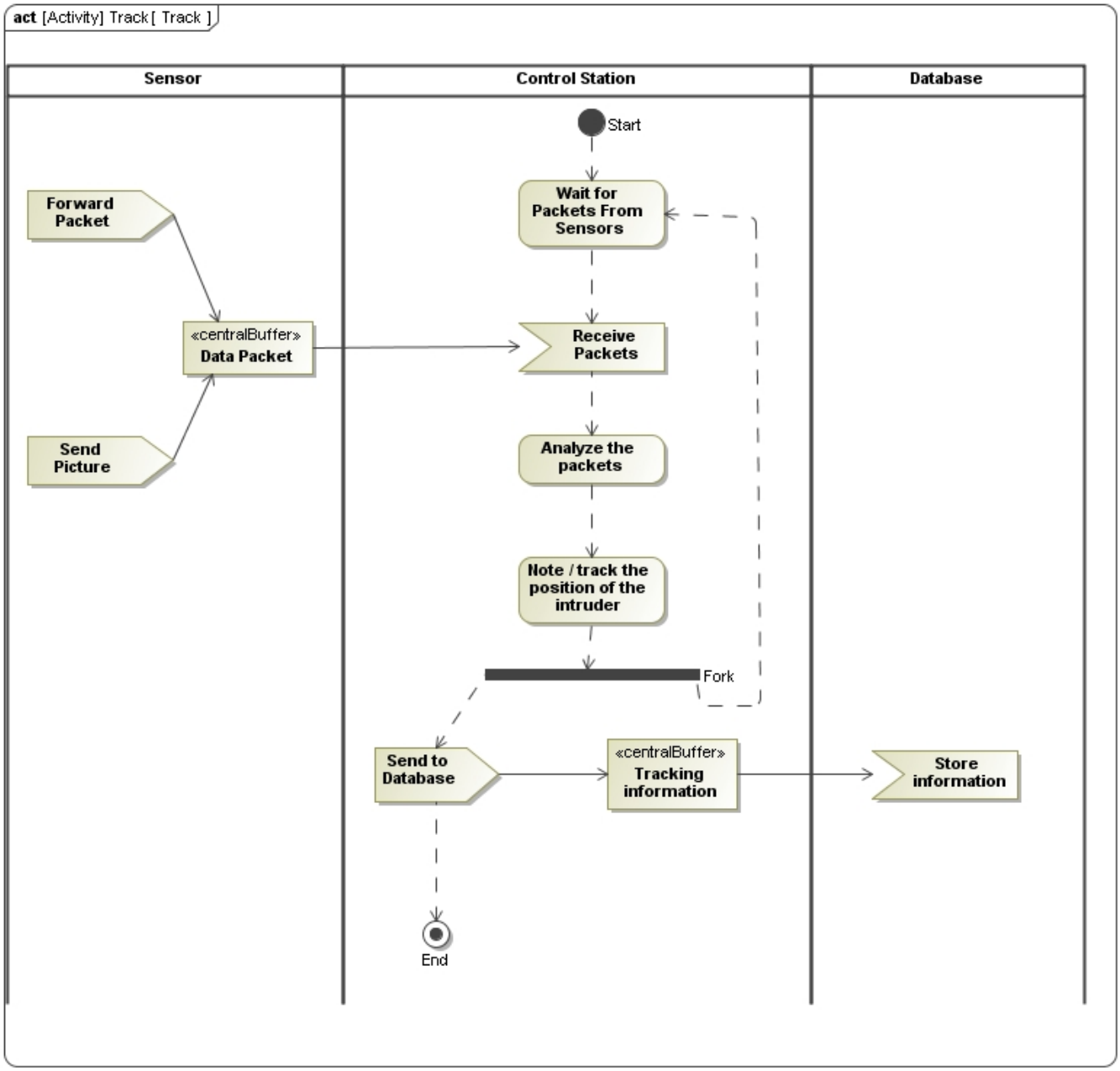


Activity Diagrams:

