Research Article

Geo-Location Spoofing on E-Scooters; Threat Analysis and Prevention Framework

Ahmet Saim Yilmaz, Haydar Cukurtepe and Emin Kugu

Abstract— **Geo-location services are widely used by a large number of applications and devices. E-scooters are one of the recent prevalent devices that use these services. Geo-location services are highly vulnerable to spoofing attacks due to their open communication. Spoofing detection and prevention techniques have been researched for a long time. Most of the research has focused on smart devices such as smartphones, unmanned aerial vehicles, or other vehicles. Due to intrinsic application limitations, these threats need to be addressed on a per-environment basis. Geo-location spoofing also poses significant threats to e-scooters in terms of user security, costs, and reliability. In this study, we analyze location spoofing threats in an e-scooter-sharing environment and propose a spoofing prevention framework. The proposed framework monitors the e-scooter's location and tracks significant changes, and its service-based structure provides differentiated levels of awareness and capability.**

Index Terms—**E-Scooter, Geo-location Spoofing, GPS, Location Security, Wi-Fi Positioning**

I. Introduction

GEO-LOCATION SERVICES are widely used by a large number of applications (i.e. navigation, delivery systems, tracking systems, etc.) and devices such as smartphones, smart home devices, and unmanned aerial vehicles (UAV). Recently, electric scooters (e-scooters) have joined the family of geo-location-enabled devices, where e-scooters are made available for short-term rentals.

Geo-location services employ different methods to calculate relative positions, namely Global Navigation Satellite Systems (GNSS), Wi-Fi, and network-based geo-location services. GNSS is a term that refers to the International Multi-Constellation Satellite System, and one broad implementation of GNSS is Global Positioning (GPS) (these terms are used interchangeably). Receivers (i.e. e-scooter) continuously listen to the signals from multiple GPS satellites and calculate their position. When GPS signals are weakened or are even blocked by solid structures, a Wi-Fi positioning system (WPS) steps in to find the signals of nearby Wi-Fi hotspots and wireless access points, thus its own location. Devices also exchange Received Signal Strength (RSS) information to calculate how far away the Wi-Fi access point is from the device. RSS is also attenuated while passing through solid objects, such as walls. Geo-location services use trilateration to compute positions. The other geo-location services (s.a. Bluetooth low energy, network-based, RFID based geo-location) services are dependent on the provider and additional hardware. Thus, these types of services are not considered in this study. In a 3D space, the intersection of 3 spheres gives the point of interest. An e-scooter continuously listens to the GPS signals and measures distance to several Wi-Fi access points, then combines this information with a propagation model to determine its position.

A spoofing attack is a malicious activity in which a program is successfully identified as someone else by forging the actual data [1], or creating fake ones. Location spoofing is a serious threat to geo-location enabled devices. An adversary can make the victim appear in a place irrelevant to the original location. The primary reason for being a serious threat is the ease of method. This threat does not require physical interference or jailbreak-root. More advanced devices (e.g. Smartphones) use various technologies together for security, with predefined priority order [2], [3] or encrypted communication [4]. Relatively easier spoofing techniques pose significant risks on e-scooters. Neither these devices are equipped with encrypted communication capability nor they employ advanced techniques to prevent geo-location spoofing attacks.

In this paper, we analyze location spoofing threats in e-scooter sharing systems and propose a spoofing prevention framework. It takes predefined prevention steps by monitoring the network properties of devices and checking if any significant changes have been made. We analyze different spoofing threats and their applicability in the e-scooter sharing environment. Although geo-location spoofing attacks on smart devices (e.g. UAVs, smartphones) have been studied in detail, this distinctive e-scooter sharing system has not been studied in detail yet. In [5], location spoofing threats against e-scooters are mentioned as a subsection, but no detailed threat analysis or a detection framework is presented. In [6], authors

AHMET SAIM YILMAZ is with the Department of Computer Engineering University of Ted University, Ankara, Turkey, (e-mail: asaim.yilmaz@tedu.edu.tr).
https://orcid.org/0000-0002-4279-684X

HAYDAR ÇUKURTEPE is with the Department of Computer and Information Science of Valparaiso University, Valparaiso, USA,(e-mail: haydar.cukurtepe@valpo.edu)
https://orcid.org/0000-0002-4670-4877

EMIN KUĞU is with the Department of Software Engineering University of Ted University, Ankara, Turkey, (e-mail: emin.kugu@tedu.edu.tr).
https://orcid.org/0000-0001-7829-8087

Manuscript received Jan 9, 2023; accepted Sep 2, 2023.
DOI: 10.17694/bajece.1231384

analyze the threats of location spoofing in e-scooter sharing environments by examining various scenarios and the principles of GPS and Wi-Fi location systems. Authors point out possible negative user experiences, compromised security, maintenance delays, and reputational damages to companies but no spoofing prevention mechanism is proposed.

Spoofing detection and prevention have been studied by many researchers, and various solutions have been proposed to disentangle the legitimate signals from spoofed ones. Jovanovic [7] detects spoofing by observing changes in the clock offset of the GNSS receiver. The authors in [8] use the data from the GNSS technologies to cross-check the data from the base station of the neighboring cell of the mobile cellular network. In [9], an algorithm is proposed for detecting Wi-Fi signal spoofing attacks using RSS. E-scooter systems are different from the other geo-location enabled devices in that they are always on-site and are not equipped with advanced computing power. Thus, e-scooter systems require their own solutions. While previous research has examined spoofing detection and prevention techniques for the devices such as smartphones, unmanned aerial vehicles or other vehicles, this study addresses the unique challenges of the e-scooter sharing environment. This focused analysis study on e-scooter sharing systems and the proposed prevention framework makes this study different from the ones in the literature.

In the rest of this study, we first explain the working principles of location services: GPS and WPS. Section 4 explains how geo-location spoofing attacks are carried out. In Section 5, location spoofing threats against e-scooter systems are presented and analyzed. Section 6 evaluates the applicability of these threats. Section 7 presents the proposed spoofing prevention framework, and Section 8 concludes the study.

