Detect and Defend System On a Stick (D^2S^2) Against GPS Spoofing Attack

MOSTAFA EL-SAID
School of Computing and Information Systems
Grand Valley State University
Allendale, MI 49401-9403
elsaidm@gvsu.edu

Alexander Arendsen
Seminole State College of Florida
Computer Science Dept
100 Weldon Boulevard,
Sanford, FL 32773
TURBO45@live.seminolestate.edu

Samah Mansour
School of Computing and Information Systems
Grand Valley State University
Allendale, MI 49401-9403
mansours@gvsu.edu

Abstract

With the wide spread of self driving cars, the need for safer and secure roadways became evident in the Intelligent Transportation Systems (ITS). For flexible deployment of smart vehicles in the ITS, smart vehicles communicate freely with each others using ad-hoc paradigm known as Inter-Vehicle Communication (IVC) over a universally available pool of channels. Unfortunately, this open access to the ITS system can be exploited by hackers to fuzz the system, break into it and cause a roadway danger.

In this paper, we examine the possible security threats in the ITS system due to the exploitation of the vehicle's GPS system. We propose a novel driver assistant system called Detect and Defend on a Stick System (D^2S^2) to detect and protect against GPS Spoofing attack.

In order to validate the D^2S^2 mechanism, our simulation experiments were focused on developing a mechanism to detect malicious vehicle (the "attacker") that would lie about its GPS coordinates and defending the target vehicle (the "victim") from taking potentially dangerous evasive maneuvers. The victim vehicle's defense system is observed under both normal non-attack and attack circumstances and positive results are obtained.

Keywords: VANET, ITS, GPS Spoofing

Introduction

There has been many research work focusing on the ITS system. Smart vehicles' radio is using the Dedicated Short Range Communications (DSRC) framework in Vehicle-to-X Communication (V2X), including the Vehicle-to-Infrastructure (V2I) and Vehicle to-Vehicle (V2V) communications paradigm.

The Society of Automotive Engineers (SAE) issued the SAE J2735 standard which defines various types of messages to be transmitted among DSRC radios on the road including the Basic Safety Message (BSM). The BSM message contains the core data elements about the vehicle itself (vehicle size, position, speed, heading acceleration, brake system status, ID) [5 and 6].

The vehicle obtains its position from the GPS satellite via the GPS radio and broadcasts it periodically in the BSM message via the DSRC radio. Each vehicle can maintain a neighbor table which contains list of

neighboring nodes and their locations. This table can be utilized to forward messages to the nearest nodes until it gets forwarded to the final destination vehicle. This approach was the foundation for developing position based routing protocols. The universal availability of the GPS radios in modern vehicles makes it possible to implement such kind of position based protocol among vehicles within range [10].

Although this creates an opportunity for V2V communication nodes to share roadway hazard notifications with neighboring vehicles based on the location of the incident, this also attracts malicious vehicles to spoof a victim vehicle's location, impersonate it and start to play its role in the network. So, messages that are forwarded to the victim vehicle for possible routing can be sent to the attack (spoofed) vehicle instead of the victim vehicle. In turn, the attack vehicle can copy these messages before re-forwarding them and no one can notice this attack while it is in progress. The attack vehicle can be even malicious and drop these messages from the network after copying them first, causing a DoS attack.

Authors in [1, 3, 8, 9 and 12] presented an overview of the possible attacks and their possible solutions in the ITS systems. Moreover, authors in [2, 7 and 11] introduced a signature based solution for GPS based systems to accept only authentic location data. The pervious effort was either lacking any form of testing and analysis for the GPS Spoofing attack or relies on solutions that can be exploited for their vulnerabilities to allow other forms of attacks to take place such as replay back attack.

In this paper, we introduce a Detect and Defend System On a Stick (D^2S^2) to detect and protect against the GPS spoofing attack. The D^2S^2 can be implemented on the vehicle's On-Board Unit (OBU). The proposed system is implemented using three stages such as follows:

- Stage-1:
  - Set up an attack scenario with one attack vehicle and one victim vehicle using PreScan simulation engine and Simulink,
- Stage-2:
  - Determine the *amount of offset the attack vehicle's GPS coordinates* must have so that it would appear to be on a crash course with the victim vehicle,
- Stage-3:
  - Develop a *reaction system* in the victim vehicle.