Activity Diagram for Detect



Activity Diagram for Track

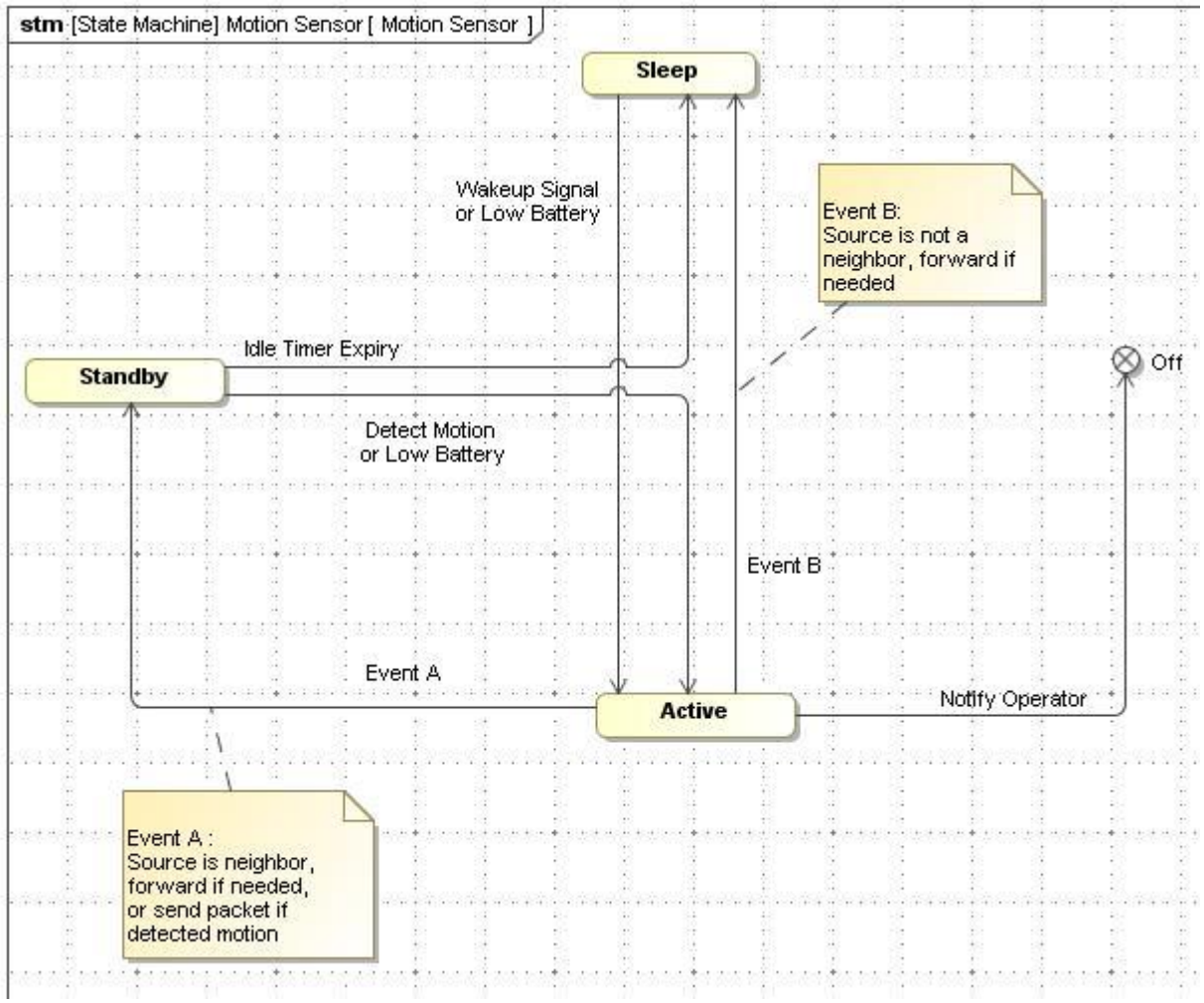


State Transition Diagrams

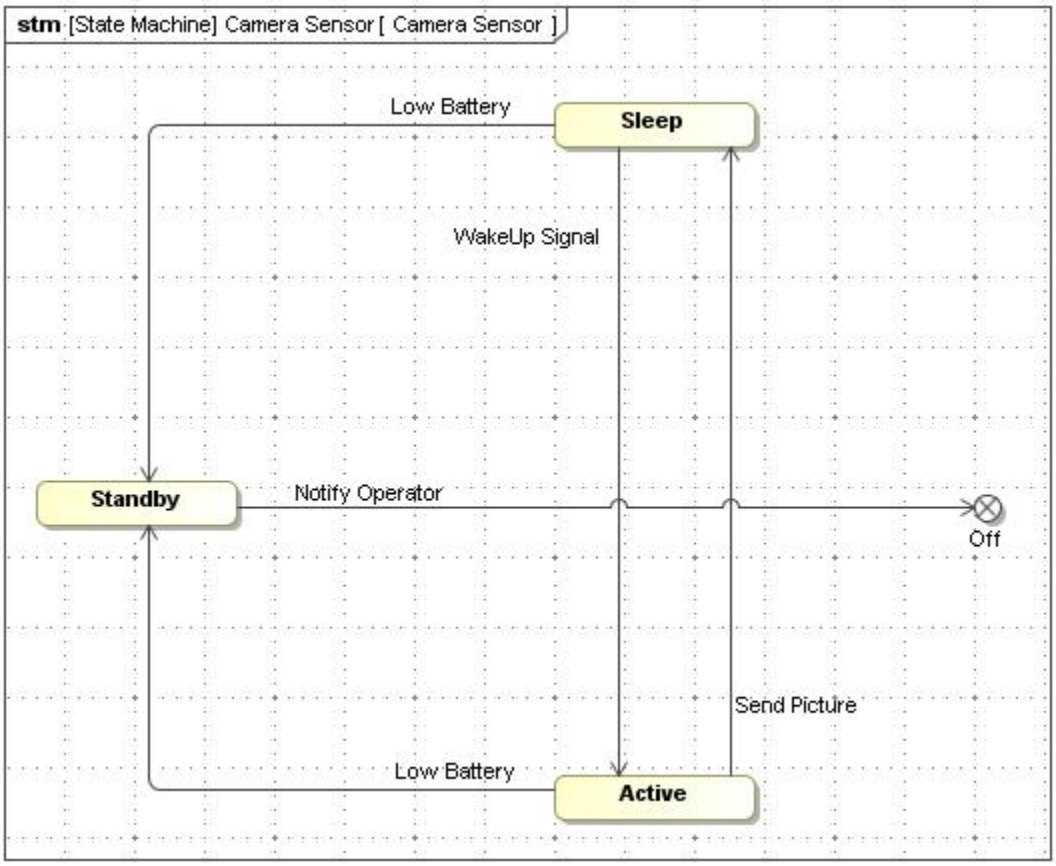
Sensor State Definition

	Motion Sensor Mote		Camera Sensor Mote	
	Sensor	Antenna	Camera	Antenna
OFF	OFF	OFF	OFF	OFF
Sleep	Sleep	Sleep	Sleep	Sleep
Standby	Active	Sleep	Sleep	Active
Active	Active	Active	Active	Active

State Diagram for Motion Sensor



State Diagram for Camera Sensor



Trade-Off Analysis:

Performance Metrics

a) Probability of Missed Detection
b) Energy Consumption
c) Costs

Design Parameters

a) Number of sensors
b) Time the sensors stay awake once woken-up.

Trade-offs -

- Increasing the time sensors stay awake decreases the probability of missed detections, but increases energy consumption.

- Increasing the number of sensors will decrease the probability of missed detection, but increase the costs.

Data Sheet

Antenna (CC2420)

Standby mode: 426 uA * 3.6 V
Sleep mode: 20 uA * 3.6 V
Transmit mode: 17.4 mA * 3.6 V
Receive mode: 19.7 mA * 3.6 V
Transmit Bit Rate: 256 kbps
P = 0 dBm
cost: $100

CPU (PXA 271)

Active mode: 570 mW
Standby mode: 186 mW
Sleep mode: 0.163 mW
cost: $150

Motion Sensor (AMN41121)

Active mode: 400 uA * 6 V
Sleep mode: 40 uA * 6 V
Standby mode: 300 uA * 6 V
Detection distance: 5 meters
Cost: $20

