Authentication and Message Integrity Verification For Emerging Wireless Networks

Final Dissertation Defense

Ebuka P. Oguchi

School of Computing

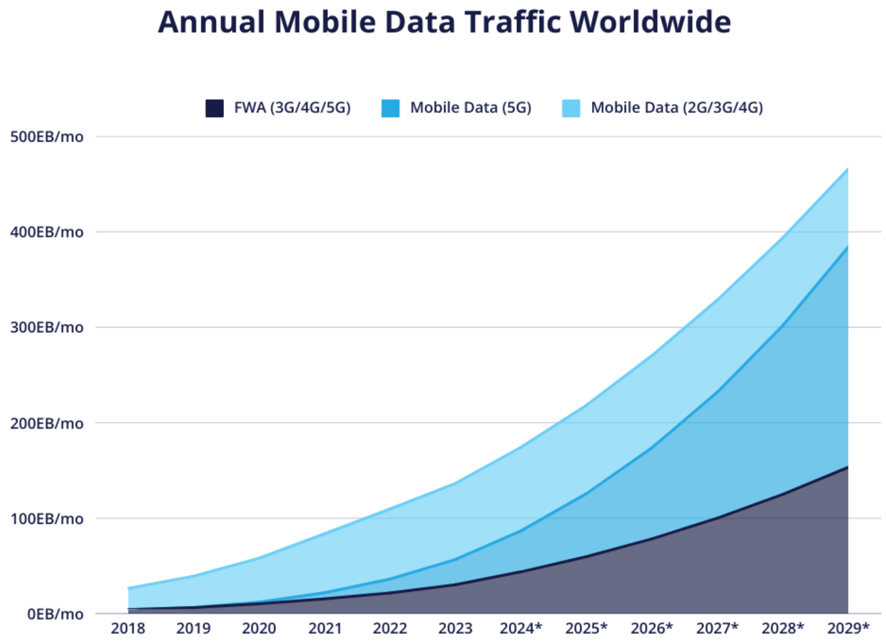
University of Nebraska-Lincoln

Advisor: Dr. Nirnimesh Ghose

Committee: Dr. Mehmet C. Vuran
Dr. Massimiliano Pierobon
Dr. Yi Qian

UNIVERSITY of NEBRASKA–LINCOLN

Emerging Wireless Networks



1 Exabyte = 10^{18} Byte

- Emerging wireless networks refer to newly developed or evolving wireless systems to meet the demands of modern applications such as high data rate, low latency, high reliability

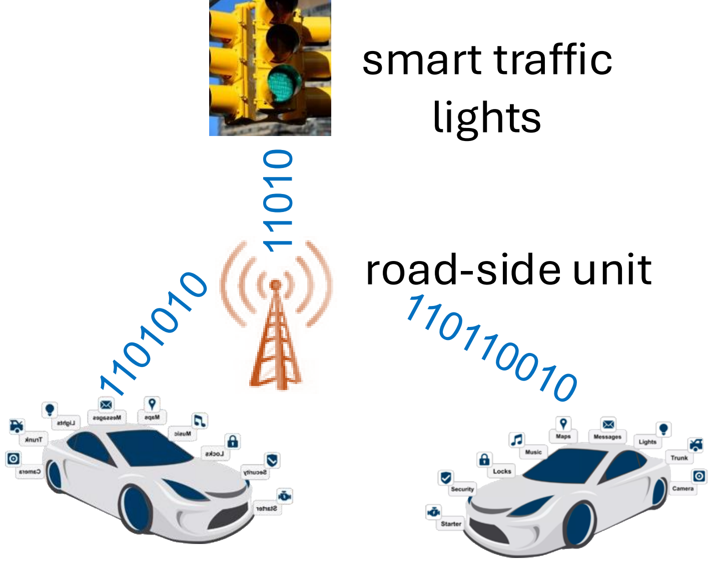
- Why Emerging wireless Networks?
  - To meet the escalating demand for faster, efficient, more reliable, and ubiquitous Connectivity.

- **Applications** (e.g., Ag-IoT, BAN, VANET)
- **Technologies** (e.g., Wi-Fi 6/7, molecular comm)
- **Enablers** (e.g., 5G+, AI, SDRs),
- **Trends** (e.g., IoT growth, infrastructure decentralization).

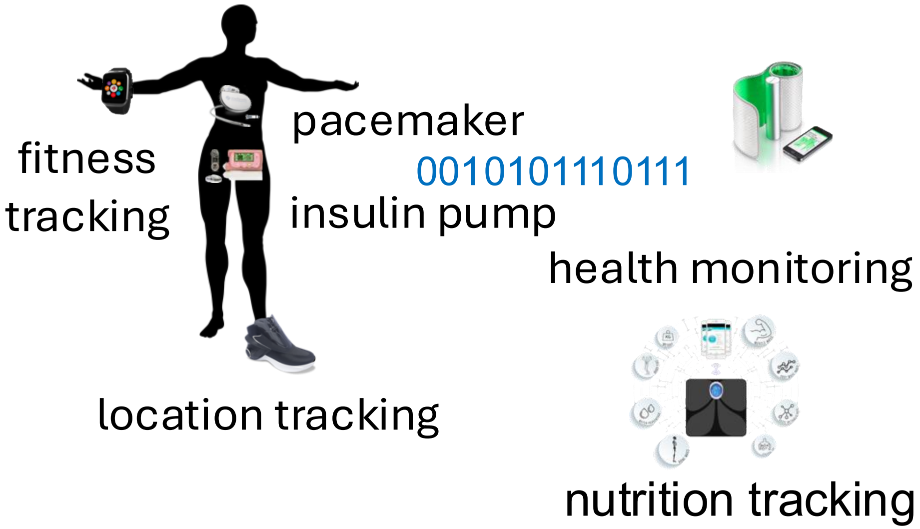
https://tridenstechnology.com/mobile-data-statistics/#:~:text=Global%20monthly%20mobile%20data%20usage,4K%20streaming%20and%20industrial%20IoT.
https://www.npr.org/2025/05/18/g-s1-67486/pope-leo-xivs-installation-mass

Emerging Wireless Networks

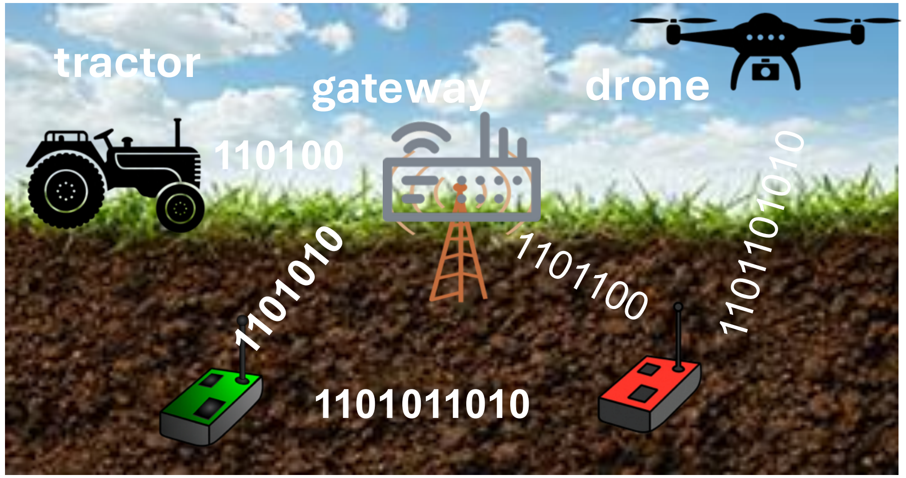
Transportation



Health



Agriculture



- Key Challenges:
  - **Security**
  - Spectrum allocation
  - Infrastructure development

Conventional Settings - Security

Alice

Can connect

Alice’s House

1. Secret-Based – keys, password
2. Stationary or slowing moving channel
3. Out-of-band technique - Display
4. Over-the-Air channel

smart lighting

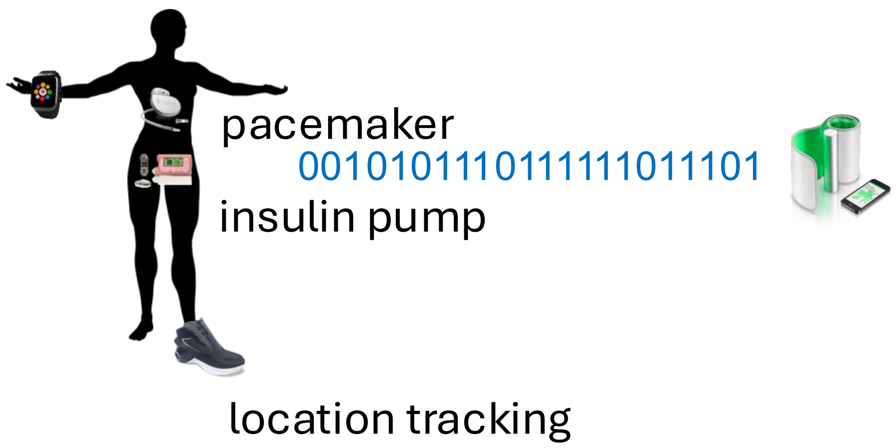
Automated door locks

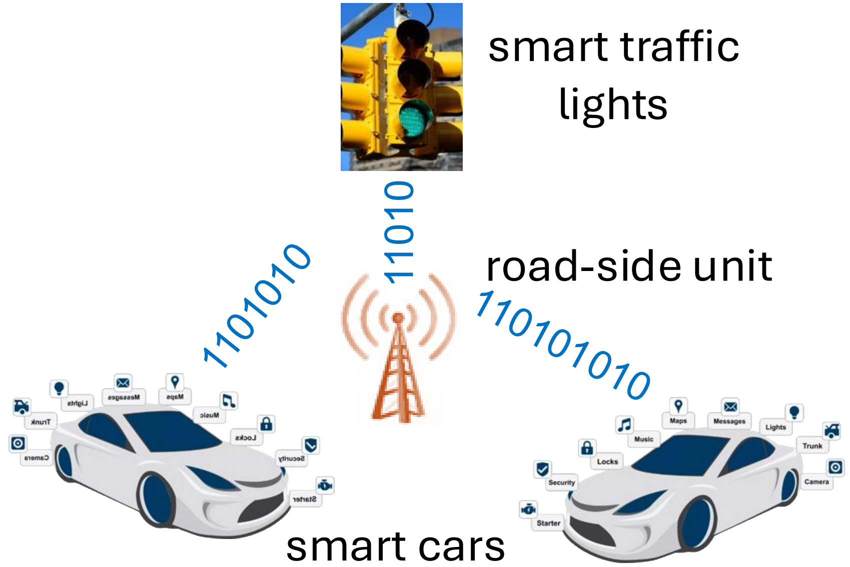
Smart fridge

Smart camera

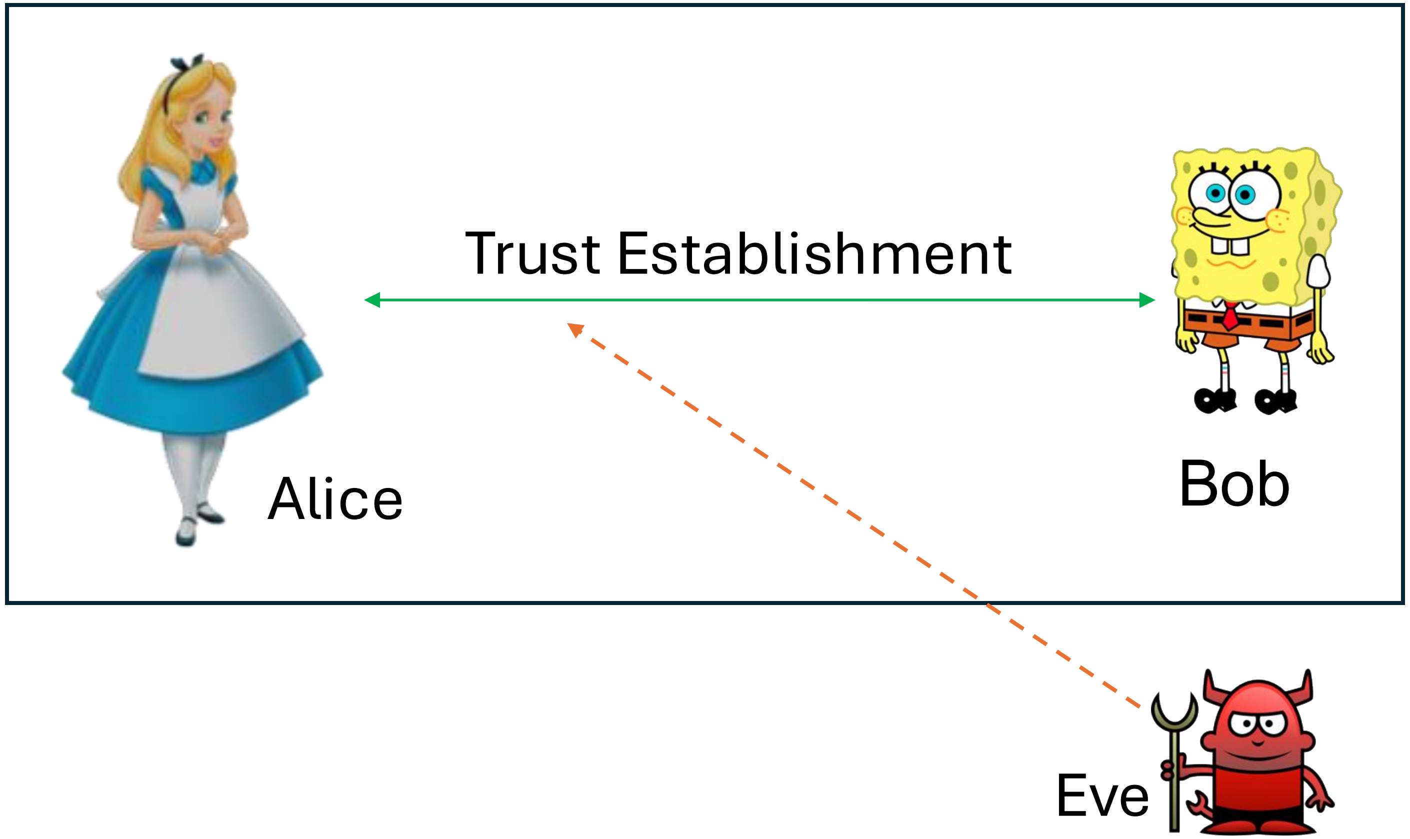
Existing Solutions

- Traditional secret-based technique
  - Manually enter passwords - Challenging to implement in devices lacking keyboards or screens.
  - Preload default passwords - Commonly left unchanged, making them prone to eventual leaks.
  - Public key infrastructure – involves complexity, overhead and dependence on centralized trust.





