CISPA
HELMHOLTZ CENTER FOR
INFORMATION SECURITY

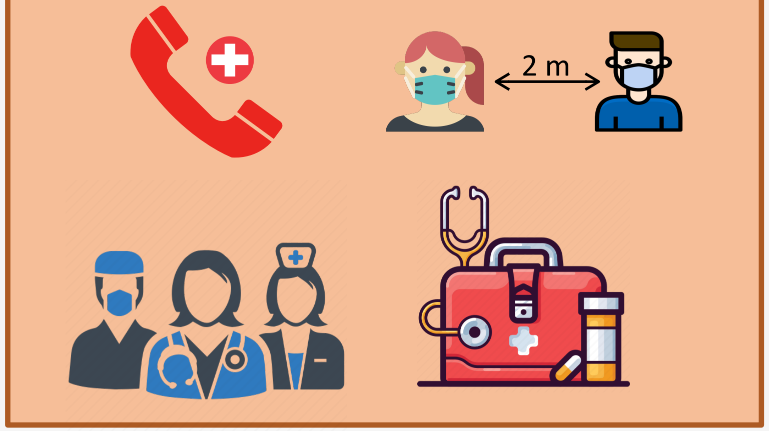
Secure Distance Estimation - Proximity to Positioning

CISPA Helmholtz Center for Information Security

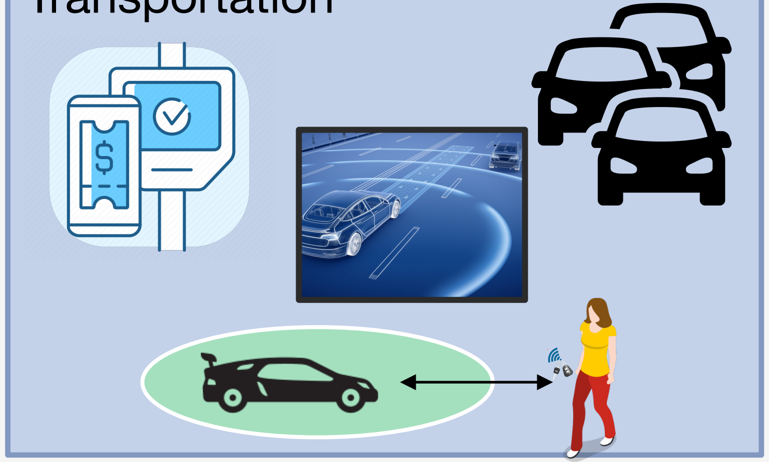
Mridula Singh | GDR Sécurité Event

Applications

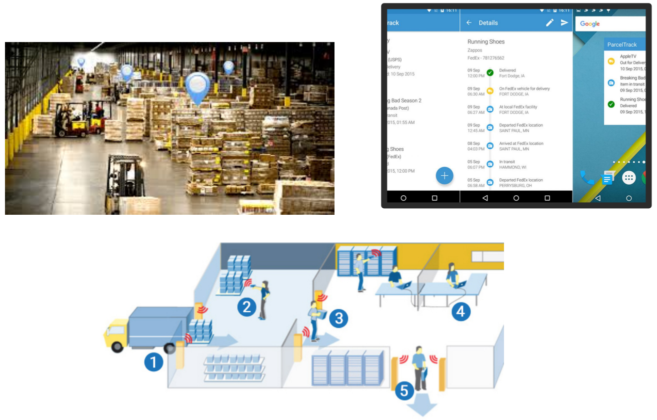
Healthcare



Transportation



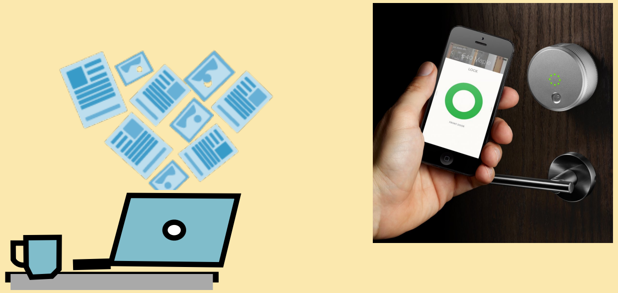
Logistic and Warehousing



Retail

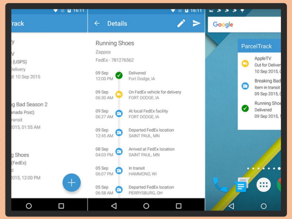
Entertainment
Services

Personal



Implications: Incorrect/Insecure Distance Measurement

Loss of money/assets



rack

y
V
(USPS)
elivery
d: 10 Sep 2015

g Bad Season 2
anada Post)
ransit
015, 01:55 AM

g Shoes
(FedEx)
d
015, 12:00 PM

Details

Running Shoes
Zappos
FedEx - 781276562

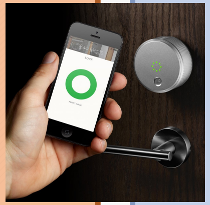
09 Sep 12:00 PM	✓	Delivered Fort Dodge, IA
09 Sep 06:30 AM		On FedEx vehicle for delivery FORT DODGE, IA
09 Sep 06:27 AM		At local FedEx facility FORT DODGE, IA
09 Sep 12:45 AM		Departed FedEx location SAINT PAUL, MN
08 Sep 04:03 PM		Arrived at FedEx location SAINT PAUL, MN
05 Sep 06:07 PM		In transit HAMMOND, WI
05 Sep 06:58 AM		Departed FedEx location PERRYSBURG, OH

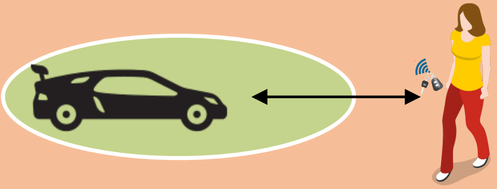
ParcelTrack

AppleTV
Out for Deliver
10 Sep 2015,

Breaking Bad
Item in transit
09 Sep 2015,

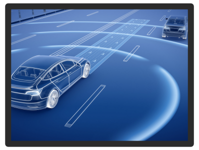
Running Shoe
Delivered
09 Sep 2015,

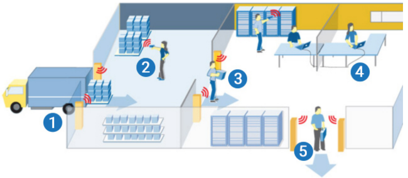




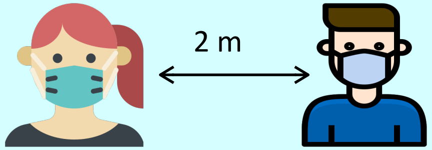
Access to confidential data/physical space

