LOCATION BOUNDING IN SMART CARS USING VERIFIABLE MULTILATERATION

Mahi Gulshan, gm1585
Akash Kandli Srinivasalu, aks735
Johnathan Apuzen, jia247
Bavneet Singh bs3485

Abstract-Smart cars nowadays have a network of processors that connect to a central computing platform which has the Ethernet, USB, Bluetooth, IEEE 802.11 interfaces and much more allowing vehicles to connect and communicate. With these features there are vulnerabilities such as GPS spoofing. In this paper, we are going to analyze the vulnerabilities of positioning techniques in wireless networks to position and distance spoofing attacks. We discuss in detail about Verifiable Multilateration which uses infrastructures to calculate locations of vehicles allowing secure positioning in wireless networks.

I. INTRODUCTION

Modern smart cars have a number of processors, sensors, EDRs, USB, Ethernet that are connected to a computing system in the car.
Some of these devices include:

1. *Event Data Recorder* collects data and records events such as car crashes
2. *GPS receiver* finds the location of the vehicle, and aids the vehicle in navigation
3. *Radars* determine if there are any obstacles in the vicinity of the vehicle.

With these advancements, vehicles can connect and communicate with each other and other devices wirelessly. As a result, users can gain information about accidents, traffic and road safety, as well as detect other vehicles in their vicinity.

With connectivity and communications, there is a risk of security and violation of privacy. The vehicles can potentially be hacked and controlled by someone who is not authorized to control it, thus causing harm to driver. A well known instance is the hacking of a jeep by two attackers. The attackers initially controlled the entertainment system, later, began to control the transmission, and finally killed the transmission to leave the jeep helpless on the middle of the highway. This was demonstrated by Andy Greenberg [4].

Privacy is also violated in cases where the driver is not aware of who has access to their information because the vehicles are connected and the information of one vehicle's whereabouts can be tracked by another vehicle's EDR.

Along with privacy, one persistent security issue is location spoofing. An attacker can hack into the system and spoof the location of the smart car such as in a crime scene, for example, and can manipulate the data.

In this paper, we will primarily focus on a solution for GPS spoofing. We will discuss verifiable multilateration, VM, as a solution for GPS spoofing which uses physical roadside infrastructure to calculate the distance and location of a vehicle. VM uses distance bounding protocols. Because of its simplicity, it can be used with a variety of systems for securing positioning

II. BACKGROUND

Many solutions suggest the installation of tamper-proof GPS receivers that can be used to register the location of vehicles. One advantage of this solution is that it does not require the installation of any

roadside infrastructure as in verifiable multilateration. One disadvantage with this solution is the lack of availability especially in urban areas. GPS signals can be blocked off in cities with high rise buildings, tunnels and bridges. Every vehicle is also required to install a tamper-resistant hardware.

Verifiable multilateration as mentioned earlier provides location of a car which is not prone to spoofing using roadside physical infrastructure to bound the location of a vehicle to a small area**.** Although it does require the installation of infrastructures, it is tamper-proof and secure.

III. THREAT MODEL

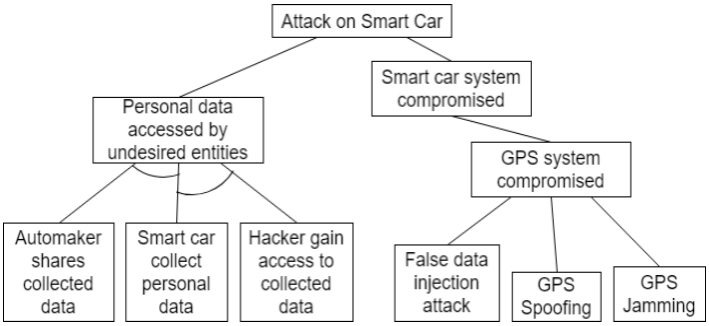

Fig 1: Attack Tree for Smart Cars

Figure 1 is a slightly modified version of the attack tree from our previous paper. It explores the general vulnerabilities of a smart car and how they can be exploited. The tree shows a violation of privacy/ confidentiality through attack on personal data and smart car's system being compromised specifically in its location system.

