Using Context in Security Design of a Search and Rescue System

Shivakant Mishra

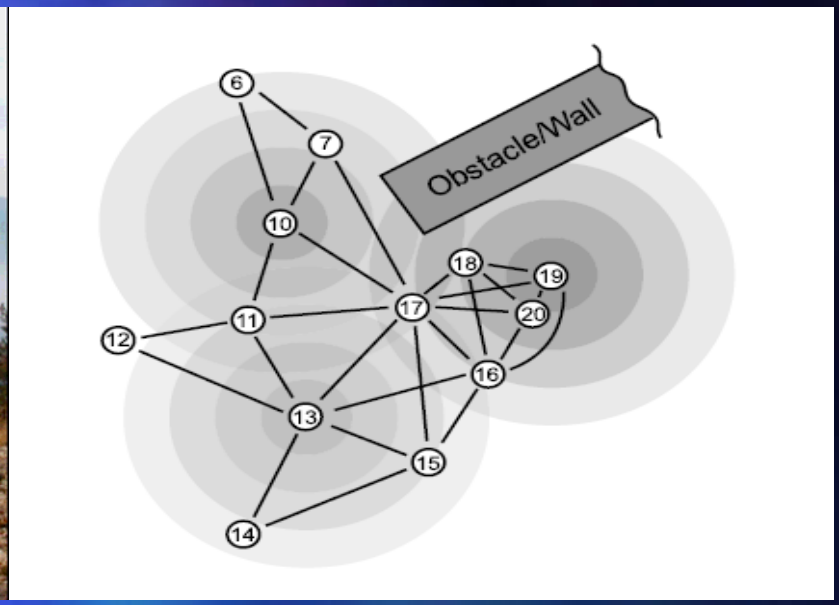
Department of Computer Science

University of Colorado at Boulder

Outline of the Talk

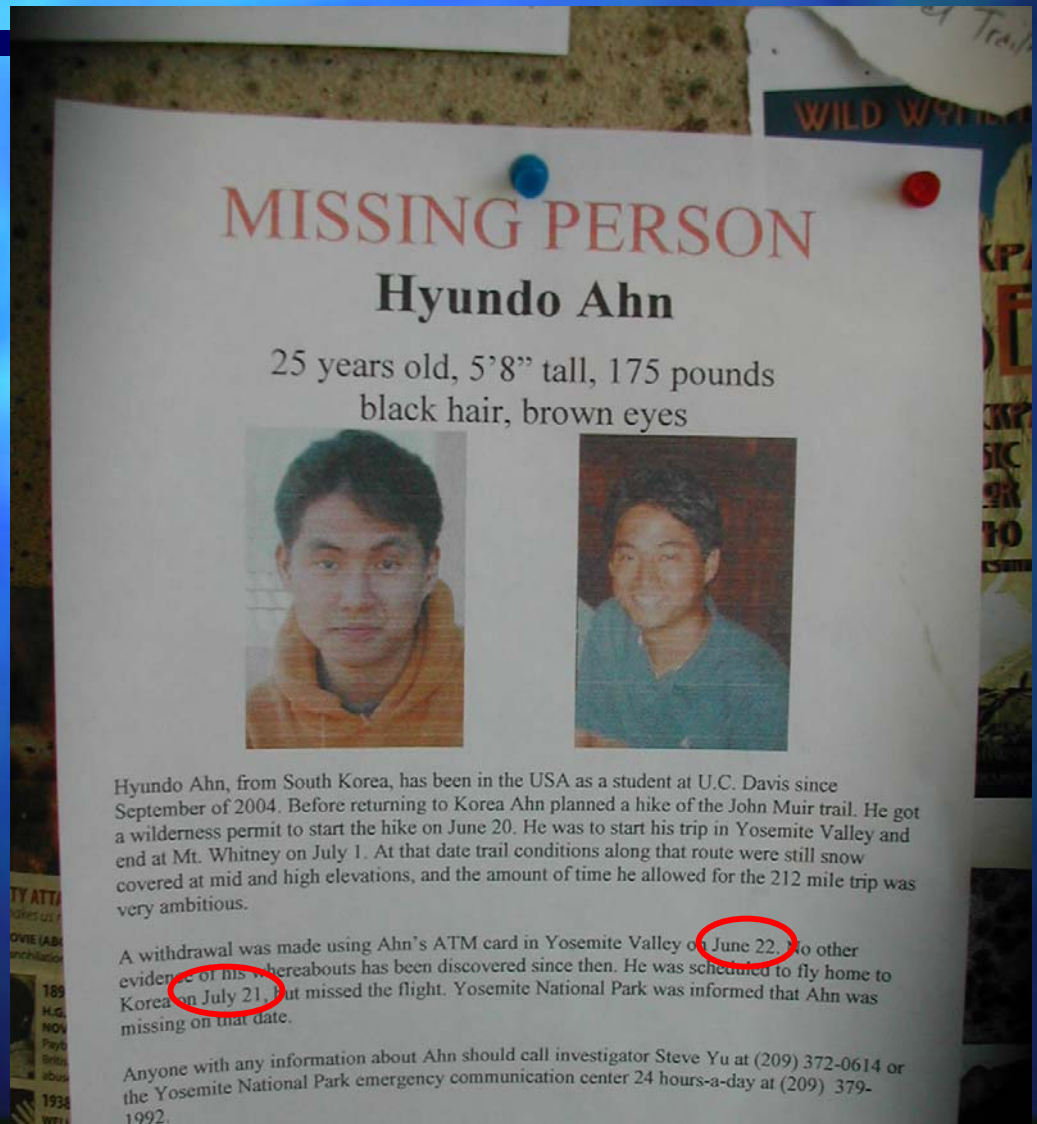
- What is Occasionally Connected Wireless Sensor Network
- Cenwits Search and Rescue System
- Security and Privacy for Cenwits
- Questions and Future Work