II. GLOBAL POSITIONING SYSTEM

Global Positioning System (GPS) is a service given by dedicated satellites, which provides location, velocity, and time synchronization. Devices receive GPS signals from satellites to calculate their location, speed, and elevation. The technique used by GPS is called trilateration.

The GPS has 3 parts: satellites, ground stations, and receivers. Ground stations make sure the satellite is in the correct position. Receivers (e.g. e-scooters) constantly listen to the signals from satellites and calculate the position.

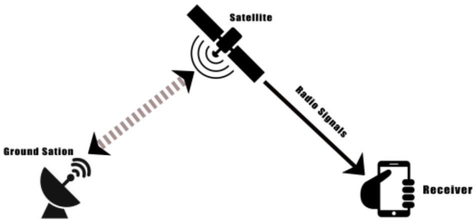

Fig. 1 Basic Concept Representation of GPS.

In Fig. 1, ground stations serve as command and control services for satellites to make sure that they are in the correct position and the receiver collects the signals coming from satellites. GPS satellites broadcast radio signals to enable GPS receivers to calculate position according to the generated signals. GPS receivers do not work well indoors or in crowded environments such as city centers, due to weakened or blocked signals. This situation makes receivers extremely vulnerable to spoofing attacks.

There are different types of GPS services for different purposes. Publicly available GPS Service provides 4.9 meters of accuracy with low cost but it does not provide high accuracy or encrypted signals. Military GPS services and Galileo provide encrypted satellite signals, but e-scooters are not equipped to receive these signals.

A. *How does it work*

GPS satellites use the L-band to transmit their signal, and the time information it uses is coordinated with the atomic clock located inside the satellite. GPS' signal structure is publicly accessible, making attacks easier to execute. The signal generated by a GPS satellite travels by line of sight. They are able to travel through water and clouds, but not solid objects such as walls, tunnels, or mountains. A GPS signal consists 3 different types of information;

- Pseudorandom code; this code holds information about the GPS itself, it tells from which satellite the signal is generated. It is the Identification Code of the GPS.
- Ephemeris data; Holds information about position and speed of the GPS. Also holds information about the satellite's health situation.
- Almanac data; Gives orbital information about GPS and tells where GPS would be located at any time of the day.

At the receiver, the user receives the GPS signal using an antenna with an RF front-end GPS receiver. After the signal is received, it goes through a number of steps such as filtering, amplification, and digitizing. Then, the received signal is converted into a baseband signal. This trimmed GPS signal is then processed to make a position computation. Its pseudorandom code is used to get information for all satellites in view, and the position is calculated based on Ephemeris and Almanac data. To calculate its position, the receiver requires 3 basic pieces of information: The location of the satellite, receiving time of each signal, transmission time of each satellite signal, this information is included in the Ephemeris and Almanac data of the GPS signal. The receiver requires 4 satellite signals to ensure accuracy.

Time of arrival (TOA) is the absolute time that a signal is received by the receiver. Position information is calculated by using differences in TOAs which is called Time Difference of Arrival (TDOA). The mathematical form is:

$$d_n = c(t_{t,n} - t_{r,n} + \Delta n) = \sqrt{(x_n - x)^2 - (y_n - y)^2 + (z_n - z)^2} \tag{1}$$

- Where, n is the satellite id (e.g. if there are 4 satellites, it goes as 1,2,3,4)
- Variable c is the speed of light which is 3x108 m/s
- $t_{t,n}$ is the time GPS satellites transmit their signal. e.g. the signal time transmitted from GPS satellite number 1 is $t_{t,1}$
- $t_{r,1}$ is the time the GPS receiver segment receives the signal coming from a specific satellite
- Δn is receiver clock error
- x, y, z are the respective coordinates of the satellite.

Since the equation has 3 unknown variables and an additional time variable, the receiver requires at least 4 GPS signals to solve the equation.

III. Wi-Fi Positioning System

Wi-Fi is a set of network protocols (IEEE 802.11 family), it allows digital devices to exchange data using radio waves. There are estimated to be around 14 billion devices having Wi-Fi capabilities [10].

The Wi-Fi positioning system receives location data from nearby Wi-Fi hotspots and wireless access points to discover the location of a device. It is especially useful in calculating locations when a device is located indoors, or at locations where the satellite signals are weak. To calculate the position, the device needs to listen to signals coming from Wi-Fi access points and analyze them to decide of the position.

The exchanged data between devices includes Received Signal Strength (RSS). It provides information about how far the Wi-Fi access point is relative to the device. While strong RSS shows the Wi-Fi access point is close to the device, weak RSS shows that device is further away. RSS weakens while passing through solid objects such as walls and windows. So, having weak RSS sometimes may not mean that the Wi-Fi access point is further away.

A. *How it works*

The strength of RSS can be modeled as shown in Equation 2;

$$P(d) = P_0 - 10n\,log_{10}(\frac{d}{d_0}) \quad (2)$$

In this equation, $P(d)$ is the received power in dB, where, d is the distance and P_0 is the received power in dB at a short reference distance d_0. Fingerprinting is an indoor positioning technology to determine a user's position. Fingerprinting approach uses RSS to make a position computation.

Position computation in Wi-Fi positioning systems is based on measuring distance to several Wi-Fi access points then combining this information with a propagation model to determine the position of the device. Trilateration is being used to make a computation. The disadvantage of this technique is that it provides an accuracy around 10 meters.

The trilateration algorithm corresponds to sphere centers. In a 3D world, the intersection of 3 spheres gives our point of interest. In order to calculate it we make use of the following equation:

$$r^2 = (x - x_a)^2 + (y - y_a)^2 + (z - z_a)^2 \quad (3)$$

Let one sphere as an origin point which is A1 in this example and simplify the equations. After radiuses of the spheres become r_1 , r_2 and r_3 the simplified equations become:

$$r_1^2 = x^2 + y^2 + z^2 \quad (4)$$

$$r_2^2 = (x - x_2)^2 + y^2 + z^2 \quad (5)$$

$$r_3^2 = (x - x_3)^2 + (y - y_3)^2 + z^2 \quad (6)$$

In short, trilateration is used to obtain a 2D point and make a position computation with a low accuracy.