Secret-Free Trust Establishment



Trust Establishment Includes

- Message Integrity Verification
- Authentication

Secure and Reliable Communication

- We want In-band trust establishment using difficult-to forge physical layer features

Can we do Trust Establishment in **unconventional settings**?

Yes!

1. Underground Wireless Networks
2. Autonomous Vehicular Networks

Motivation - Unconventional Settings

- Underground Wireless Networks
  - Different channel properties underground vs. over-the-air (OTA)
  - No access for out-of-band verification
  - Time sensitive messages

- Autonomous Vehicular Networks
  - Rapidly moving channel (High mobility)
  - Time sensitive nature of messages

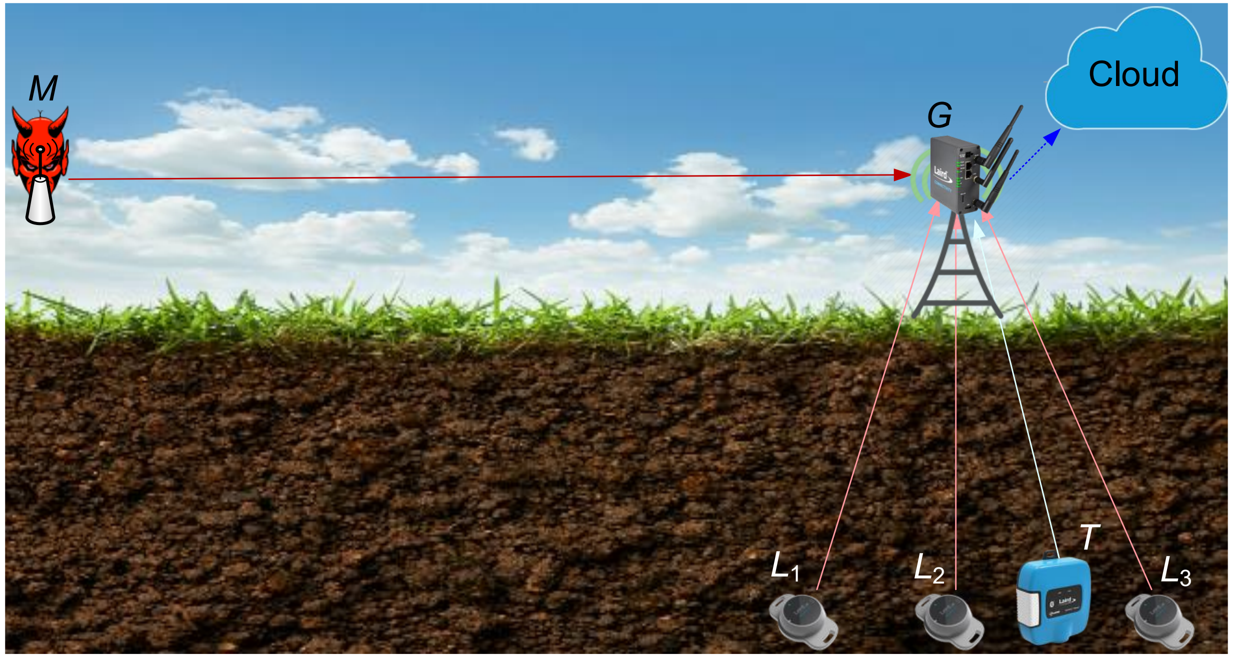
Objective

- Use hard-to-forge physical layer characteristics for device authentication and secure key establishment.
  - Received Signal Strength (RSS) -> Underground Wireless Networks
  - Channel Impulse Response (CIR) -> Over-The-Air and Underground Wireless Network
  - Trajectory and Motion Vectors (TMV) -> Autonomous Vehicular Networks

Security in Underground Setting for Ag-IoT

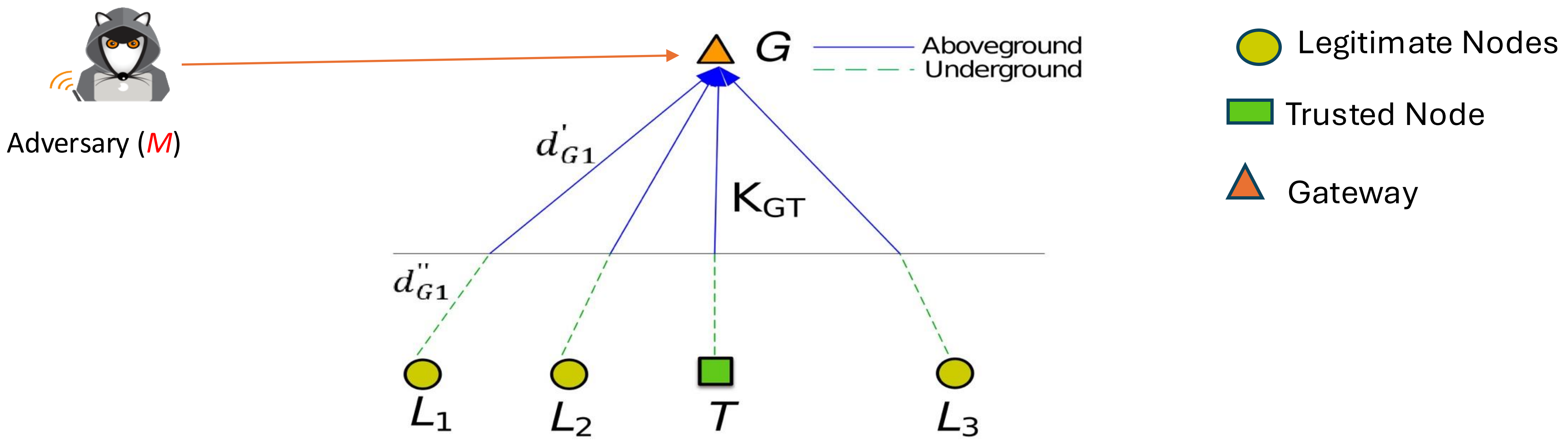
STUN: Secret- Free Trust Establishment Protocol for Underground Networks

- Benefits:
  - Increased productivity and crop yield
  - Prevents flooding and soil drought



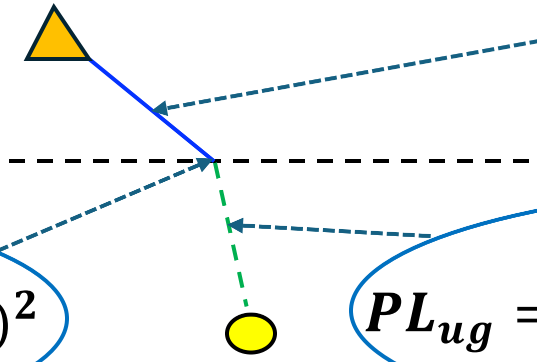
- Motivation:
  - Secured transmission and reception of data
  - Prevention of active signal injection attacks

System Model



- Underground and aboveground wireless channel properties are not the same.
- Underground-to-Air channel Model $P_{r_i} = \dfrac{P_{t_G} \times G_G \times G_i}{PL_{ug} \times PL_{ag} \times PL_R}$.

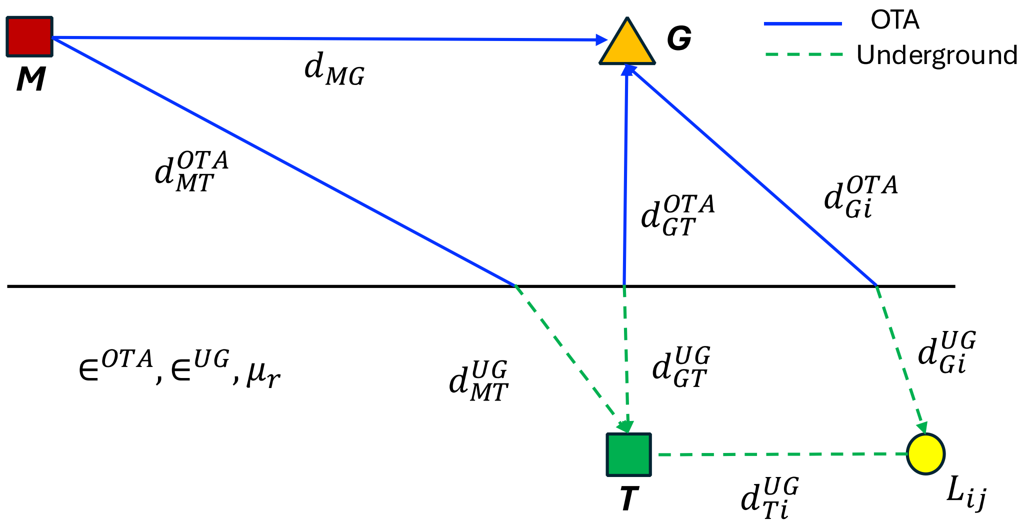
$$PL_{ag} = \frac{(d_{Gi}^{ag})^{\eta} \times f^2}{10^{14.76}}$$



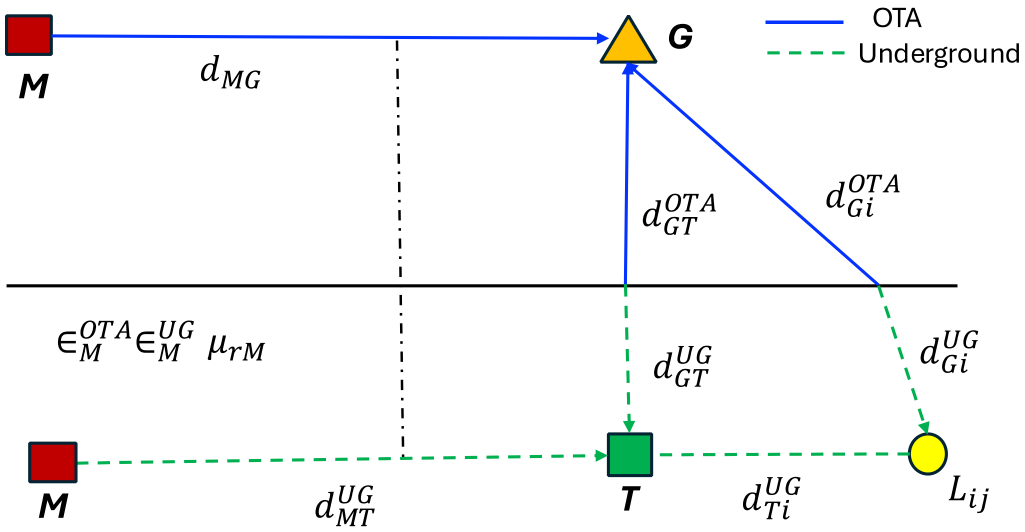
$$PL_R = PL_{R_{AG-UG}} = (r + {}^1\!/_4)^2$$

$$PL_{ug} = 10^{(0.64+0.89\alpha d_{Gi}^{ug})} \times (d_{Gi}^{ug} \times \beta)^2$$