Introdu



- Wireles
  - Sens
    other
- Occasionally Connected Wireless Sensor Network(OCWSNs)
  - Sensor nodes are in the range of each other occasionally and it's ok to fetch data with longer delay. Nodes are mobile
- OCWSNs Can be divided into two categories:
  - Closed Trail: Hiker tracking; Vehicular Network
  - Open Field: Wildlife monitoring; Soldier Tracking

Motivation: Improve "last seen point" Technology



MISSING PERSON

Hyundo Ahn

25 years old, 5'8" tall, 175 pounds
black hair, brown eyes

Hyundo Ahn, from South Korea, has been in the USA as a student at U.C. Davis since September of 2004. Before returning to Korea Ahn planned a hike of the John Muir trail. He got a wilderness permit to start the hike on June 20. He was to start his trip in Yosemite Valley and end at Mt. Whitney on July 1. At that date trail conditions along that route were still snow covered at mid and high elevations, and the amount of time he allowed for the 212 mile trip was very ambitious.

A withdrawal was made using Ahn's ATM card in Yosemite Valley on June 22. No other evidence of his whereabouts has been discovered since then. He was scheduled to fly home to Korea on July 21, but missed the flight. Yosemite National Park was informed that Ahn was missing on that date.

Anyone with any information about Ahn should call investigator Steve Yu at (209) 372-0614 or the Yosemite National Park emergency communication center 24 hours-a-day at (209) 379-1992.

Cenwits: A Search and Rescue System

- Goal: To build a search and rescue system that can pinpoint missing person's last seen point in wilderness areas
  - Lost hikers, stranded climbers, injured skiers, …
  - Difficult now because of lack of timely information about the historical locations
- "Last seen point" is critical for search and rescue actions

Current Search and Rescue Technologies

- The Old School Way – Ask
- Personal GPS receiver and Satellite transmitter – Power greedy; Must operate manually to send your location
- Localization system and GSM transmitter – Need GSM network coverage
- Avalanche beacon/RFID reflector – Limited usage

