A Location Validation Technique to Mitigate GPS Spoofing Attacks in IEEE 802.11p based Fleet Operator's Network of Electric Vehicles

Ankita Samaddar (Vanderbilt University, USA)

Arvind Easwaran (Nanyang Technological University, Singapore)

Contents

Vehicle Rebalancing Application

A-to-B electric car-rental business model provides car rental services to customers, e.g., rent a car at a station, drop a car at any station (not necessarily the same pick-up station).

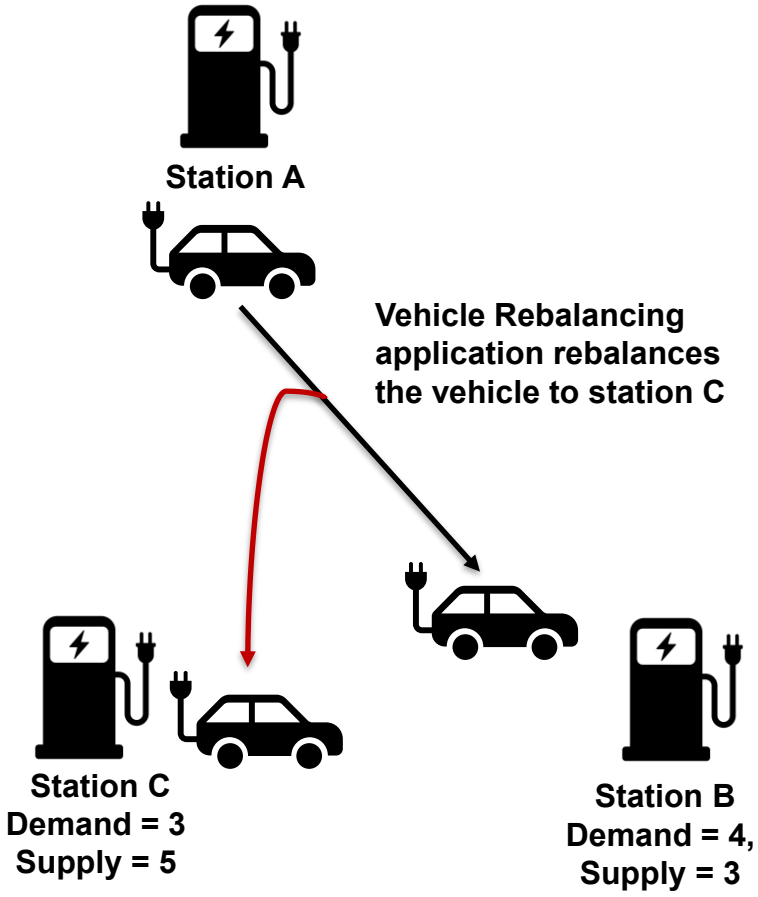
Drawbacks: A large number of customers remain unserviced due to disparity in the vehicle demand vs vehicle supply at different charging stations.

To overcome the imbalance between vehicle demand vs vehicle supply, *vehicle rebalancing* application has been adopted by car rental service providers.

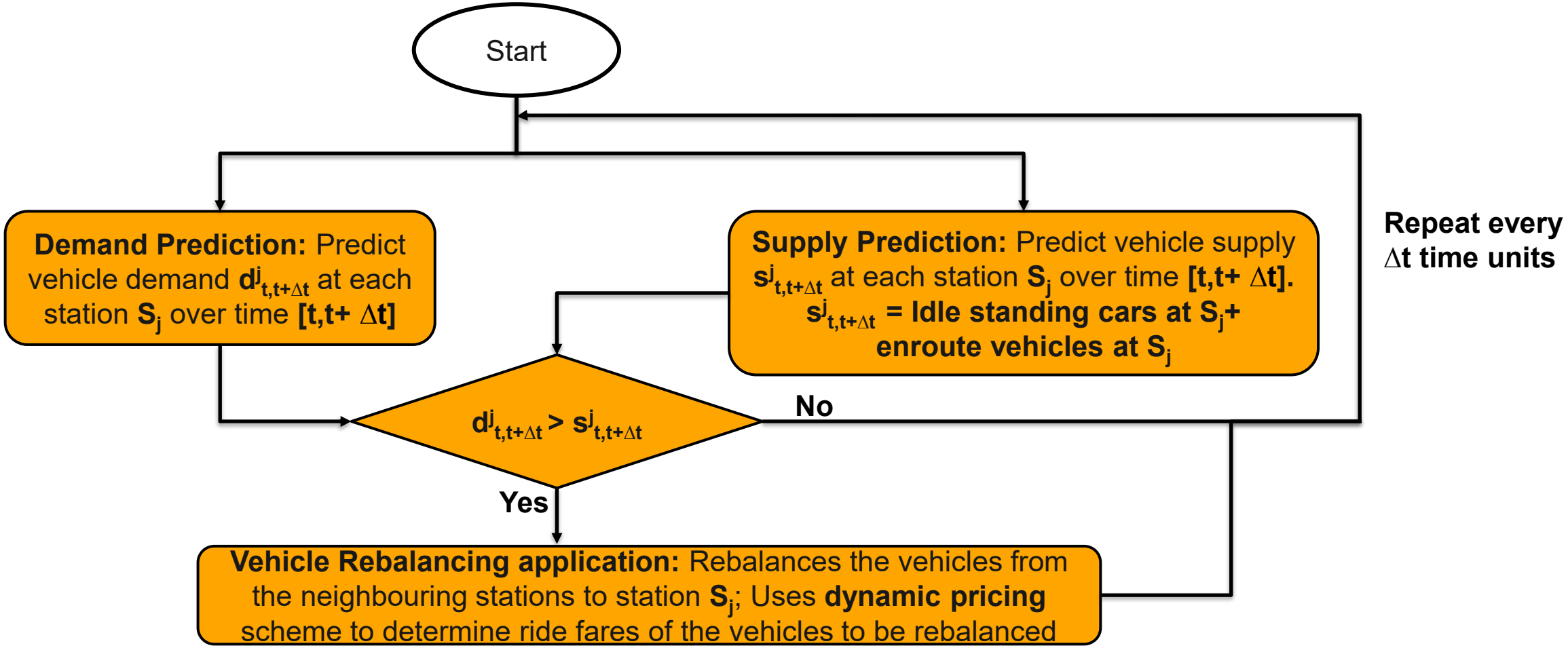
Vehicle Rebalancing application predicts the future demands of the vehicles at each charging station and redistributes the vehicles to the stations with higher demand so that

