# Wireless Network Security
## Spring 2016

Patrick Tague

Class #18 – Location Service Security

# Class #18

- Location services and how they work

- Attacks on location services

# GPS

- Global Position System was developed by the US DoD initially in the 1970s and completely operational in 1994
  - Similar to other systems deployed by Russia, EU, China, India, and others

- Satellites broadcast current time and their location to allow receivers on Earth (and elsewhere) to localize

# Things using GPS

- GPS is used for:
  - Automobile navigation (and autonomous driving)
  - Mobile geo-location (for LBS, etc.)
  - Livestock / wildlife tracking
  - Aircraft and ship navigation and autopilot

  - Power grid synchronization
  - Financial transactions & trading
  - Telecom system operations
  - ...

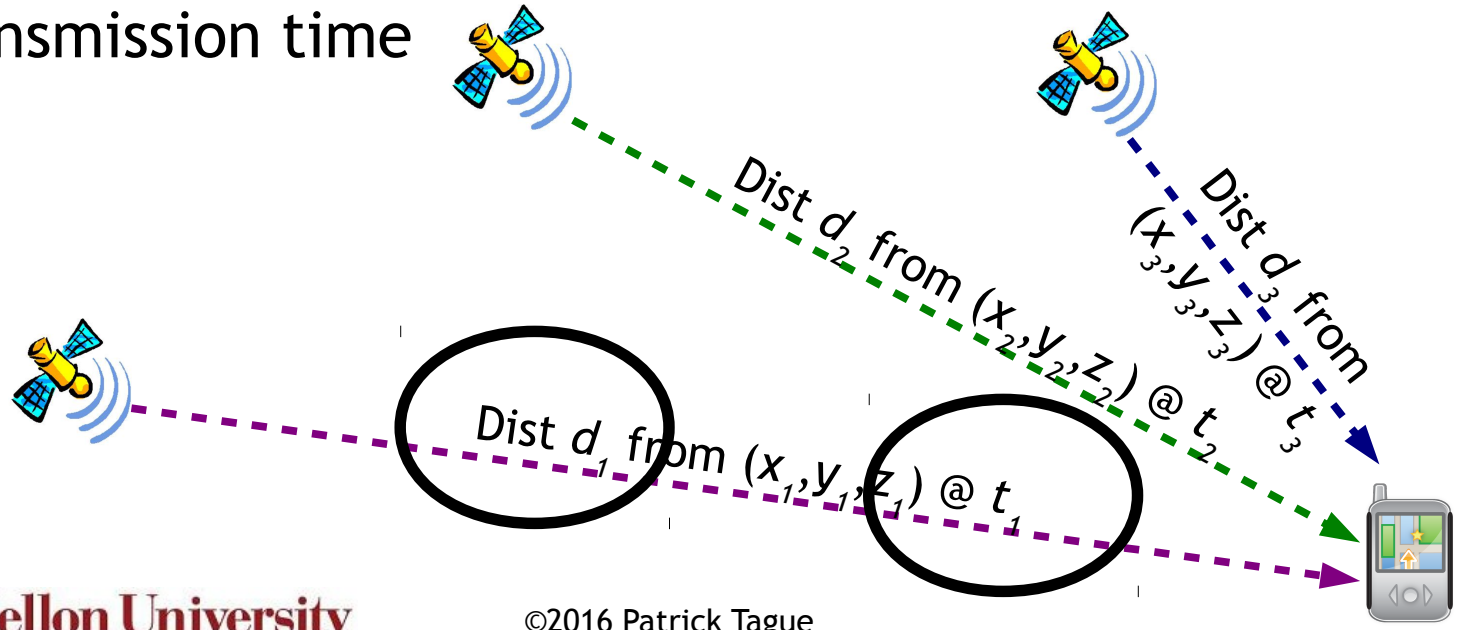
# So, how does GPS actually work?

# GPS Signals

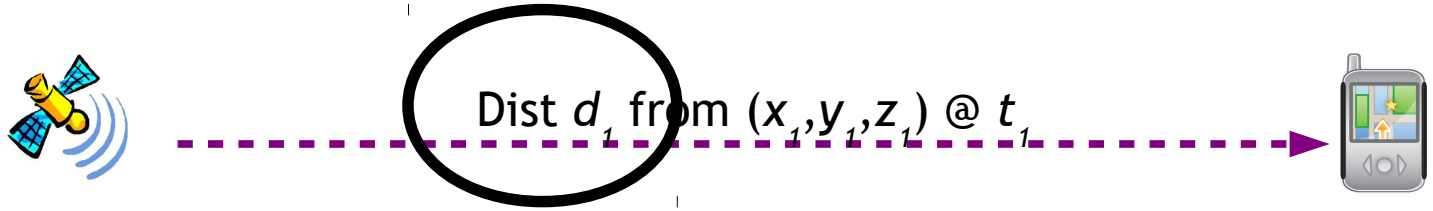
- GPS satellites send several different signals
  - On the L1 band (1575.42 MHz), coarse-acquisition (C/A) signal, encrypted precision (P(Y)) signal, L1 civilian (L1C) and military (M) codes
  - On the L2 band (1227.60 MHz), P(Y) code, L2C and M
  - Three other bands (L3, L4, L5) used for other purposes
    - Nuclear detonation detection, atmospheric correction, civilian safety-of-life

# Multilateration

- GPS satellites serve as mobile reference points for Earth-based receivers
  - All satellites have high-precision, tightly synchronized clocks and precisely known locations
  - Each receiver hears a coordinate and timestamp from each transmitter, measures the distance based on the transmission time