- Need a better, cheaper, reliable system

Design Goals for CenWits

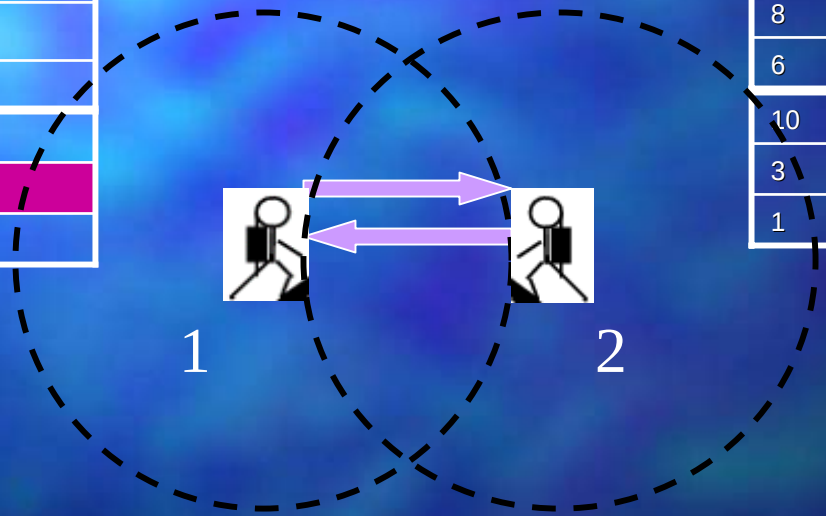
- Self-Operate, long life time
- Small and light weight(2.2oz)
- Non intrusive; no infrastructure needed
- Power and memory efficient
- Cheap($20~$50)
- Meets security and privacy requirements

Cenwits

- A Connection-less Sensor-Based Tracking System Using Witnesses
- Comprised of
  - RF sensors
  - GPS receivers
  - Access points
  - Location points
  - Control center

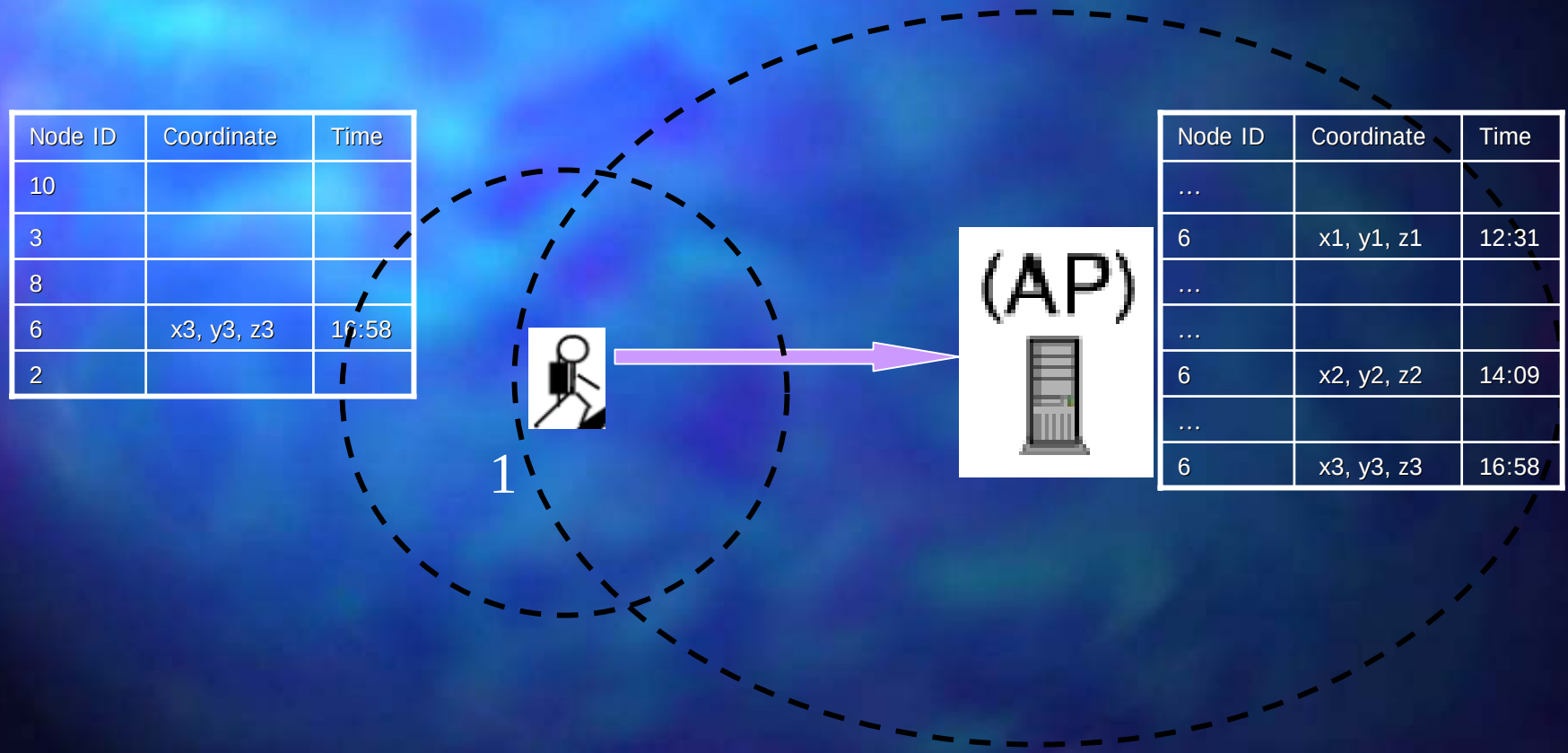
Cenwits – How it Works (I)