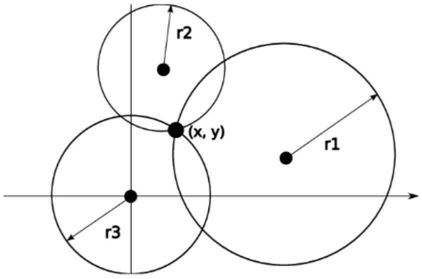

Fig. 2 Trilateration.

As shown in Fig. 2, the circle with radius r3 taken as origin point and trilateration is used accordingly. Intersection point of 3 circles represents the location.

IV. Geo-Location Spoofing

A. *GPS Signal Spoofing*

In GPS spoofing, the malicious user uses a radio transmitter to send counterfeit GPS signals to a receiver antenna to interfere with legitimate GPS satellite signals. Most of the location systems are designed to use the strongest GPS signals, and the strong fake signals are able to override the weaker legitimate signals. In [11], authors launched GPS spoofing attacks on various devices and successfully falsified the location of the device. In [12], the authors successfully execute a spoofing attack to the navigation system using a satellite simulator and manage to navigate a victim to locations 1 kilometer away from the original destination. Aside from the navigation system, authors have also successfully spoofed devices (i.e. iPhone 6, Samsung S7) using Hack-RF based spoofers.

The GPS spoofing techniques can be classified into two:

1) Spoofing with GPS Signal Simulator: In this type of attack, Software-Defined Radio (SDR) is needed to generate baseband signals and then transmit them to the receiver using an antenna. Time synchronization is not necessary with the real GPS signals. The important thing is that the generated GPS Signal strength must be stronger than authentic signal. The attack model using GPS Signal Simulators is as follows: First step is to choose an SDR platform to generate baseband signals. There are couple of options (i.e. BladerRF, RTL-SDR, LimeSDR, SDRplay, USRP, YARD stick etc.). HackRF is an open source SDR platform operating on frequency bands between 10MHz and 6GHz. After selecting the proper SDR, signals are generated, then it comes to a point where the generated signals are transmitted using an antenna.

2) Spoofing with Receiver-Based Spoofers: Receiver Based Spoofers synchronizes the signals with target GPS signals. It extracts time, velocity and position information in order to have a 3D vector of the transmit antenna. Unlike GPS Signal Simulators, the generated signal is authentic and synchronized to the real GPS signals.

When the adversary has complete knowledge of the location of the GPS receiver, the adversary can potentially place multiple RF based antennas to generate GPS signals. Let's call authentic satellite S_j as the satellite that an adversary wants to impersonate and use S_j^a to represent the satellite that is emulated. Let S^a be the entire set of emulated satellites making each fake GPS signal coming from satellite S_j^a. Now the adversary needs to assign values to these variables in order to execute a GPS spoofing attack.

The next step is to summarize the adversary's variables for each emulated satellite S_m^a in order to generate fake GPS signals to falsify the GPS receiver's position. Let $\hat{l}_m^a$ be the falsified location and $\hat{t}_m^a$ is falsified time. First the adversary needs to announce its orbital information and claim to be at $\hat{l}_m^a$ at $\hat{t}_m^a$ second. Let l_i^r be the true location and $t_{i,m}^r$ be the true time on the instant of reception, the adversary sets the true location for the antenna as l_m^a and true time as t_m^a to represent when the signal is sent. t_m^a is associated with $\hat{t}_m^a$ by clock delay making the equation $\hat{t}_m^a = t_m^a + \delta_m^a$. Finally, local timestamp becomes $\hat{t}_{i,m}^r = t_{i,m}^r + \delta_{i,m}^r$. The claimed time of arrival equation of the adversary can be derived as $c\left(t_{i,m}^r - t_m^a\right) = |l_i^r - l_m^a|$.

This represents the adversary's intended time that is generated from Receiver-Based Spoofer. l_i^r is calculated location of the receiver when the message is received from S_m^a. The same equation for the authenticated GPS signal can be shown as $c\left(\hat{t}_{i,m}^r - \hat{t}_m^a\right) = \left|\hat{l}_i^r - \hat{l}_m^a\right|$.

The left-hand side of this equation represents the range between satellite and GPS receiver which is called Pseudorange.

The adversary connects with its fake satellite data with the intended locations and time offsets for which a receiver would be spoofed to solve for the variable. All variables can be related by taking the difference of 2 equations.

$$|l_i^r - l_m^a| + c\left(\hat{\delta}_{i,m}^r - \delta_m^a\right) = \left|\hat{l}_i^r - \hat{l}_m^a\right| \tag{7}$$

The adversary's goal is to solve for the variable sets that satisfy the following equation. Once all variables are solved, the adversary can successfully falsify the GPS receiver's location in a synchronized way using receiver based spoofer.

B. Wi-Fi Signal Spoofing

Fabricating APs from another location, the WPS on a smartphone can be fooled into thinking that the device is currently in that specified location. As discussed in the earlier sections, WPS infers the location based on Basic Service Set Identifiers (BSSIDs) or MAC addresses of nearby APs. It is possible to generate BSSIDs and falsify the Wi-Fi positioning system. Those generated APs are called fake Wi-Fi access points which are set up by configuring a wireless card to act as an access point [13].

V. Problem Statement and Analysis

E-scooter systems let users unlock and book through mobile applications. Locations of the nearby e-scooters are shown in the app to assist users find available e-scooters. Companies running these systems (i.e Lime, Voi scooters, Link and Martı), plan their maintenance and logistic activities according to the location of the devices. Safety regulations are applied for user safety, and precautions are applied against theft or sabotage risks. For instance, an e-scooter company may restrict the scooter's speed on specific roads or prohibit riding a scooter on sidewalks to ensure pedestrian safety. In this paper, we based our analysis on common terms of use of major companies to meet on a common ground. Geofencing technology is being widely used by e-scooter sharing companies.