- The waiting time of the customers is reduced
- The fleet utilization is maximized

Due to absence of dedicated drivers in car-rental setting, there is dynamic pricing scheme associated with the rebalancing decisions that dynamically generates ride fares for the customers to increase the fleet utilization.

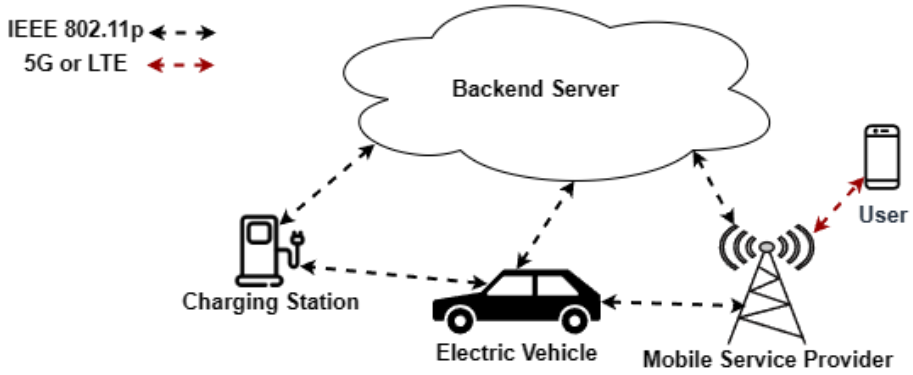


Flow Chart of Vehicle Rebalancing Application



IEEE 802.11p or Wireless Access in Vehicular Environment (WAVE)

- Operates at **5.9 GHz**
- Uses **carrier sense multiple access (CSMA)** based communication
- Bandwidth is sub-divided into **Control Channel** (CCH) and **Service Channel** (SCH)
- A set of vehicles forms a **WAVE Basic Service Set (WBSS)** with a unique ID. The backend server periodically sends a **WAVE Service Advertisement (WSA)** packet with SCH access pattern and synchronization messages on the CCH
- Vehicles within a specific WBSS contend among themselves to send data using CSMA based on SCH access pattern.
- Any vehicle which has the WBSS ID can join the WBSS without any authentication at any point in time.