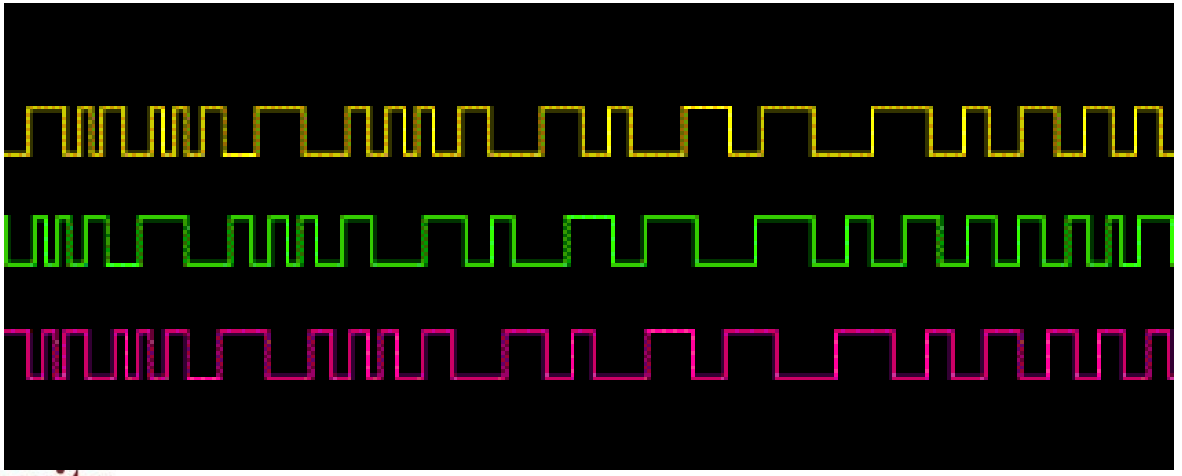


# Measuring Distance

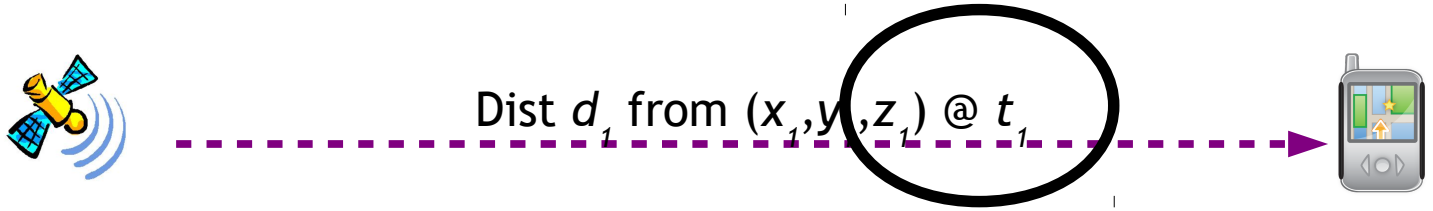



- How to measure distance from the satellite?

- Well, *distance* = *speed of light* * *time*, so just measure time...



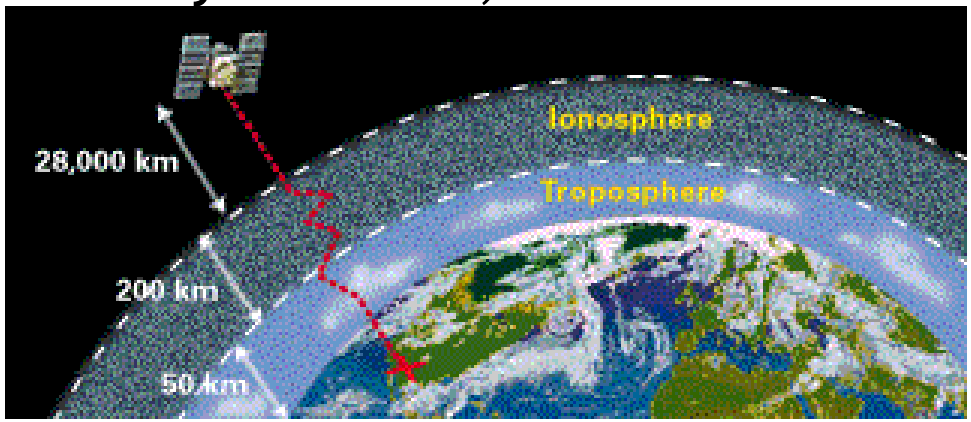
# Receiver Timing




- Satellites themselves use atomic clocks to maintain ground truth
  - Receivers have to synchronize with the satellites
  - Remember, 1ns time error → 1ft distance error
- With clever processing, an extra satellite signal provides required synchronization
  - 3 satellites for space, 4 for space+time

# Errors

- Errors arise for many different reasons
  - Scattering through Earth's atmosphere, reflection off buildings, time sync errors, etc.




  - Much of this can be handled by incorporating proper models in the distance estimation process
    - But, no longer just *distance* = *speed* * *time*
  - Some receivers get diversity from using military & civilian signals

# Military v. Civilian GPS

- Civilian GPS uses an unencrypted and unauthenticated signal for location and time synchronization

- Military GPS devices can be keyed to use an encrypted and authenticated signal for high assurance location and timing
  - Military GPS requires key management, often in the form of manually entering long keys into handsets
  - Use of the military signal can provide much higher accuracy, error correction, etc.

# Military GPS Rumors

- Since manual key management is often an impediment to mission-critical activities, there have been reports that a large number of soldiers use GPS in civilian mode

# Selective Availability

- When GPS was originally designed, it was intended to provide coarse-grained location for civilians and fine-grained location for military
  - Does anyone remember when GPS accuracy was 20-30 meters and that was good enough for most things?