Geo-fencing is a location-based service for setting up a virtual boundary where the user is allowed to ride. When it is crossed, actions are taken by the companies such as warning the user or stopping the e-scooter for pedestrian safety. Adversaries may attack the e-scooter environment to harm user experience and e-scooter companies.

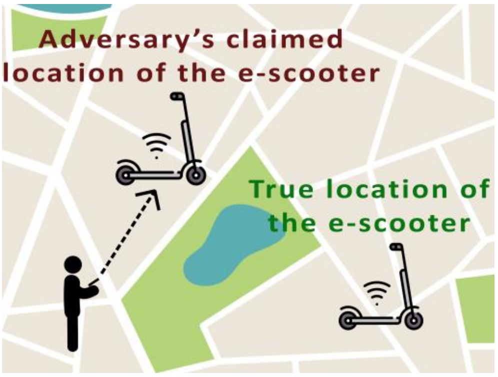

Fig. 3 Exploiting the Pre-Book Feature & Misleading the User.

A. Threats

1) Exploiting the pre-book feature & misleading the user: E-scooter companies allow users to pre-book e-scooters and unlock them, preventing others from booking the same e-scooter. Each minute the e-scooter is pre-booked, the user is charged respectively. An adversary may spoof the location of the e-scooter and mislead the user. Both time and money would be wasted until the user figures out the e-scooter is not in the supposed location.

As shown in Fig. 3, the adversary exploits the pre-book feature using location spoofing procedures in section 4 to fool the user and rent an e-scooter irrelevant to position showing in the app.

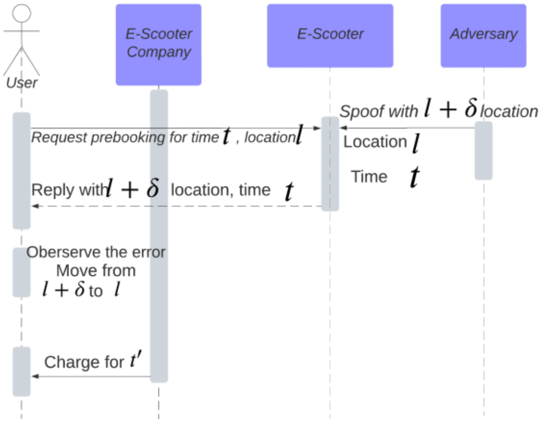

Fig. 4 Exploiting the Pre-Book Feature-Sequence.

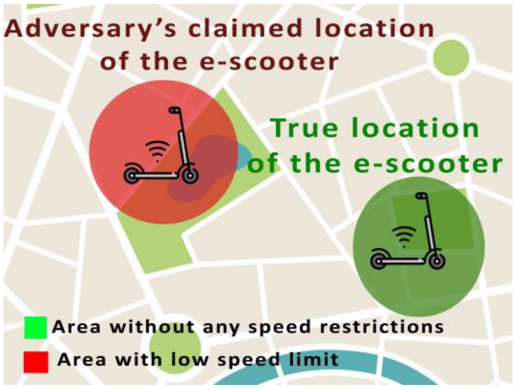
Adversary's claimed location of the e-scooter
True location of the e-scooter
Area without any speed restrictions
Area with low speed limit

Fig. 5 Prevent User from Ending the Ride.

In Fig. 5, the adversary uses spoofing location methods to falsify e-scooter's location and show up in an area where the user is not allowed to ride.

In Fig. 4, let l be the true location of the e-scooter and t be the real time. Adversary uses location spoofing procedures in section 4 to falsify the location of the e-scooter and show up in another location which is real location l plus the adversary's spoofed location S. This would mislead the user to go the wrong direction. The time t' and money would be wasted until the user figures out the e-scooter is not located in the supposed location which shows up in the app.

2) Prevent User from Ending the Ride: There is a virtual boundary where the user is able to ride the e-scooter. When the user wants to end the ride out of those allowed areas, a message is prompted by the app telling "return the area to end the ride". Adversaries may spoof the location of the e-scooter, making it show up in the unallowed area and prevent the user from ending the ride.

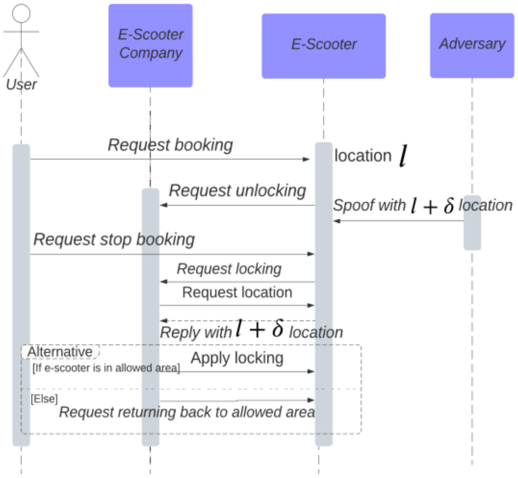

Fig. 6 Prevent User from Ending the Ride-Sequence.

In Fig. 6, user wants to end the ride by locking e-scooter at location l. Adversary uses location spoofing to make the e-scooter show at $l + S$ which is not an allowed zone for users to end the ride. The user won't be able to end the ride until the e-scooter is at a position with allowed boundaries.

3) Limiting the Scooter's Top Speed on the Ride: There are specific places where e-scooter companies limit the speed of e-scooter to protect pedestrians and users. Adversary may falsify the location so that the device is supposedly in the areas with speed limits constantly limiting the speed of the e-scooter vice versa.