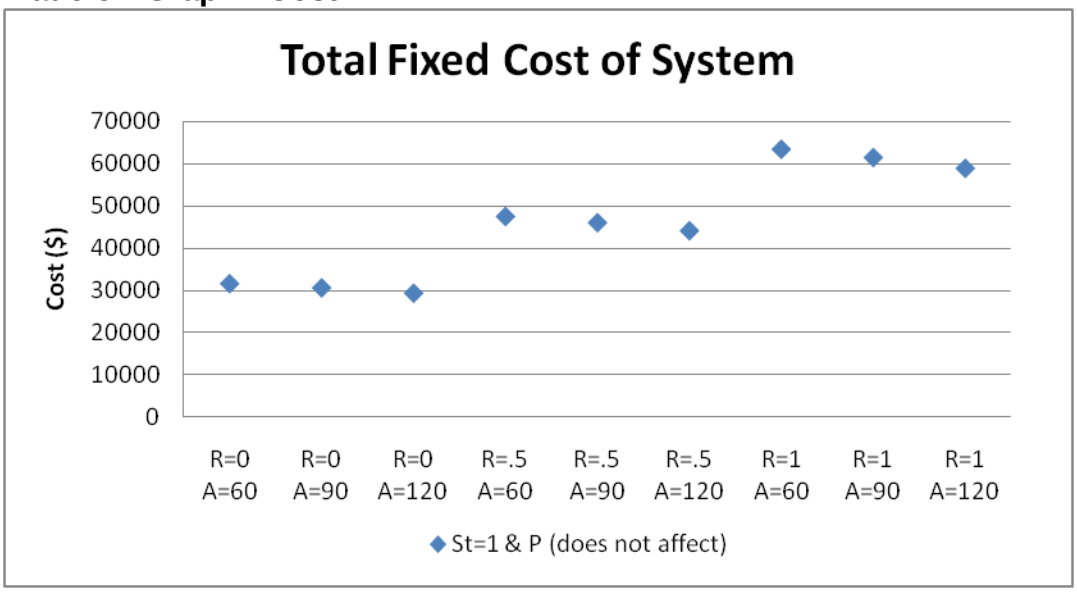
Camera Sensor (OV7649)

Active mode: 40 mW
Sleep mode: 30 uW
Standby mode: 40 mW
Angle of view: 120 degree
Number of Pixels: 3 x 10^5 pixels
Cost: $120