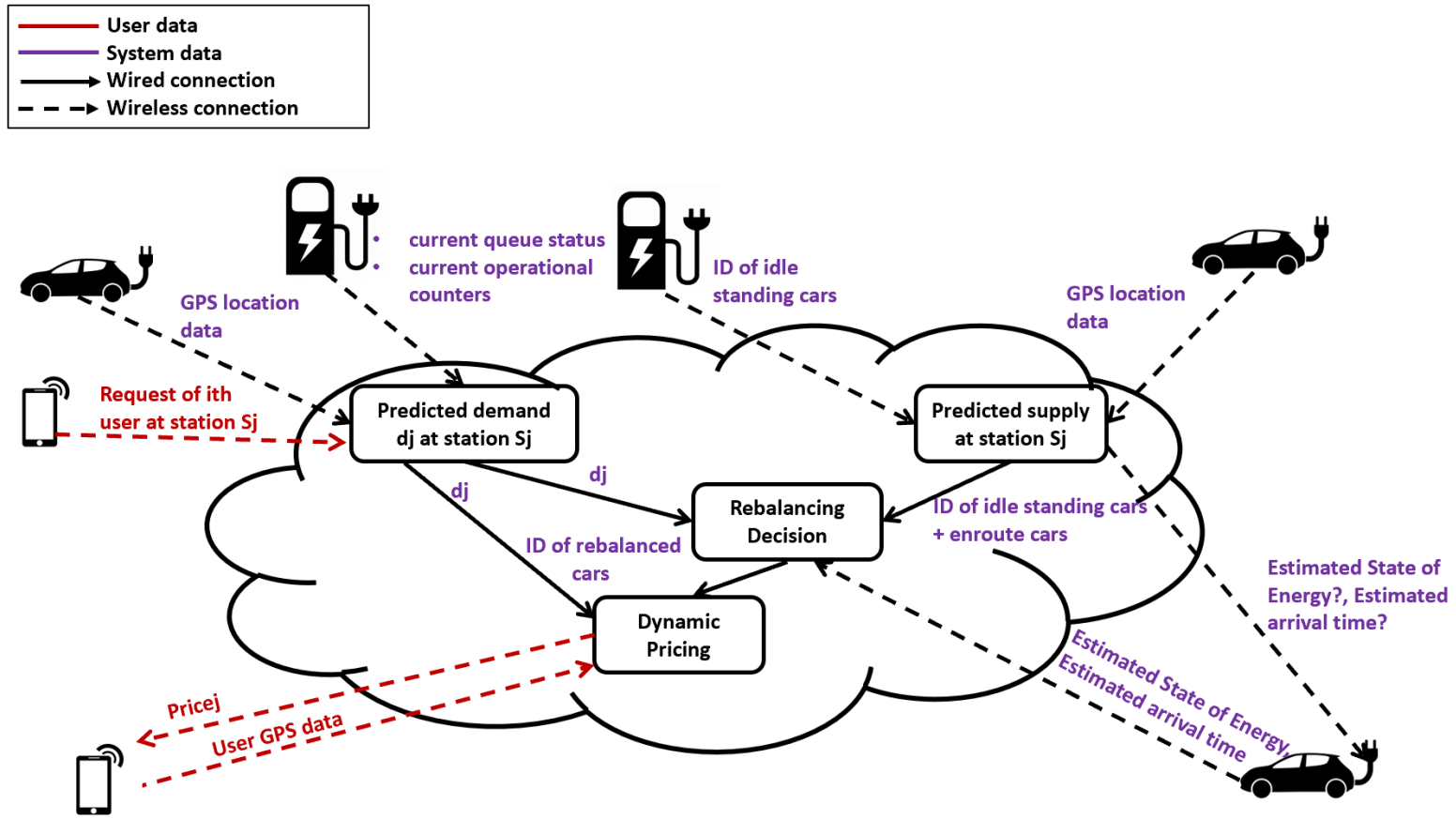


Data transmissions among different components in a fleet

Motivation

Predicted Supply at Station S_j uses ***GPS location data*** of vehicles

Spoofing of GPS location data leads to wrong supply prediction at S_j resulting in wrong rebalancing decision



Data Flow Diagram of Vehicle Rebalancing Application

Motivation

GPS location data is transmitted between the vehicle and the backend server *periodically* using *IEEE 802.11p*.

GPS Spoofing Attack

↓

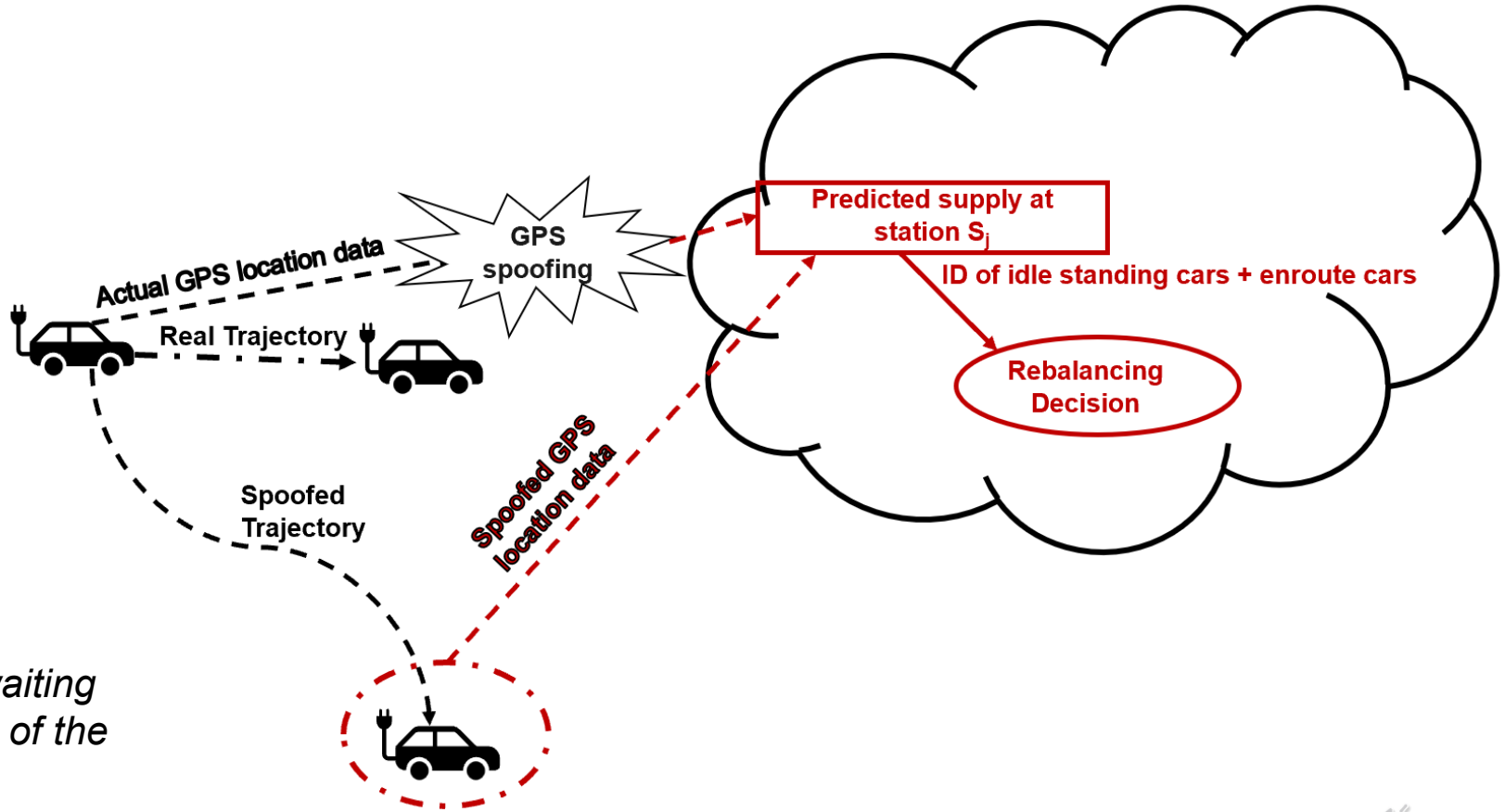
Impacts **Predicted Supply** (Idle standing cars + enroute cars) at $\mathbf{S_j}$