Incorrect location

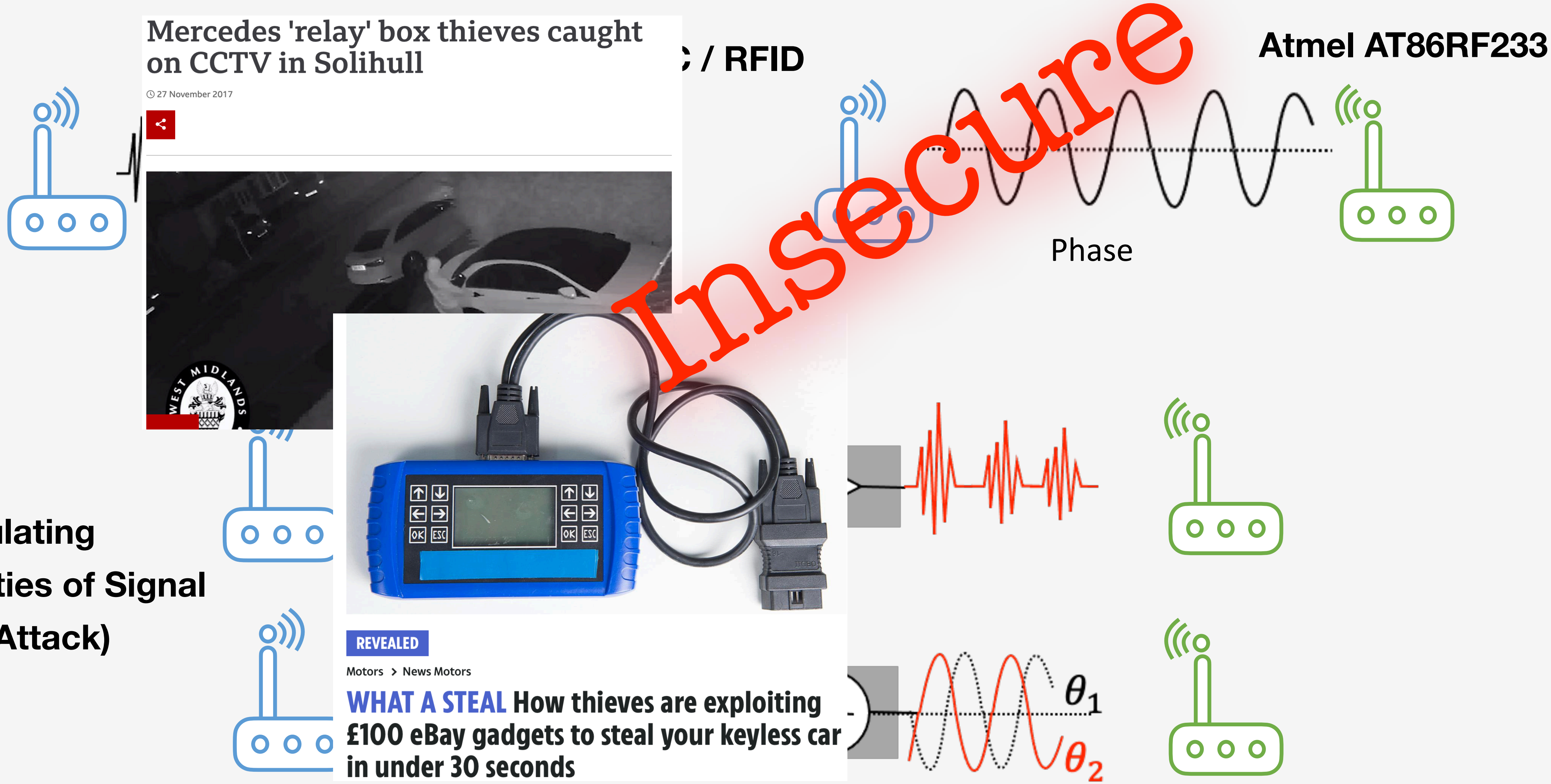




Health Hazards



Ranging Techniques



Mercedes 'relay' box thieves caught on CCTV in Solihull

27 November 2017

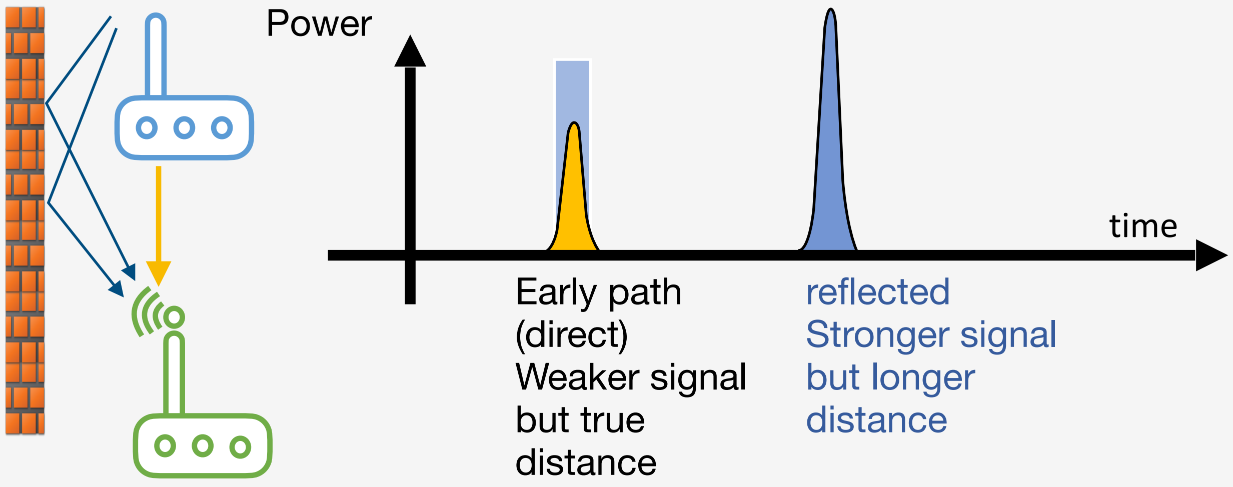
REVEALED

Motors > News Motors

WHAT A STEAL How thieves are exploiting £100 eBay gadgets to steal your keyless car in under 30 seconds

Manipulating Properties of Signal (Relay Attack)

Ranging Techniques (Time-of-Flight)



Early path (direct) Weaker signal but true distance

reflected Stronger signal but longer distance

CARCONNECTIVITY consortium®

FiRa The Power to Be Precise

Ultra Wideband (UWB)

IEEE 802.15 WPAN™ Task Group 4z Enhanced Impulse Radio

WiFi

IEEE 802.11mc (Std 802.11-2016)

IEEE 802.11az Next Generation Positioning (NGP)

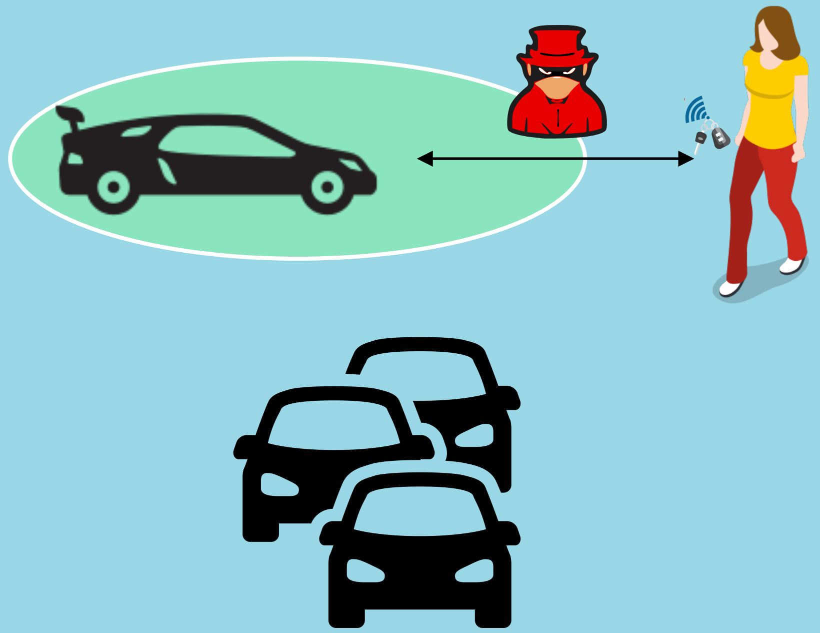
5G

3GPP A GLOBAL INITIATIVE

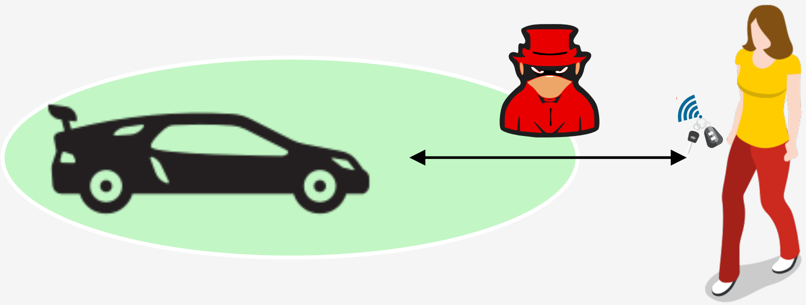
Security depends on logical and physical layer design

Proximity

Upper and lower bound on the measured distance



Proximity



Attacker Model: Mafia Fraud

Precise and **Performant ranging** under different channel conditions

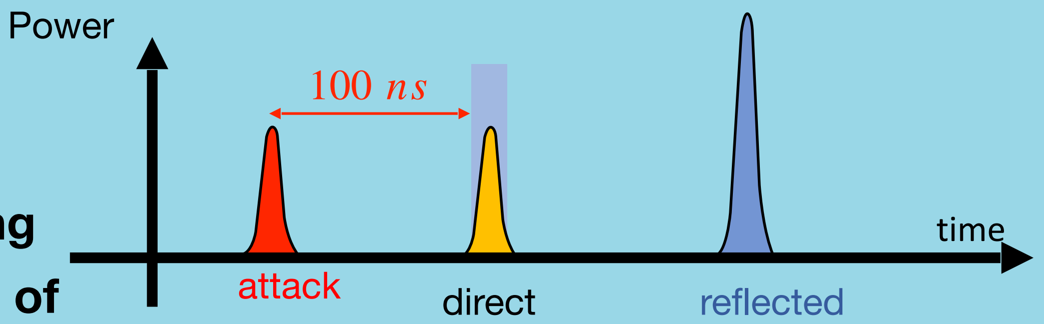
Secure against distance manipulation attacks.

(Reduction and Enlargement Attack)