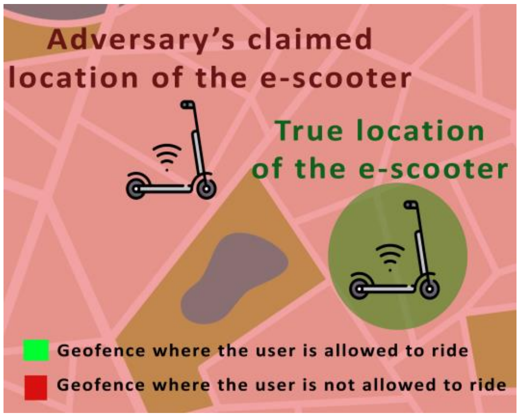
Adversary's claimed location of the e-scooter
True location of the e-scooter
Geofence where the user is allowed to ride
Geofence where the user is not allowed to ride

Fig. 7 Limiting the Scooter's Top Speed on the Ride.

In Fig. 7, the adversary uses spoofing location methods to falsify e-scooter's location and show up in an area with low speed rules making it slow down.

In Fig. 8, user rides e-scooter at location l. Adversary uses location spoofing to make the e-scooter show at $l + S$ which is a low speed zone. By this way the adversary makes the e-scooter slow down and harm user experience.

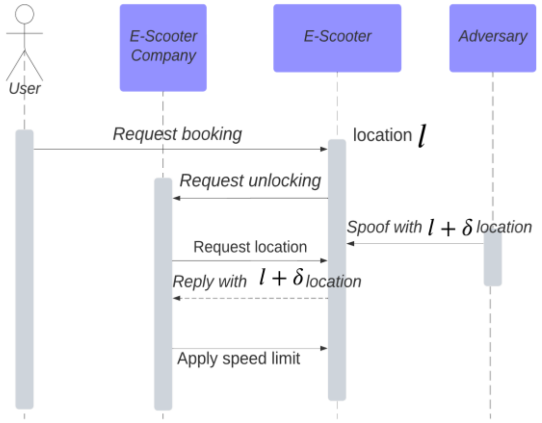

Fig. 8 Limiting the Scooter's Top Speed on the Ride-Sequence.

4) Preventing companies from making e-scooters maintenance: E-scooter companies need to constantly charge the scooters and make maintenance. A typical e-scooter battery lasts around hours of driving. This requires companies charging them on a daily basis. Adversaries could potentially use both GPS and WPS spoofing depending on the situation of the e-scooters and prevent companies seeing the e-scooters at a falsified position.

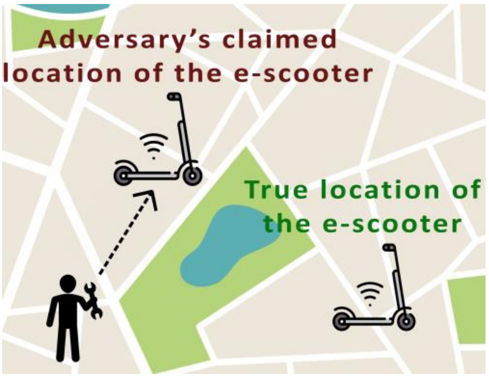
Adversary's claimed location of the e-scooter
True location of the e-scooter

Fig. 9 Preventing Companies from Making E-scooters Maintenance.

In Fig. 9, the adversary uses location spoofing to prevent maintenance crew to find the e-scooter so that they could not be charged nor taken to service.

In Fig. 10, maintenance crew checks the e-scooter's position and goes location $l + \delta$ to repair and charge the device. But the location crew is going is the spoofed location of the adversary, the true location of e-scooter is location l.

5) Theft or sabotage on e-scooters: Adversary may spoof location of the e-scooters to show them up in irrelevant places. So, the adversary could physically steal or sabotage the e-scooter without being noticed.

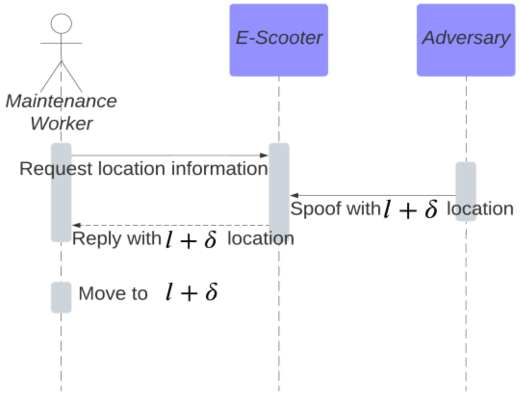
Maintenance Worker
E-Scooter
Adversary
Request location information
Spoof with $l + \delta$ location
Reply with $l + \delta$ location
Move to $l + \delta$

Fig. 10 Preventing Companies from Making E-scooters Maintenance-Sequence.

VI. Applicability of Threats

Adversaries can use different location spoofing techniques for different scenarios depending on the circumstances. For instance, in WPS spoofing techniques fake access points cannot be dynamically created in the direction of movement of the device hence this kind of spoofing technique will fail against non-stationary e-scooters. Applicability of spoofing techniques could be analyzed based on 2 scenarios which are stationary and non-stationary e-scooters.

A. Spoofing the location of a stationary e-scooter

When the goal is to harm the user and the company by falsifying the location information, as in threats 1,4 and 5, adversaries could use both WPS and GPS location spoofing techniques.

- Step 1 (Choosing the ideal target location): Most of the time geo-location capable devices use GPS based location calculation prior to Wi-Fi Positioning System. Having a healthy signal coming from various GPS signals makes Wi-Fi spoofing almost impossible. In order to have a successful spoofing attack, the target location must be somewhere surrounded by buildings having low GPS signals.
- Step 2 (Collecting falsified position information): Then, the adversary needs to generate Wi-Fi Hotspot Tags. To do that adversary may use Wigle.net or Skyhook to collect Wi-Fi Hotspot tags in use around the world.
- Step 3 (Broadcasting Wi-Fi Access Points): After fake BSSIDs are generated having target position, beacons are generated and broadcasted. The SkyLift project can be used for this purpose. SkyLift is an open source tool for broadcasting Wi-Fi beacon frames with a low cost Wi-Fi microcontroller.