↓

Impacts **Vehicle Rebalancing Decision**

↓

Leads to *unmet demands, long waiting time of the customers and misuse of the rebalancing application*



Related Works

Literature	Description	Shortcoming
[1], [2]	Detects spoofing attack on GNSS data when received by the vehicle from satellite	Not applicable to attacks when GPS location data is transmitted between the vehicle and the backend server using IEEE 802.11p
[3]	Countermeasure at the physical layer by adopting in-line RF device connecting a GPS antenna and a legacy civil GPS receiver to mitigate spoofing attack when GNSS signal is received	
[4]	Multiple attack surfaces leading to vulnerabilities in automotive systems	Does not provide solution to any specific attack
[5]	Detects GPS spoofing attack using recurrent neural network by analysing the GNSS signals received from the satellite	Not applicable to attack on GPS location data transmission through IEEE 802.11p
[6]	Detects GPS spoofing attack in UAV swarm based on the distance between any two swarm members.	Attack detection technique is not applicable to fleet where each vehicle's position is independent of other vehicles in the fleet
[7]	Models origin-destination flows and destination choices using GPS data in truck movement model	No solution that shows how to estimate the position of the truck if the GPS data gets spoofed

Our countermeasure validates the current GPS location of a vehicle in a fleet based on its previous GPS location and the roadmap data to mitigate GPS spoofing attack in EVs.

System Overview

- Each vehicle in the fleet operator's network sends GPS location data to the backend server periodically using IEEE 802.11p to inform its position. The GPS location data packet consists of the following information

[Vehicle ID, Latitude, Longitude, Bearing Angle, Timestamp]

- The backend server maintains a table to store the position of each vehicle in the fleet at each timestamp

Vehicle ID	GPS Location data	Timestamp

- Vehicle Rebalancing application uses this data to predict the supply of vehicles at each station and decides which of the vehicles to rebalance

Overview of GPS Spoofing Attack

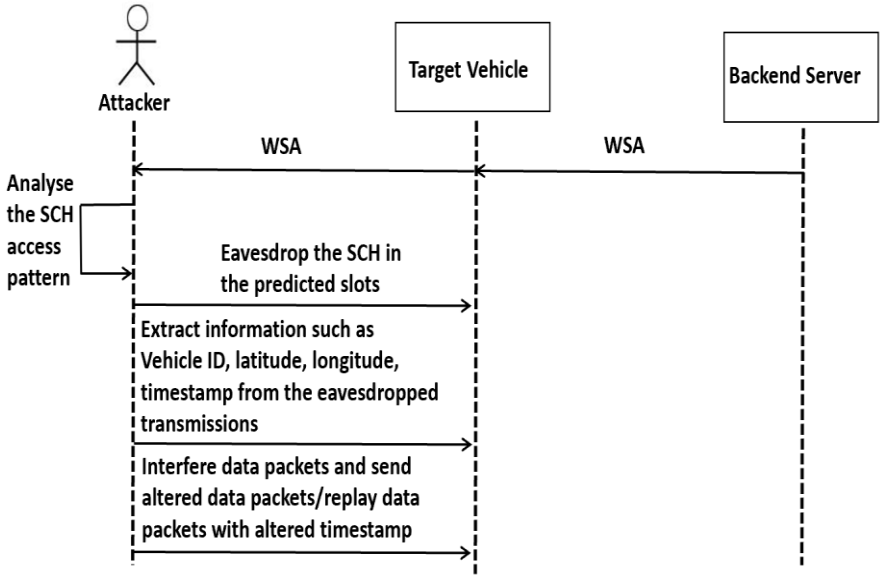
GPS Spoofing attack occurs in two phases:

Phase 1 : Detection of the time slots associated with the victim car:

- From the WSA, the attacker extracts the SCH access pattern of the WBSS.
- It then eavesdrops the SCH based on its access pattern to determine the time slots in which the target vehicle transmits GPS location data to the backend server.
- While eavesdropping it uses its timer to estimate the time interval between two successive GPS location data transmissions from the target vehicle to the backend server.