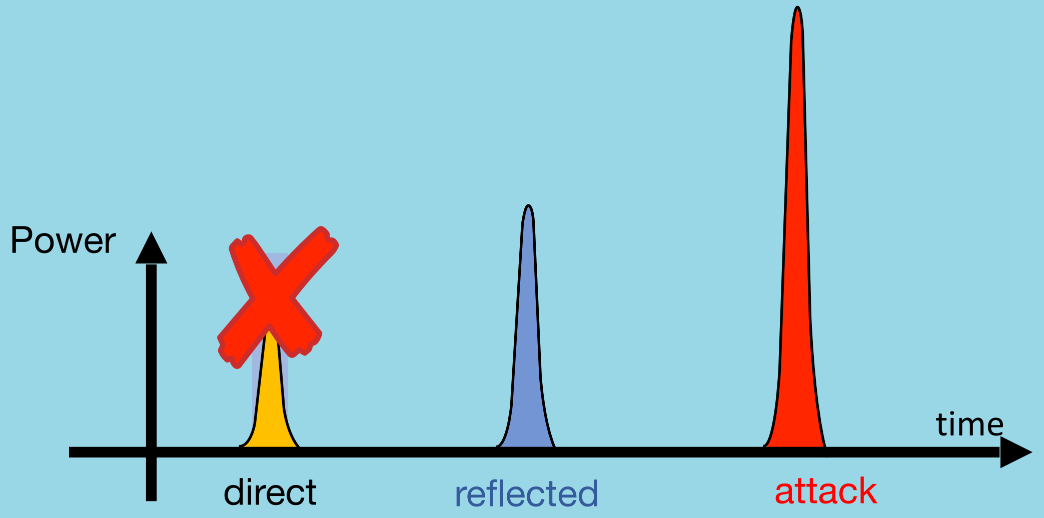
Distance Reduction

Distance Enlargement

Manipulating Arrival time of Signal

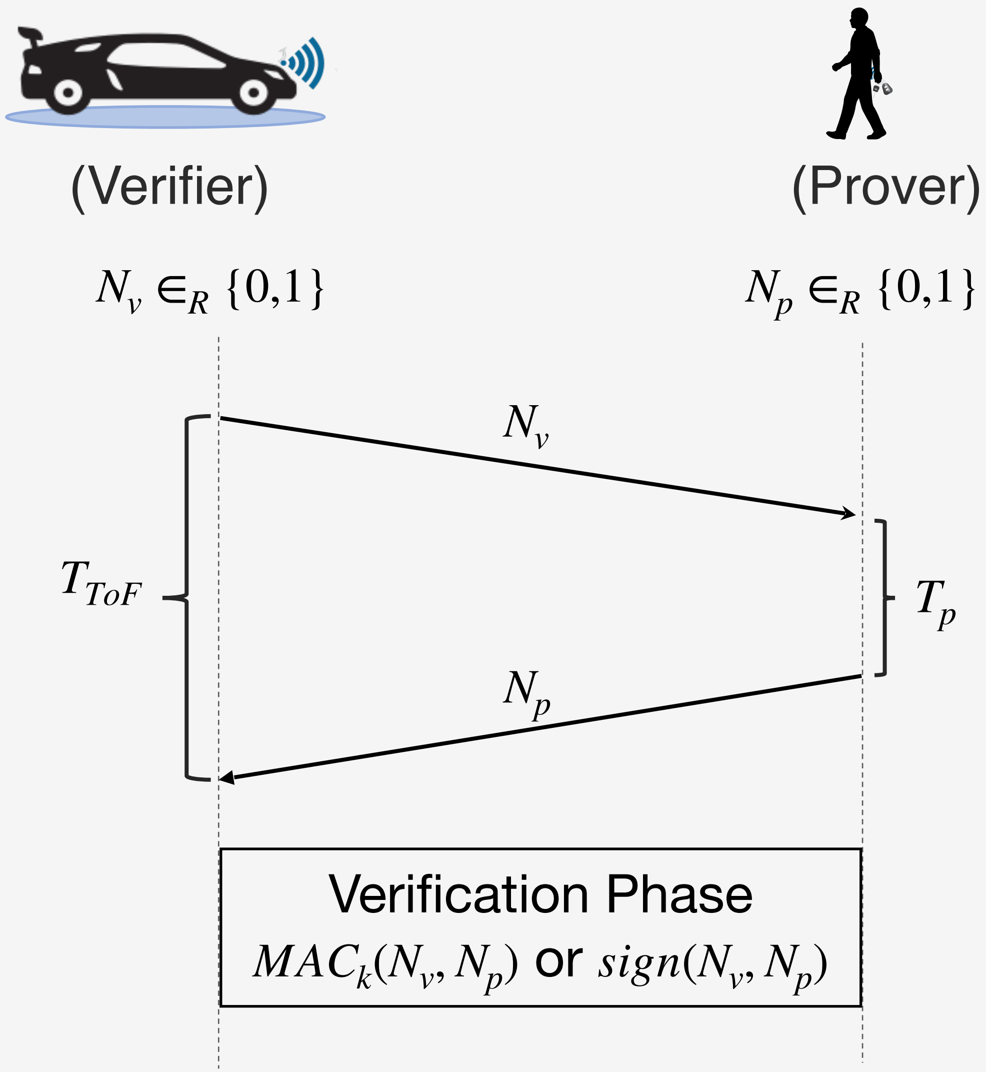


Distance Reduction
(Cicada, Early Detect Late Commit)



Distance Enlargement
(Annihilation and Replay)

Logical Layer - Distance Bounding



(Verifier)

(Prover)

$N_v \in_R \{0,1\}$

$N_p \in_R \{0,1\}$

N_v

T_{ToF}

T_p

N_p

Verification Phase

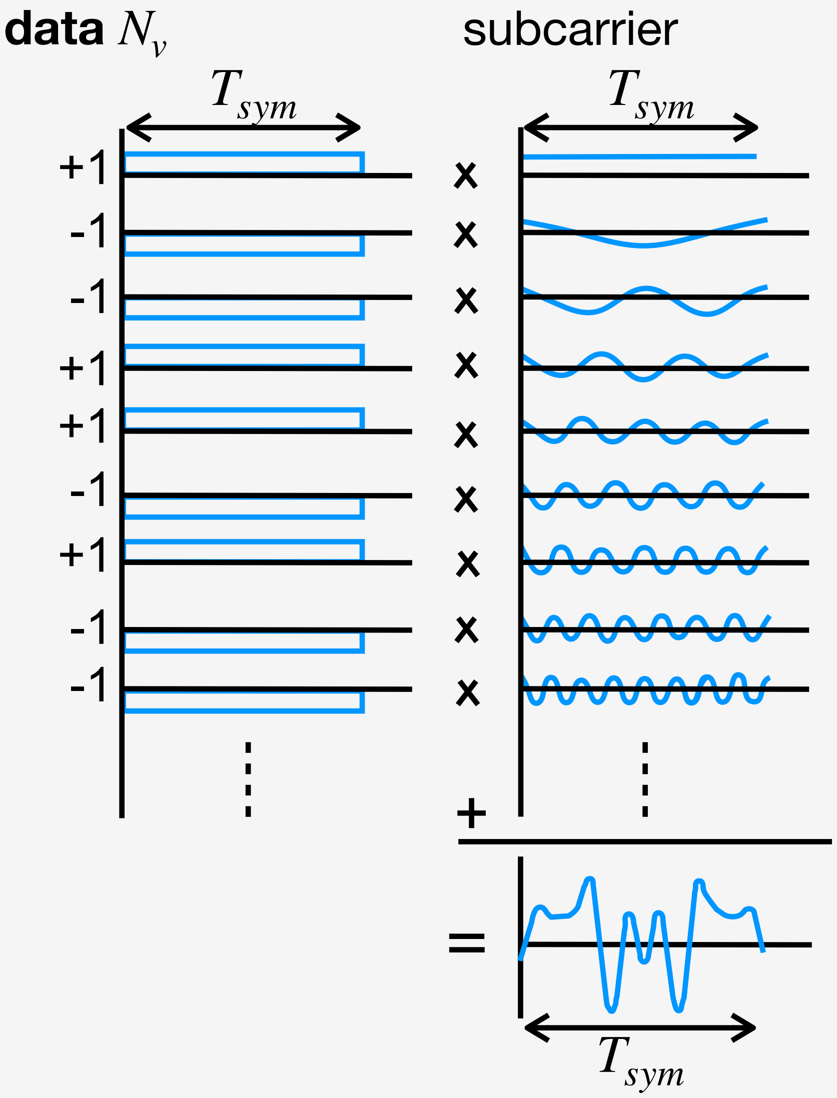
$MAC_k(N_v, N_p)$ or $sign(N_v, N_p)$

- Challenge-Response protocols

- Prevent distance reduction by relay attacks

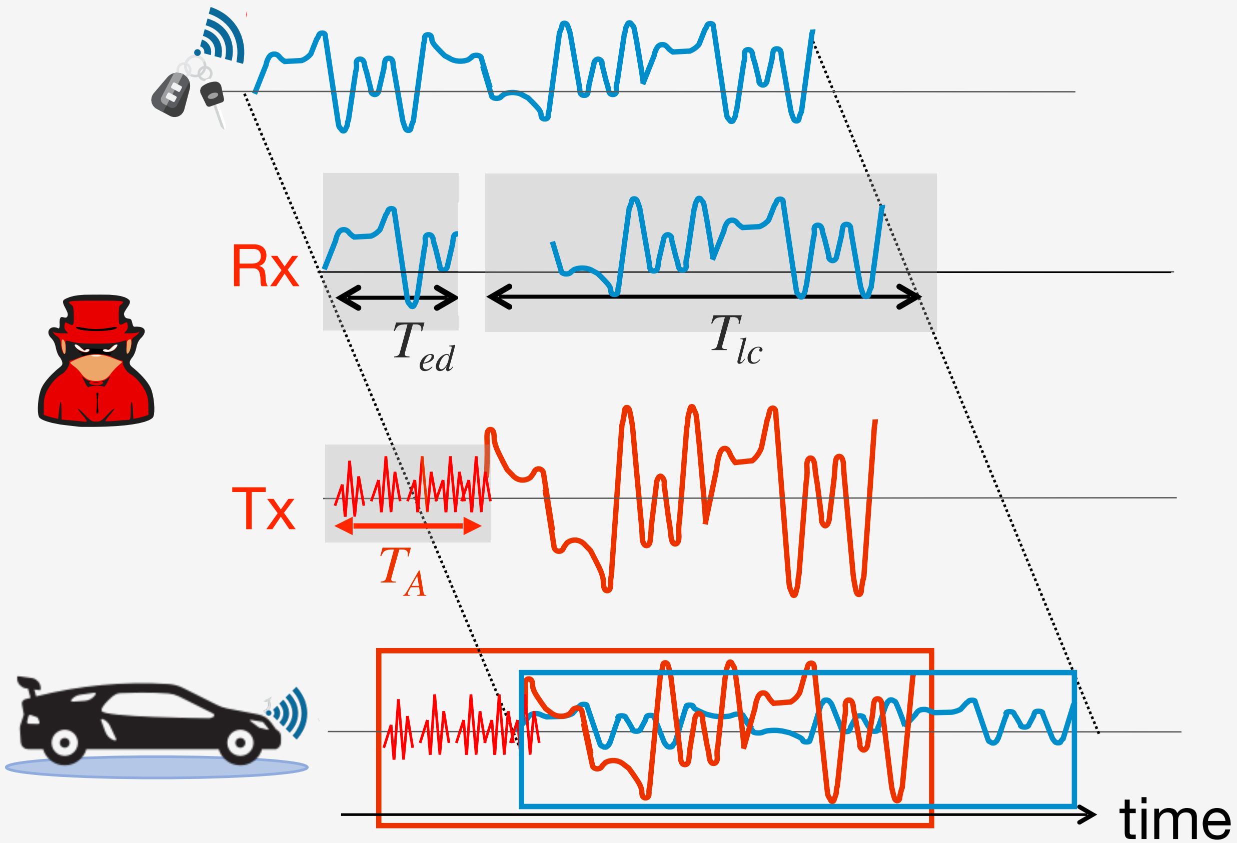
- Probability of distance reduction depend on the attacker’s ability of predict (N_v, N_p)

Logical to Physical Layer



- Orthogonal frequency-division multiplexing (OFDM)
- Used in 5G and WiFi

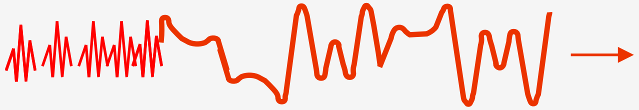
Distance Reduction Attack (ED/LC)