- Selective Availability was eliminated around 2000 to provide higher accuracy for civilian applications
  - Usually, we can get <5 meter accuracy

# Differential GPS

- For applications that require even better accuracy
  - Differential GPS uses an additional signal sent from a ground station to compensate for errors in data sent by satellites
  - E.g., DGPS stations can send difference between location claimed by satellite and its observed location
  - Accuracy of ~10cm can be achieved using DGPS
    - Appropriate for autonomous / swarm vehicle applications

# Jamming

- GPS is based on wireless communication, so it's subject to interference
- GPS RSS is on the order of femtowatts (~$10^{-15}$ W or -120 dBm) [some sources say .1fW or 100 attoWatts]
  - Jamming is pretty easy

*Traffic on busy I-95 highway passes close by Newark Airport*

# What are the possible security issues with GPS?

# Replay Attacks

- Replay of GPS transmissions would involve stale timestamps and location information
- The content of the message would be good
- But the time sync step would fail and most likely give unreasonable results
  - Unless the timing is precisely controlled...more in a minute

# GPS Spoofing

- Instead of replaying old GPS signals, fabricate new ones and pretend to be a satellite
  - Spoofing leverages lack of authentication in civilian GPS signals
- Provides invalid information to the receiver to force it to compute an incorrect location
- Practical spoofers have been demonstrated

# Timed Replay Spoofing

- Todd Humphreys's team built a spoofer (see [Humphreys et al., ION GNSS 2008])
  - It receives signals, analyzes them, and replays them after a precise delay
  - The delay affects the distance measurement, thereby affecting the location result
  - Precise control of delay allows gradual error accumulation or “drifting”, so detection is difficult

# Many More Attacks

- GPS receivers are also vulnerable to a number of signal- and software-based attacks
  - e.g., Middle-of-the-Earth attack
  - See [Nighswander et al., CCS 2012]

How could you protect against these GPS attacks / threats...

without replacing or upgrading the satellite systems?

# Deployment Constraints

- Because of the deployment cost, upgrading or replacing satellites is not really an option
  - Maybe very slowly over time, but not any time soon
  - So authentication is out

- GPS receivers have to respect what the GPS transmitters are sending even if they cannot authenticate them

# Alternatives

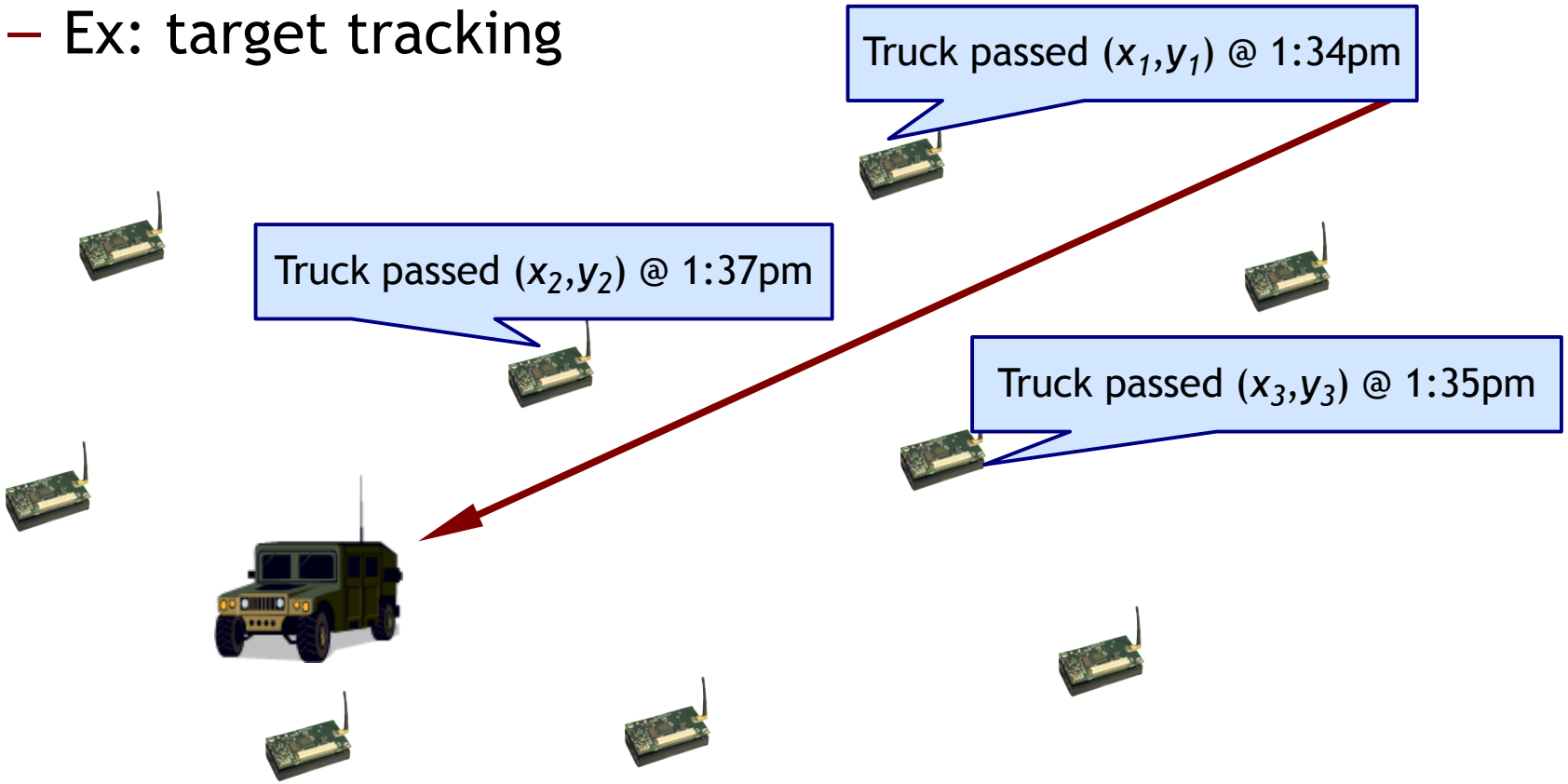
- Several defense / mitigation strategies have been proposed by the GNSS community
  - Modifying GPS receivers to use multiple antennas to verify angle of arrival consistency
  - Augment receiver software to compare changes in location over time
  - Incorporate sensor data (GPS says you're moving but gyro says you're not → ?)
  - Incorporate other GNSS systems for diversity

What about devices or scenarios where GPS is inappropriate?