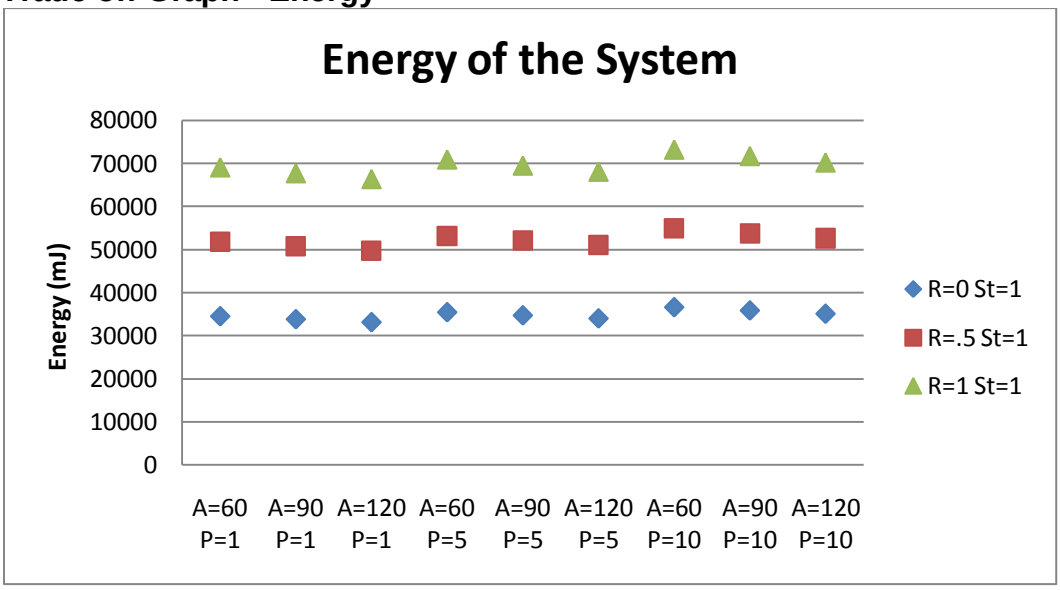
Trade-off Analysis Table

Design parameter	Probability of Missed Detection	Energy Consumption (% Increase)	Cost (% Increase)
Redundancy			
0	0.300%	0%	0%
0.25	0.200%	25%	20%
0.5	0.100%	50%	40%
0.75	0.050%	75%	60%
1	0.002%	100%	80%
Angle of View (Degrees)			
60	0.300%	N/A	65%
75	0.200%	N/A	54%
90	0.100%	N/A	37%
105	0.050%	N/A	18%
120	0.002%	N/A	0%
Idle Time (Minutes)			
1	1.000%	0%	N/A
5	0.500%	10%	N/A
10	0.250%	20%	N/A
20	0.125%	40%	N/A
Transmit Power (mW)			
1	1.00000%	0%	N/A
5	0.50000%	20%	N/A
10	0.02500%	40%	N/A
20	0.01250%	80%	N/A