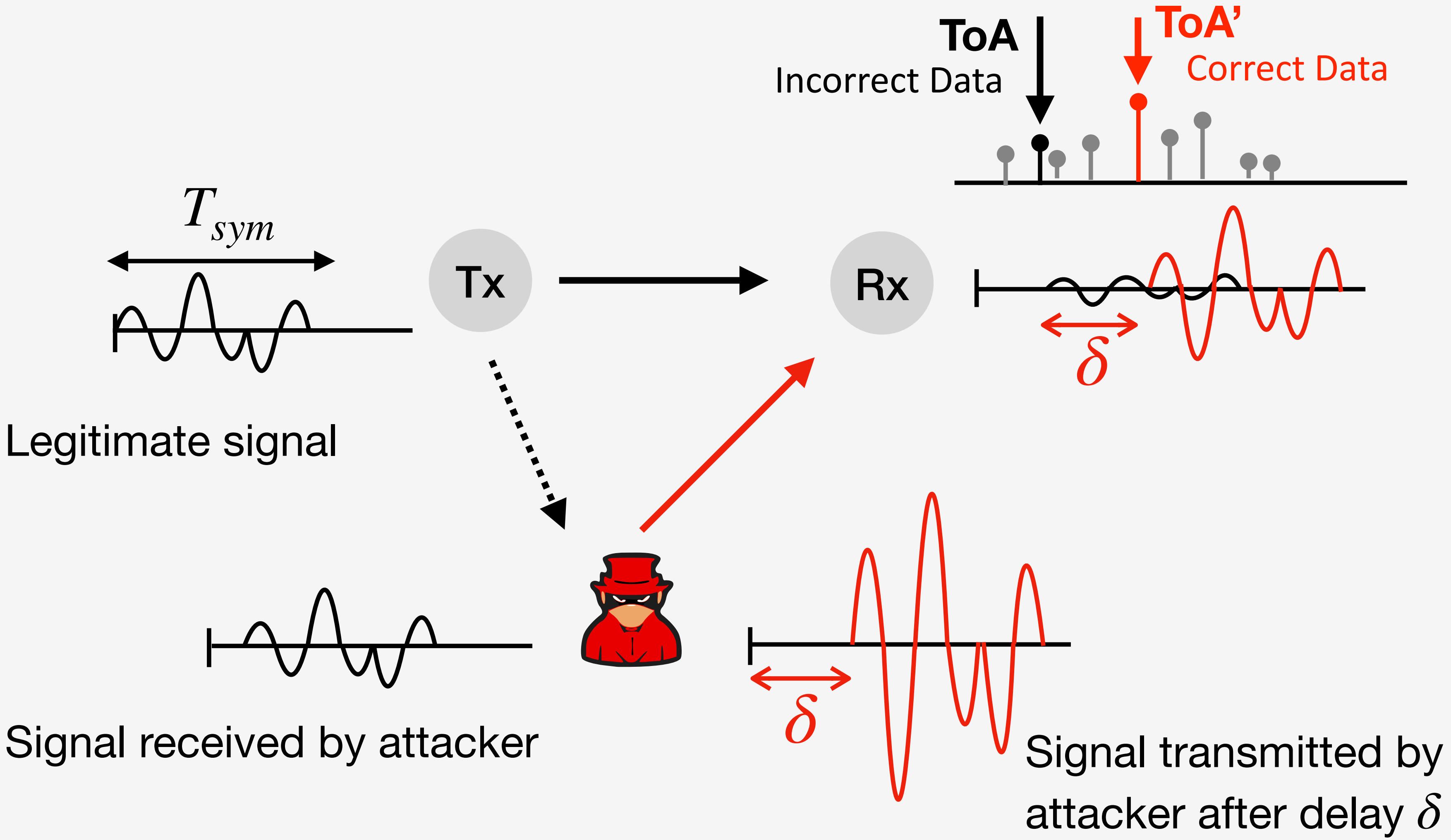
Early-detect/late-commit (ED/LC) Attack

Steps to insert earlier path

- Send noise in time T_A
- Learn shape of the symbol in time T_{ed}
- Commit correct symbol in time T_{lc}



Distance Enlargement Attack (Overshadowing)

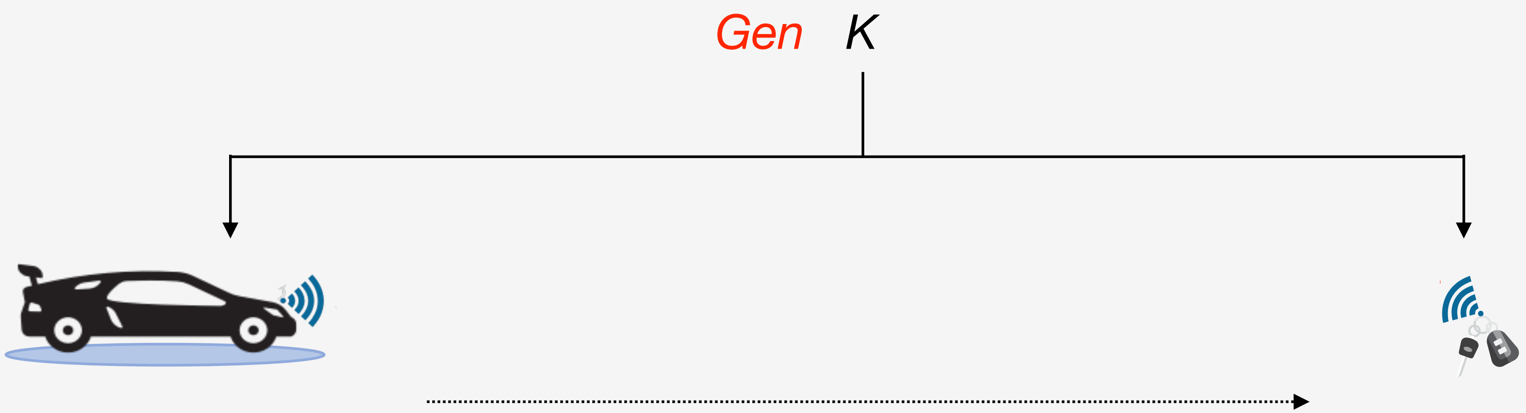


Legitimate signal

Signal received by attacker

Signal transmitted by attacker after delay δ

Message Time of Arrival Codes (MTACs)



Gen K

Mtac

$c \;\; => c'$

Vrfy

$N_v \in \{0,1\}^N$

$c \leftarrow MTAC_K(N_v)$

$c = [c_1, c_2, \ldots, c_n]$

$b := Vrfy(N_v, c')$

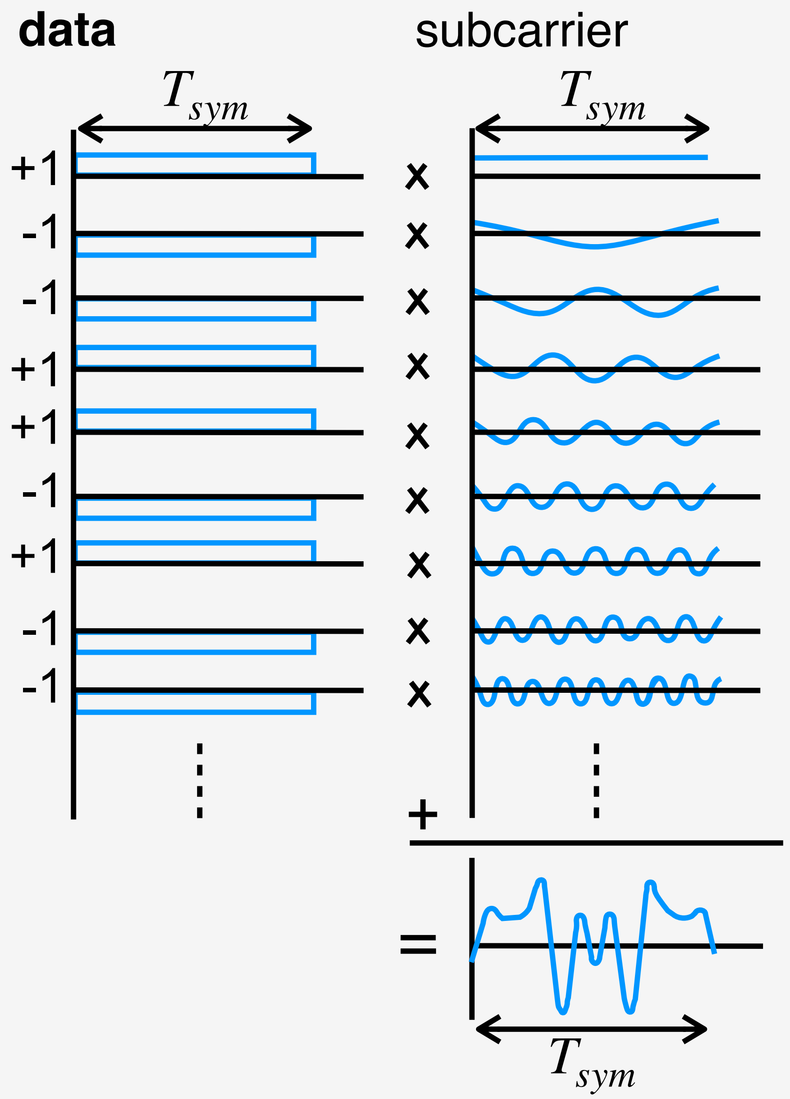
Use c' for ToF estimation when $b = 1$

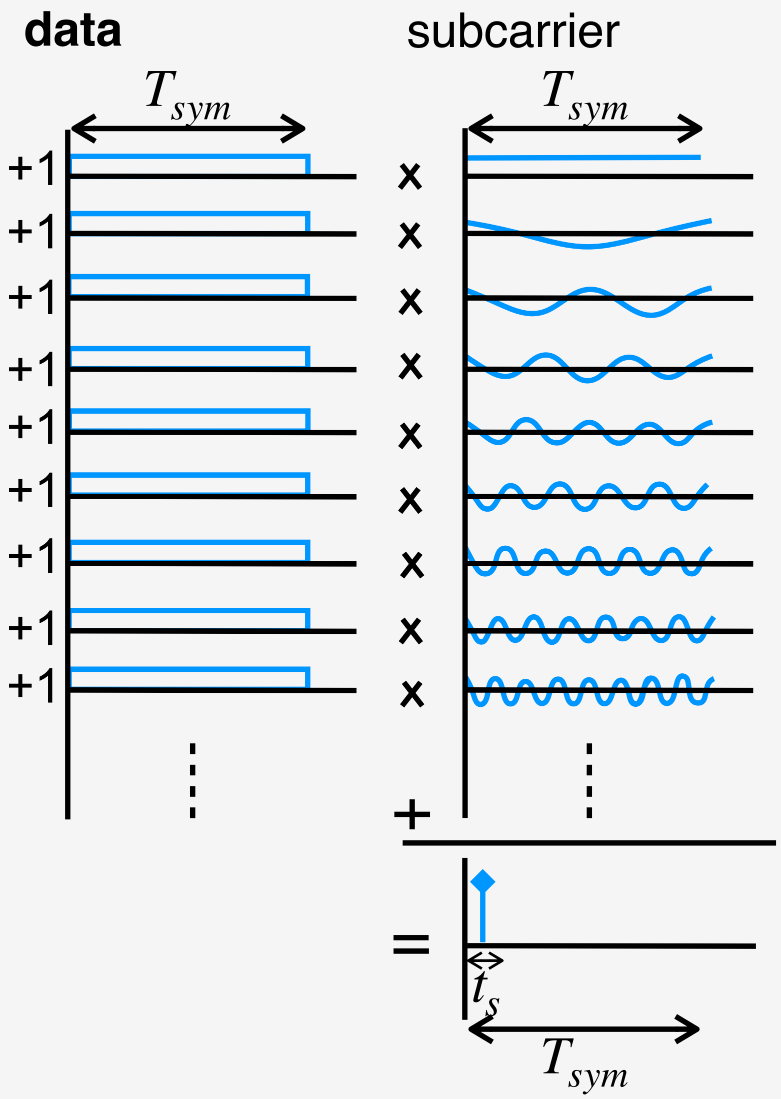
Mtac — Encode message m to a sequence c

Vrfy — Check integrity of c' at physical and logical layer for ToF measurement

Patrick Leu, Mridula Singh, Marc Roeschlin, Kenneth G. Paterson, Srdjan Capkun, **Message Time of Arrival Codes: A Fundamental Primitive for Secure Distance Measurement** in IEEE Symposium on Security and Privacy (S&P), 2020