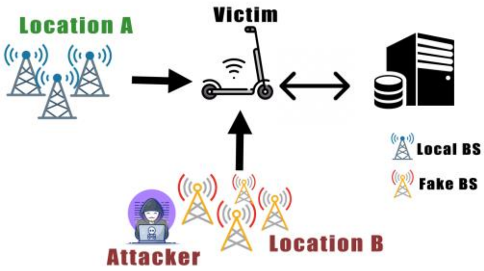

Fig. 11 Wi-Fi Spoofing Attack.

In Fig. 11, an adversary generates fake Wi-Fi access points to falsify the victim's position making it appear at ”Location B” instead of ”Location A”.

To spoof GPS, an adversary needs to transmit GPS signals via antenna to falsify the target e-scooter's position. GPS Signal Simulator or Receiver Based Spoofers can be used as explained in section 4.

There are various GPS Signal Simulators available on the market, such as Hack-RF, bladeRF, NESDR Nano 2+, USRP or NESDR SMArt HF Bundle. They all serve the same purpose, with different capabilities. For instance, USRP has the greatest bandwidth and speed amongst all. NESDR Nano 2+ is the smallest SDR which is even smaller than a usb flash drive, if the adversary's priority is portability then it is the right choice. Hack-RF is an open source and cost friendly SDR platform. Here is a sample command line argument to transmit generated signals using HackRF:

```
hackrf_transfer -t gpssim.bin -f 1575420000 -s 2600000 -a 1 -x 0 -R
```

To execute the command successfully, -t file name, -f frequency, -s sample rate and -a amp enable (1 or 0) needs to be given as an input. After the command, HackRF transmits those signals using an antenna. The target device calculates its position based on the falsified GPS signals and GPS position spoofing occurs.

When an adversary wants to spoof an e-scooter that is checking time synchronization of GPS signals as a security mechanism then Receiver Based GPS Spoofer could be used. Adversary needs to place the spoofer close to the e-scooter where it could gather GPS signals and puzzle out the time information of authentic GPS signals. After this step, time synchronized GPS signals could be transmitted to the e-scooter.

In addition to spoofing, jamming attacks also pose a significant threat against WPS and GPS. Jammer could possibly block Wi-Fi enabled devices from successfully getting signals to calculate the position. On the other hand, it can also hide or change GPS signals before it is being received by the device. In [14], authors successfully execute a GPS jamming attack using Software Defined Radio and prevent devices from receiving GPS signals.

B. Spoofing the location of a non-stationary e-scooter

When the adversary's goal is to falsify the location of a nonstationary e-scooter as in threats 2 and 3, the GPS location spoofing techniques can be used. In WPS spoofing technique, fake access points cannot be dynamically created in the direction of movement of the device hence this kind of spoofing technique will fail. In addition, if an e-scooter starts to get healthy GPS signals while moving from one location to another, WPS spoofing would not work properly. On the other hand, GPS spoofing techniques could be used against a non-stationary e-scooter.

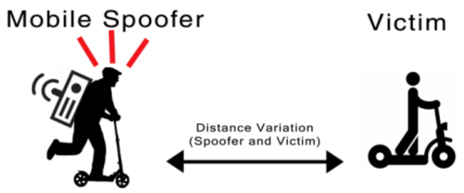

Fig. 12 Mobile Wi-Fi spoofing attack.

Both Receiver Based Spoofer and GPS Signal Simulator should be attached to a mobile vehicle and follow the e-scooter. In Fig. 12, the vehicle carries a spoofer and location spoofs the target device. For the sake of portability, adversaries may use NESDR Nano 2+ as an SDR.

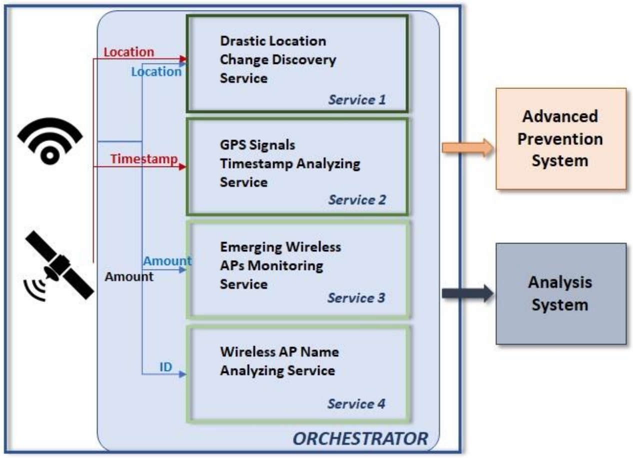
Location
Location
Drastic Location Change Discovery Service
Service 1
Timestamp
GPS Signals Timestamp Analyzing Service
Service 2
Advanced Prevention System
Amount
Amount
Emerging Wireless APs Monitoring Service
Service 3
Analysis System
ID
Wireless AP Name Analyzing Service
Service 4
ORCHESTRATOR

Fig. 13 Conceptual Model of SPFES.

VII. Spoofing Prevention Framework for E-Scooters (SPFES)

E-scooter geo-location spoofing poses significant threats to user security, regulations and e-scooter sharing companies' costs and prestige. Spoofing Prevention Framework for E-Scooters (SPFES) is a framework designed to detect the location of spoofing attacks on e-scooters, thus enabling taking preventive measures. A properly configured framework can prevent e-scooters from misleading both users and companies.

The proposed framework has a service-based architecture. It relies on GPS and WPS receivers in e-scooters. E-scooter having both capabilities are able to employ more services. The framework collects and processes rich information in GPS signals.