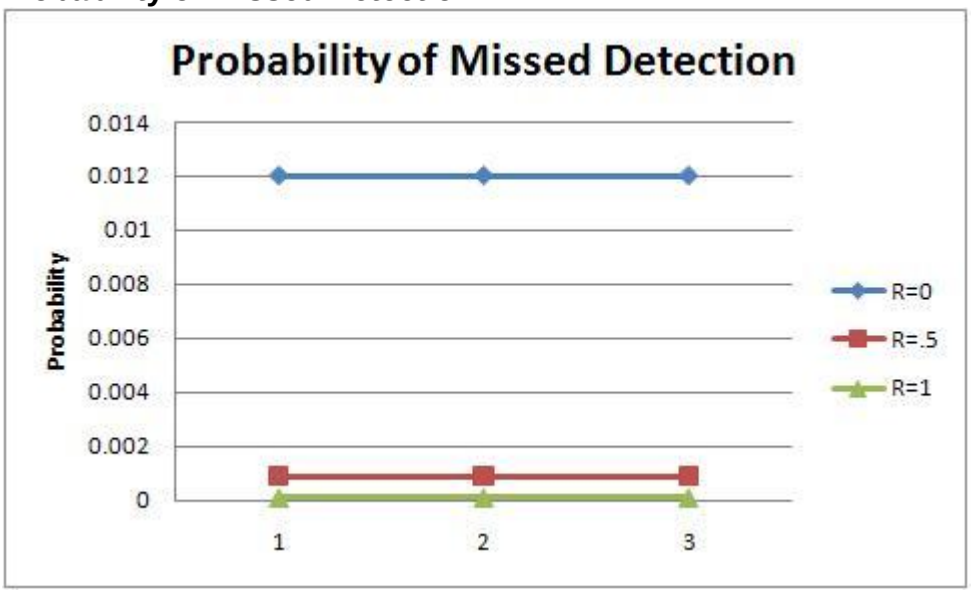
Trade off Graph - Cost



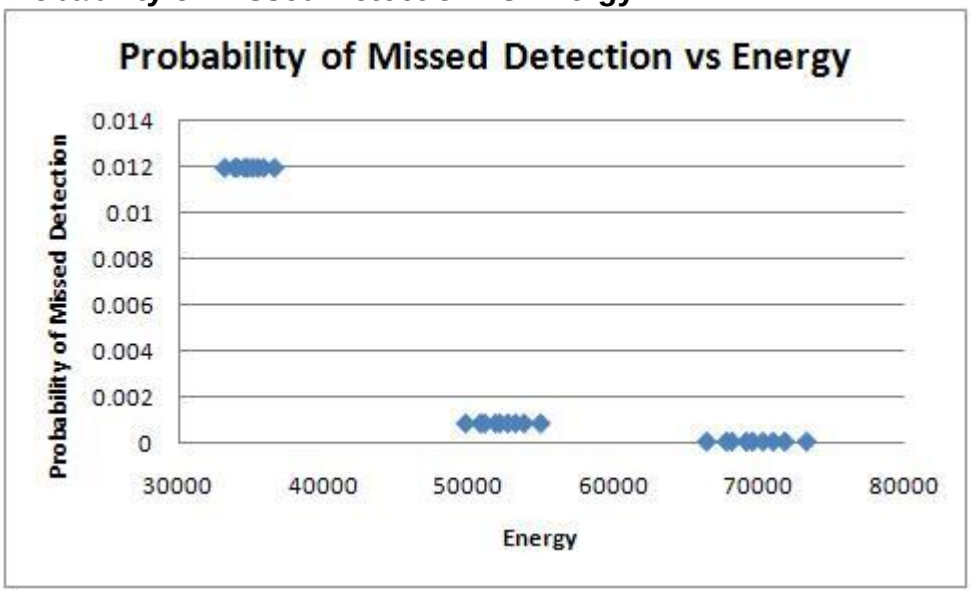
Trade off Graph - Energy



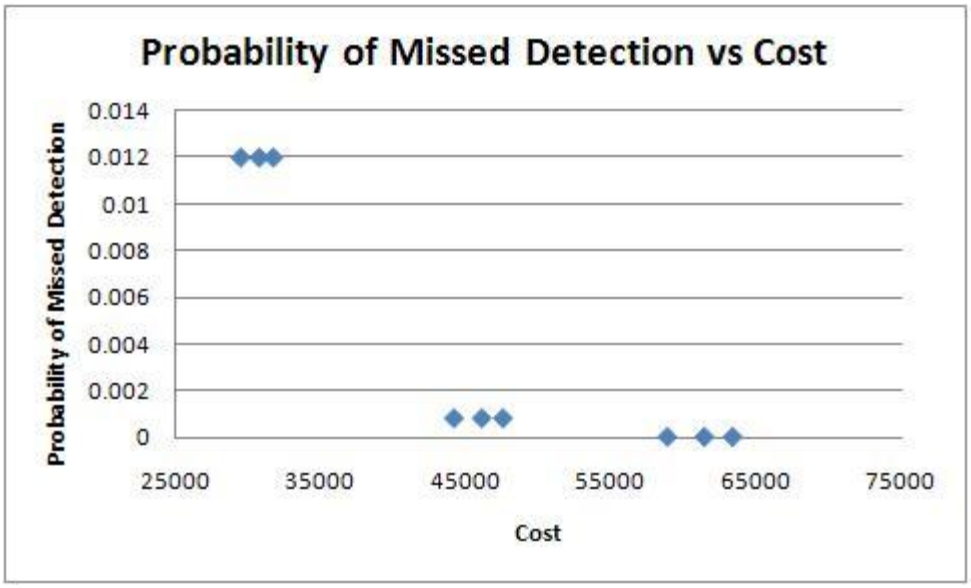
Probability of Missed Detection



Probability of Missed Detection vs Energy



Probability of Missed Detection vs Cost



R = Redundancy Factor
A = Camera Sensor Field of View Angle
St = Stand By Time
P = Transmit Power of Antenna

Test and Validation

- Use UPPAAL to verify the state transitions for the motion and camera sensors with timing information and that there are no deadlocks.
- Verify by inspection that the component level-requirements are met.
- Verify each sensor is individually working properly
    - motion sensor senses motion in its vicinity; the detection threshold is set appropriately.
    - camera sensor captures good quality picture.
    - sensors change their states according to proper timing or event-triggers.
- Test functionality of subsystems
    - alarm subsystem generates alarm.
    - database stores pictures and responds to queries by the controller.

    - controller properly authenticates a picture of a authorized personnel captured by one of the camera sensors.

- Test system level requirements by trial runs with a dummy intruder.
    - The system detects the entry
    - Sensors send and forward messages appropriately
    - Sensors change state properly
    - The controller correctly tracks the motion of the intruder
    - Camera sensors capture picture.

- Testing of sensor failure scenarios (security and resilience to failure)
    - Sensors generate low battery signal appropriately.
    - Other sensors detect loss of neighboring sensors, notify the controller and modify their functionalities accordingly.
    - Controller keeps track of failed sensors
    - Controller analyzes data to identify malicious sensor.
    - Controller sends alarm if too many sensor nodes compromised.

- Verifying performance requirements are met through analysis
    - Using parametric diagrams, and solvers like Mathematica and Matlab, compute the performance metrics and verify the margin of error from performance requirements.