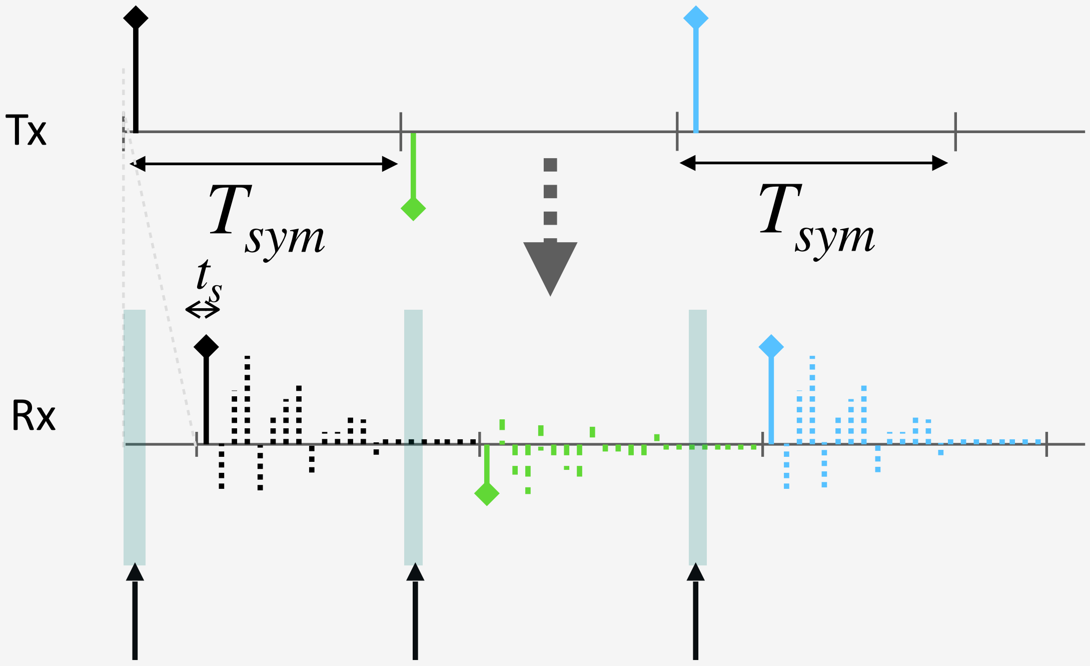
VRange : MTAC





Mridula Singh, Marc Roeschlin, Aanjhan Ranganathan, Srdjan Capkun, **V-Range: Enabling Secure Ranging in 5G Wireless Networks** in Network and Distributed System Security Symposium **(NDSS 2022)**

VRange : Vrfy



Search for the legitimate signal

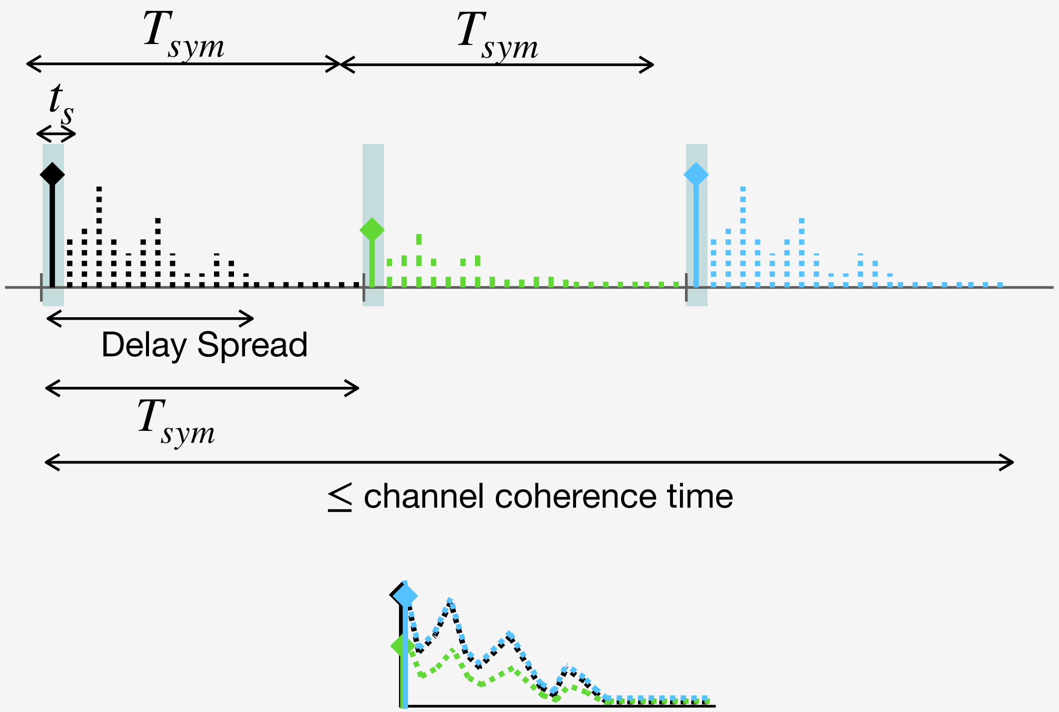
Samples collected in time t_s are sufficient to verify ToA (as single carrier symbols)

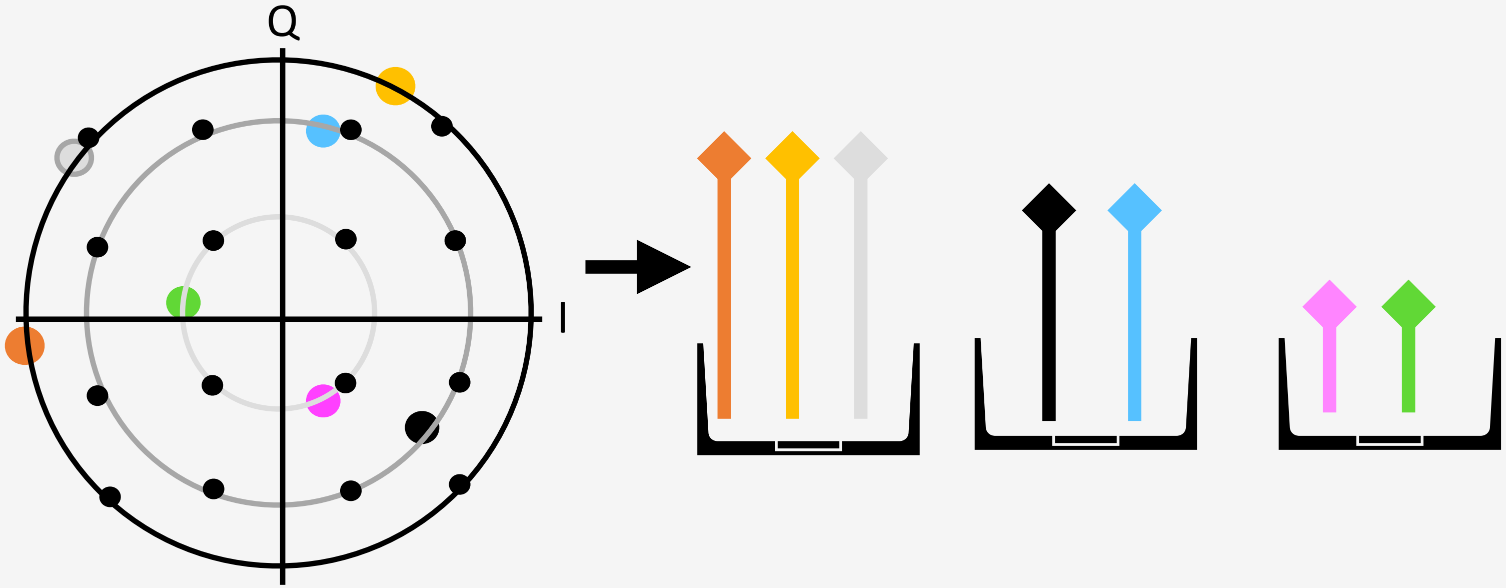
- High granularity leads to higher precision
- Can differentiate between legitimate signal, noise (multipath) and attack signal

Signal integrity check

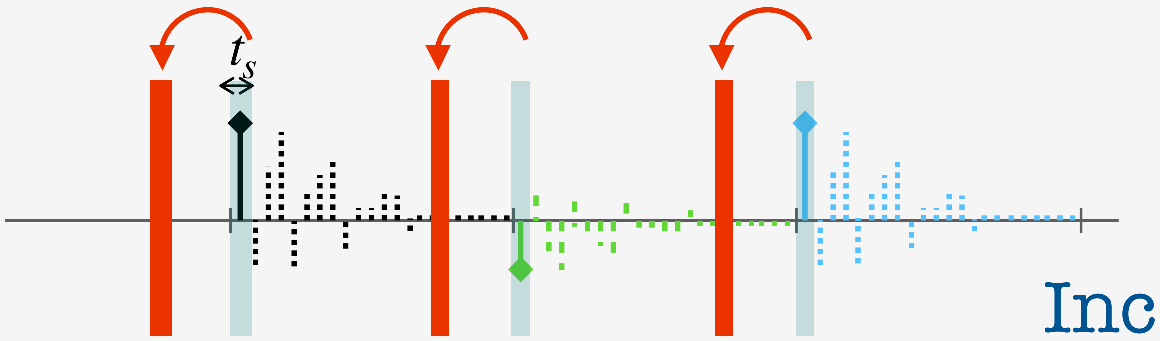
Signal transmitted with the same power are also received with same power