Sensor networks, underground, etc.

# Time & Location in WSN

- Many applications and protocols require fine-grained node location and event timestamping
  - Ex: target tracking



# WSN Sync & Loc

- Time and location services for WSN must be:
  - **Energy efficient** – energy spent for sync & loc should be minimized (noting significant cost for continuous CPU use and radio listening)
  - **Scalable** – large networks should be supportable
  - **Robust** – adaptable to network dynamics
  - **Ad hoc** – functionality without prior configuration or infrastructure

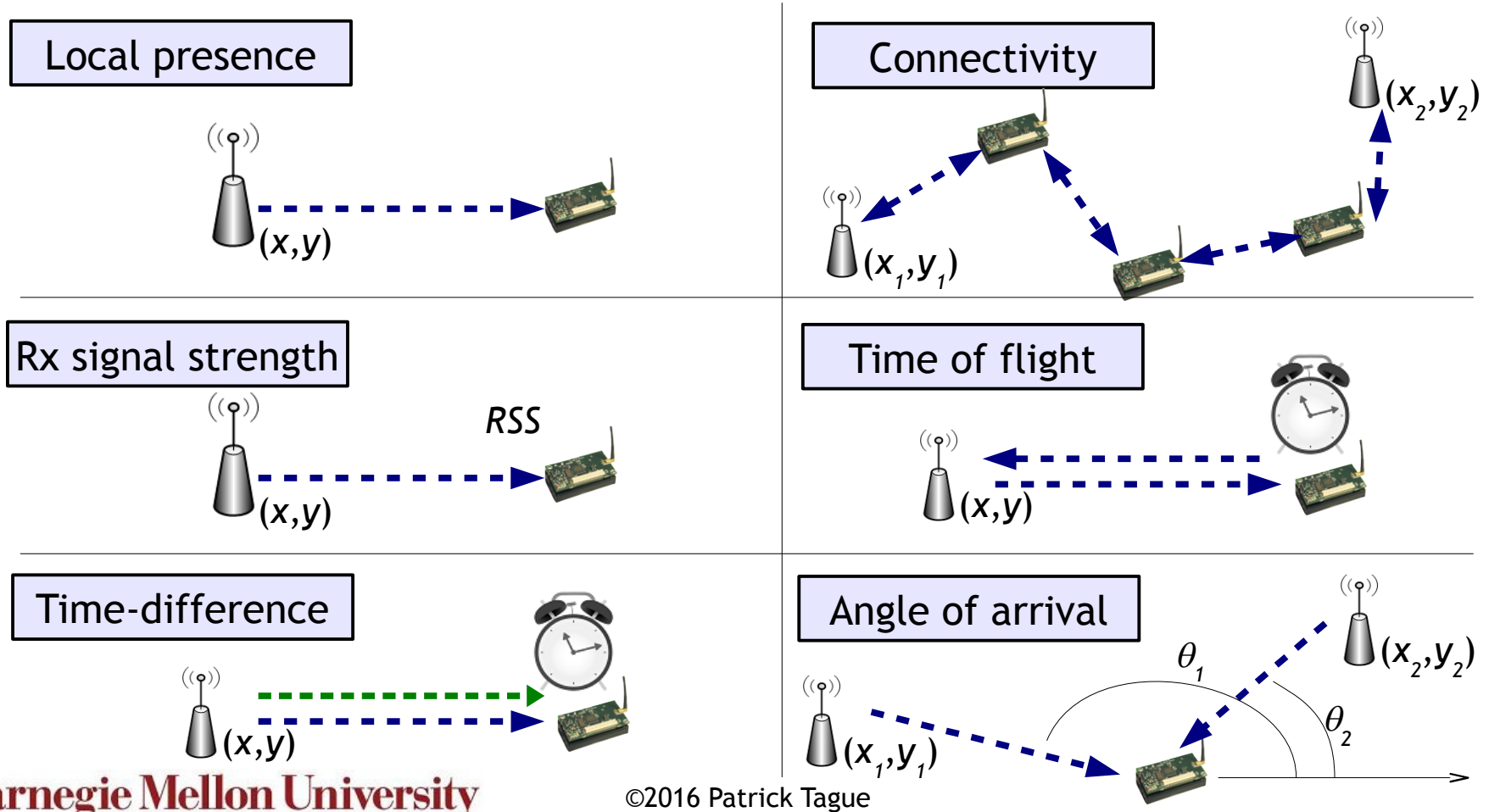
Many of the techniques used in synchronization and localization are similar

# Relative Measurements

- Just as in GPS and NTP/PTP, time sync and localization mechanisms for wireless networks are based on relative measurements from others
  - Receive a message from a neighbor
  - Content in message gives some information
  - Measurement about signal reception gives more

# Relative Measurements

Each localizing device collects geometric relationships relative to several reference points $(x_i, y_i)$



# Securing Relative Measurements

- Measurements taken with respect to reference points should be:
  - Authentic
    - Measurements from authorized reference points only
  - Verifiable
    - Integrity of measurement should be guaranteed
    - If possible, physical measurement should be unforgeable
  - Highly available
    - Location information should be ready when needed
  - Protected from various forms of attack