Threat Model



Type 1 Adversary

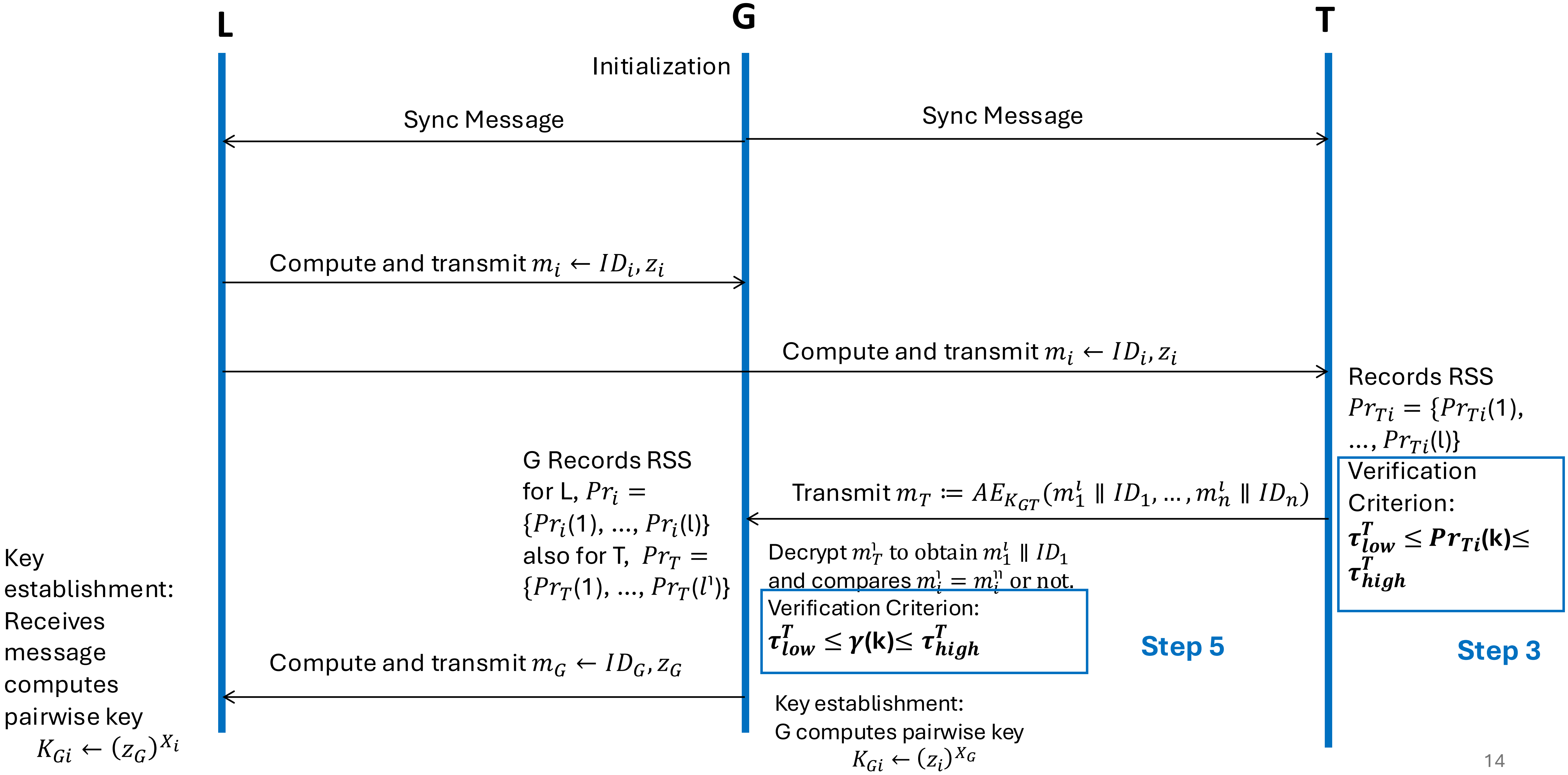


Type 2 Adversary

- Type 1 adversary which attempts to inject its signals simultaneously at G and T
- Adversary is outside the perimeter of the farm.

- Type 2 adversary can deploy additional nodes above and underground to achieve the receive signal strength (RSS) at G and T

STUN: Trust Establishment Protocol



STUN: Received signal strength verification

- Verification at T (step 3):

RSS at T

$$\tau_{low}^{T} \leq Pr_{T_i}(k) \leq \tau_{high}^{T} \; \forall i = 1, \ldots, n$$

- Verification at G (step 5):

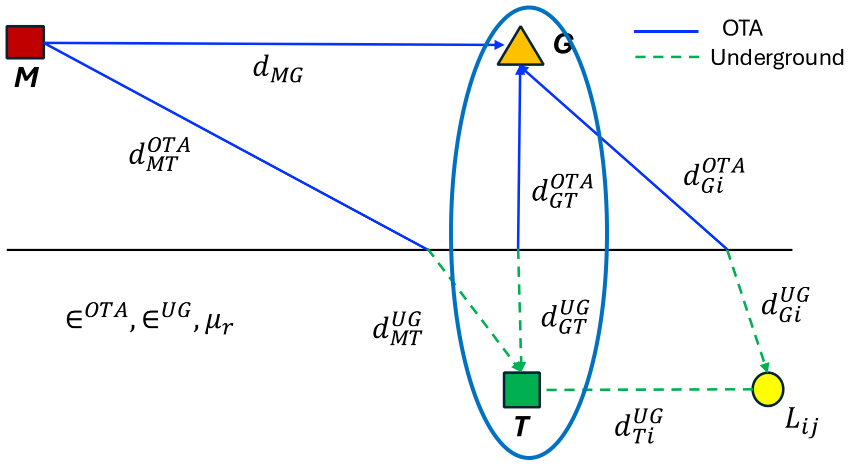
RSS at G

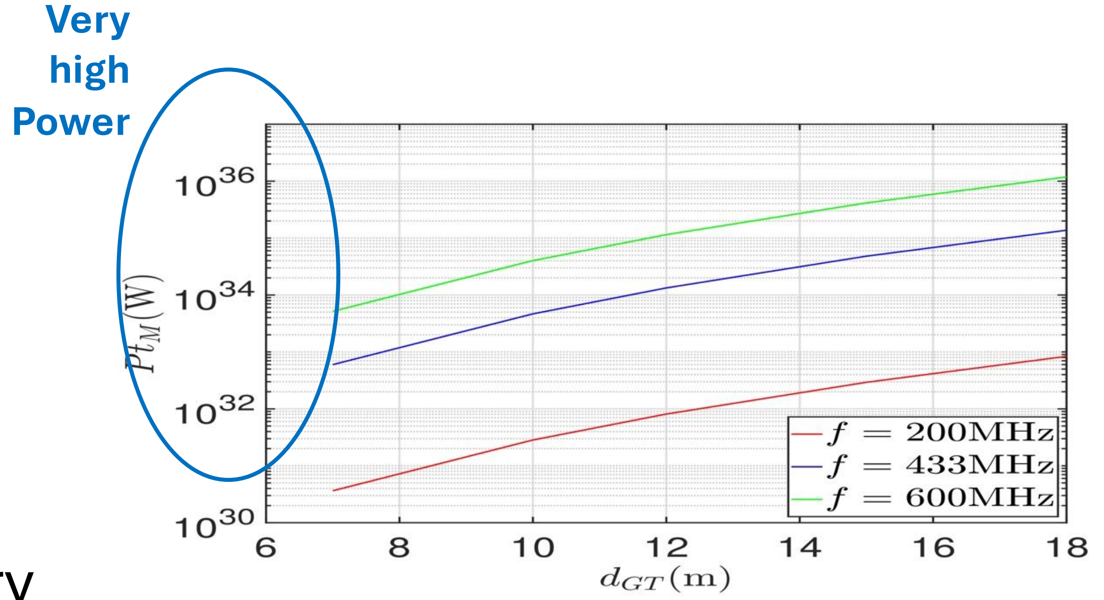
$$\tau_{low} \leq \gamma(k) \leq \tau_{high} \forall k = 1, \ldots, l$$

Experimental Setup

- We utilize a 433 MHz Underground testbed with 30% volumetric water content.
- Testbed utilizes antenna with $\lambda =$ 30-69cm
- G uses Full-Wave dipole antenna
- L and T uses Single Ended Elliptical antenna with 10dB gains
- Distances d_{GT}^{UG} = 0.35m, d_{Gi}^{UG} = 0.40m, d_{GT}^{OTA} = 7.8m, $d_{Gi}^{OTA} = 7.0m, d_{Ti}^{UG} \approx 2m$
- Power transmit =10mW, 37 bytes packet size, 100ms inter packet time and TinyOS app to implement message transmission between nodes.

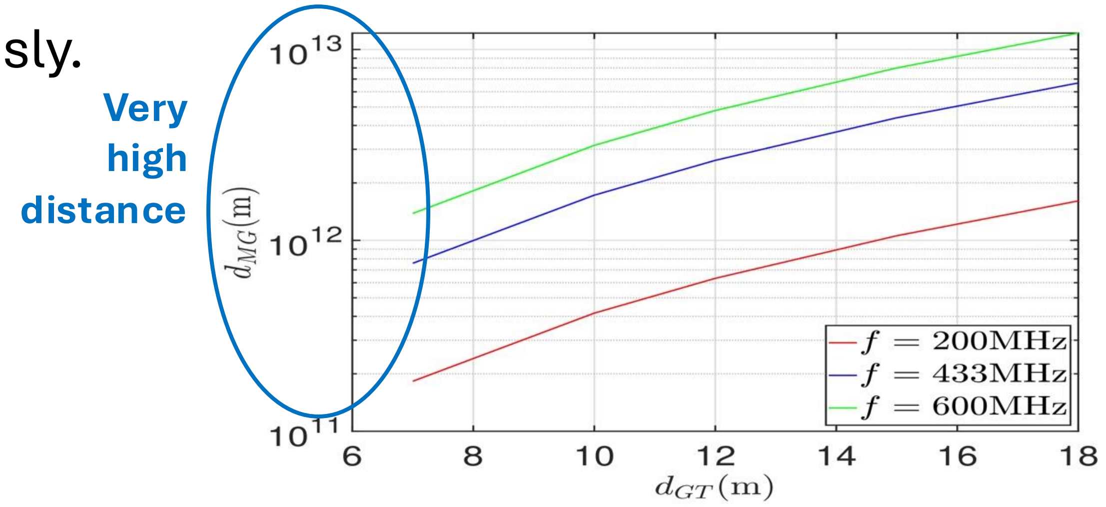
Experimental Evaluation: Type 1 Adversary





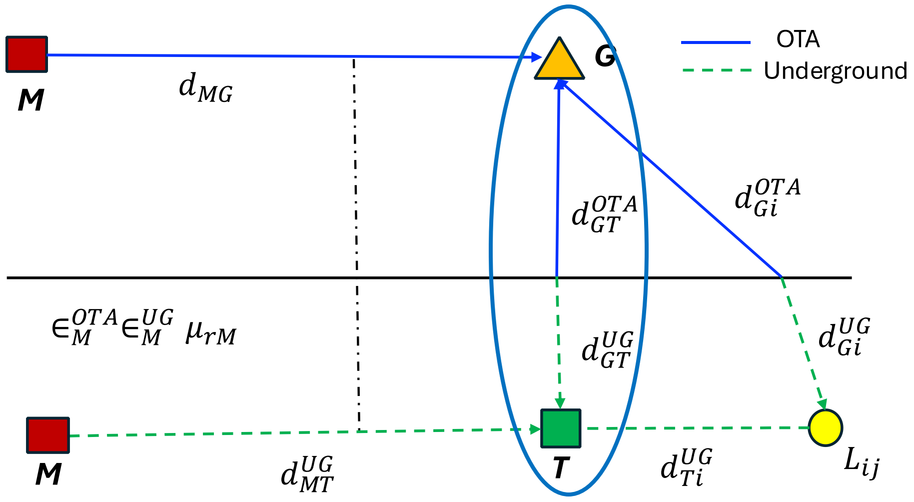
Plot of distance and power transmitted against distance between T and G.

- Condition for adversary to defeat type 1 adversary
  - Equal transmit powers in step 3 and 5 to pass the verification at the distance, d_{MG} simulataneously.

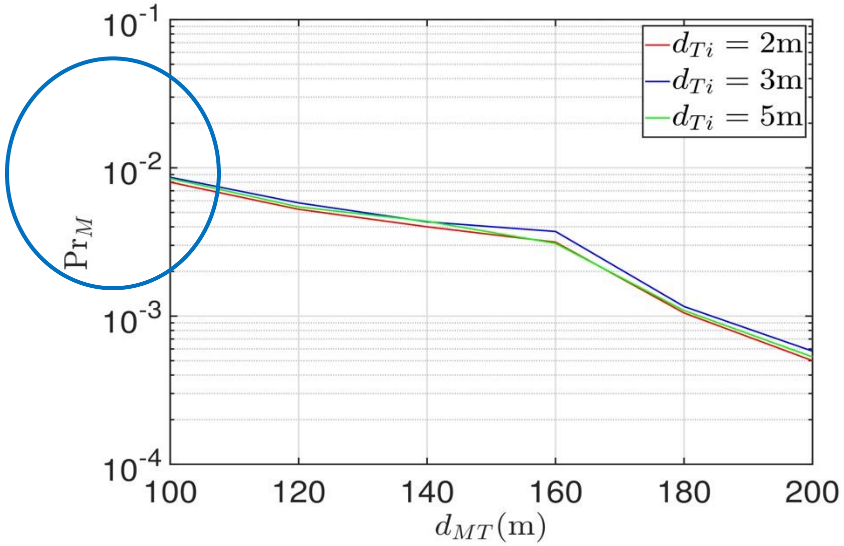


- M must be place extremely far from G
  - Step 3 fails
  - High attenuation.
  - Adversary needs to transmit very high power (L transmit on 3W)

Experimental Evaluation: Type 2 Adversary

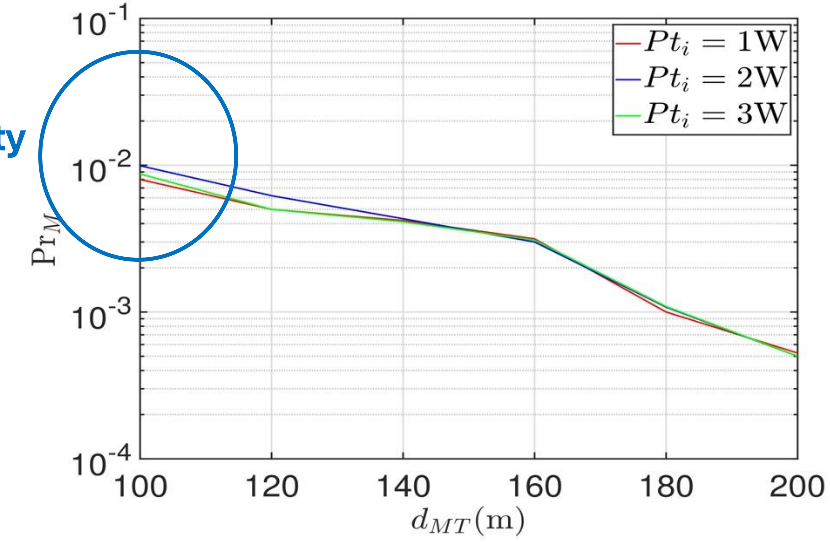


Very low Success probability



Success probability of Type 2 adversary against distance between M and T

Very low Success probability



- Threshold, τ_{low}^{T} = 2.512 × $10^{-7} mW$ to τ_{high}^{T} = 6.309 × $10^{-7} mW$.
- The success probability, 8.6×10^{-3} and 5.8×10^{-4} (very low probability)
- Even though verification at G maybe possible since the channel is visible.
- Verification at T fails. It has to compute a system of equations which is NP-hard

Summary

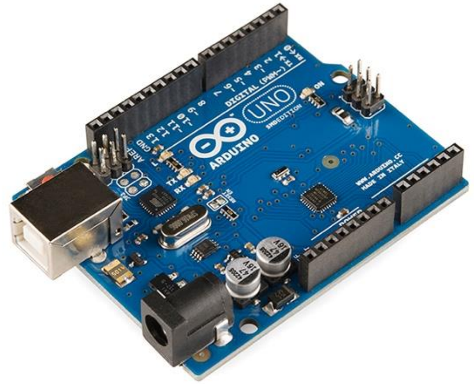
- We address the problem of Trust Establishment for underground wireless networks.
- We used hard-to-forge underground wireless propagation laws to achieve in band node authentication and secret establishment.
- We demonstrated that STUN is resilient to advanced attacks.