— variance of their received power is less than threshold V_{noise}

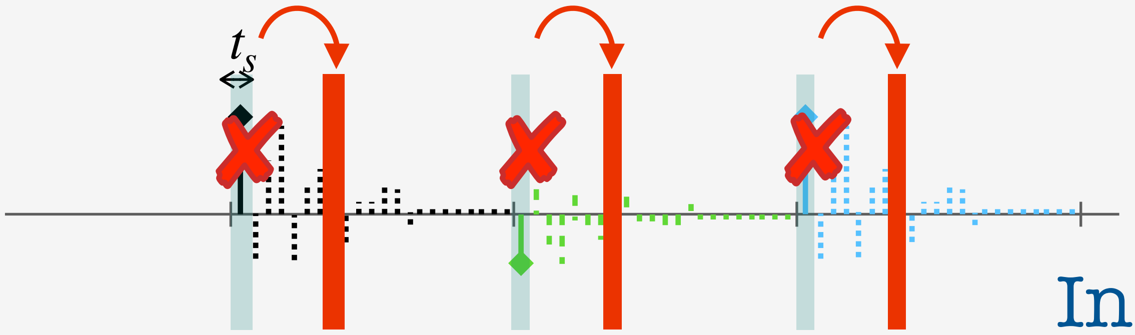




Distance Manipulation attacks on VRange



Incorrect data

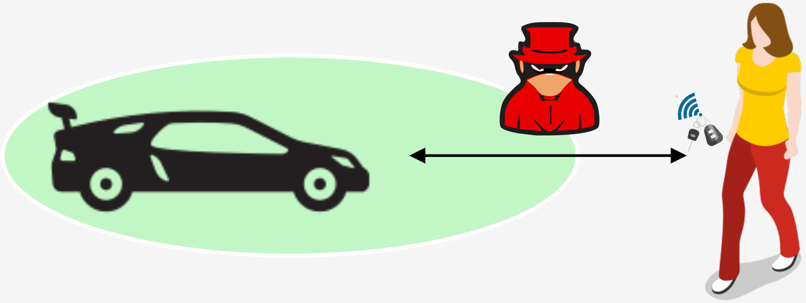


Increased Variance

Distance Reduction

Distance Enlargement

Proximity



- Upper and Lower Bound on the measured distance

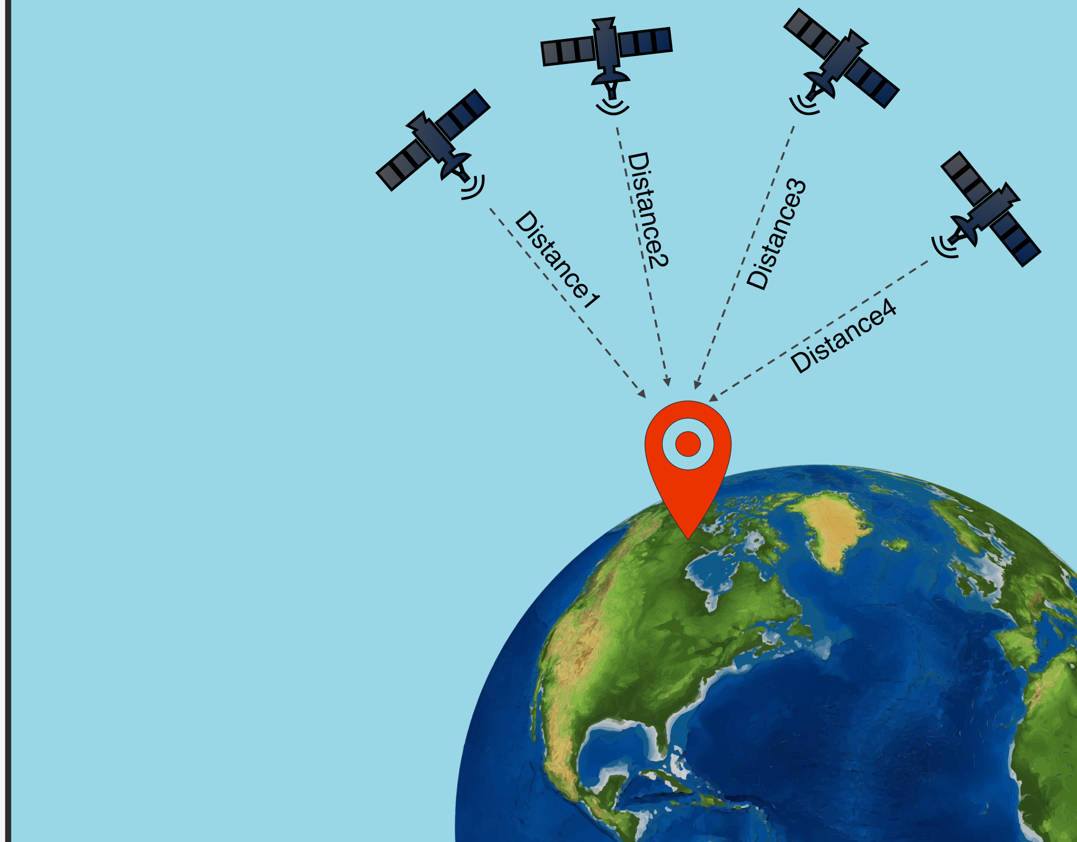
- Attacker Model: Mafia Fraud

- Distance Bounding at logical layer
- MTAC at the physical layer
- Integrity checks at the receiver

(e.g., VRange, UWB-PR,UWB-ED)

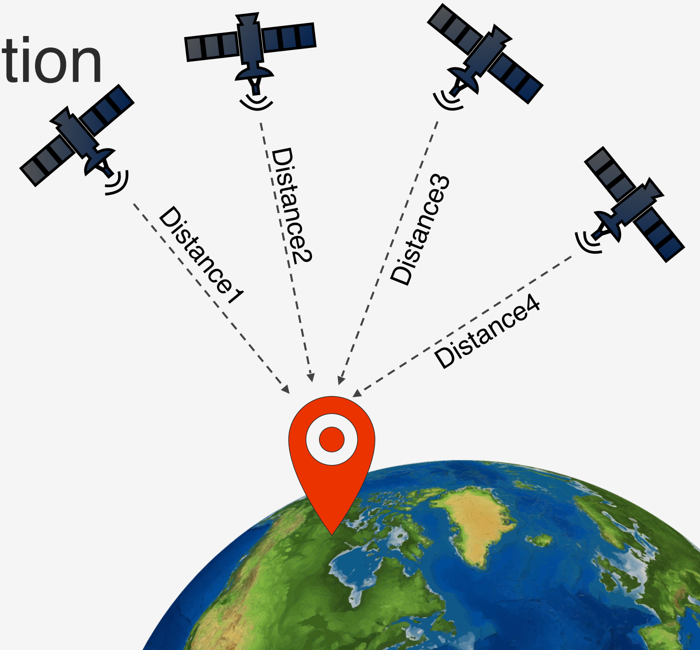
Positioning

Localization, Navigation and Tracking

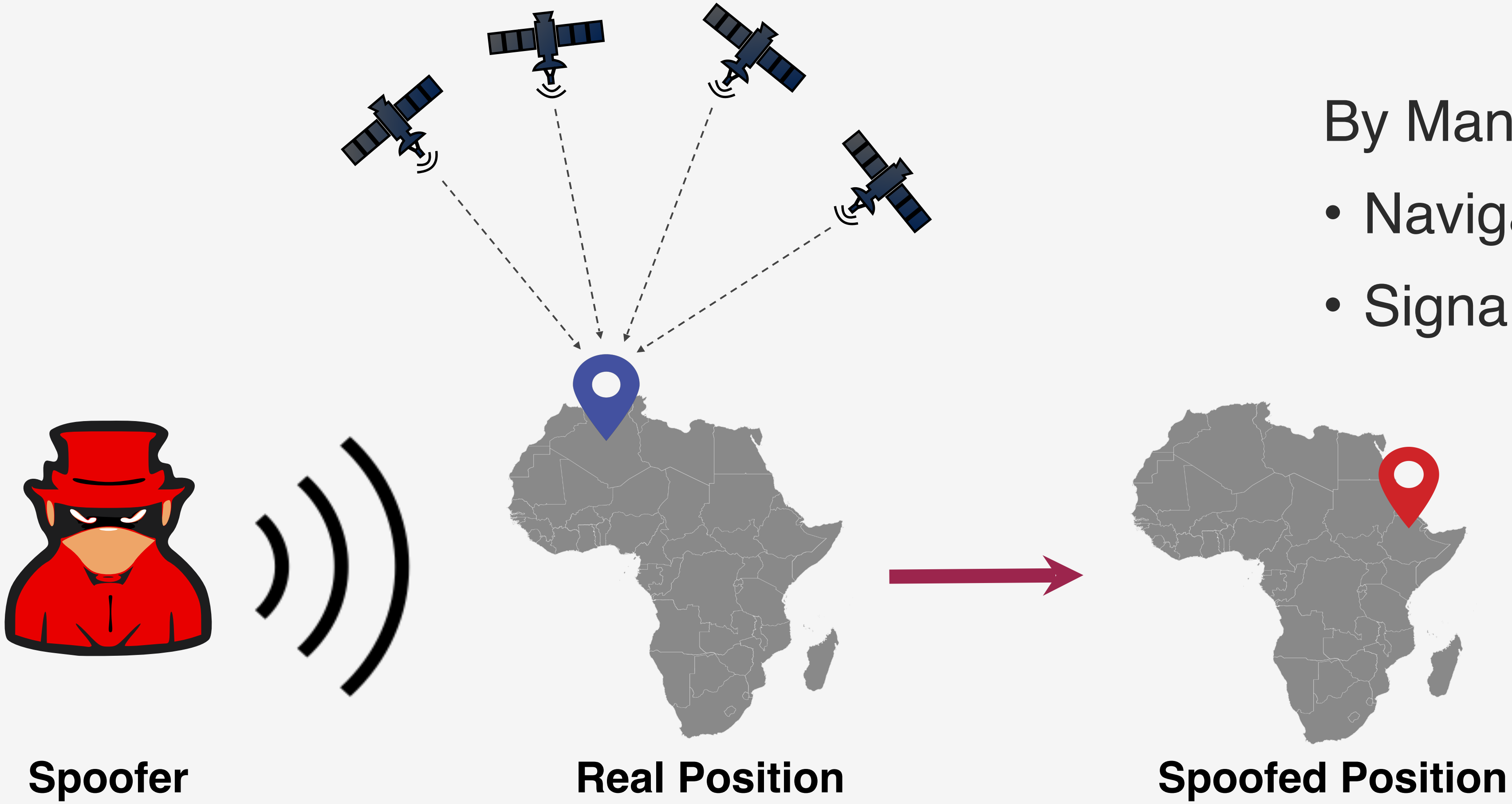


GNSS Positioning

- The de-facto outdoor localization systems for navigation and tracking.
- Each satellite transmits navigation messages containing its location and precise time of transmission
- Unique pseudorandom codes are used
- GPS receiver measures each navigation message’s arrival time and estimates its distance to the satellite.
- Receiver’s position and time is calculated using trilateration