# Threats to Loc & Sync

- Most of the threats are related to lying
  - In both services, nodes act as references for each other
  - Malicious nodes can simply give false reference information
  - Bad information may be worse than no information, so this can be more serious than DoS

# Secure Sync & Loc

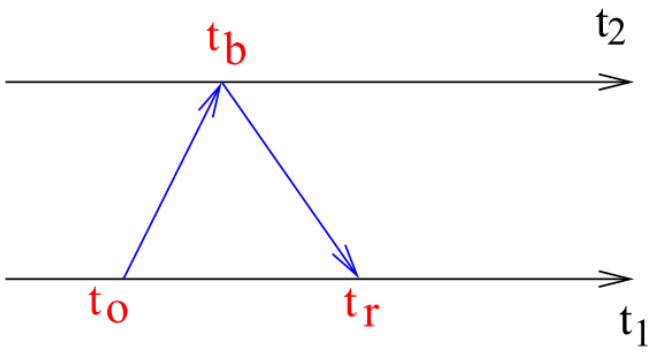
Is it possible to secure the sync and loc processes?

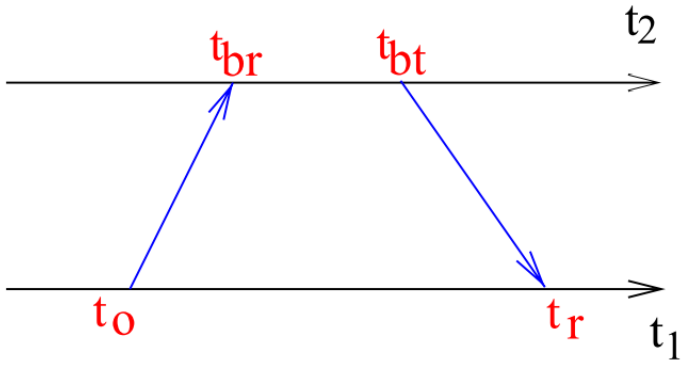
- Processes are based on reference data
  - Is the source trustworthy?
  - Can the data be verified?
  - Is the data reliable?
- Sync & loc estimation services can be attacked
  - Vulnerabilities?
  - How to mitigate them?
- Reference data may be noisy or imprecise
  - How to incorporate redundancy for reliable estimation?
- System or devices may be tightly constrained
  - How efficient is the estimation algorithm?
  - What are the trade-offs?

# Simple WSN Time Sync

[Sichitiu & Veerarittiphan, 2003]

- Approximate *i*'s clock as: $t_i(t) = a_i t + b_i$
  - $t$ is true time, $a_i$ is drift rate, $b_i$ is offset
- Relative clocks 1,2 related as: $t_1(t) = a_{12} t_2(t) + b_{12}$



