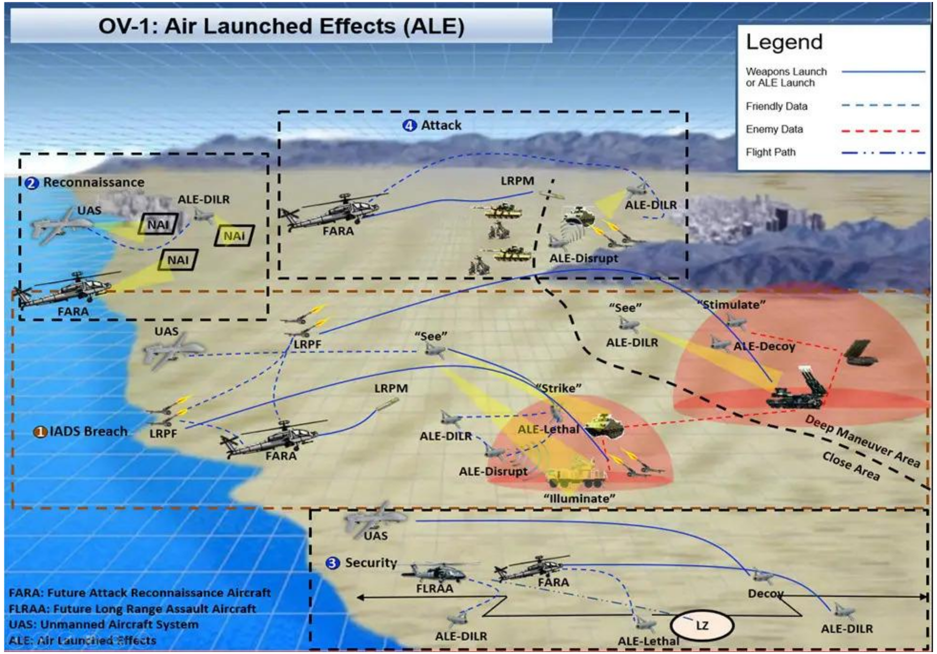
Towards Effective Swarm-Based GPS Spoofing Detection in Disadvantaged Platforms

Enguang Fan, Anfeng Peng, Matthew Caesar, Jae Kim, Josh Eckhardt, Greg Kimberly, Denis Osipychev

Motivation

- UAV platforms provide critical services to the modern contested battlespace
- GPS is critical to mission success, must be resilient in highly contested environments
- Unfortunately, GPS is prone to attack; jamming, interception, termination can render GPS inoperable, making entire communications ecosystem fragile



Large platforms can counter effects of GPS spoofing, but smaller platforms such as **Air Launched Effects** *(ALEs), with limited sensors suites, can be vulnerable*

Key idea

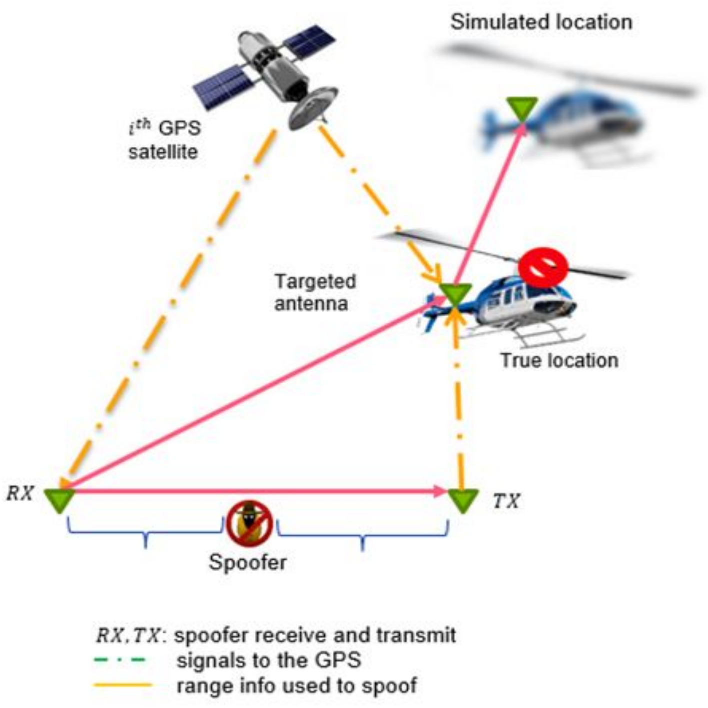
Could we use other sensors on the UAV to give "hints" about its current location?