In *stage 1 and 2*, simulation circuit is designed using PreScan and Simulink [] to:

(1) Simulate the attack vehicle's behavior to transmit malicious GPS coordinates
In order for the attack vehicle to be able successfully impersonating the victim vehicle, the attack vehicle has to:

a. impersonate the victim's vehicle-ID and
b. impersonate the victim's location

The victim's ID is advertised in the BSM message and can be captured by any nearby vehicle. The victim's position is impersonated based on adjusting the actual distance between the victim and attack vehicles.

In *stage 3*, simulation circuit is designed using PreScan and Simulink [4] to:

(1) Simulate the defense system's reaction to detect the attack vehicle's behavior and triggering an alert as though it were a real emergency.

The remainder of the paper is organized as follows. Section 2 describes how the GPS spoofing attack will be implemented. Section 3 describes how the proposed system reacts to the GPS Spoofing attack. Sections 4 and 5 conclude the paper and outline the future work.

2. GPS Spoofing Experiment Setup and Execution

The attack circuit was designed using the PreScan environment along with the Simulink software such as shown in figure 1. PreScan was chosen to implement the simulation environment because it supports the BSM message format used in the DSRC communication

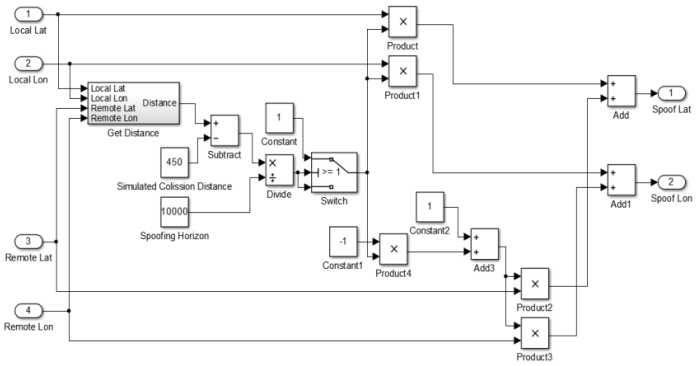

Figure 1 GPS Spoofing Attack Simulation Circuit

In the attack circuit, there are four inputs:

- Two for the attack vehicle's GPS coordinates (labeled "Local"), and
- Two for the victim vehicle's ("Remote").

The two outputs are the affected GPS coordinates to be transmitted ("Spoof").

Inside of the circuit, there are two parameters that are installed:

- Simulated Collision Distance and
- The Spoofing Horizon.

The Simulated Collision Distance defines at what distance the two vehicles should actually be when the GPS coordinates collide. The Simulated Collision Distance is set to a value of 450 units. The Spoofing Horizon defines a boundary distance for the attack; when the distance between the two vehicles is greater than the Spoofing Horizon, the attack vehicle will simply transmit its actual GPS location. The Spoofing Horizon is set to unrealistic value of 10000 units to trigger an aggressive attack on the victim vehicle.

The two vehicles are traveling towards each other at the same constant speed and then pass. Using this circuit, the attack vehicle will gradually adjust its GPS coordinates proportionately to the distance between it and the victim so that, at the time of collision, it will be transmitting 100% of the victim's GPS signal. The distances shown in the attached graphs verify that the spoofed GPS signal conveys a collision, while the actual distance is safe.

Figure 2 presents a graphical comparison of the actual distance between the two vehicles, and the distance conveyed by the spoofed GPS coordinates.