- **[Oguchi, Ghose, Vuran, 2022, IEEE INFOCOM Wkshp Wireless-Sec]**
- **[Oguchi, Ghose, Vuran, 2024, IEEE TWC (Under-submission)]**

Location Authentication for Over-The-Air and Underground Wireless Networks

* This work is a collaborative effort with Hakim Lado.

Radio Frequency (RF) Fingerprinting



- Operating Principle:
  - No two devices have the same fingerprint
- Uses:
  - Device Identification
  - Device Authentication
  - Indoor positioning and tracking

- Uniqueness Causes:
  - Hardware impairment / Manufacturing process variation
  - Serves as discriminative features

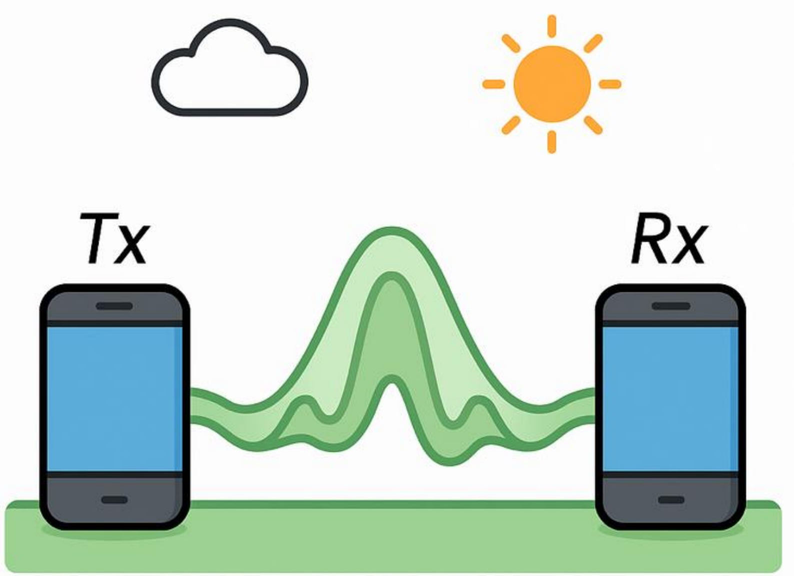
- Examples: Phase Noise, IQ imbalance

Can we leverage physical-layer channel features for location authentication across different environmental setups?

Yes!

CIR-based CNNs with fine-tuning

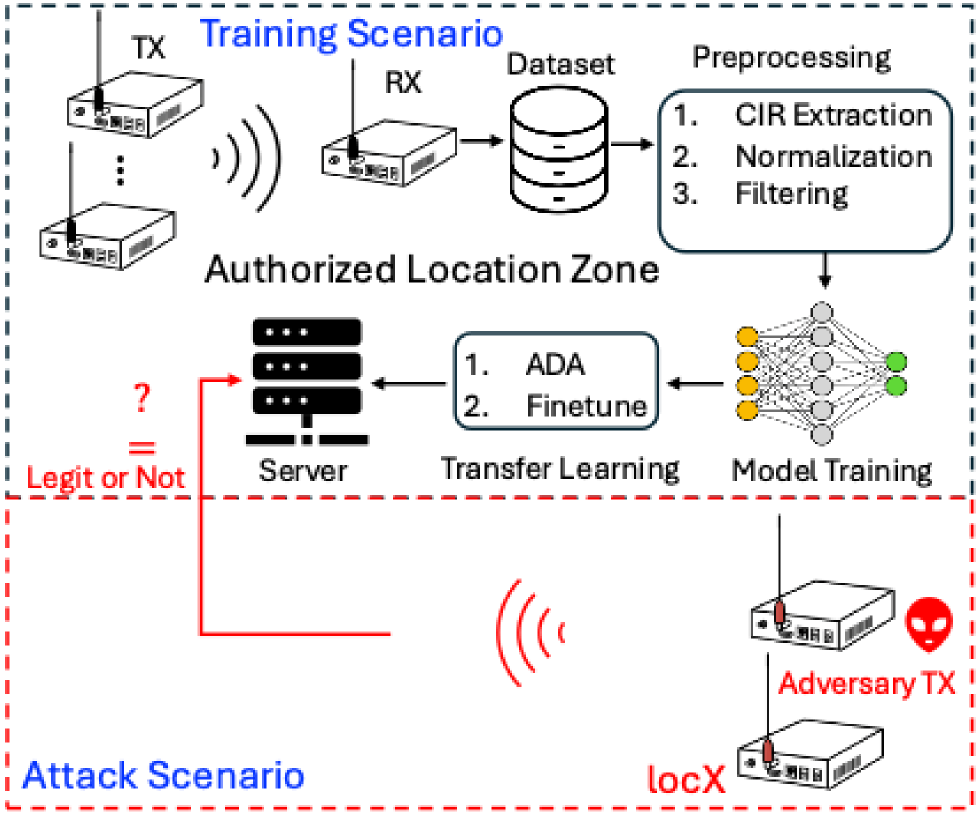
RF Fingerprint-Based Location Authentication for Over-The-Air and Underground Wireless Networks



- Why is CIR Hard-to-Forge?
  - Location Specific -> captures multipath profiles of wireless channel
  - Fine-Grained: Sensitive to small spatial and temporal variations, ideal for CNN learning
- Device-agnostic but environment-sensitive:
  - Even if an attacker uses the same hardware, small location changes can significantly alter the CIR due to phase shifts and reflections.
- Non-linear Mapping:
  - CIR features used in deep learning are extracted via complex, high-dimensional transformations, which are not easily invertible or imitable.

System Overview

- Transmitter (Tx_i): Sends signals from authorized locations (l_i).
- Receiver (Rx_i): received I/Q samples then extracts CIR.
- Server (S): Compares received CIRs to determine legitimate vs. adversarial location.

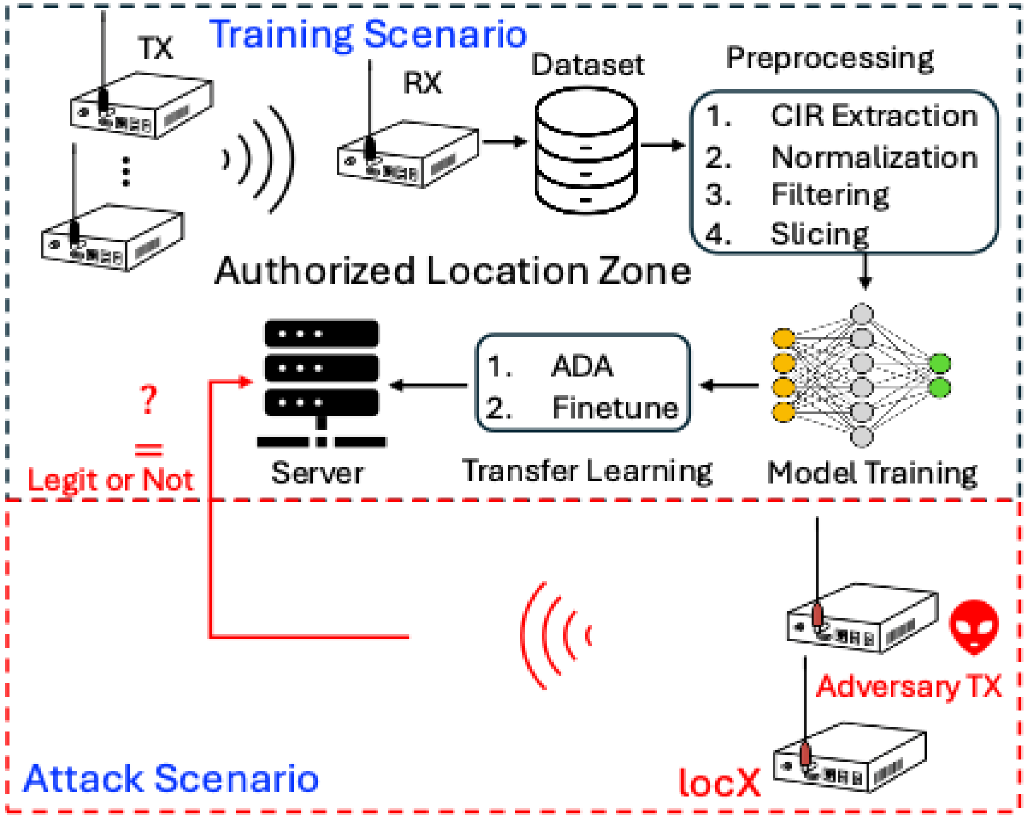


Key Assumptions:

- No pre-shared secret or encryption needed.
- CIR is used as a **location fingerprint**.
- System is **agnostic** to modulation, protocol, and minor device variations.

Threat Model

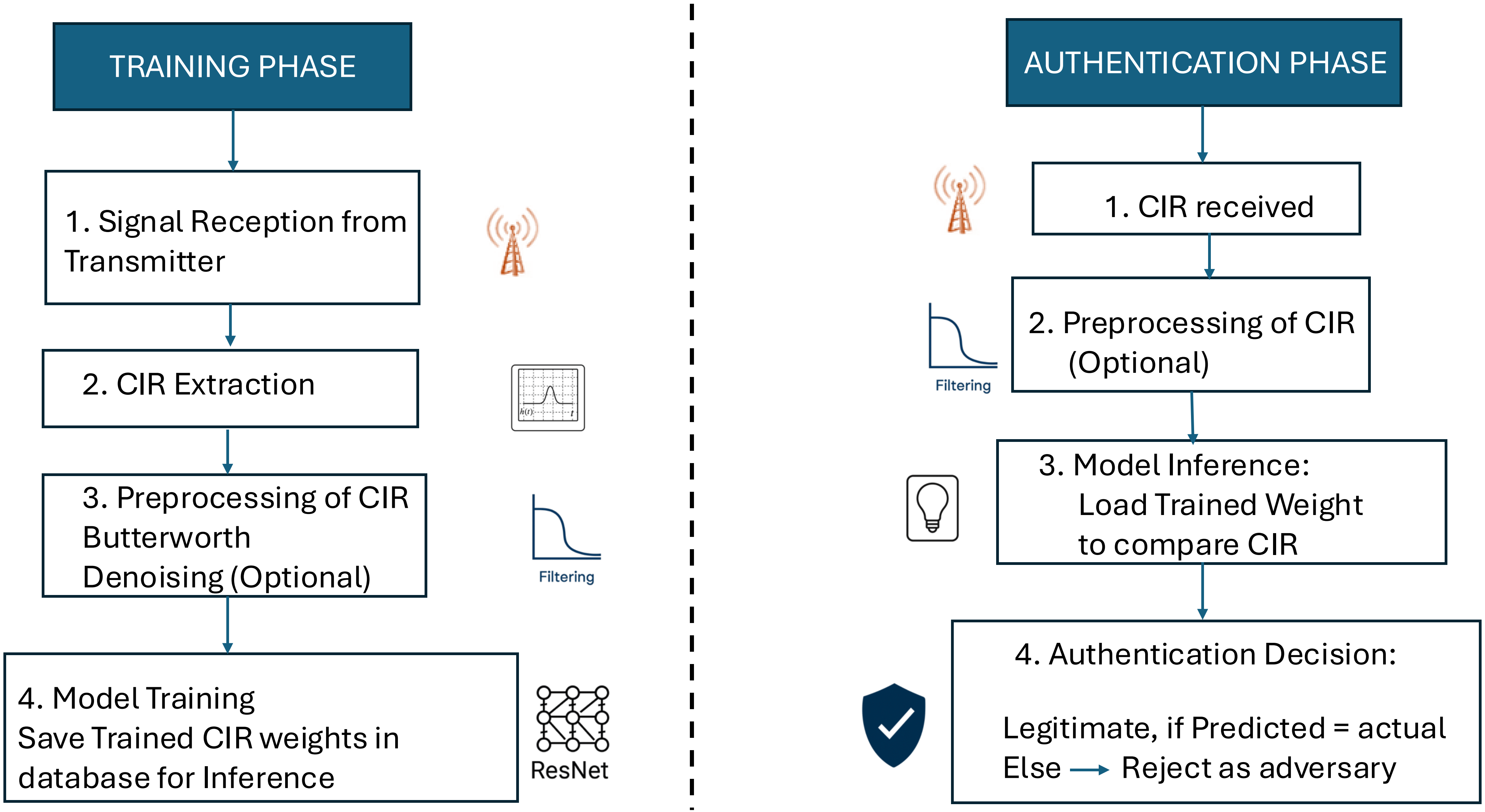
- Adversary Types:
  - Friis Empirical Attacker
    - Knows only distance information
    - Can estimates CIR using Friis' equation
    - Ignores multipath and noise effects
  - Ray-Tracing-Enhanced Adversary
    - Better mimics multipath reflections and physical layout
    - More powerful than Friis attacker



Assumption: No access to the server and legitimate CIR for spoofing

Goal: Fool the model by imitating location fingerprints from different zones

RF Fingerprint-Based Location Authentication Framework



Note: Signal is received from transmitter from one location and can test transmitters at multiple locations.