- E.g., my Inertial Measurement Unit is showing sudden changes, but that's not reflected in my GPS readings.
- E.g., several of my neighbors in radio range have GPS values very different from mine

UAVs have a number of sensors that could be used for such hints

- Signal strength to neighbors, camera/LIDAR to known waypoints, IMU changes since last-known good position, ALEs can also exchange GPS readings, etc.

Can we develop a formal framework to collect these "hints", and merge them together so as to maximize our ability to estimate our location?



Key idea

If we could do this, it would help correct if GPS is taken out by adversary or becomes obstructed

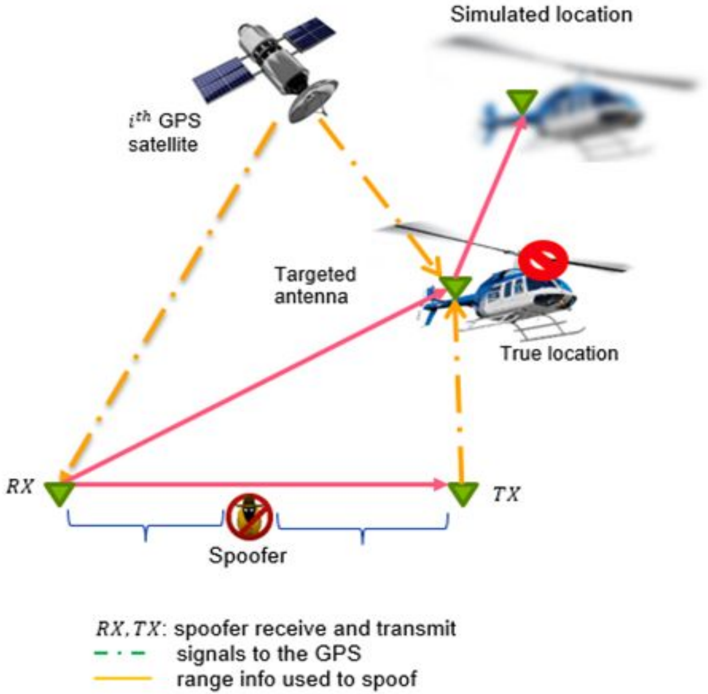
- Can also help detect if GPS information is being spoofed

Challenge: ALE sensor suites are limited

- Sensor precision, effectiveness and applicability depends on characteristics of onboard radios and sensors, density of swarm, geographical dispersion, and the nature of attack

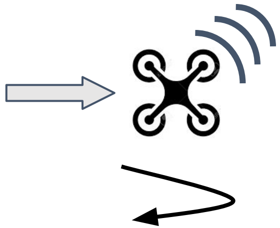
Can we develop intelligent sensor fusion techniques to remediate GPS spoofing on ALE platforms?

- Our approach: Leverage distributed nature of swarm to detect inconsistencies and reconstruct positions, providing robustness and recovery from GPS attacks

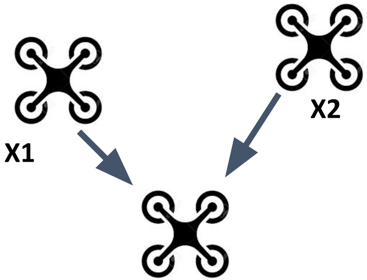


Example ways we can use sensors

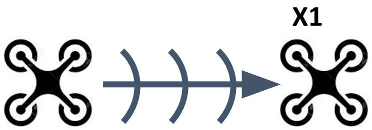
1. IMU: Use **Inertial Measurement Unit** (linear acceleration+angular velocity) and last known good position to perform dead reckoning



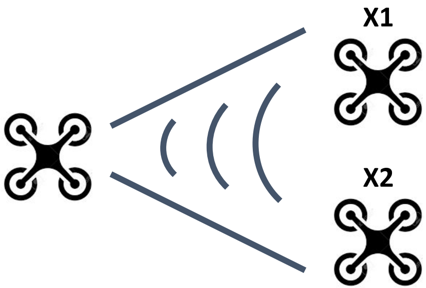
2. Communications: Request GPS coordinates of neighbors, combine them together (e.g., averaging)