The proposed location spoofing detection and prevention framework provides four different services. (i) Discovering the drastic differences in the location, (ii) checking the new number of Wireless Access Points that have appeared, (iii) analyzing GPS signals timestamps, and (iv) analyzing the names of the Wireless Access Points. The working logic of the services is explained below, and the conceptual model of the SPFES framework is given at 13. Each service can be configured to work as a standalone service or a part of a multiple-service combination. Advanced prevention system module implements recent prevention techniques at the edge. Using edge computing, the detected spoofing attacks are prevented at the vicinity without latency.

A. Service 1: Drastic Location Change Discovery Service

The first service compares perceived location shift and error threshold to detect a location spoofing between two consecutive timestamps. Perceived location shift is calculated by using the latitude and longitude data taken from both GPS and Wi-Fi sensors. Most of the e-scooters of the e-scooter sharing companies have a very limited top speed which is around 20 kilometers per hour due to safety concerns [15]. Hence, they are not able to make drastic-location changes. Service 1 focuses on drastic location change in a limited time span. The applied speed limitation and e-scooters' physical speed limits are the rationale of this service. It checks whether or not there is a drastic difference between two consecutive timestamps by comparing error threshold and perceived location shift. It is considered to be a spoofing attack, if this service notices such a shift.

B. Service 2: GPS Signals Timestamp Analyzing Service

As stated in section 4, GPS Signal Simulator attack could be used to spoof GPS signals. It generates strong GPS signals to override the genuine ones. This type of attack is easy and effective but does not synchronizes the timestamp. Because it is easy and low-cost, usually spoofing attacks take place by using GPS Signal Simulator. Service 2 focuses on the weakness of this type of attack by analyzing GPS signals timestamps. If the timestamps are not coherent with the latest stored timestamps, then it is considered to be a spoofing attack.

This service would fail if the adversary uses receiver-based spoofers, which synchronize the signals with target GPS signals. Although this type of attack is complex and expensive to execute, and it is not expected to be used too often, the SPFES relies on more than one service to overcome this threat.

C. Service 3: Emerging Wireless APs Monitoring Service

Service 3 monitors emerging Wireless Access Points. In WPS spoofing attack, the adversary creates fake Wi-Fi Access Points to falsify the Wi-Fi Positioning system. While doing so, the adversary needs to create necessary fake access points to successfully spoof the location. The number of signals coming from fake access points would be strong enough to have an effect on the trilateration method. This situation requires a significant increase in the number of Wi-Fi Access Points. Service 3 checks the newly emerged access points to determinate location spoofing attacks.

D. Service 4: Wireless AP Name Analyzing Service

Service 4 focuses on analyzing the names of the Wireless Access Points. The fake access points created by spoofing tools (i.e. “SkyLift”) has similar names by default. Most of the time, attackers do not pay attention to changing names of the access points. Too much similarity between the names of surrounding access points is considered to be a possible spoofing attack. Service 4 analyzes the names of surrounding Wi-Fi Access Points and detects location spoofing attacks.

These services can be configured to run per se or collectively in different combinations, according to the requirements of the provider. E-scooter systems are different from other smart systems (i.e. smartphones, automobiles) in that they do not have immense computation capability, and implementing more complex detection systems are not always cost efficient in terms of running hardware and computation.

E. Orchestrator

The Orchestrator is the entity that runs on top of all services. The Orchestrator has multiple tasks: (i) It enables the dynamical configuration of effective services. The service provider can access devices, on-premise or online, to configure the services properly. (ii) It coordinates the smooth running of services together. It checks the running services, ensures the elimination of deadlocks, and keeps a log of the service activities. (iii) When the services detect any malicious activity, the orchestrator either communicates with the edge computing device for advanced prevention, or takes predefined prevention steps to keep services running. Necessary computation is done at the edge and rapid decision and reaction are taken without latency. Advanced prevention capability using edge computing is not planned as a mandatory service.

F. Limitations & Discussion

Since SPFES is a service-based framework, it is able to accommodate state of the art spoofing detection techniques. It is also able to cooperate with advanced prevention systems, or advanced analyzing systems. SPFES enhances the security and reliability of the e-scooter system. On the other hand, this framework brings power consumption cost to the e-scooter system.

SPFES is devised to prevent the advanced spoofing attacks, but it also employs basic defense steps such as discarding the possible spoofing threat signals. It is a simple but effective solution to implement. These predefined steps can be adjusted to implement a certain amount of time and then the advanced system can be called. These adjustments affect the performance of the SPFES.

Another limitation of the framework is that SPFES assumes that the legitimate geo-location signals are available prior to location spoofing attacks. SPFES will not detect spoofing attacks if the spoofing attack starts from the beginning of the journey and keeps going along.

VIII. Conclusion

Geo-location services become more popular because of the expanding scale of location-based applications. Global Positioning System and Wi-Fi Positioning System are most commonly used techniques for positioning. E-Scooters have joined geo-location enabled devices with the growing industry of e-scooter sharing. An adversary could use location spoofing techniques to prevent users and maintenance crew from finding an e-scooter, lower the quality of the ride, prevent users from ending the ride or limit the e-scooters speed, and show them in unallowed areas. There could be serious harm done to E-Scooter Companies and users in terms of time, money and prestige. In this study, we explained working principles of positioning systems, analyzed the location spoofing threats on e-scooter sharing environments, and demonstrated unique implementations of different spoofing attacks. We also proposed a spoofing attack prevention framework for e-scooters (SPFES) that is able to detect any malicious activity via monitoring location information and tracking significant changes around. The proposed service-based framework is able to provide different levels of awareness, and enabled capabilities.

Implementation of the SPFES framework will be the next phase of our studies. In future, SPFES implementation can be improved using artificial intelligence (AI) and machine learning algorithms. AI enabled edge computing will also help to detect anomalies with better accuracy.

REFERENCES

[1] Jindal, K.; Dalal, S.; Sharma, K. K. “Analyzing Spoofing Attacks in Wireless Networks”. 2014 Fourth International Conference on Advanced Computing Communication Technologies: (February 2014), 398–402. doi:10.1109/ACCT.2014.46. ISBN 978-1-4799-4910- 6. S2CID 15611849.