Node ID	Coordinate	Time
10		
3		
8		
6		
2		



Node ID	Coordinate	Time
8		
6		
10		
3		
1		

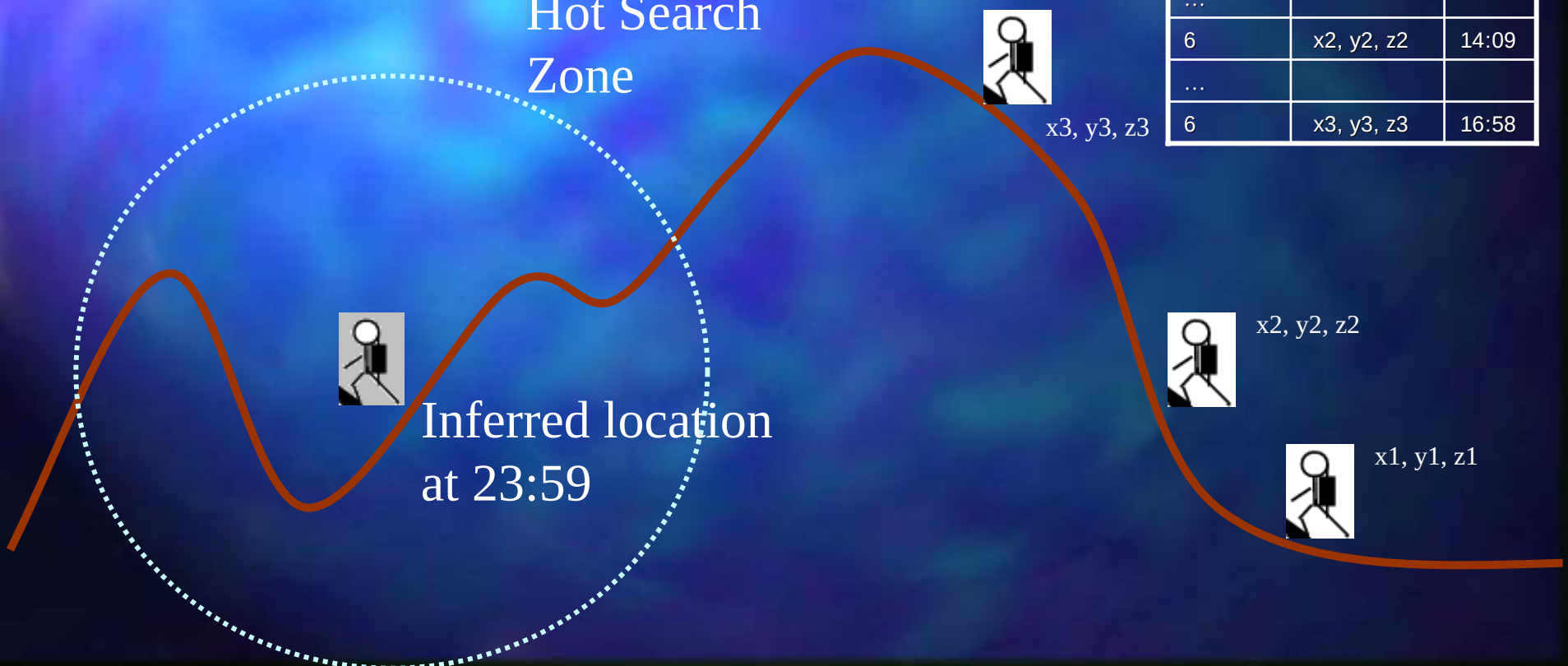
Cenwits – How it Works (II)