3. RSSI: use **Radio Signal Strength Indicator** to estimate distance and angle to neighboring ALEs, ground stations



4. Camera: use visual odometry to estimate distance, heading, from observing other ALEs and landmark features

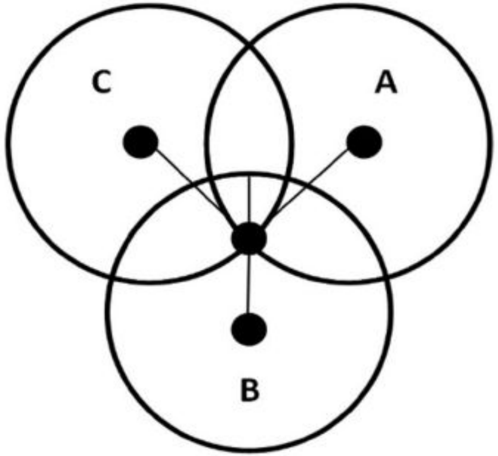


RSSI Multilateration

- $RSSI = A - 10 \cdot \eta \cdot \log_{10}(d) + \varepsilon_{RSSI}$
- Estimator: $\hat{d} = 10^{\frac{A - RSSI}{10\eta}}$
- $\hat{p} = argmin \sum_{i=1}^{n} (\hat{d}_i - ||p - p_i||)^2$

- A: reference distance
- η: path loss exponent
- ε_{RSSI}: white gaussian noise
- $\hat{d}_i$: RSSI-infered distance to the i^{th} neighbors
- p_i: neigbours position

- Based on **lognormal shadowing path loss model**[1], distance between transmitter and receiver can be inferred from RSSI, multiple RSSI from neighbors allow us to perform multilateration.
- Solving $\hat{p}$ can be treated as an optimization problem, we solve it by Levenberg-Marquardt method.



IMU Dead-Reckoning

State Variables

$$\boxed{\mathbf{R}_{t+1}} = \mathbf{R}_t \exp\left((\boldsymbol{\omega}_t dt)_\times\right)$$

$$\boxed{\mathbf{v}_{t+1}} = \mathbf{v}_t + \left(\mathbf{R}_t \mathbf{a}_t - \mathbf{g}\right) dt$$

$$\boxed{\mathbf{p}_{t+1}} = \mathbf{p}_t + \mathbf{v}_t dt + \frac{1}{2}\left(\mathbf{R}_t \mathbf{a}_t - \mathbf{g}\right) dt^2$$

R_t : directional rotation matrix

v_t : velocity

p_t : Position

g: gravity

a_t : acceleration read from IMU

ω_t: angular velocity read from IMU

- We develop systems of equations to model sensor properties
  - E.g., state propagation models for IMU dead-reckoning
  - The pose of UAV can be inferred provided continuous reads from IMU.
- Naïve IMU Dead-Reckoning will be erroneous after a few seconds, due to the bias and noise from IMU reading.

IMU noise and bias analysis

$$\boldsymbol{\omega}_m = \boldsymbol{\omega} + \boxed{\omega_{\boldsymbol{b}} + \omega_{\boldsymbol{n}}}, \rightarrow \text{Error}$$

$$\boldsymbol{a}_m = \mathbf{a} + \boxed{\mathbf{a}_{\boldsymbol{b}} + \mathbf{a}_{\boldsymbol{n}}},$$