GNSS Spoofing

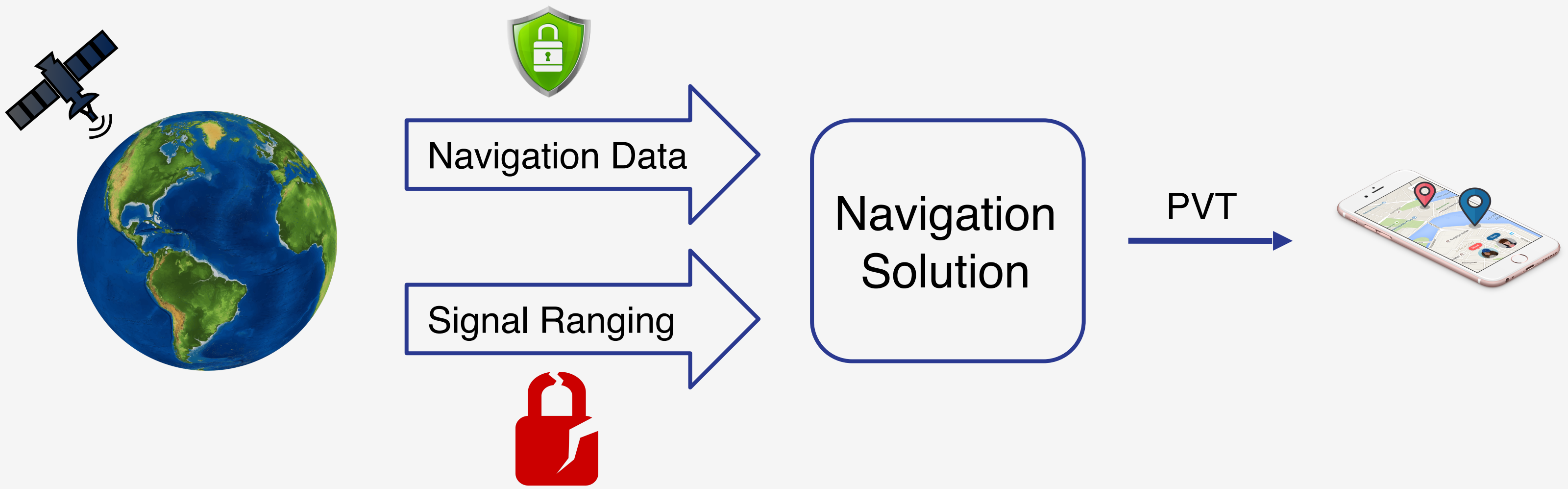


By Manipulating

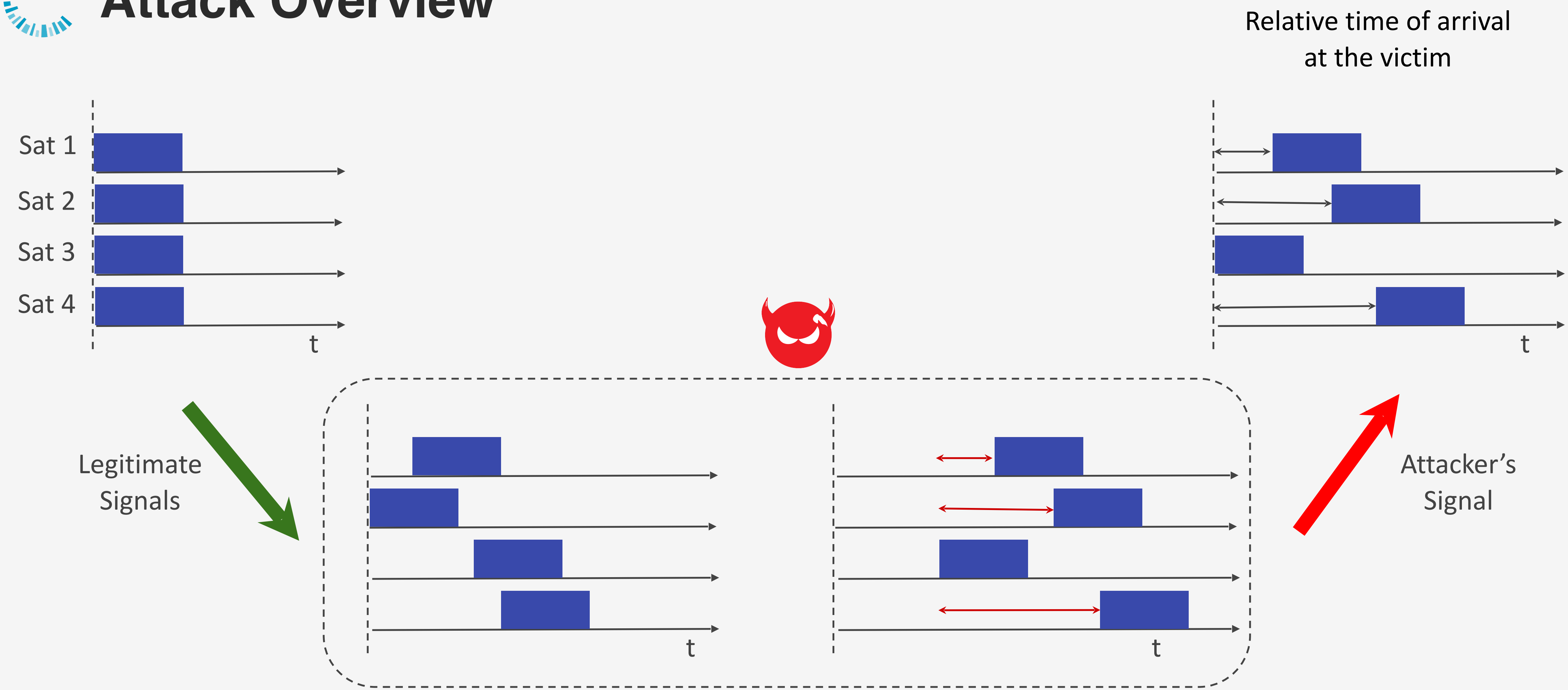
- Navigation Data
- Signal Arrival Time

Navigation Message Authentication

GALILEO: Open Service Navigation Message Authentication (OSNMA)



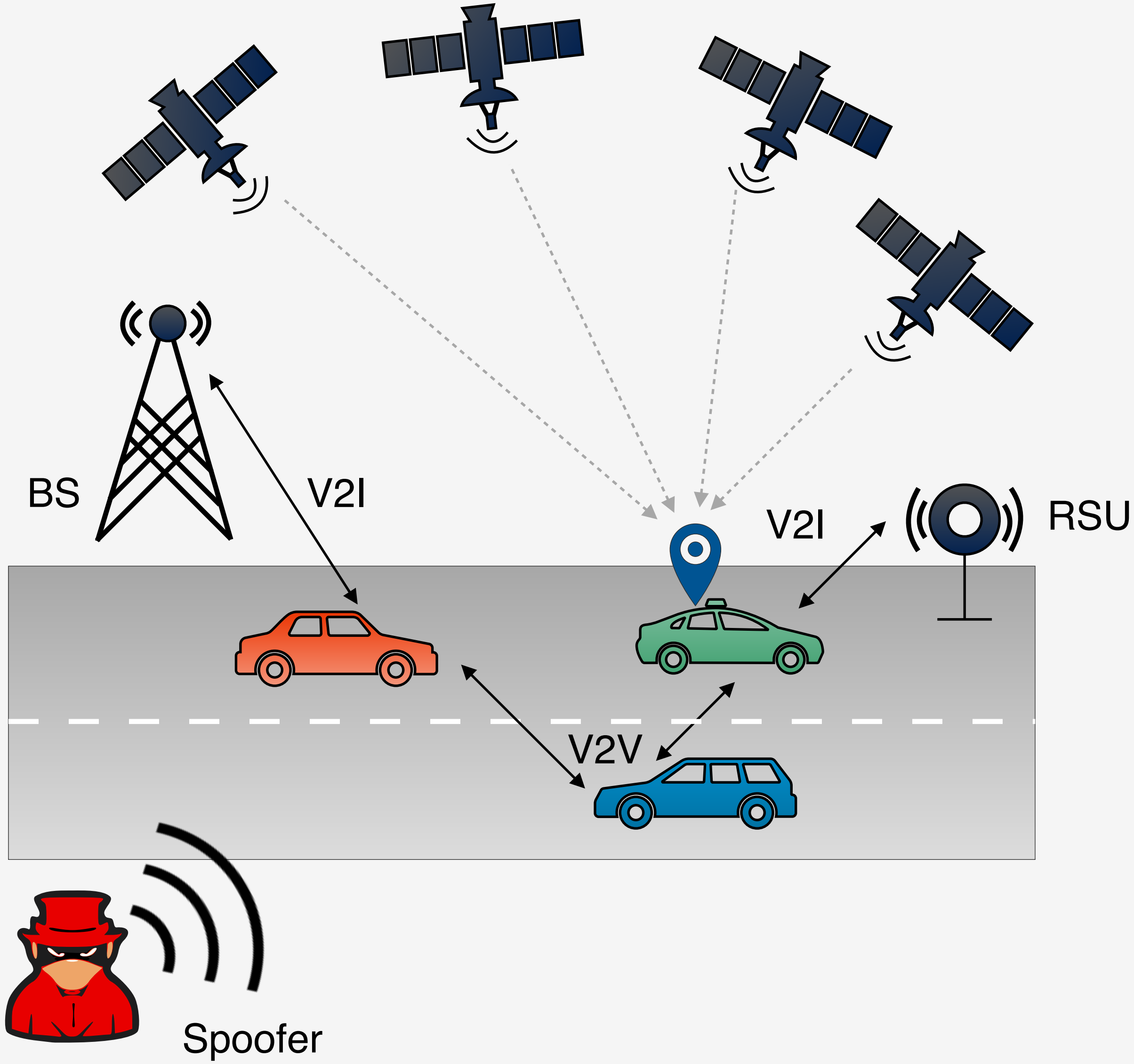
Attack Overview



Manipulating **common reception time** estimation at the GNSS receivers

Maryam Motallebighomi, Harshad Sathaye, Mridula Singh, and Aanjhan Ranganathan, **Location-independent GNSS Relay Attacks: A Lazy Attacker's Guide to Bypassing Navigation Message Authentication** in WiSec'23 (to appear)