Phase 2 : GPS location data alteration:

- After predicting the transmission patterns of the GPS location data, the attacker can alter the content of the GPS location data (latitude, longitude) in the predicted transmissions. The attacker can even alter the timestamp information and resend a data packet at a later point in time.



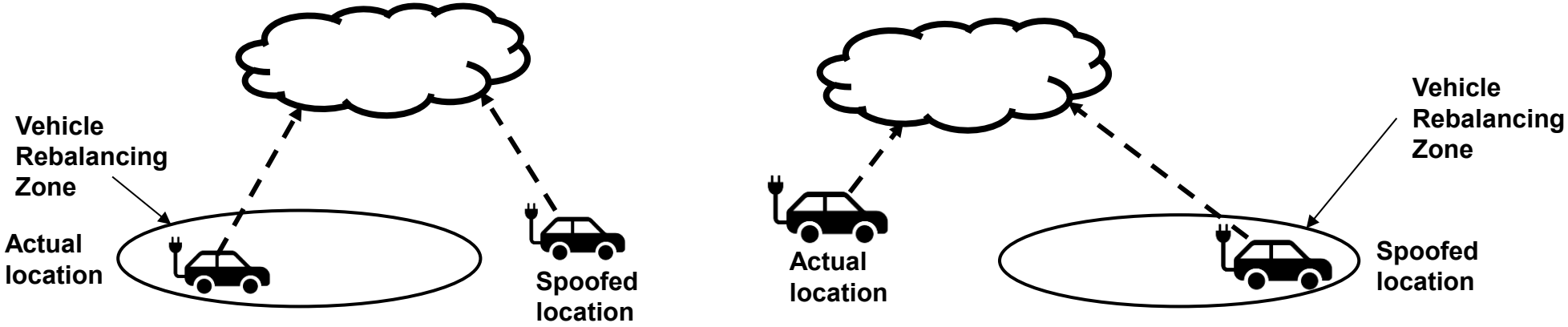
Sequence Diagram with the interactions in sequence to launch GPS Spoofing Attack

Overview of GPS Spoofing Attack

Attack Consequences

1. Impacts rebalancing decision. E.g., a victim vehicle may appear in the list of enroute vehicles although it is far away from the rebalancing station. Or, the victim vehicle may not get selected in the list of enroute vehicles though it is in the area of rebalancing station.

2. Wrong rebalancing decision leads to under utilization of the fleets, high waiting times of the customers and unmet demands.



Attack Illustration with an example

Content of GPS location data packet transmitted through SCH of IEEE 802.11p

<Vehicle ID : 10010, Lat : 1.302, Long : 88.24, Bearing Angle : 30, Timestamp : 09/05/2023:11:05:24

Actual Data Packet

After GPS spoofing attack, alteration of Longitude :

<Vehicle ID : 10010, Lat : 1.302, Long : 88.04, Bearing Angle : 30, Timestamp : 09/05/2023:11:05:24

Spoofed packet

Consequence : Based on the modified longitude data, this enroute vehicle may get selected in the list of enroute vehicles arriving at station S_j although it is far away from S_j. Or, it may not get selected in the list of enroute vehicles although it can reach the S_j and serve the demand. This leads to improper utilization of the fleet and results in unmet demands.

Proposed Countermeasure

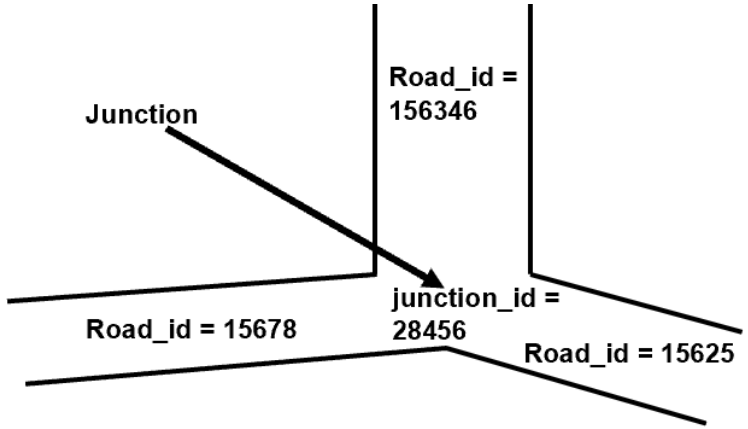
Our proposed countermeasure runs at the backend server and consists of

1. An **Offline Pre-processing** phase
2. An **Online Attack Detection** phase
3. An **Online Attack Prevention** phase that runs only if an attack is detected