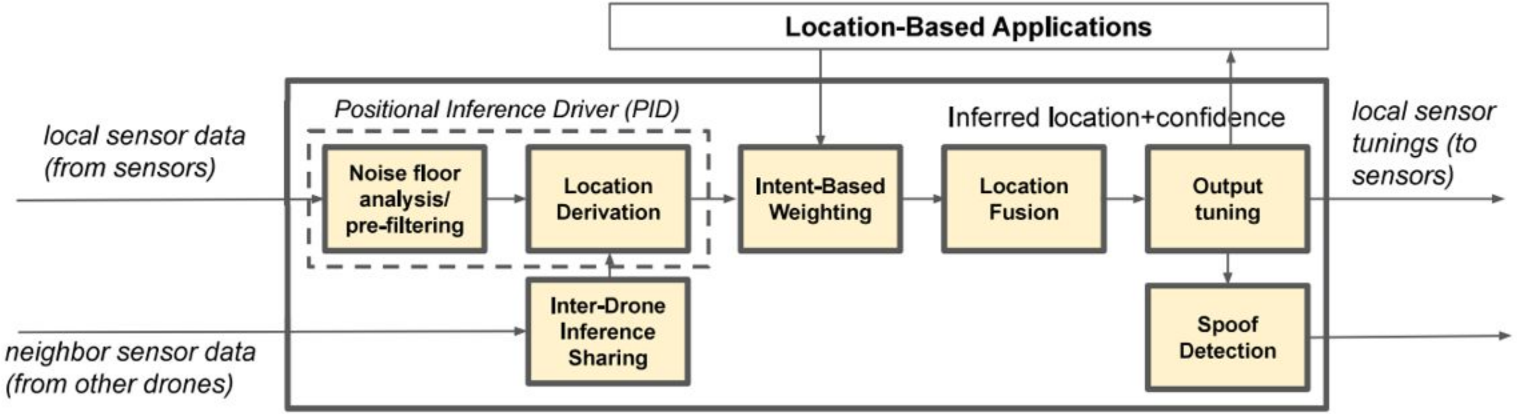
$$\delta\omega_{\boldsymbol{b}} = \omega_{\boldsymbol{b}}^{\boldsymbol{t}} - \omega_{\boldsymbol{b}}^{\boldsymbol{t-1}} = \epsilon_{\boldsymbol{r}}^{\boldsymbol{\omega}}$$

$$\delta a_{\boldsymbol{b}} = \mathbf{a}_{\boldsymbol{b}}^{\boldsymbol{t}} - \mathbf{a}_{\boldsymbol{b}}^{\boldsymbol{t-1}} = \epsilon_{\boldsymbol{r}}^{\boldsymbol{a}}$$

ω_m , a_m: Measured value from IMU
ω , a: True value
ω_b , a_b : Measurement bias
ω_n , a_n : Measurement gaussian noise
ϵ_r^w, ϵ_r^a: Random-walk gaussian noise

- The bias and measurement noise both contribute to the error between measured value from IMU and the ground truth value.
- The bias is not static, but driven by a random-walk, which controlled by ϵ_r^w, ϵ_r^a .
- Neglecting the bias and noise can drift our pose estimation far away from the ground truth. Hence, we need to model the bias and noise properly. **More on sensor fusion part**.

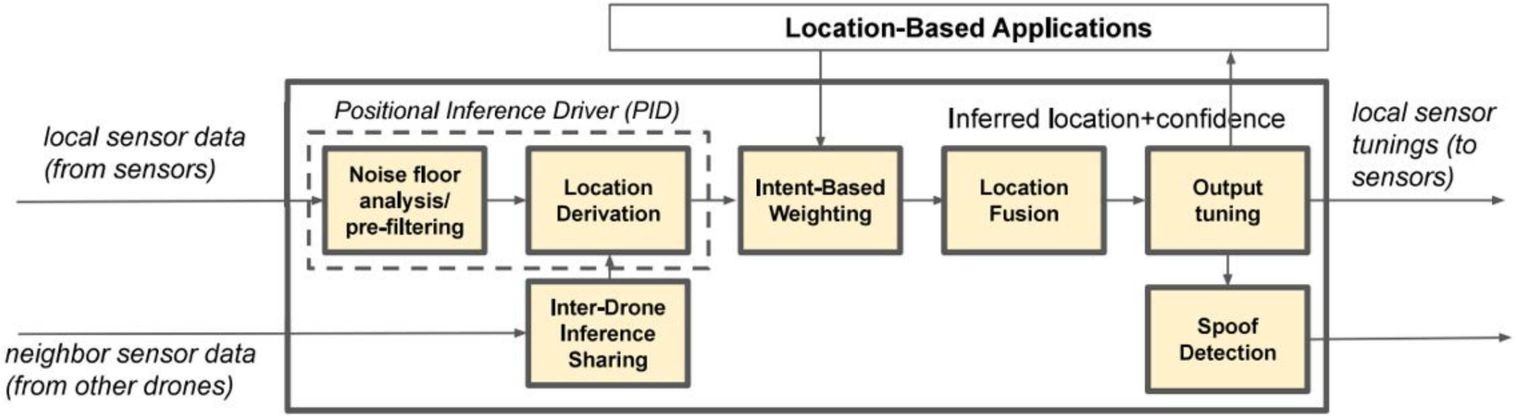
System Overview



Key idea: Kalman filtering to combine sensors to maximize ability to remediate GPS spoofing; multi-stage pipeline to iteratively improve localization