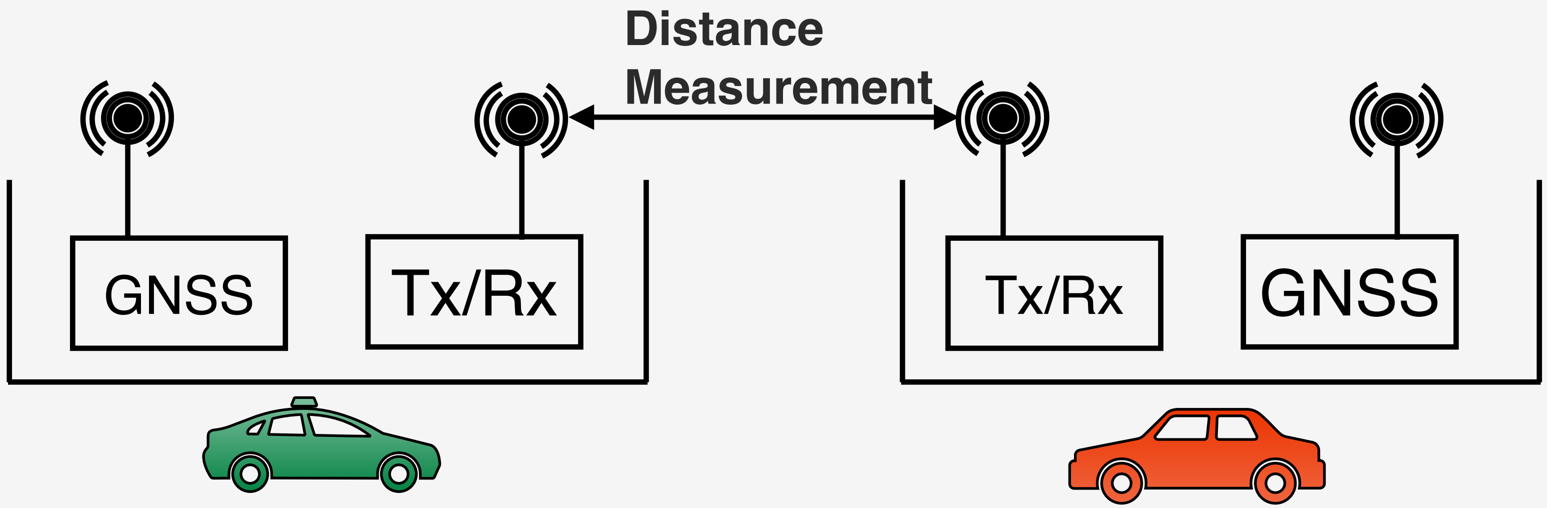
Distance Bounding for Position Verification



Can we use proximity of users to detect GNSS spoofing?

- Unique and dynamic nature of the road traffic

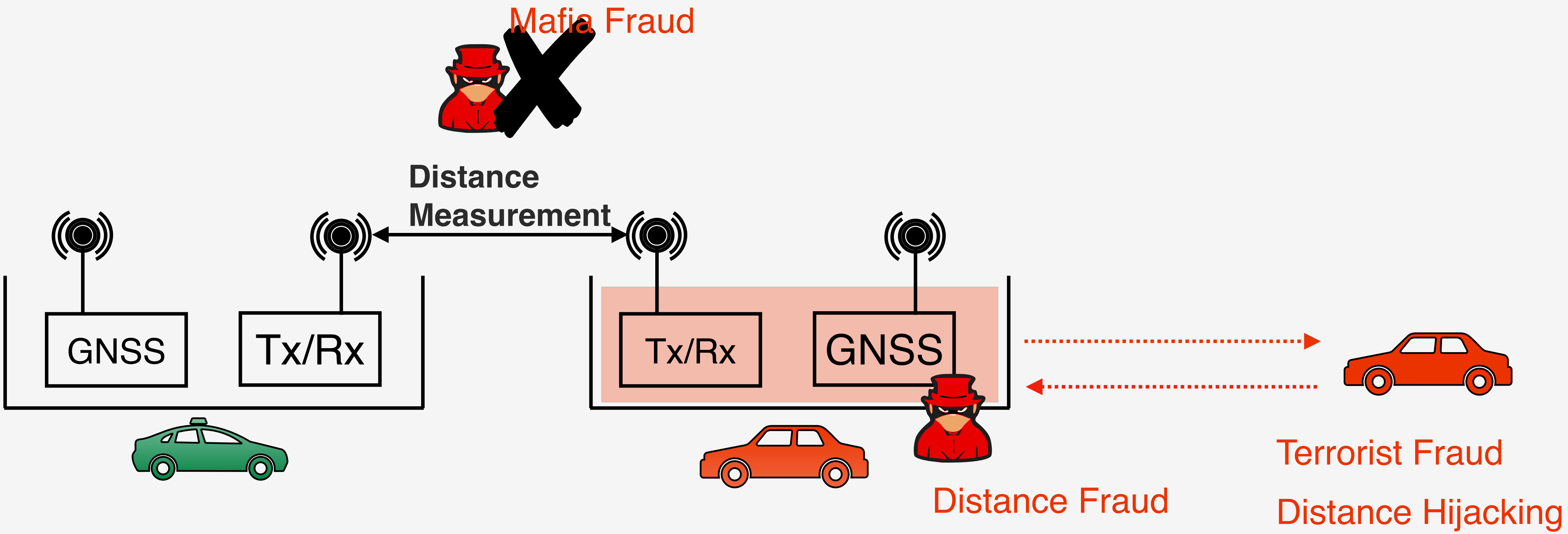
Basic Idea



Users share GNSS coordinates and perform Distance Measurement

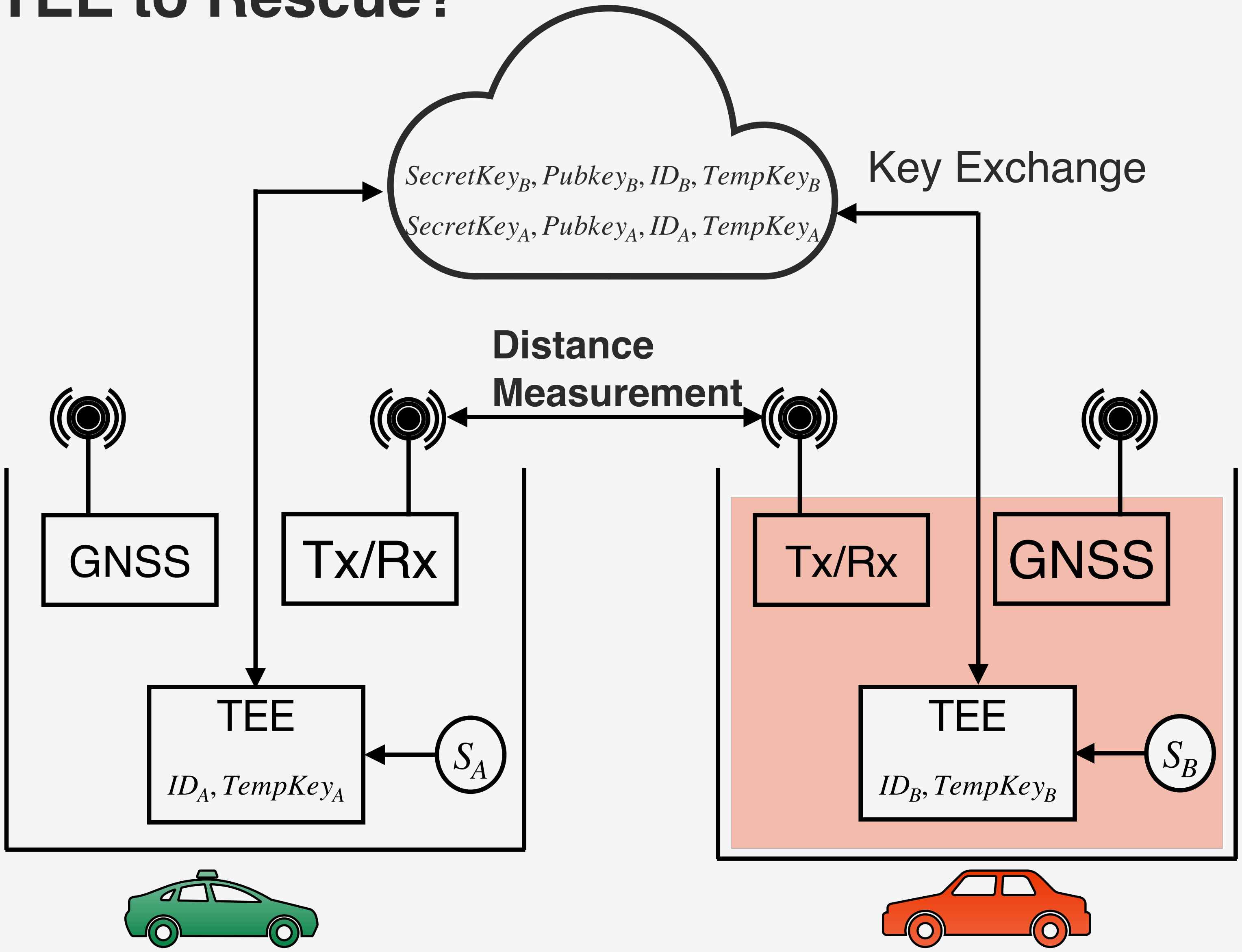
Compare GNSS coordinates and ToF estimate to validate their position information

Extended Attacker Model



Compare GNSS coordinates and ToF estimate

TEE to Rescue?



Deter users from colluding

Distance Fraud is still possible

Thank You