Mitigating Device Bias in CIR

- CIR Is primarily location-dependent
  - Reflects propagation environment between a transmitter (Tx) and receiver (Rx): multipath, delay spread, attenuation, etc.
- CIR can still be device-affected
  - Hardware imperfections: Different oscillators, filters, ADCs.
  - Antenna patterns: Even slight variations can change received paths.
- Techniques to remove device effects from CIR
  - Filtering/preprocessing, Denoising, Transfer Learning / Fine-Tuning

System Architecture

COMPLETE MODEL PERFORMANCE ANALYSIS FOR LOCATION AUTHENTICATION

Model	Best Performance	Reliability	Key Characteristics
ResNet-50	85–95%	Excellent across all scenarios	Deep residual learning, handles complex spatial features
ResNet-34	80–92%	Very Reliable, best overall	Optimal depth-performance balance, consistent across environments
ResNet-18	75–90%	Very Reliable	Lightweight yet effective, good for resource-constrained deployment
In-Lab Model	70–85%	Reliable in controlled settings	Custom 5-layer CNN, baseline comparison model
GoogleNet	60–70%	Reasonably Reliable in ADA + Filtered settings	Inception modules provide moderate feature extraction
VGG16	50–60%	Inconsistent across TX/distance	Too deep without skip connections, suffers from vanishing gradients
VGG19	∼33%	Unreliable, fails to generalize	Severe vanishing gradient problem, cannot learn location features

- Machine Learning Models
  - ResNet-18/34/50 (Better)
  - Compared with: In-lab, VGG16/19, GoogleNet
  - Metrics: Accuracy, Stability, Reliability

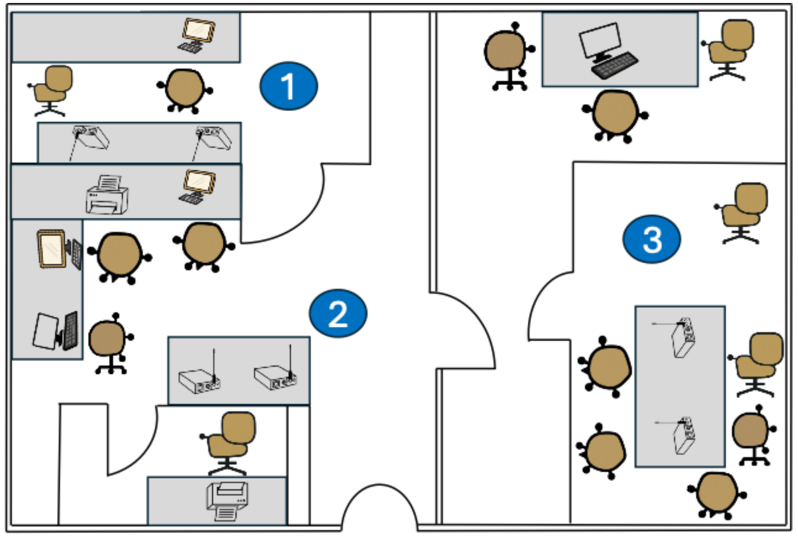
- Processing Pipeline:
  - Filtering -> Butterworth (Better)
  - Compared with: Moving Average, Elliptic
  - Denoising Autoencoder

COMPARATIVE PERFORMANCE ANALYSIS OF FILTERING METHODS FOR LOCATION AUTHENTICATION

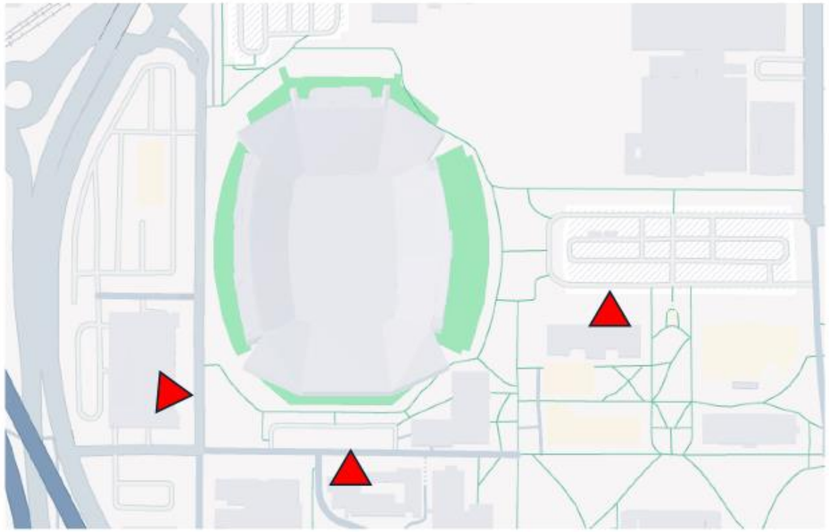
Filtering Method	Best Performance	Stability	Reliability
Butterworth	80-90%+	High	Excellent
Moving Average	∼50-60%	Very Poor	Unreliable
Elliptic	∼60-70%	Extremely Poor	Completely Unreliable

- Domain adaptation / fine-tuning -> Improve our results

Experimental Setup



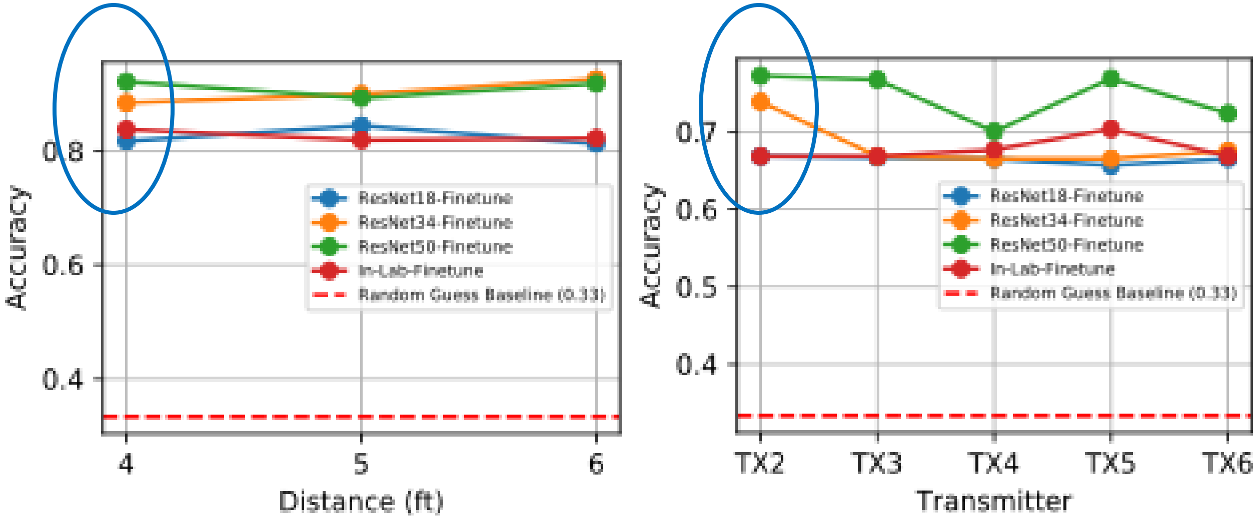
(a) Indoor setting



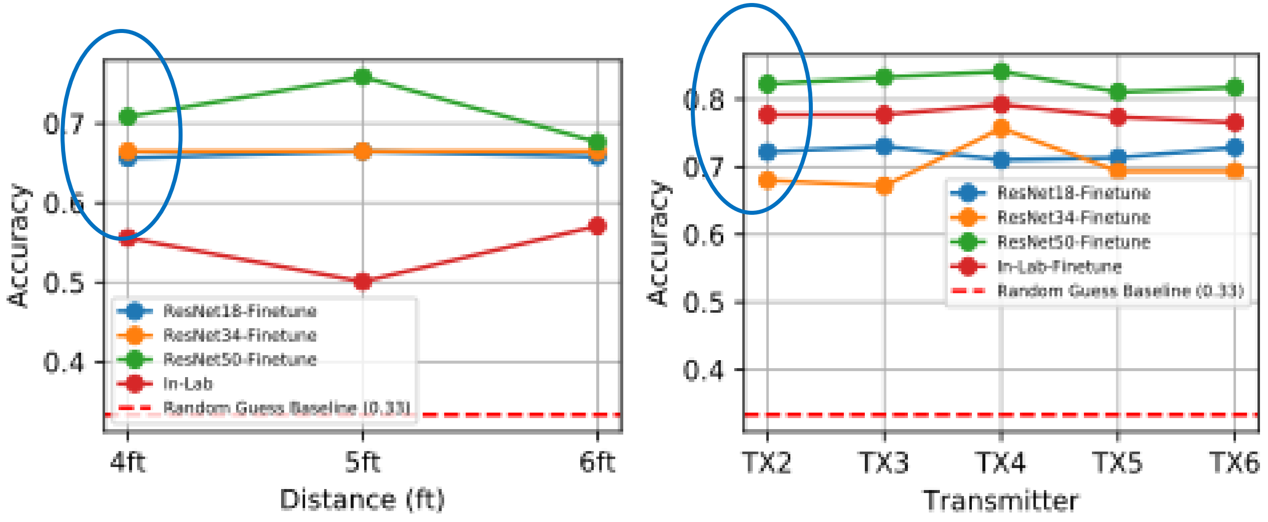
(b) Outdoor setting

- OTA testbed
  - Varying USRP (B-series) Transmitter/Receiver devices at various fixed locations
    - Same R_x Different T_x
    - Different R_x Different T_x
  - Varying USRP distances (4ft, 5ft, 6ft)
    - Same R_x Different T_x
    - Same R_x Same T_x

Outdoor Evaluation: Accuracy



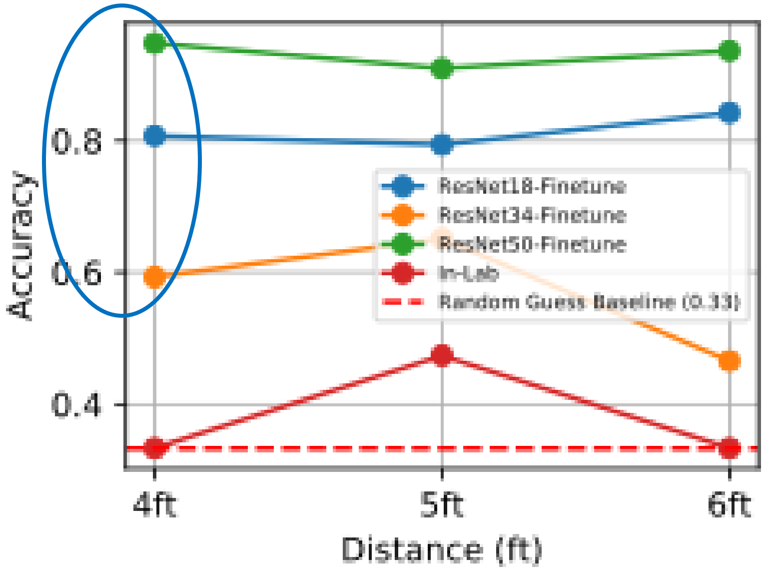
(a) Butterworth Finetune



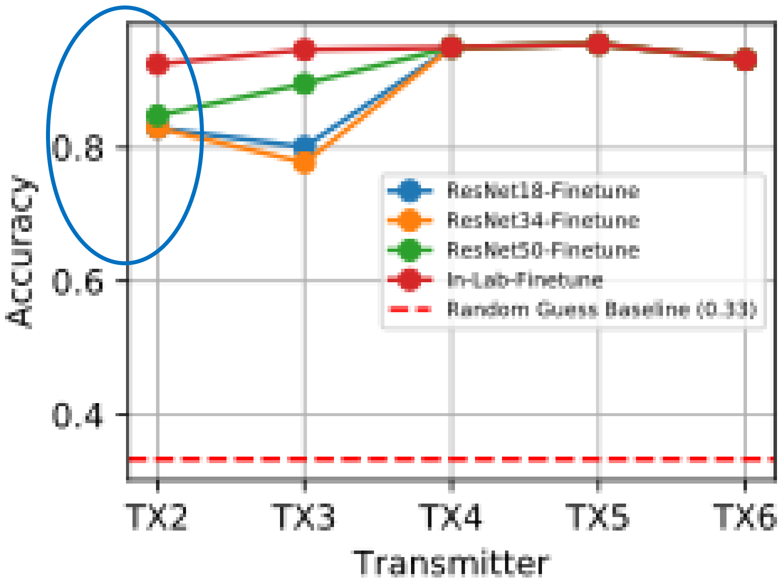
(b) Denoised Finetune

- ResNet-50 achieved > 80% across devices and distance
- Fine-tuned models + filter outperform baselines -> Best performance
- Domain adaptation/finetune improves generalization