- Noise floor analysis removes background noise and attacker-introduce randomness from sensor inputs, Sensor-specific weightings compute heuristic curve to weight based on parameter, combining readings across sensors with Kalman filter

System Overview



Input is non-positional sensor inputs, output is inferred location with estimation confidence (feedback to sensors, GPS-leveraging applications)

- Approach: convert sensor data into location information, weighting by confidence, then fusing locations into single estimation
- Key questions: how to convert non-positional sensor data into locations, how to determine weights of sensors?

Error-state Extended Kalman Filter

IEEE MILCOM IEEE ComSoc

- State Propagation (IMU)

$$\delta x \leftarrow f(x, \delta x, u_m) = F_x(x, u_m) \cdot \delta x + G_x(x) \cdot w$$

$$x \leftarrow F(x, u_m)$$

- $\delta \mathbf{x} \triangleq [\delta p, \delta v, \delta \theta, a_b, \omega_b]^T$
- $\mathbf{x} \triangleq [p, v, q]^T$
- $u_m \triangleq [a_m, \omega_m]^T$
- $w \triangleq [a_n, \omega_n, \delta a_b, \delta \omega_b]^T$

- State Update (RSSI)

$$y = h(x) + v$$

$$h(x) = A - 10 \cdot \eta \cdot \log_{10}(||p - p_i||)$$

y are RSSI measurements

Algorithm 1 ES-EKF Algorithm

Input: $x_{initial}$, $\delta x_{initial}$, $P_{initial}$, u_m, V, Q

Output: $\hat{x}$, $\hat{\delta x}$, P

loop

$\boxed{\hat{u} = CORRECTION_{bias}(u_m, \hat{\delta x})}$

$\hat{x} \leftarrow F(\hat{x}, u)$

$P \leftarrow F_x P {F_x}^T + G_x Q {G_x}^T$

if *RSSI measurement available* **then**

$H = H_x \cdot X_{\delta x}$

$K \leftarrow PH^T(HPH^T + V)^{-1}$

$P \leftarrow (I - KH)P$

$\hat{\delta x} \leftarrow K(y - h(\hat{x}))$

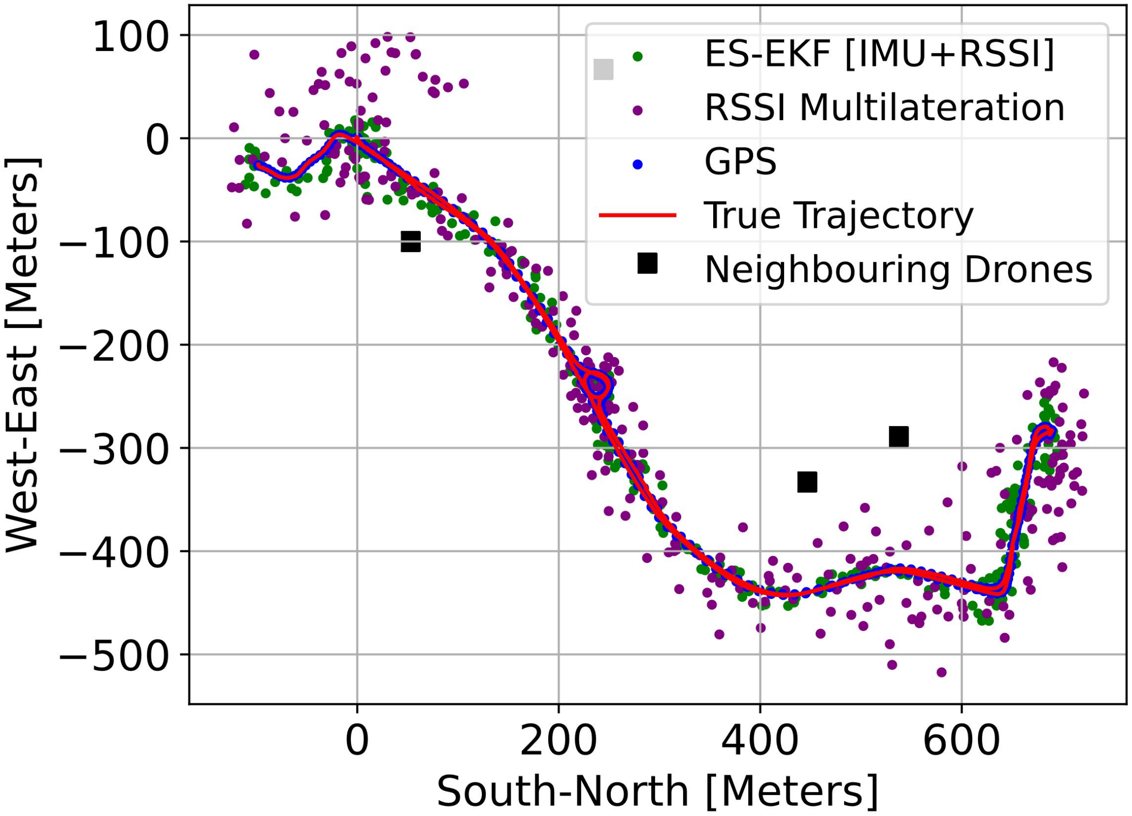
$\boxed{\hat{x} = CORRECTION_{perturbation}(\hat{x}, \hat{\delta x})}$

end

end loop

Compensate

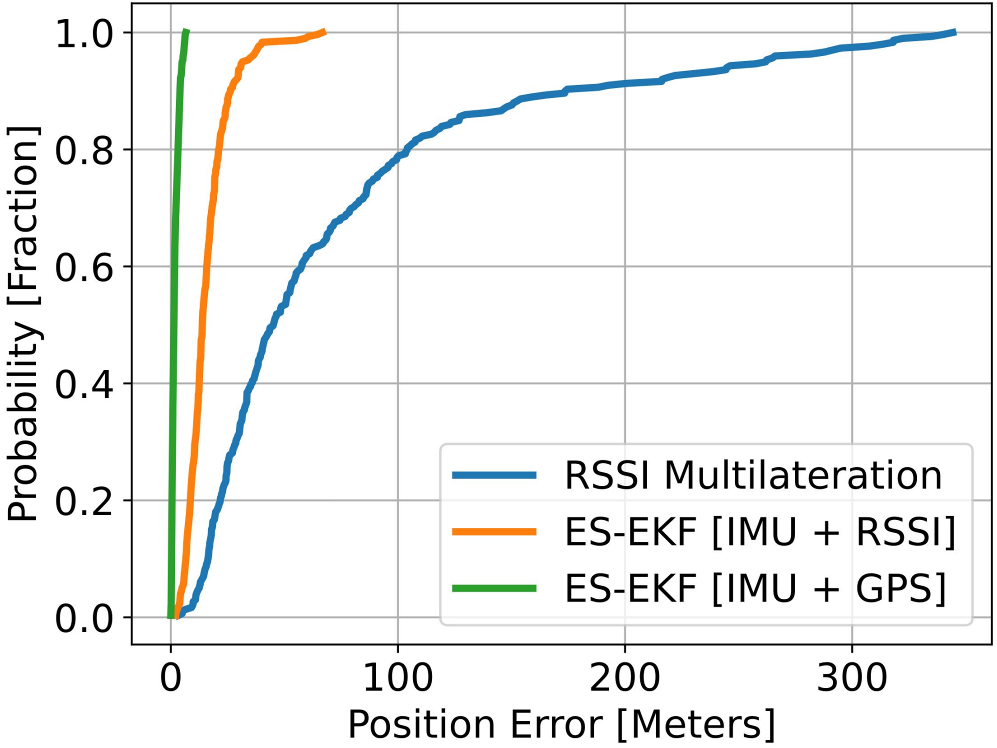
Evaluation Results



- True trajectory is based on valid GPS data.
- RSSI Multilateration is prone to have outliers, also deviates more from true trajectory.
- Sensor fusion with IMU+RSSI removes most of outliers, closely align with the true trajectory.