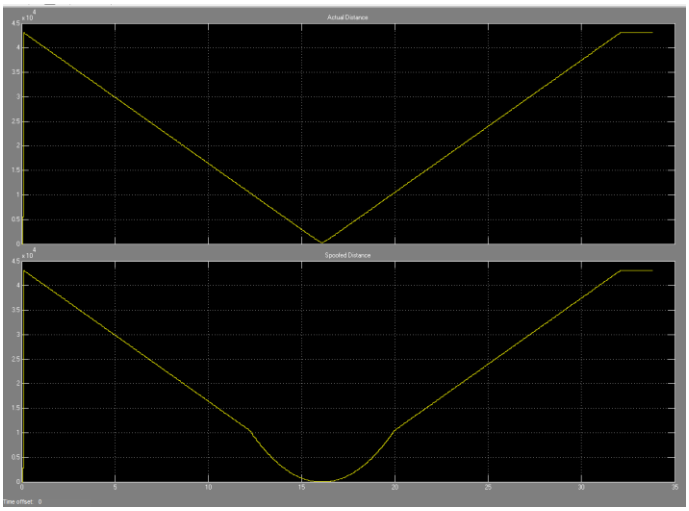

Figure 2 Spoofed Distance versus Actual Distance between (in micro units) the 2 ICV nodes

In figure 2, the top graph shows the actual distance between the two vehicles, while the bottom graph shows the distance conveyed by the spoofed GPS coordinates.

The top graph is a "V" shape, as would be expected since the two vehicles are traveling towards each other at the same constant speed and then pass. The bottom graph looks similar; except for when the distance is less than the value of the Spoofing Horizon (the spoofing horizon is set to 10,000, for which there is a tick mark). The graph then assumes a curved shape, which is the intent of the attack: a gradual, presumably difficult-to-notice approach. On the road, this would make it seem as though the attack vehicle is drifting slowly into the victim's lane and accelerating.

Figure 3 is just a zoomed-in version of figure 2 We scaled the graph differently; the Y-axis maximum for the top graph is around 5000, where the bottom one is around 100 to get a closer look on the area where we expect the attack to be successful.

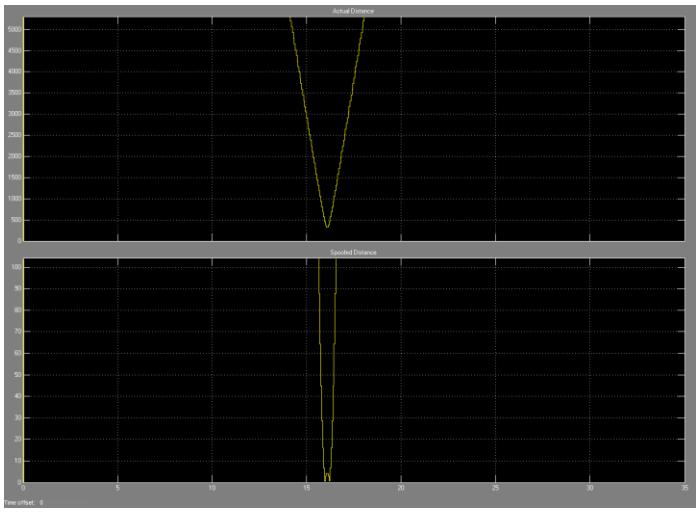

Figure 3 Zoomed-in Version of the Spoofed Distance versus Actual Distance between the 2 ICV nodes

Figure 3 shows that, while the actual distance between the vehicles reaches a minimum of about 450, the distance according to the spoofed GPS coordinates does reach zero (causes a GPS coordinates "crash"). Their widths are different because of different scaling factor (the Y-axis maximum for the top graph is around 5000, where the bottom one is around 100).

Also, figure 3 demonstrated the effect of the Simulated Collision Distance in such a way that when the top graph reaches a value of 450 (the set simulated collision distance), the bottom one reaches 0. The

vehicles, in actuality, become a bit closer than 450 units, so there is a brief interval of time with "negative" distance (the very small rebound in the middle of the bottom graph).

Therefore, the attack vehicle is able to manage and carry out a GPS Coordinates Collision/Spoofing when they are within a close margin of being equal. The time of collision is when the GPS coordinates collide, which will also be when the actual distance is equal to the Simulated Collision Distance.

3. Reaction System in the Victim Vehicle

To accomplish our goal of getting the victim vehicle to become aware of the potential collisions (attack), and distinguish real GPS signals from false ones, a reaction system for the victim vehicle has been developed. The proposed relies on two important factors in the vehicle's perception of a potential collision (Collinearity and Proximity).