Indoor Evaluation: Accuracy



(a) Distance



(a) Devices

- ResNet-50 achieved > 85% across devices and distance
- In-lab – unstable compared to ResNet
- Fine-tuned models + Butterworth + ReLU-> Best performance
- Denoising does not do well for Indoor Scenarios

Robustness Analysis – Friis-Based Adversary

- Friis-Based Adversary Model:

$$h_{Friis}(d) = \sqrt{G_t G_r}\left(\frac{\lambda}{4\pi d} e^{-j\frac{2\pi d}{\lambda}}\right)$$

- Attacker constructs synthetic channel using:

$$X_{Adv} = h_{Friis}(d_{Tx-Rx})\, h_{Rx-Adv}$$

- Goal: Mimics legitimate CIR

$$Y = \boxed{h_{Rx-Adv} X_{Adv} + n \approx h_{Rx-Tx} X + n}$$

- Legitimate:

$$Y = h_{Rx-Tx} X + n$$

- Adversary:

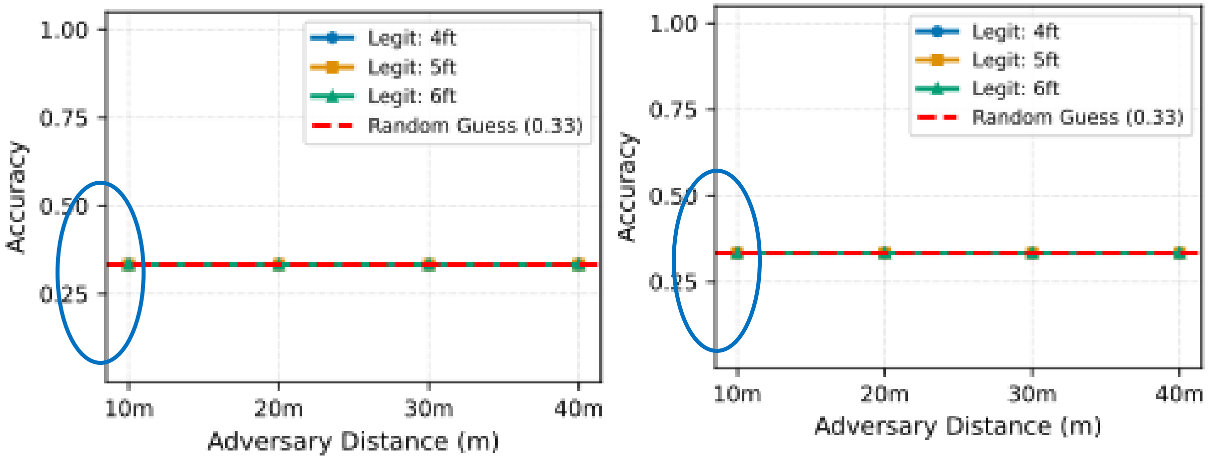
$$Y = h_{Rx-Adv} X_{Adv} + n$$

$$X_{Adv} = h_{Friis}(d_{Tx-Rx}) X$$

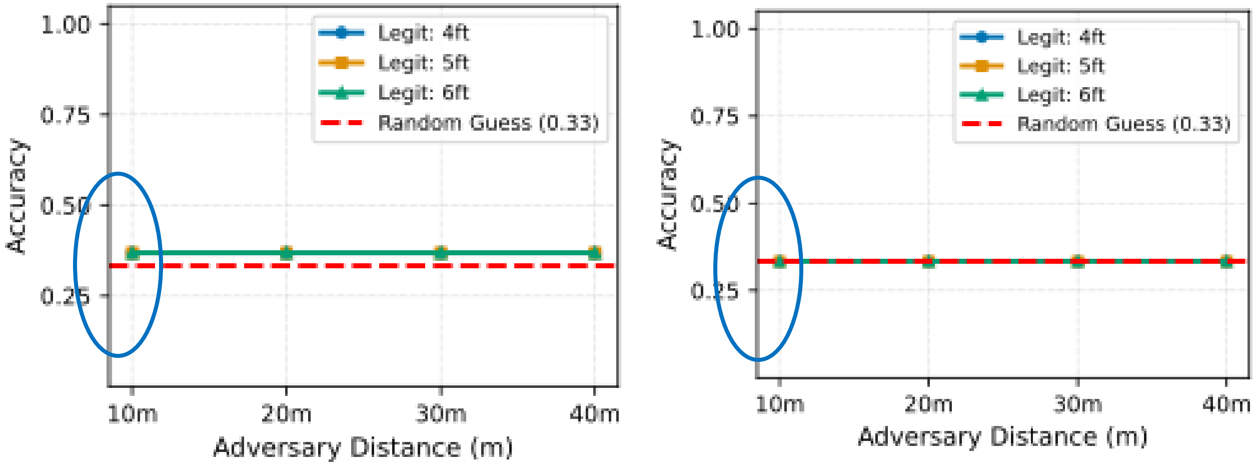
Friis attackers fail to replicate fine-grained CIR features due to:

- Environmental multipath variability – Minimal or no knowledge
- A single-tap approximation
- Inability to mimic deep features captured by CNNs

Robustness Analysis: Ray-Tracing-Enhanced Adversary



(a) indoor



(a) outdoor

Evaluation Findings:

- **It still fails to breach model defenses**: accuracy for adversary remains ~33–35%
- CNNs learn **non-trivial spatial-temporal patterns** difficult to replicate

Our Conclusion:

- Even with ray-tracing-generated CIRs, attackers fail to replicate the true distribution of legitimate channel responses, reinforcing the robustness of our location authentication system.

Summary

- Location Authentication with RF fingerprinting is viable in dynamic environments
- Deep learning + CIR features can resist advanced spoofing
- No secrets or key exchange required

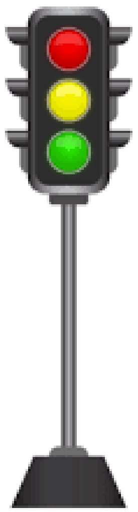
Future Work

- Investigating the cutoff distance/range in indoor and outdoor experiment.
- Test with underground dataset

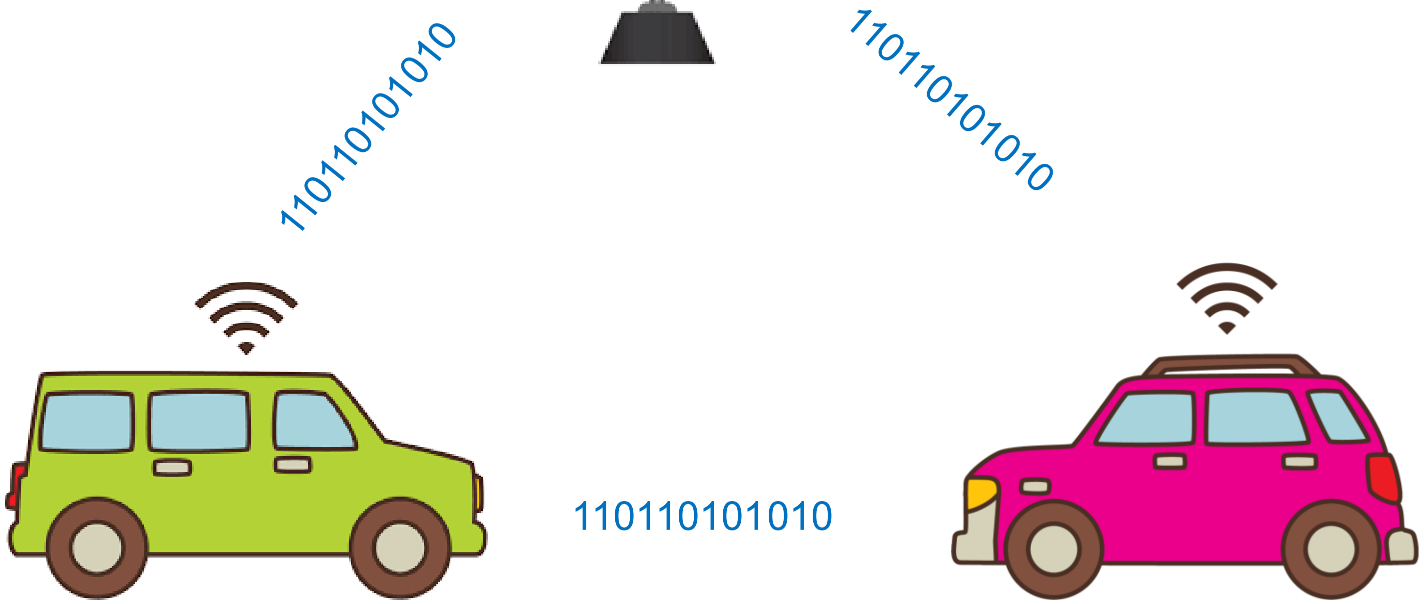
[Oguchi, Lado, Ghose, Wang, Vuran, 2025 – In Preparation]

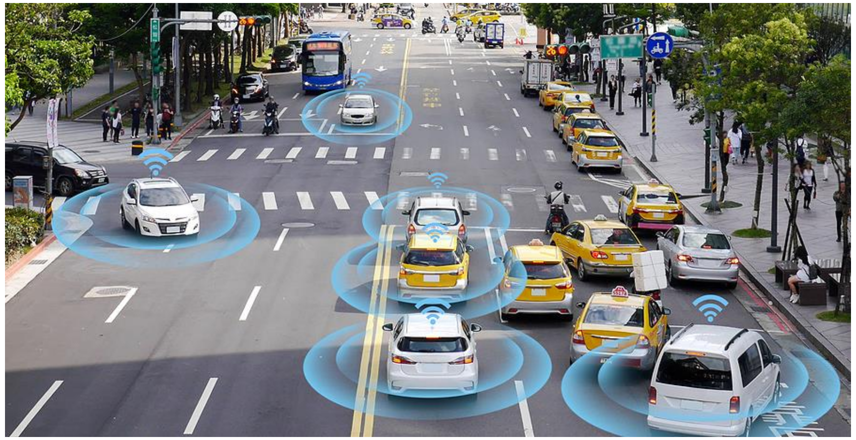
Security in Mobile Setting for Connected Autonomous Vehicles

Vehicular and Ad-hoc Networks



- Enhanced road safety
- Improved traffic management
- Passenger infotainment
- Reduced Traffic Congestion
- Better driving decision making





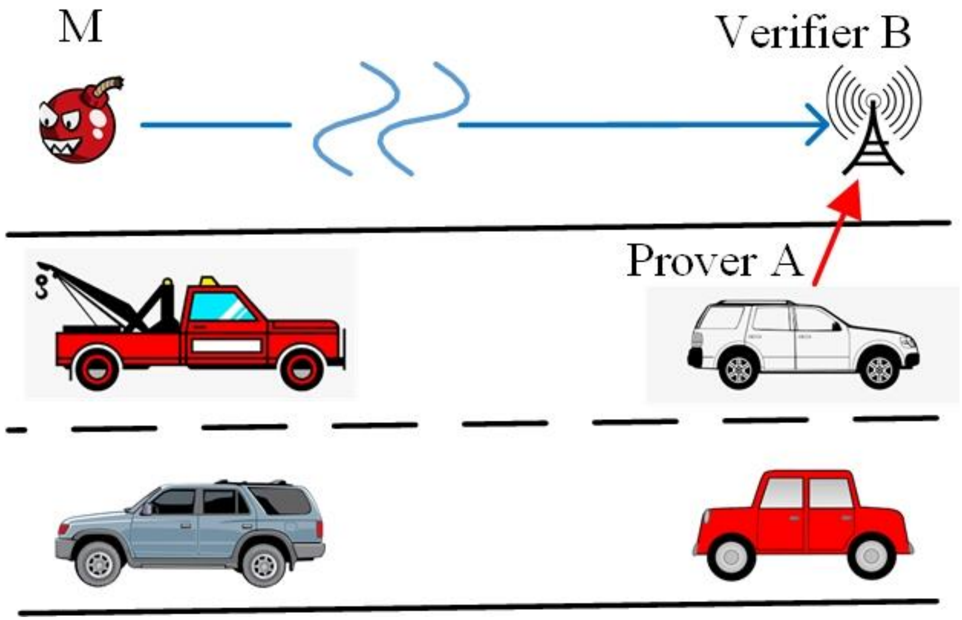
Can we securely verify the truthfulness of the location and velocity claims of an incoming vehicle to prevent attacks?

Yes!