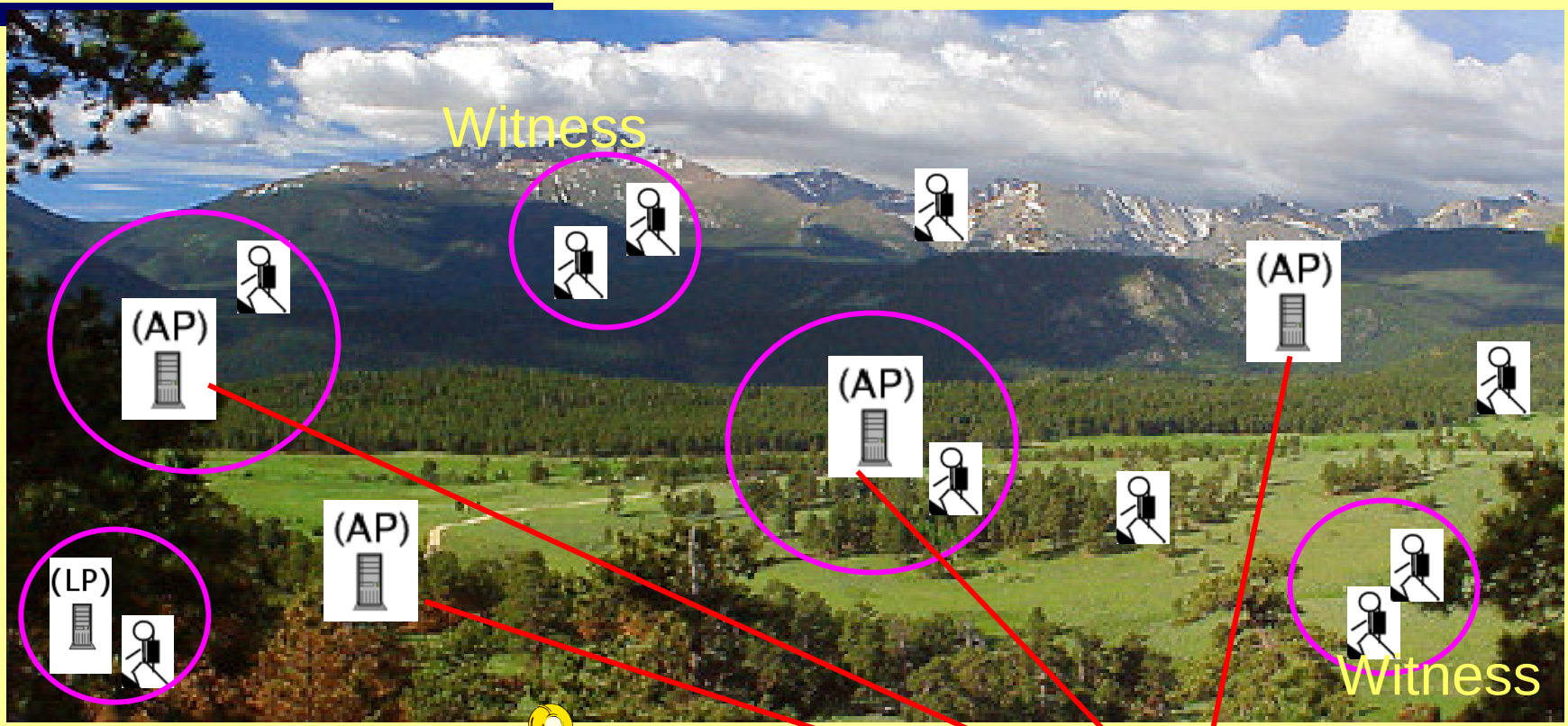
Cenwits – How it Works (III)

Hiker 6 is reported missing at 23:59

Node ID	Coordinate	Time
…		
6	x1, y1, z1	12:31
…		
…		
6	x2, y2, z2	14:09
…		
6	x3, y3, z3	16:58



CenWits – System Structure



Search & Rescue Team

Control Center

Security and Privacy

- CenWits can be used to track a person's location and movement
  - Stalking
  - Major hindrance in a wider deployment of CenWits

Two Conflicting Issues

- Smaller and more accurate search area
  - Collect as much location and movement info as possible
  - It is in the interest of a person to give out as much info as possible
- Prevent location and movement tracking
  - Give out little info

A multi-level security and privacy framework.