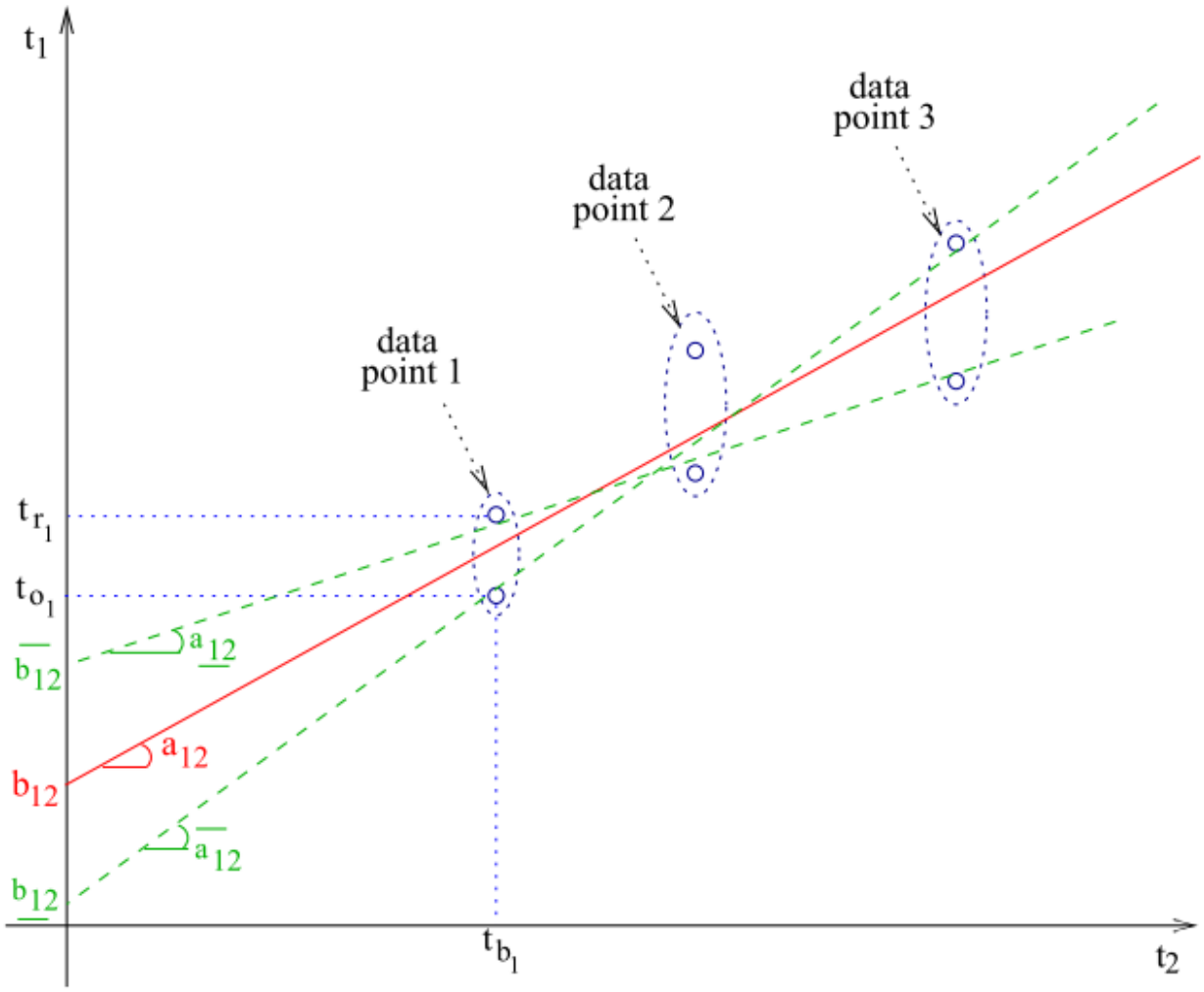




$$t_o(t) < a_{12} t_b(t) + b_{12}$$
$$t_r(t) > a_{12} t_b(t) + b_{12}$$

Two data points for $(t_o, t_{br}, t_r)$, $(t_o, t_{bt}, t_r)$ exchanges

# Sync Offset

- Two nodes can then estimate the coefficients using a sequence of inequalities



# Secure Pairwise Sync

[Ganeriwal et al., TISSEC 2008]

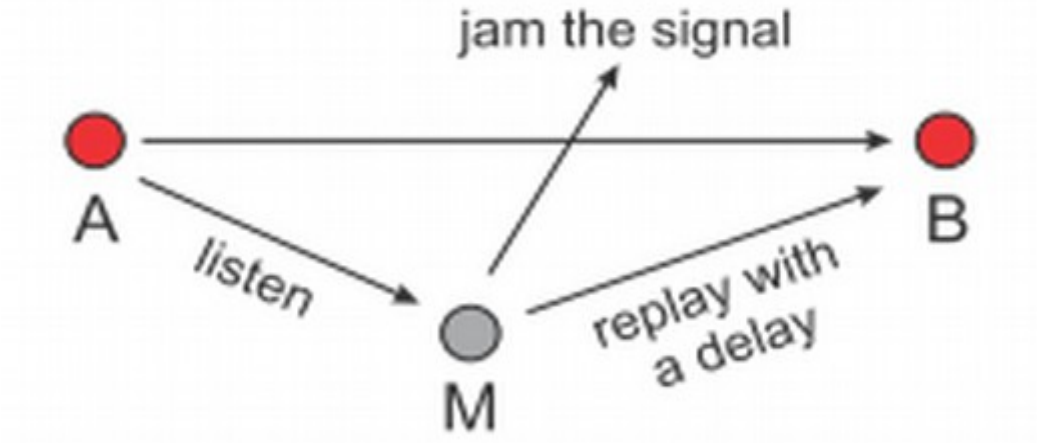
- Goal of secure SPS is to estimate clock difference and transmission delay pairwise
  - If the transmission delay is within an expected amount, then adjust the clock using the difference

**Secure Pairwise Synchronization (SPS)**

1. $\mathrm{A}(T1) \rightarrow (T2)\mathrm{B}: A, B, N_A, sync$
2. $\mathrm{B}(T3) \rightarrow (T4)\mathrm{A}: B, A, N_A, T2, T3, ack,$
   $MAC_{K_{AB}}[B, A, N_A, T2, T3, ack]$
3. A calculates delay $d = \frac{(T2-T1)+(T4-T3)}{2}$
   $If\ d \leq d^*\ then\ \delta = \frac{(T2-T1)-(T4-T3)}{2}\ else$ abort

# Benefits of SPS

- Protects against the "pulse-delay attack" or at least limits the effect to the threshold transmission delay




When it Exceeds 30$\mu s$, the Attack is Always Detected

| Experiment | Average error | Maximum error | Minimum error | Attack detection probability |
|---|---|---|---|---|
| Non Malicious | 12.05 $\mu s$ | 35 $\mu s$ | 1 $\mu s$ | NA |
| $\Delta$ = 10 $\mu s$ | 19.44 $\mu s$ | 44 $\mu s$ | 1 $\mu s$ | 1% |
| $\Delta$ = 20 $\mu s$ | 30.92 $\mu s$ | 61 $\mu s$ | 1 $\mu s$ | 37% |
| $\Delta$ = 25 $\mu s$ | 35.67 $\mu s$ | 75 $\mu s$ | 16 $\mu s$ | 82% |
| $\Delta$ = 30 $\mu s$ | NA | NA | NA | 100% |

# Limitations of SPS

- SPS assumes the radio can include an authenticated response in a timely manner before replying to the initial sync message
  - Hardware limitations that may not be supportable by sensor platforms
  - Software support provided by TinySec ([Karlof et al., SenSys 2004])
  - Most likely works only for low-rate radios (e.g., CC1000, not CC2420)