Verifiable multilateration uses a distance bounding protocol to determine the location of the smart car. This protocol is used in conjunction with four verifying base stations to securely determine the location of the car. The distance bound protocol ensures that the car's location system cannot pretend to be closer to a verifying base station than it actually is. It can, however, pretend to be further from it, which can be done through a distance enlargement attack (see Figure 2). As a result, if a car does pretend to be further from one base station, it would have to prove that it is closer to at least two other base stations. Since each base station uses the distance bound protocol to determine its distance from the car, pretending to be closer to other stations would hypothetically not be possible.

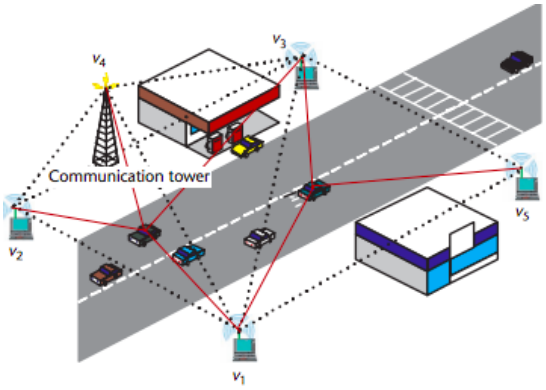

Fig 2. Example of verifiers

Verifiable multilateration provides a way to prevent spoofing and false data injection attacks, and therefore lessens the threat of a smart car's location system becoming compromised.

IV. DESIGN

The proposed solution uses roadside infrastructure to verify the location of a smart car using a system called verifiable multilateration. Verifiable multilateration is designed in the following ways:

1. A central authority installs a set roadside infrastructure called base stations in specific roads and highways.

2. In three dimensions, four base stations are required and they calculate the distance

bound of a vehicle. In two dimension, only three base stations are required

3. If the calculated distance of the vehicle falls into the triangular pyramid that the verifying base stations create, then the location of the vehicle is considered accurate.

Figure 2 shows verifiable multilateration in action [1]. Verifiers or base stations v1, v2, v3, and v4 form a triangular pyramid and if a car is within that pyramid, v1, v2, v3, and v4 can determine that vehicle's location in three dimensions.
Verifiers v1, v3 and v5 form a triangle and they can determine the location of a vehicle in two dimensions if it is within that triangular area.

Along with the base stations, the car and the stations use a distance bound protocol.

V. IMPLEMENTATION

The protocol is implemented in the following ways [2].

1. A vehicle, we will call it C for claimant, is authenticated, and a verifier base station, v, is also authenticated.

2. After authentication is successful, C will generate two random numbers NC and NC' which is the result of a collision-resistant one-way hash function h [1].

3. These hashed values are sent to v. The verifier sends C a "challenge" by generating Nv.

4. C must respond to this challenge with Nv ⊕ NC within an expected time. Note that C cannot respond correctly to the challenge until after the challenge is sent [1]. C must either send the response to v immediately after the challenge is sent or delay the response.

5. The response time, tvC, is measured and C's distance is estimated. When v is calculating the distance of C, it considers C's processing delay.

6. C sends NC' as a second response to the challenge which is also C's signature.

7. v uses NC' to verify C.

u : **Generate** random nonce N_u
: commitment $(c, d) = \text{commit}(N_u)$
$u \rightarrow v$: c
v : **Generate** random nonce N_v
$v \rightarrow u$: N_v *(bits sent from MSB to LSB)*
$u \rightarrow v$: $N_u \bigoplus N_v$ *(bits sent from LSB to MSB)*
v: **Measure** time t_{vu} between sending N_v and receiving $N_u \bigoplus N_v$
$u \rightarrow v$: $N_u, N_v, d, MAC_{K_{uv}}(u, N_u, N_v, d)$
v: **Verify** MAC and verify if $N_u = \text{open}(c, d)$

Fig 3. shows the distance bound protocol in more detail.

VI. EVALUATION

After discussing the designs and implementation of verifiable multilateration using distance bound protocol, we believe it would be a beneficial addition to a smart car's location system. It would add a layer of security to the car's system, eliminate vulnerabilities, and make location spoofing much more difficult. It would require the installation of various verifying bases, but we believe the cost of building those infrastructures would be worth it. Additionally, the simple design allows this system to be used by many devices and not just smart cars.