The Collinearity is a number expressing how directly the attack vehicle is heading toward the victim vehicle. Therefore, Collinearity expresses how closely the victim vehicle's GPS position falls on a line created by the attack vehicle's previous GPS position and its current one, using a predetermined maximum value if it is exactly on that line. Lower values the further it is away from that line. The Proximity is the distance between the victim and the GPS coordinates it receives.

Using these parameters, the victim vehicle can calculate a "danger" level based on the following formula:

$$\text{Danger} = \text{Collinearity}/\text{Proximity}$$

Where, the Danger is a resulting index by which the vehicle can decide whether or not evasive action should be taken.

The PreScan software is used to implement the proposed reaction system using a simulation circuit such as in figure 4. The simulation circuit is used to calculate the Collinearity, Proximity, and the Danger index as vehicles behave over time under both normal non-attack and attack circumstances.

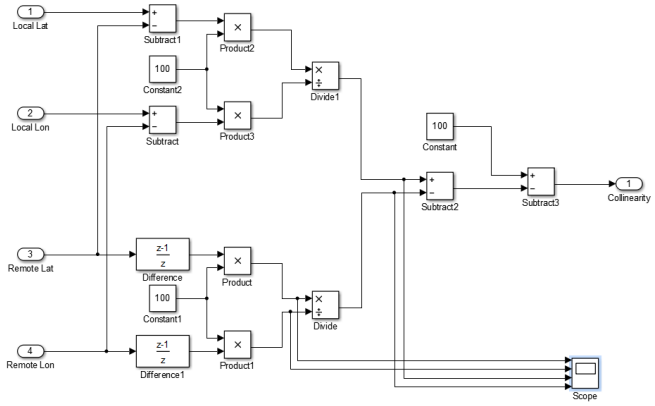

Figure 4. Reaction System Simulation Circuit

We've run a simulation experiment without GPS spoofing (attack vehicle transmitting its actual GPS coordinates) to evaluate the behavior of the reaction system under regular conditions.

We observed that as the two cars pass, as shown in figure 5 and 6, the "danger" value does increase, but not nearly as much as it does when under attack. So, under normal conditions, the "danger" factor reaches a maximum of about *0.33*, while under a GPS spoofing attack it reaches a maximum of about *3.4*.

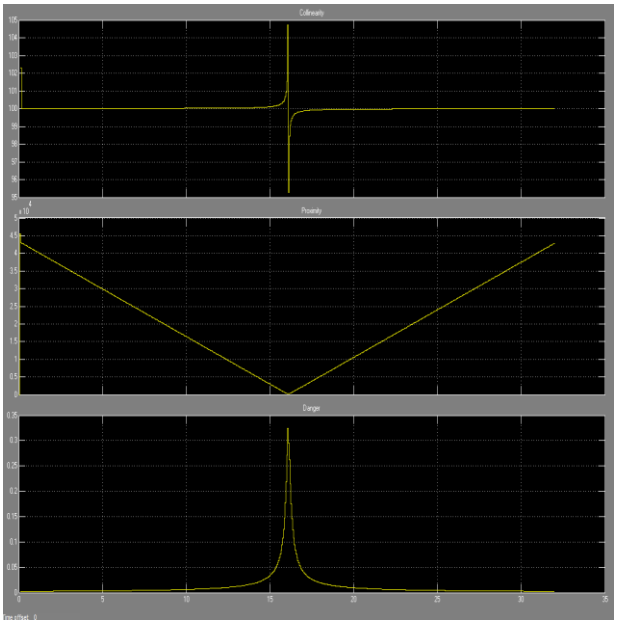

Figure 5. Collinearity, Proximity, and the Danger Index Simulation Results (NO Attack Scenario)