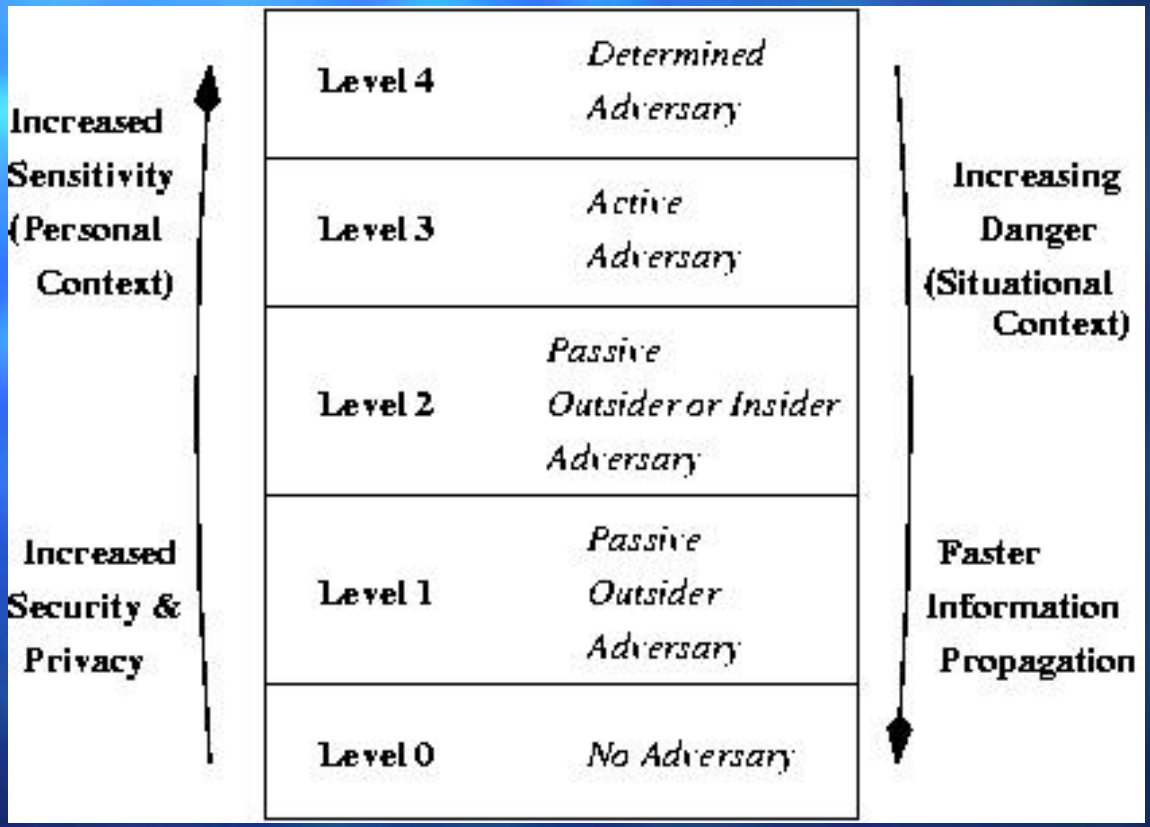
Context Awareness

- Security and privacy support is strongly context-dependent
  - Situational Context
    - Level of danger as perceived by a person
  - Personal Context
    - Level of comfort a person has in divulging his/her movement info

Multi-Level Framework

- Individual sensitivity towards tracking location and movement info varies based on situation.
- A lower level of security generally translates to a faster propagation of one’s location and movement info.

Multi-Level Security Framework



Multi-Level Framework

- Level 0
  - Absence of any security and privacy support
  - No attempt for confidentiality, authentication, or tamper resistance
  - No overhead, fast info propagation
  - Extreme danger
- Level 1
  - Protection from passive, outsider adversary
  - Support for confidentiality: a single, system-wide symmetric key

Multi-Level Framework

- Level 2
  - Passive adversary – outsider or insider
  - Support for message confidentiality and detecting duplicate records
  - Separate shared keys between AP and each sensor node.
- Level 3
  - Protection from active adversary
  - Separate shared key between each hiker and the AP
  - Support for confidentiality, authentication, tamper resistance, detecting replay attack, …

Multi-Level Framework

- Level 4
  - Protection from a determined and powerful adversary
    - Destroy the system
  - Unlikely scenario

Discussion

- Carefree user: level 0 or 1
- Security/privacy sensitive user: level 2 or 3
- A user must understand the implications of his/her security level setting
- A user can change his/her security setting
- Automatic change in security levels?

Current Status

- Technical design is complete
- Asymmetric and Symmetric key cryptography has been used
- Asymmetric crypto
  - Authentication
- Symmetric crypto
  - Confidentiality, tamper resistance, …