Table 1: Summary of Verfiable Multilateration

	External attackers	Single internal attacker	Single internal + external attacker	Colluding internal/ cloning internal
VM-RF-DB + DF	Yes	Yes	Yes	Yes
VM-RF-DB	Yes	Yes	Yes	No
VM-US-DB	No (Yes UW)	Yes	No	No
VM-RF-AR	Yes	No	No	No
VM-US-AR	No (Yes UW)	No	No	No

The effectiveness of verifiable multilateration depends on the way it is implemented. An analysis by Capkun and Hubaux [2] performed on various implementations shows which attacks each implementation protected against. Table 1 above shows their findings. *VM* stands for verifiable multilateration, *RF* is radio communication between verifiable base stations and the entity, *US* is ultrasonic communication, *DB* means it uses distance bounding, *AR* uses authenticated ranging instead of distance bounding, *DF* is device fingerprinting which means the entity being located has a unique identification, and *UW* means the base stations are underwater. From the table, we can see that verifiable multilateration is most secure when it uses distance bounding, radio communication, and device fingerprinting.

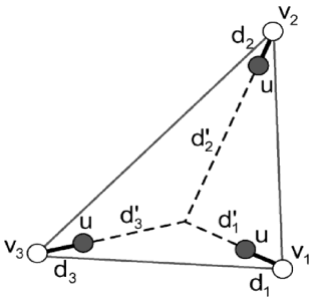

Fig 4. Multiple Device Attack

Device fingerprinting prevents attacks that use multiple spoofing devices [2]. Figure 4 shows an example of this where an attacker, or multiple attackers, place a device near each verifying base station. Each device can then spoof a location to their respective base station that is larger than their actual distance, which allows them to fake a location that is inside the verification triangle between the base stations. This would be harder with device fingerprinting, since the base stations will detect that there are multiple devices projecting a location, instead of just one car.

VII. RELATED SOLUTIONS

A. Packet Leashes

Packet Leashes prevent hackers from recording packets at one location, tunneling them and retransmitting them in different network allowing the attacker to gain unauthorized access, or perform a Denial-of-Service(DoS) attack [3]. This type of attack is called wormhole attack. The two types of leashes are geographic leashes and temporal leashes. In Geographical leashes, location and timestamp are attached to packets sent from sender and are validated at receiver end and all the nodes at sender and receiver end should have their clocks loosely synchronized. The time at which the packet was sent and the place from where it was sent is compared to check for travel time. If the travel time is within the bounded range it is accepted. It is not tamper-proof. Temporal leash is similar to Geographic leash but in this a temporal leash can be constructed by including in the packet an expiration time, after which the receiver should not accept the packet.

B. Symmetric Encrypted Broadcast Signal

In this solution, packets are encrypted and sent, and only the receiver with correct key can decrypt it. But if anyone can build or reverse engineer a receiver they will know the secret key needed to spoof others. This can only be used in closed user communities like military or in modules protecting the common key.

VIII. CONCLUSIONS

In this paper, we discussed about smart vehicles that are susceptible to various attacks mainly GPS spoofing. We, then, discussed about verifiable multilateration which uses base stations and distance bound protocol to determine the location of vehicles to prevent against these attacks. We then further evaluated verifiable multilateration that were implemented in various ways to understand which implementations are most affective. We determined that verifiable mutilateration implemented with distance bound protocols and finger printing are the most affected.

REFERENCES

[1] Hubaux, J.P. & Capkun, Srdjan & Luo, Jun. (2004). The Security and Privacy of Smart Vehicles. Security & Privacy, IEEE. 2. 49 - 55. 10.1109/MSP.2004.26 https://www.researchgate.net/publication/3437601_The_Security_and_Privacy_of_Smart_Vehicles

[2] Hubaux, Jean-Pierre & Capkun, Srdjan. (2006) Secure Positioning in Wireless Networks. Security & Privacy, IEEE. 221 – 232 https://ieeexplore.ieee.org/document/1589104/

[3] Hu, Y.-C. & Perrig, A & Johnson, D.B. (2003). A Defense Against Wormhole Attacks in Wireless Networks. Security & Privacy, IEEE. https://ieeexplore.ieee.org/document/1209219

[4] Greenberg, Andy. “Hacker Remotely Kill Jeep in Highway”. Wired. 2015 https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/