[2] Getting the User’s Location, Apple Developer Documentation. [Online]. [Accessed: 10-Dec-2022]. Available: https://developer.apple.com/documentation/corelocation/gettingtheuserslocation.

[3] Geolocation API, Google. [Online]. [Accessed: 10-Dec-2022]. Available: https://developers.google.com/maps/documentation/geolocation/overview

[4] EUROPEAN GNSS (GALILEO) OPEN SERVICE Issue 2.0, January 2021 NAVIGATION SOLUTIONS POWERED BY EUROPE SIGNALIN-SPACE INTERFACE CONTROL DOCUMENT

[5] N. Vinayaga-Sureshkanth, R. Wijewickrama, A. Maiti, and M. Jadliwala, “Security and privacy challenges in upcoming Intelligent Urban Micromobility Transportation Systems,” Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security, (2020). doi:10.1145/3375706.3380559

[6] A. S. Yılmaz, H. Çukurtepe and E. Kuğu, "Analysis of Location Spoofing Threats on E-Scooter Sharing," 2022 30th Signal Processing and Communications Applications Conference (SIU), Safranbolu, Turkey, 2022, pp. 1-4, doi: 10.1109/SIU55565.2022.9864946.

[7] Jovanovic, A., et al.: Multi-test detection and protection algorithm against spoofing attacks on GNSS receivers. 2014 IEEE/ION Position, Location and Navigation Symposium (PLANS), (May 2014), pp. 43–49. doi:10.1109/PLANS.2014.6851501

[8] F. Formaggio, S. Ceccato, F. Basana, N. Laurenti, S. Tomasin, GNSS Spoofing Detection Techniques by Cellular Network Cross-check in Smartphones, in: Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS+ 2019. doi:10.33012/2019.17076.

[9] Khan, F.; Al-Atawi, A.A.; Alomari, A.; Alsirhani, A.; Alshahrani, M.M.; Khan, J.; Lee, Y. Development of a Model for Spoofing Attacks in Internet of Things. Mathematics (2022), 10, 3686. https://doi.org/10.3390/math 10193686

[10] Tzeng C.L. Global Wi-Fi Enabled Devices Shipment Forecast, 2020–2024. Market Intelligence Consulting Institute (MIC); Taiwan, China: (2020)

[11] D. -K. Lee et al.,” Detection of GNSS Spoofing using NMEA Messages,” 2020 European Navigation Conference (ENC), (2020), pp. 1-10, doi: 10.23919/ENC48637.2020.9317470.

[12] Kexiong Curtis Zeng, Yuanchao Shu, Shinan Liu, Yanzhi Dou, and Yaling Yang. A Practical GPS Location Spoofing Attack in Road Navigation Scenario. In Proceedings of the 18th International Workshop on Mobile Computing Systems and Applications (HotMobile ’17). Association for Computing Machinery, New York, NY, USA, (2017) 85–90. https://doi.org/10.1145/3032970.3032983

[13] Celestin M, Achara JP, Cunche M, “Short: Device-to-Identity Linking Attack Using Targeted Wi-Fi Geolocation Spoofing,”Acm Conference on Security Privacy in Wireless Mobile Networks, (2015). doi:10.1145/2766498.2766521

[14] R. V. Karpe and S. Kulkarni, “Software defined radio based Global Positioning System jamming and spoofing for vulnerability analysis,” 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), (2020). doi:10.1109/ICESC48915.2020.9155565

[15] Ma, Q.; Yang, H.; Mayhue, A.; Sun, Y.; Huang, Z.; Ma, Y. E-Scooter Safety: The Riding Risk Analysis Based on Mobile Sensing Data. Accid. Anal. Prev. (2021), 151, 105954. https://doi.org/10.1016/j.aap.2020.105954

[16] Yu, D. Y., Ranganathan, A., Locher, T., Capkun, S., Basin, D. Short paper: Detection of GPS spoofing attacks in power grids. WiSec 2014 - Proceedings of the 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks, (2014), 99–104. https://doi.org/10.1145/2627393.2627398

[17] Wang, K. Time and Position Spoofing with Open Source Projects. (2015).

[18] Meng, L., Yang, L., Yang, W., amp; Zhang, L. A survey of GNSS spoofing and anti-spoofing technology. Remote Sensing, 14(19), 4826, (2022). https://doi.org/10.3390/rs14194826

[19] Huang, J., Lo Presti, L., Motella, B., amp; Pini, M. GNSS spoofing detection: Theoretical Analysis and performance of the ratio test metric in open sky. ICT Express, 2(1), (2016), 37–40. https://doi.org/10.1016/j.icte.2016.02.006.

[20] Ye, A., Li, Q., Zhang, Q., Cheng, B. Detection of Spoofing Attacks in WLAN-Based Positioning Systems Using WiFi Hotspot Tags. IEEE Access, (2020), 8, 39768–39780. https://doi.org/10.1109/ACCESS.2020.2976189

BIOGRAPHIES

AHMET SAIM YILMAZ received the B.S. degree from Ted University, Ankara, Turkey, in 2022. He is currently a researcher in TÜBİTAK-MAM working on an Energy Management System in Turkish Power Grid called as Load Dispatcher Information System (YTBS).

HAYDAR ÇUKURTEPE received the B.S. degree from Turkish Military Academy, master's degree from Air Force Academy in Software Engineering, and PhD from Istanbul Technical University, Computer Engineering Program in 2014. He served as Information System Staff in the Turkish Armed Forces, and NATO missions. Currently, he is Asst. Professor at Valparaiso University/IN, USA.

EMIN KUĞU received the B.S. degree from Istanbul University Computer Science Engineering Department, his master's degree from Air Force Academy Software Engineering and his doctoral degree from Old Dominion University Electrical and Computer Engineering program. He worked as a part-time lecturer at different universities. He worked as a project manager in the Air Force Command Information System (HvBS) project, and took part in the software development processes of international defense projects.