In the backend server, we store the following information:

Vehicle :
V_i.id *: unique ID of the vehicle,* ***V_i.key*** *: Unique key associated with the vehicle*

Station *:*
S_i.id *: unique ID of the station,* ***S_i.loc*** *: GPS location of the station*



RoadMap :
We represent the roadmaps of a particular region/city as a graph ***G = {J, R},*** *where J denotes the set of junctions or vertices connecting two or more roads and R denotes the set of roads. Each road $r_i \in R$ is associated with a unique ID, length and a set of GPS co-ordinates along the road. Each junction $j_i \in J$ is associated with a unique ID and a GPS co-ordinate.*

Proposed Countermeasure : Offline Pre-Processing Phase

1. *For each vehicle V_i in the fleet*
   Initialize each vehicle and store in the backend server

2. *For each station S_i in the network*
   Initialize each station and store in the backend server

3. *For each junction j_i in the graph G.J*
   Assign unique id and location to each junction and store it in a list of junctions

4. *For each road r_i in the roadmap G.R*
   Store the unique road id, the length of the road, the maximum and minimum GPS coordinates on that road and the maximum allowable speed of the road
   Store the GPS coordinate data along each road r_i at 1 meter apart

Proposed Countermeasure : Online Attack Detection Phase

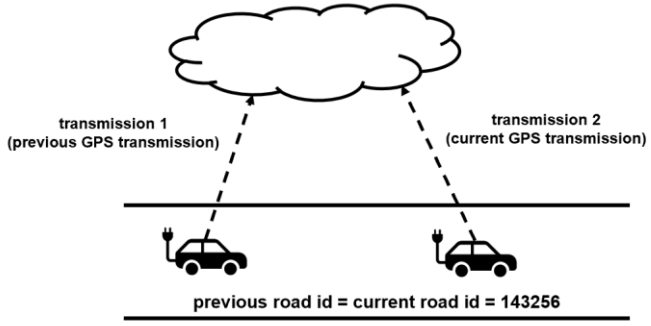
Uses an ***error function*** $E = \frac{d}{Max\_dist}$ to detect an attack.

where ***d*** is the distance covered by the vehicle between two successive GPS data transmissions following the roadmap, ***Max_dist*** is the maximum distance that a vehicle can cover in that duration

1. *For each received GPS location data packet*
   Extract the vehicle ID, current GPS location data, timestamp
   Calculate E to validate the current vehicle position based on its previous position following the roadmap data

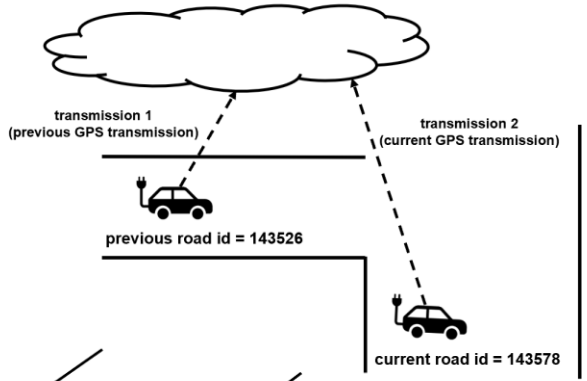
Four cases can occur based on the location of the vehicle and the roadmaps

Case 1: The current and previous locations of the vehicle are on the same road

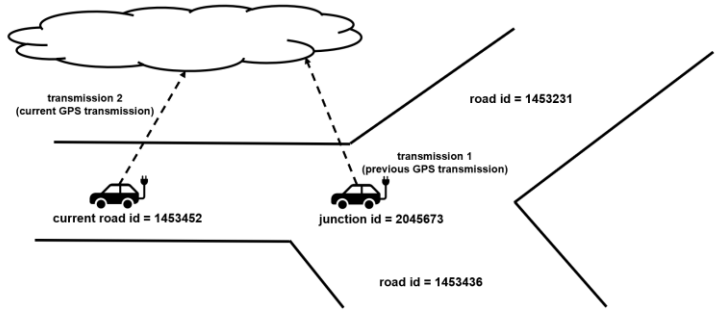


Countermeasure : Online Attack Detection Phase

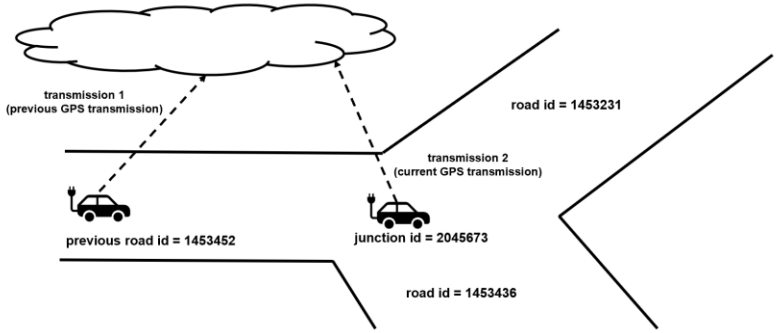
Case 2: The current and previous locations of the vehicle are on two different roads



Case 3: The previous location of the vehicle is in a junction and the current location of the vehicle is on a road