Trajectory and Motion Vectors (TMV)

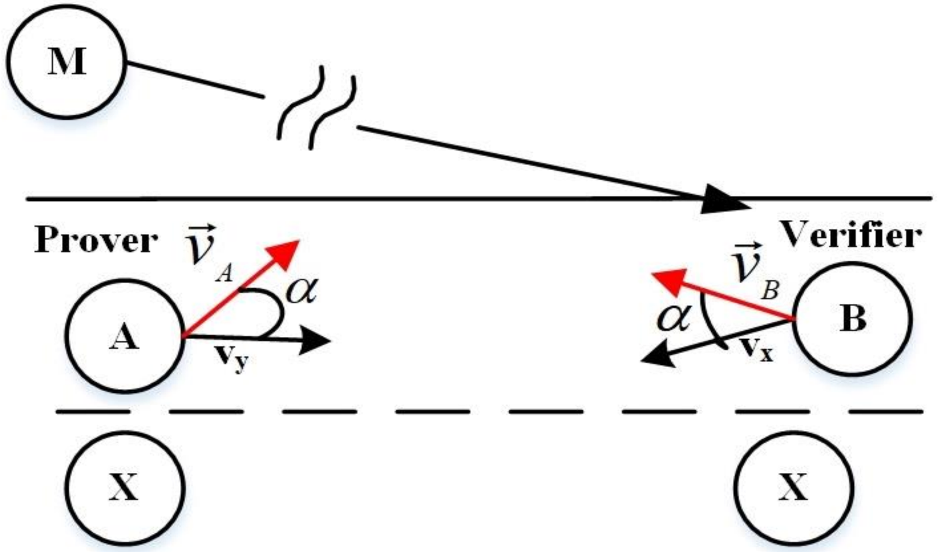
VET: Autonomous Vehicular Credential Verification using Trajectory and Motion Vectors

- Location and Velocity Information
  - Location = Direct Estimation
  - Velocity = Frequency of Arrival

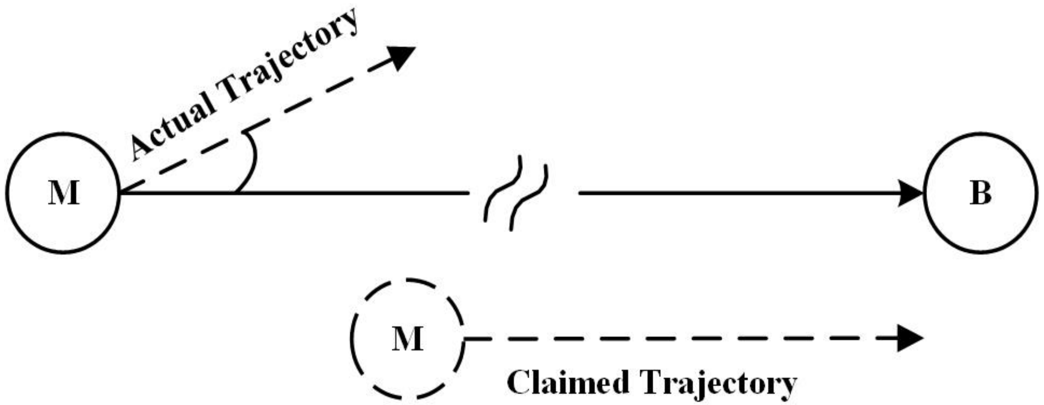


System Model

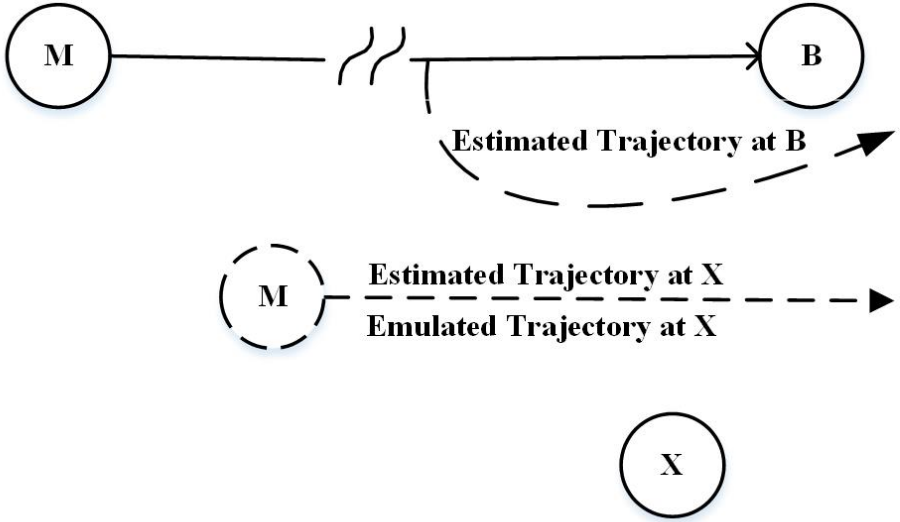
- The Legitimate Prover A
  - A uses omnidirectional antenna
  - Has valid credentials (PKI or Symmetric key)
- The Verifier B
  - Other truthful verifier X
  - Perform verification independently
  - Verifiers do not require mutual trust.



Threat Model



Remote Attacker

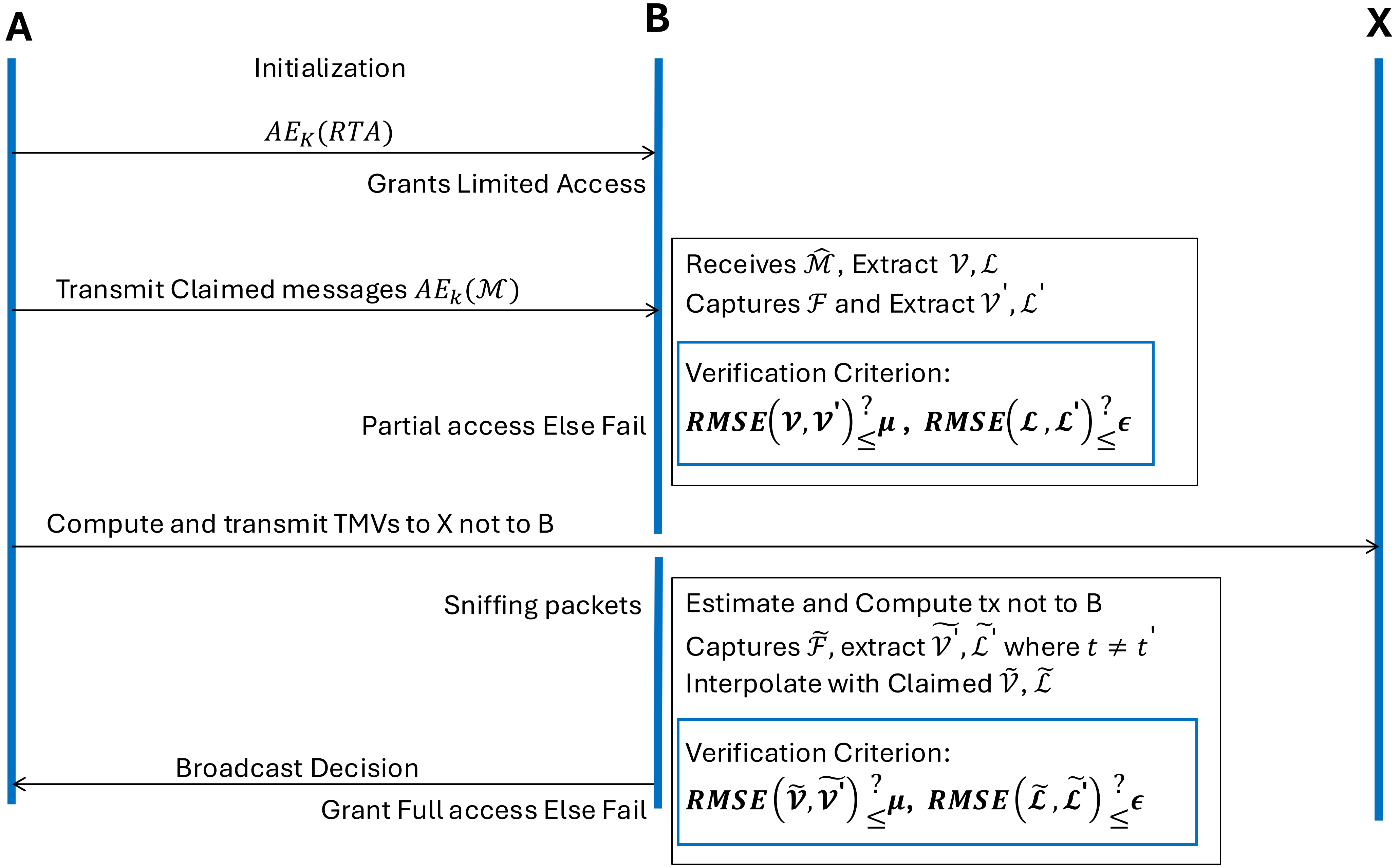


Remote Advanced Attacker

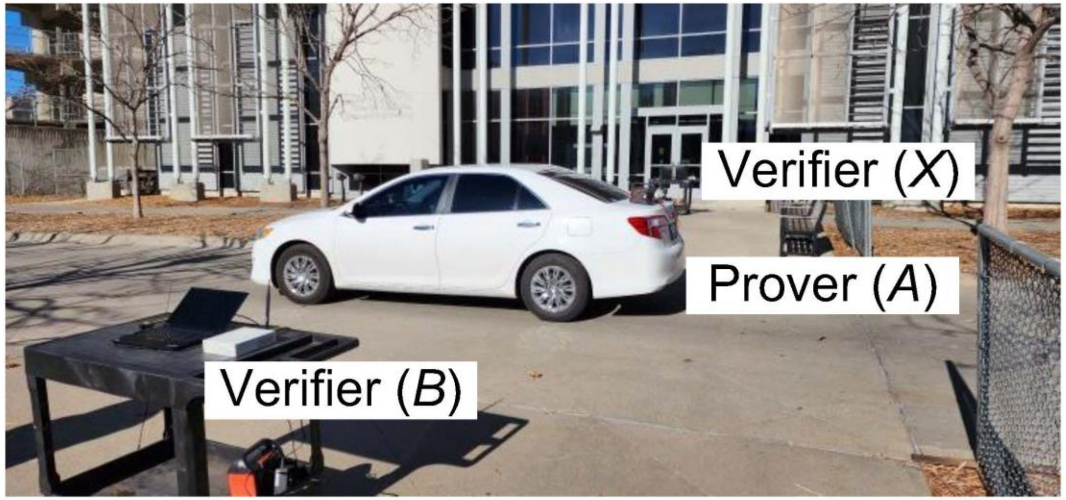
- Has valid credentials
- Within the communication range of B
- Attempting to Inject messages without modifying PHY-layer data

- Has valid credentials
- Can additionally intentionally modifying PHY-layer data.

VET: Credential Verification using Trajectory and Motion Vectors

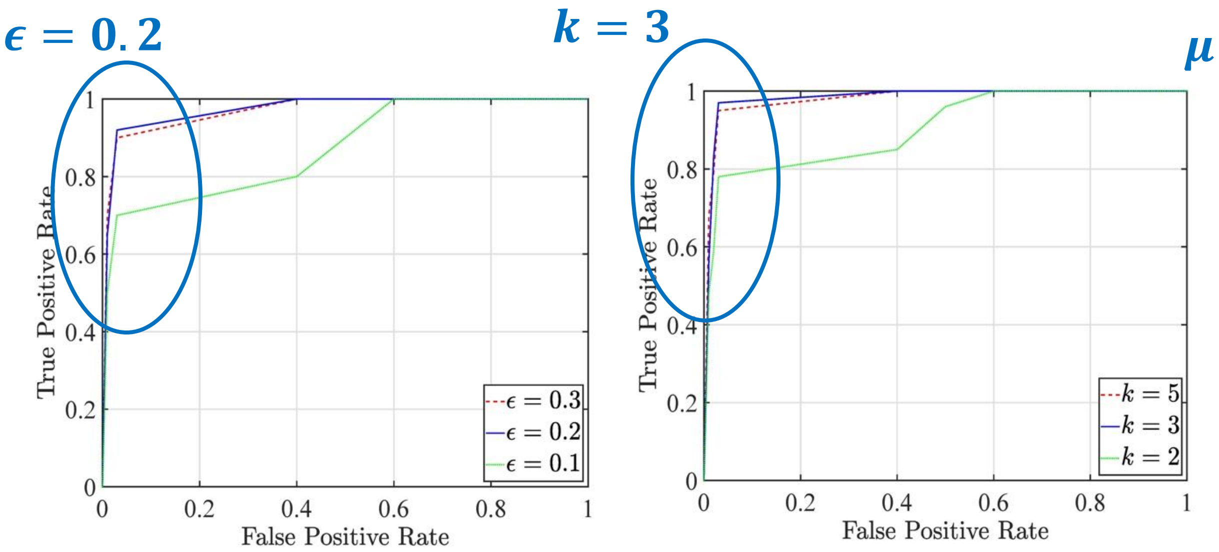


Experimental Setup

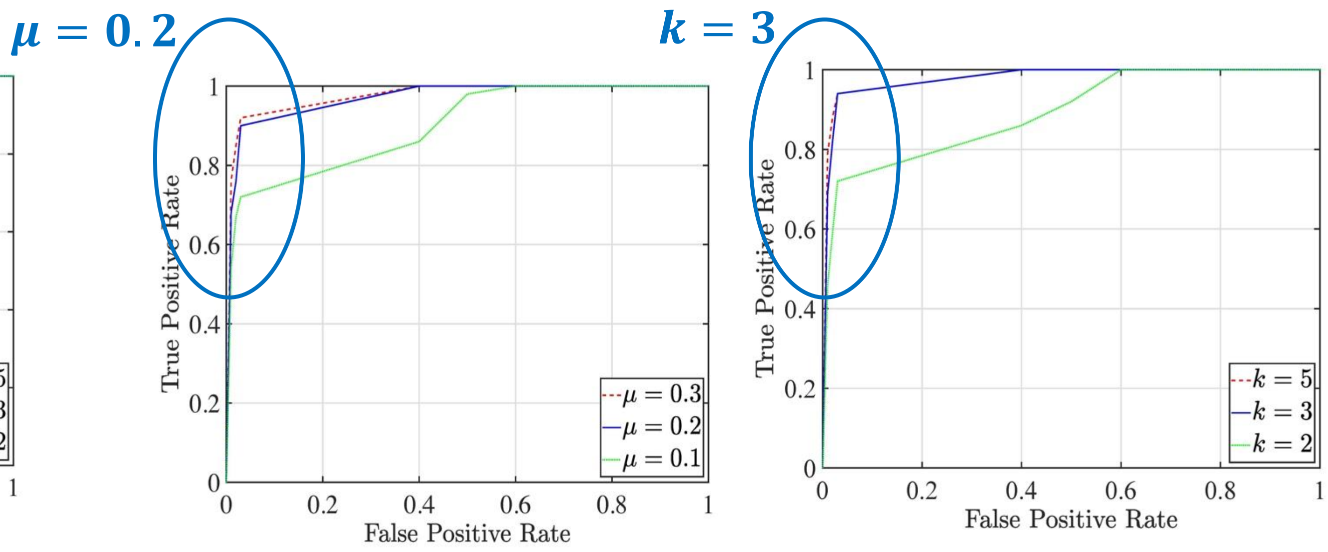


- We utilize a USRP 2922 for the prover A, verifiers B, and X
- We broadcast BPSK signals at center frequency $f_o = 915MHz$ running GNU radio code.
- The prover and verifiers are connected to a Lenovo ThinkPad T14 laptop
- A GPS enabled phone that collects the ground truth location and velocity
- All laptops and phone are synchronized to use the same Network time protocol server.