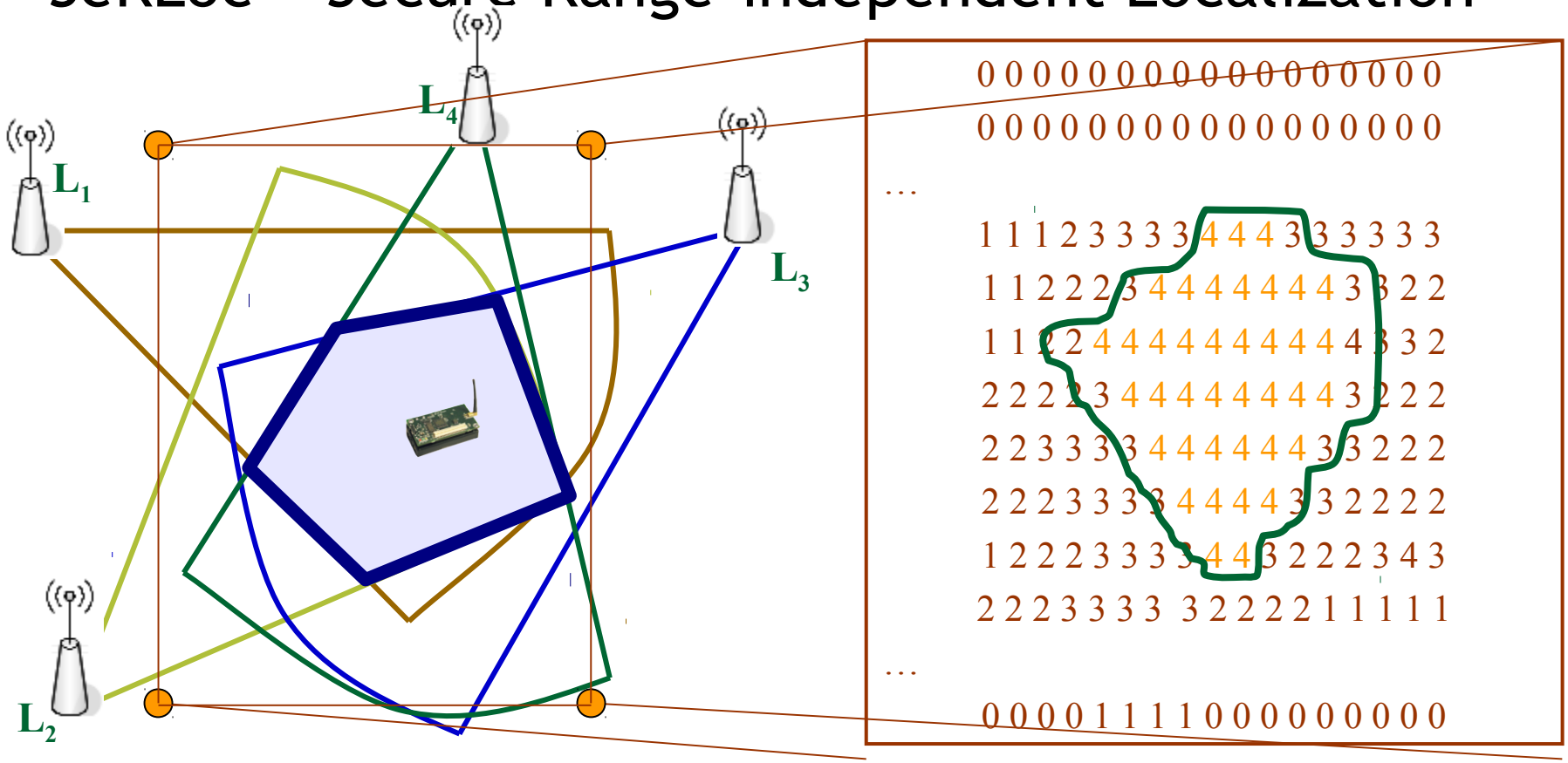
# Pairwise to Global Sync

- If connectivity is fairly dense:
  - Redundant pairwise synchronization can lead to global synchronization
- If connectivity is not dense enough:
  - Attempts at global synchronization will lead to excessive error propagation

# SeRLoc

[Lazos & Poovendran, 2004]

- SeRLoc = Secure Range-independent Localization




$$L_i : \{ (X_i, Y_i) \,||\, (\theta_{i,1}, \theta_{i,2}) \,||\, (H^{n-j}(PW_i)), j, ID_{Li} \}_{K0}$$

# SeRLoc Security Mechanisms

- Authenticity of references:
  - Encryption of location signals implies signal comes from a valid node – prevents external attack
  - Also limits scalability due to key mgmt requirements

- Identify verification of references:
  - Use of secret “password” with hash chain protects against location spoofing by internal attackers – forces attacker to compromise a valid locator