Case 4: The previous location of the vehicle is on a road and the current location of the vehicle is in a junction



Countermeasure : Online Attack Prevention Phase

If **E > 1**, the **Online Attack Prevention Phase** is triggered

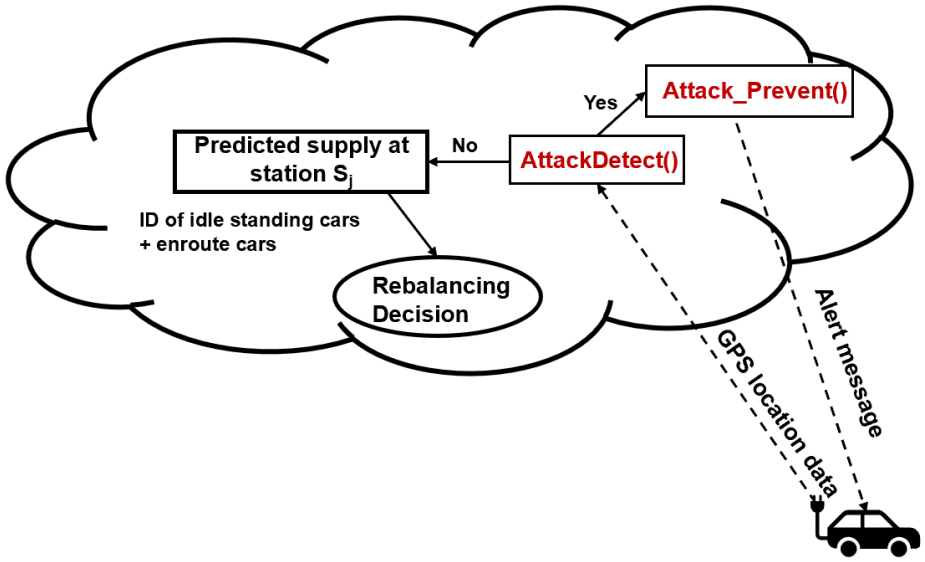
1. *Transmit alert message from the backend server to the victim vehicle V_i*

2. *For next t transmissions associated with the vehicle V_i*
   HMAC_Authenticate(V_i.id,V_i.key)

Integration of the Countermeasure

- Integrated **Attack Detection** phase before the vehicle supply is predicted so that the estimated location of the vehicle is verified before predicting the vehicle supply

- If an attack is detected, then the **Attack Prevention** Phase is triggered at the backend sever that sends an alert message to the victim vehicle so that the subsequent **t** message transmissions are authenticated using Secured Hashed MAC (SHA-512) authentication



Experiments and Evaluation

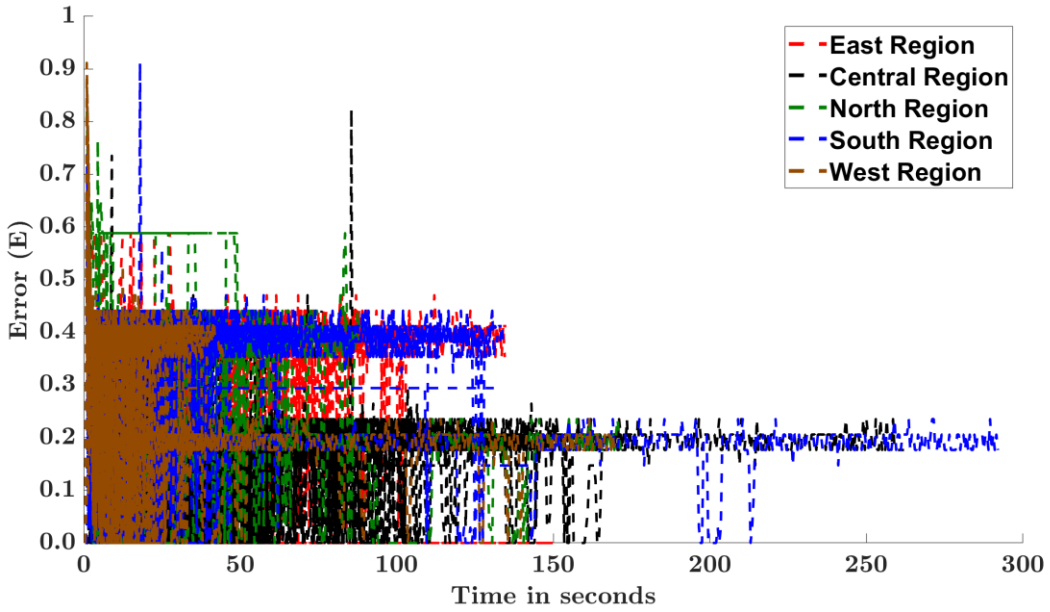
Experiments

- Collected roadmaps of Singapore using OpenStreetMap and used the Traffic Control Interface in SUMO simulator to extract roadmap data from OpenStreetMap
- Divided the roadmaps of Singapore into five regions - Central, East, West, North and South and generated the roadmap data for each region
- Generated **380 random trips** of cars on the roadmaps of Singapore with varying time duration of up to **10 minutes** and collected the trajectory data of the cars from the SUMO simulator
- Implemented our countermeasure in Python and ran experiments on the generated trajectories