Experimental Evaluation: Correctness Analysis



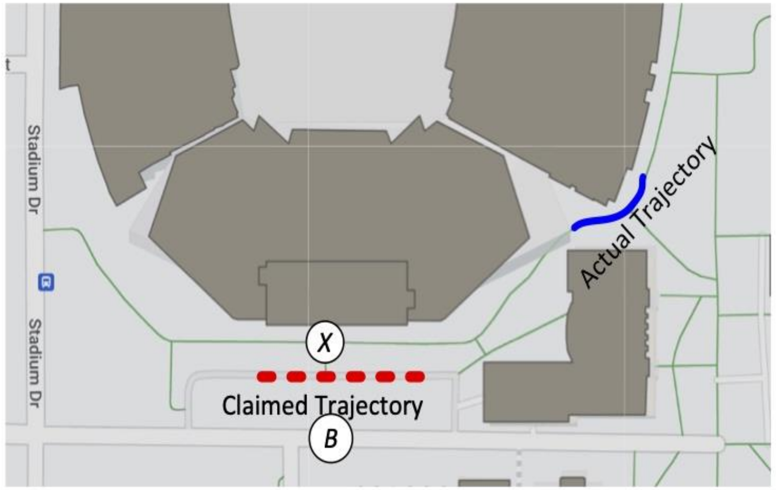
ROC for Location



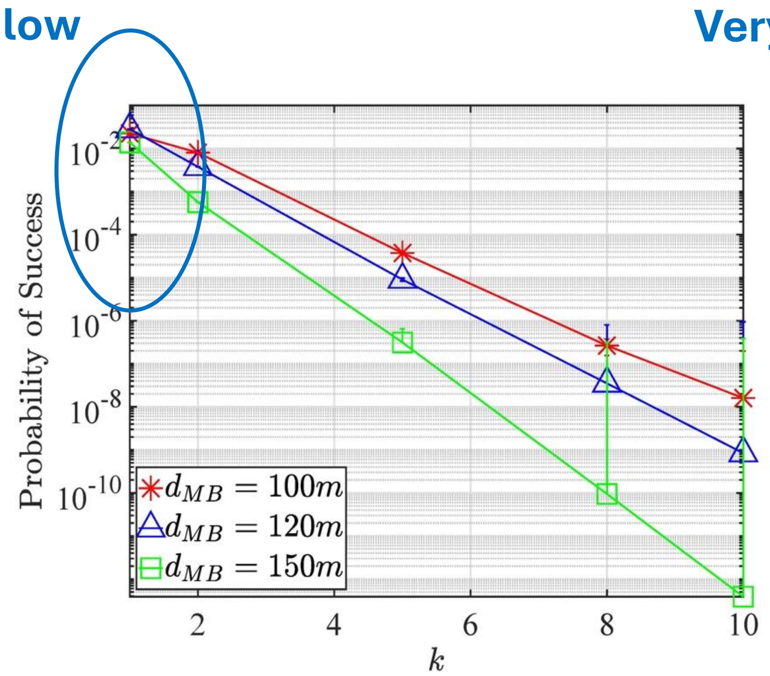
ROC for velocity

- We implement FOA and Direct location estimation and compute the ROC
- We compare our results with ground truth data.
- We evaluate two parameters
  - The acceptable errors (ϵ, μ) to set
  - The number of trajectory point (k) required to complete the verification.

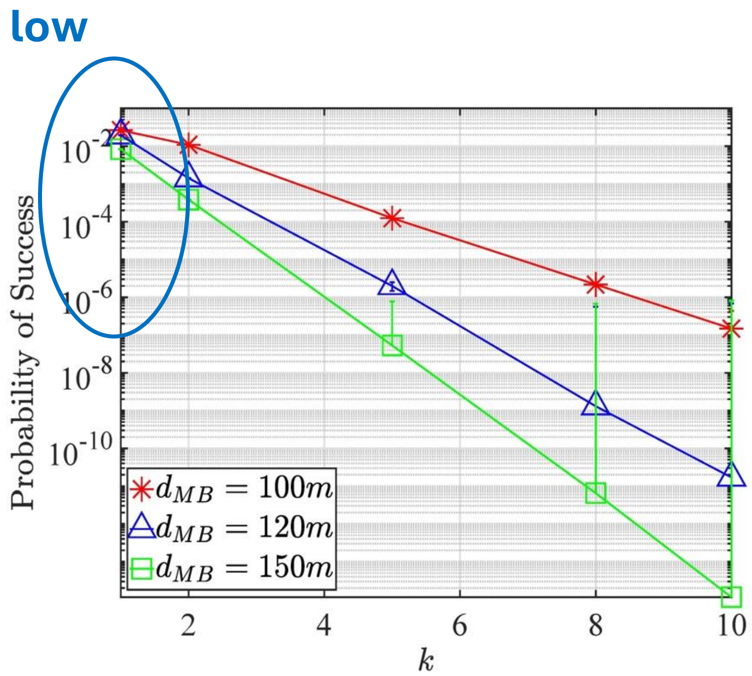
Experimental Evaluation: Robustness Analysis



Trajectory



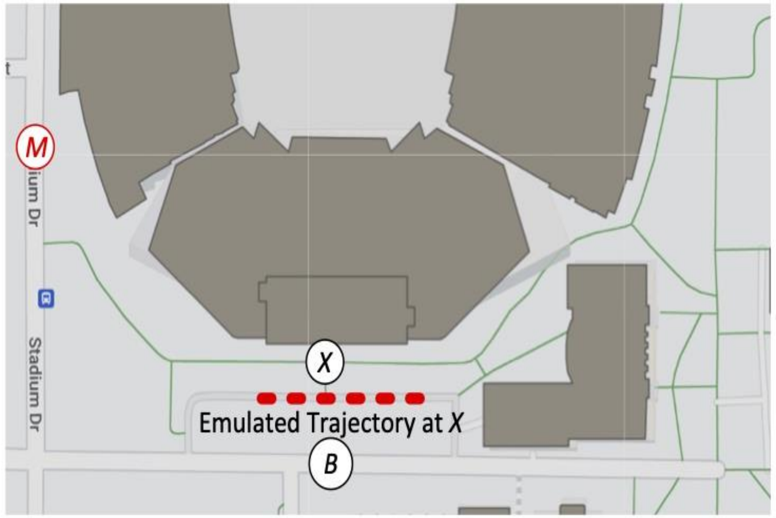
Location



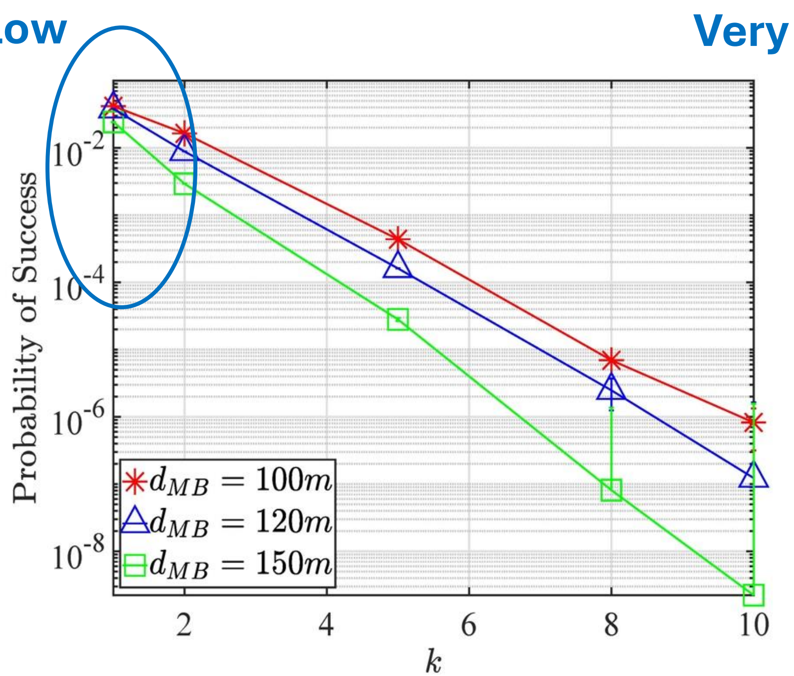
Velocity

- The Remote Attacker
  - VET can detect remote moving adversary attempting to inject rogue messages
  - As distance increases, the probability of success decreases.

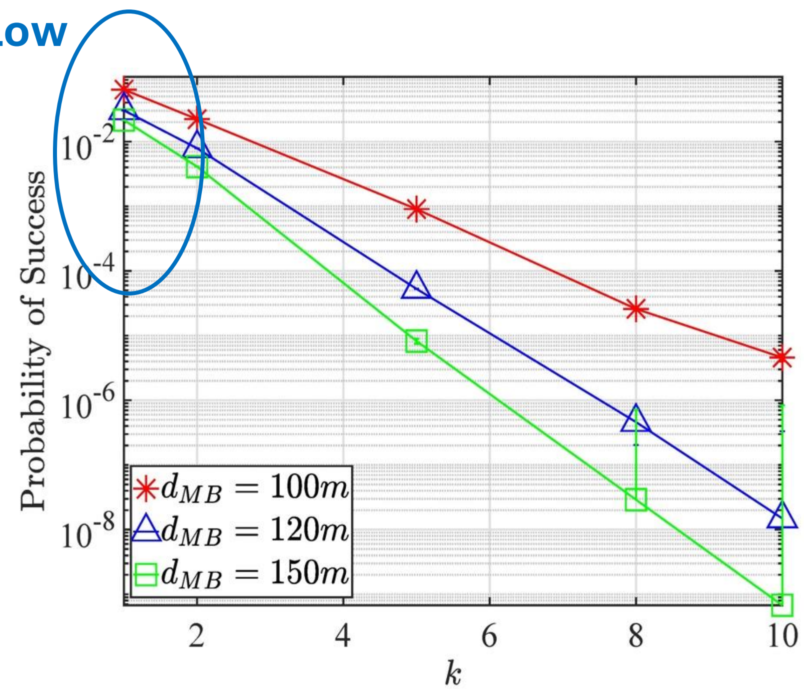
Experimental Evaluation: Robustness Analysis



Trajectory



Location



Velocity

- A Remote Advanced Attacker
  - We compute wireless Channel h_{MB} and h_{MX}
  - Adversary utilize the knowledge of the channel to emulate X
  - Probability of Success is very low

Summary

- We address the problem of secure veracity verification for automomous vehicles using trajection and motion vectors
- We implement a location and motion based strategy that verifies the claimed TMVs from randomly estimated TMVs
- VET can detect remote adversary injecting spoofed messages with 97% true positives

[Oguchi, Ghose, 2023, EAI SecureComm]

List of Publications

Peer-Reviewed Conference Publications

1.Oguchi, Ebuka; Ghose, Nirnimesh *"VET: Autonomous Vehicular Credential Verification using Trajectory and Motion Vectors"* In Proc. of EAI SecureComm 2023, Hong Kong SAR, pp. 1–23, Oct. 19–21, 2023. (Acceptance rate: 30.3%)

2. Oguchi, Ebuka; Ghose, Nirnimesh; Can Vuran, Mehmet *"STUN: Secret-Free Trust Establishment For Underground Wireless Networks"* In Proc. of IEEE INFOCOM Workshp on Wireless Security (Wireless-Sec), Virtual Event, pp. 1–6, May 2–5, 2022.

Under Review / In Preparation

1. Oguchi, Ebuka; Ghose, Nirnimesh; Can Vuran, Mehmet *"Soil Assisted Trust-Establishment for Underground Internet-of-Things"* Under Review at IEEE Transactions on Wireless Communications (TWC), 2025.

2. Anderson, Malcolm I.; Duong, Truc T.; **Oguchi, Ebuka**; Wisniewska, Anna; Ghose, Nirnimesh *"Systematization of Knowledge for Security in Molecular and Nano-communications" in* Preparation for IEEE Transactions on Molecular, Biological, and Multi-Scale Communications (TMBMC), 2025.

3. Oguchi, Ebuka; Lado, Hakim; Ghose, Nirnimesh; Wang, Boyang; Can Vuran, Mehmet *"RF Fingerprint-Based Location Authentication for Over-The-Air and Underground Wireless Networks"* In preparation for submission to the Network and Distributed System Security Symposium (NDSS), 2025.

Appreciation

- Collaborations: (special thanks to my advisor and other collaborators)

SWAN LAB
Security in Wireless & Ad-hoc Networks

CYBER PHYSICAL NETWORKING
LAB

WASHINGTON STATE UNIVERSITY
VANCOUVER

- Funding Support

NEBRASKA CENTER
FOR ENERGY SCIENCES RESEARCH

NSF
National
Science
Foundation

Thank you!

&

Questions?