Evaluation Results

Distribution of positional error



RSSI Multilateration:
- High positioning error.
- Long-tailing effect.
- Worst 10% deviations exceed 174 meters.

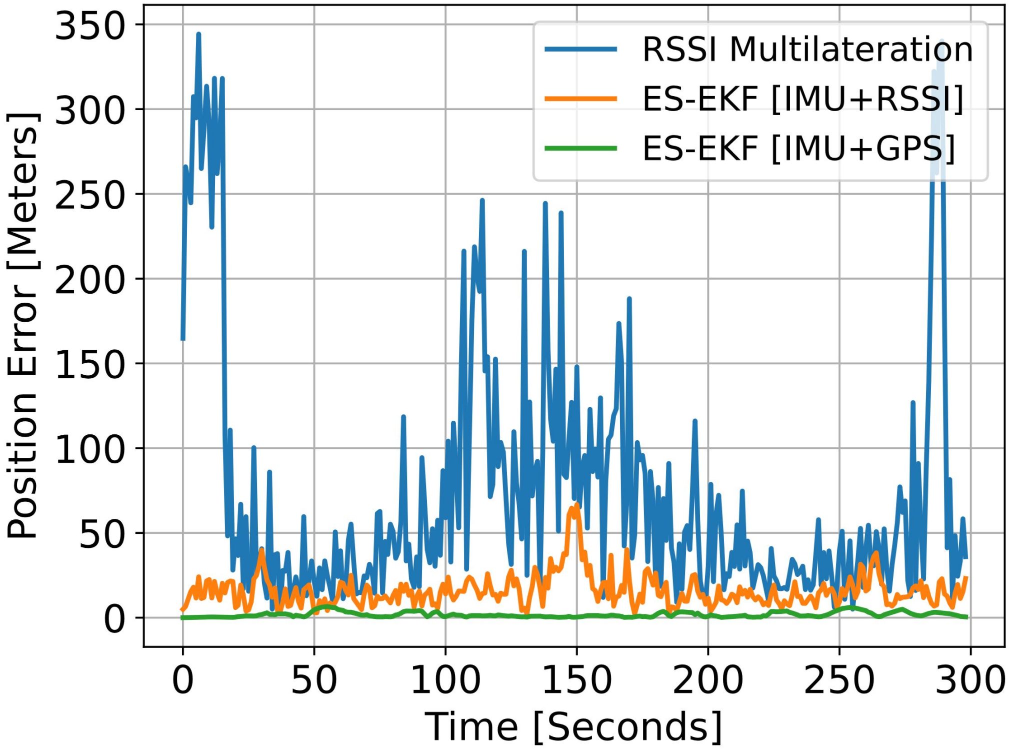
ES-EKF Fusion of IMU and RSSI:
- Alleviates long-tailing effect.
- Increases positioning accuracy.
- Worst 10% deviations only exceed 26 meters.

Improvement with ES-EKF Fusion:
- Nearly 80% improvement in positioning accuracy over RSSI multilateration.

Evaluation Results

IEEE MILCOM IEEE ComSoc

Time-series variation in position error



ES-EKF vs. RSSI Multilateration:

- Similar error peaks at the same time periods.
- Magnitude of error peaks significantly lower in ES-EKF.
- Sensor fusion significantly attenuates RSSI error.

Variance Reduction:

- Similar patterns observed among different algorithms.
- ES-EKF fusion eliminates variance in position uncertainty.
- Achieves a two-magnitude reduction in positioning error variance compared to RSSI multilateration.

Conclusions

GPS spoofing can cause significant damage to ALE assets

- Strategic adversaries can amplify power of these attacks across time and space

Leveraging common, low-cost sensing infrastructures can offer substantial protection

- Kalman-filtering based combination outperforms individual and statically weighted combinations
- ES-EKF prevents introduction of non-linear errors and boosts performance compared to sole reliance on individual sensors

Future work: leverage deep learning to fuse sensor inputs, develop real-time navigation algorithm robust to GPS attacks, develop flight algorithms that change flight plan to maximize ability to correct coordinates in presence of spoofing.