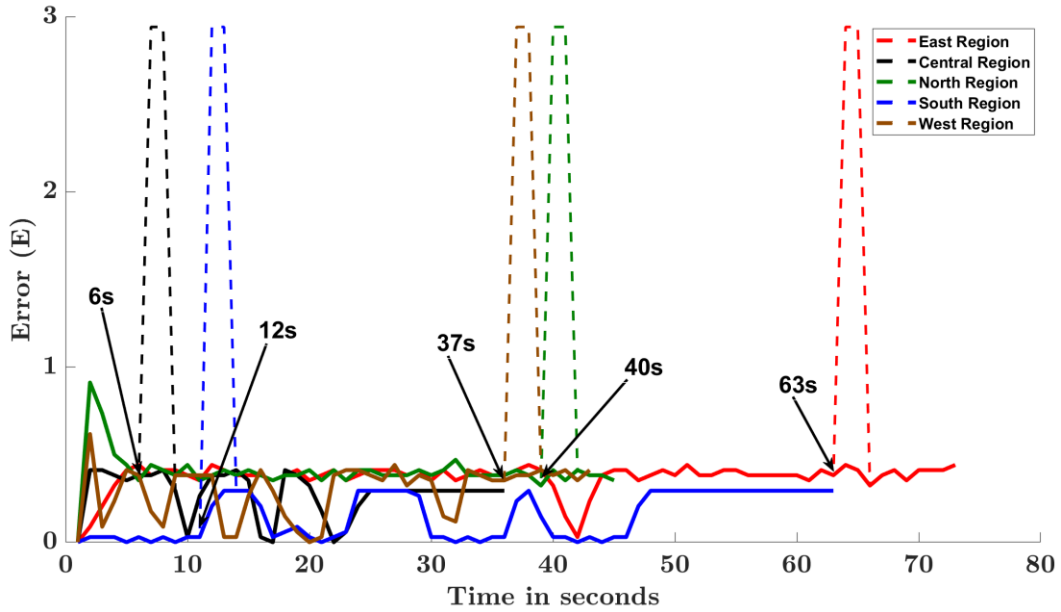
Evaluation

- Used the **error function *E*** to evaluate our proposed countermeasure
- Under normal condition, ***E*** lies within [0, 1]
- If ***E* > *1***, then GPS spoofing attack is detected, and the attack prevention phase is triggered

Results



Error function (E) on 380 trips across Singapore over 10 minutes



Random trajectories in different regions of Singapore without GPS spoofing attack (solid lines) and with GPS spoofing attack (dashed lines)

Observation 1 : *Error function E always remains between [0,1] without GPS spoofing attack*

Observation 2 : *Error function E immediately shoots above 1 on launching GPS spoofing attack triggering the attack prevention phase immediately and making the attack detectable*

Conclusion and Future Works

Conclusion

- We presented **GPS spoofing attack** in **Vehicle Rebalancing application**
- To **detect** and **prevent** the attack, we proposed a **location tracking technique** that can **validate** the current location of the vehicle based on its previous location and roadmap data
- We ran our experiments on the **roadmaps of Singapore** and was able to **detect** GPS spoofing attack **immediately** under all conditions

Future Work

- We want to extend our countermeasure for a more complex system with **traffic data** into consideration

References

[1] Z. Zhang, M. Trinkle, L. Qian and H. Li, "Quickest detection of GPS spoofing attack," MILCOM 2012 - 2012 IEEE Military Communications Conference, Orlando, FL, USA, 2012, pp. 1-6, doi: 10.1109/MILCOM.2012.6415722.

[2] M. Kamal, A. Barua, C. Vitale, C. Laoudias and G. Ellinas, "GPS Location Spoofing Attack Detection for Enhancing the Security of Autonomous Vehicles," 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Norman, OK, USA, 2021, pp. 1-7, doi: 10.1109/VTC2021-Fall52928.2021.9625567.

[3] Ledvina B, Benzce W, Galusha B, Miller I, An in-line anti-spoofing device for legacy civil GPS receivers, **Proceedings of the 2010 international technical meeting of the Institute of Navigation**, 2010.

[4] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. 2011. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX conference on Security (SEC'11). USENIX Association, USA, 6.

[5] Peng Jiang, Hongyi Wu, Chunsheng Xin, DeepPOSE: Detecting GPS spoofing attack via deep recurrent neural network, Digital Communications and Networks, Volume 8, Issue 5, 2022, Pages 791-803, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2021.09.006.

[6] Mykytyn, Pavlo & Brzozowski, Marcin & Dyka, Zoya & Langendoerfer, Peter. (2023). GPS-Spoofing Attack Detection Mechanism for UAV Swarms. 10.48550/arXiv.2301.12766.

[7] Merkebe Getachew Demissie, Lina Kattan, Estimation of truck origin-destination flows using GPS data, Transportation Research Part E: Logistics and Transportation Review, Volume 159, 2022, 102621, ISSN 1366-5545, https://doi.org/10.1016/j.tre.2022.102621.

Thank You

Any Questions?