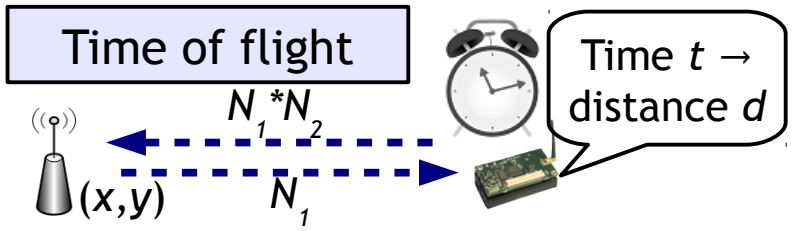
# SeRLoc Security Mechanisms

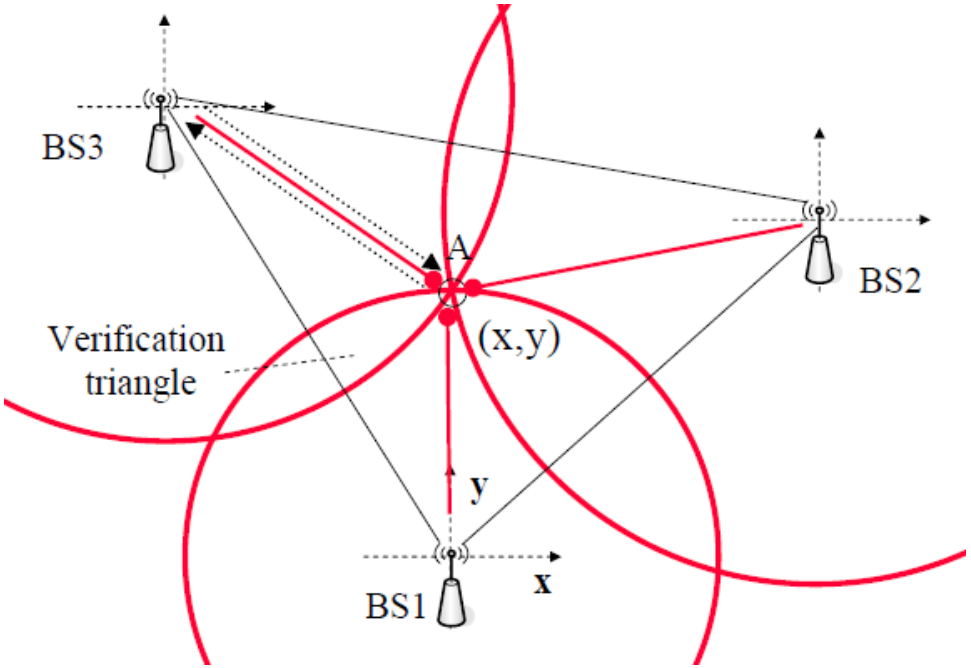
- Majority voting further protects against internal attack, forces attacker to compromise more than ½ of the locators heard by a sensor
- Consistency checking of location reference information helps protect against replays, spoofing, Sybil, and wormhole attacks
- Provides a recovery mechanism for use when attacks are detected

# Verifiable Multilateration

[Čapkun & Hubaux, 2005]

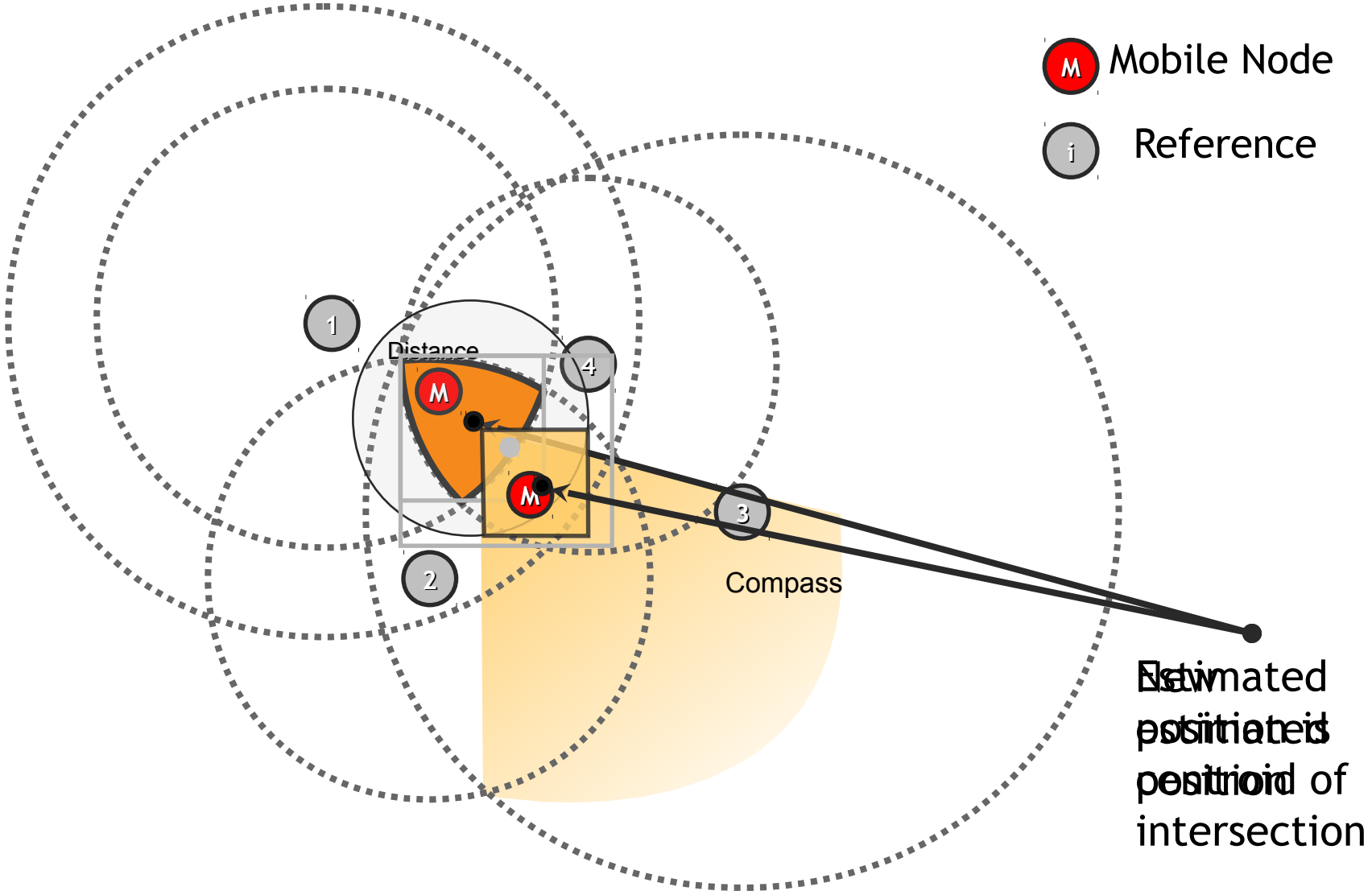
- Basic idea of VM:
  - Using distance bounding, an attacker can only increase the measured distance




- VM benefit:
  - Increasing distance measurements will either have negligible effect on location or be large enough to detect misbehavior

# Mobility Helps Localization



# Open Questions

- Secure localization and synchronization are still open research areas, especially in some aspects of BSN, VANET, etc.

- What aspects of relative measurement and reporting can actually be verified?

- How to trust reports of relative measurements?

# Mar 29:
# NO CLASS

# Mar 31:
# Progress Presentations

# Apr 5:
# Exam