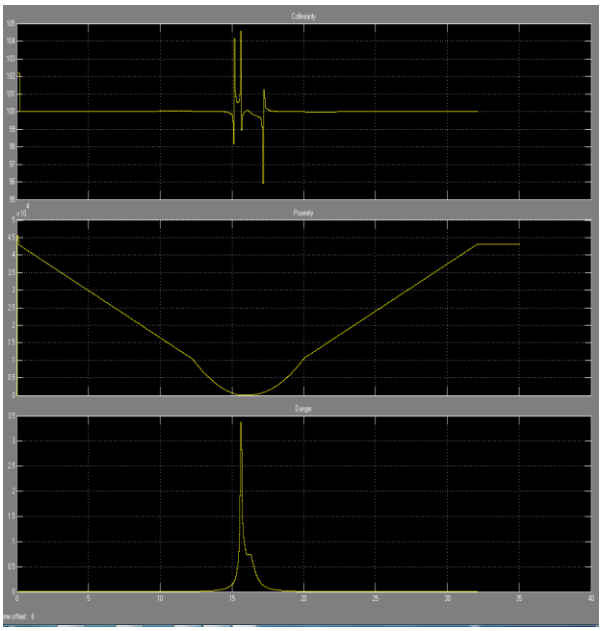

Figure 6. Collinearity, Proximity, and the Danger Index Simulation Results (GPS Spoofing Attack)

The D^2S^2 system can alert the victim vehicle's driver by displaying the danger index value in the vehicle's dashboard. The driver may have to reset the vehicle's GPS or report the incident to law enforcement authority.

4. Conclusion

Authors focused on developing a driver assistance mechanism to detect and alert the driver against the possibility of having GPS Spoofing attack. This attack is in which a malicious vehicle (the "attacker") would lie about its GPS coordinates and attempt to prompt its target (the "victim") to take potentially dangerous evasive maneuvers. After designing a circuit in the attacker to transmit malicious GPS coordinates, authors then attempted to design a circuit in the victim which would allow it to detect that it was in danger.

Simulation analysis is carried out using PreScan and Simulink software to test the efficiency of the proposed system. Simulation results indicate that the proposed system is able to detect the possibility of having GPS Spoofing attack with a high degree of accuracy.

5. Future Work

Authors would like to investigate the details associated with the designing of an RSU in the PreScan simulator. The RSU will create and dynamically disseminate a neighboring list of trusted vehicles. This list can be used to filter out malicious/spoofed messages coming from outsiders.

References

[1] Deshpande, S. (2013). Classification of Security attack in Vehicular Ad Hoc network: A survey. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* 2(2), p.371-377

[2] He, L. & Zhu, W.T.(2012). Mitigating dos attacks against signature-based authentication in VANETs. *IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, 3 p. 261–265.

[3] Hoa LA, V., & CAVALLI, A. (2014). Security Attacks And Solutions In Vehicular Ad Hoc Networks: A Survey. *International Journal on AdHoc Networking Systems (IJANS), 4*(2).

[4] https://www.tassinternational.com/prescan, Retrieved February 20, 2015

[5] http://grouper.ieee.org/groups/scc32/dsrc/ Retrieved February 20, 2015
[6] http://www.sae.org/, Retrieved February 20, 2015
[7] Hubaux ,J. Capkun , S. & Luo, J. (2004). The security and privacy of smart vehicles, *IEEE Secur*ity, 2 (3) p. 49–55.
[8] Nidhal Mejri, M., Ben-Othman, J., & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions, *Vehicular Communications*, Elsevier Inc.
[9] Rawat, A. Sharma, S., Sushil, R.(2012). Vanet: Security Attacks And Its Possible Solutions". *Journal of Information and Operations Management*, 3(1), pp-301-304
[10] Song, H., Wong, V. and Leung, V. (2008) "Secure Location Verification for Vehicular Ad-Hoc Networks" IEEE Global Telecommunications Conference.
[11] Wolf, M. (2009). Vehicular security mechanisms, in: Security Engineering for Vehicular IT Systems, *Springer*, p. 121–165.
[12] Zeadally, S., Hunt, R., Chen, Y., Irwin, A. & Hassan, A. (2010). Vehicular ad hoc networks (VANETS): status, results, and challenges, *Springer Science*, Business Media, LLC