ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Transport safety in VANET by Detecting GPS Spoofing attack using Two Navigators

Rizwan uz zaman wani* and Dr M.Nandhini
* Department of computer science Pondicherry university, Puducherry, India
Assistant professor, Department of computer science, Pondicherry University, Pondicherry, India

Abstract: In VANET GPS (Global Positioning system) is used for locating and Tracking the position of the vehicles. GPS Spoofing in the form of Transmitting False location information and denying services is an emerging threat to the VANET. It is the attack by which GPS receivers get the false navigation results and the receivers are not known about the attack. In the process of spoofing, the spoofer transmits the slightly more powerful misleading signal, stronger than the original GPS signal, fooling the receiver into using fake signals for positioning calculations. In this paper we introduce GPS spoofing detection theory using two navigators works, and to get a basic grasp of GPS spoofing detection theory and terminology.

***Keywords*:** VANET, Global positioning system, spoofing

I. INTRODUCTION

Vehicular ad hoc networks (VANET) are emerging as a prominent form of mobile ad hoc networks (MANETs), where the mobile nodes are the vehicles with a restricted mobility pattern with dedicated units for communication that are installed in vehicles allowing them to exchange data, whereas the fixed nodes are the roadside units (RSU) deployed in critical locations. Communications in VANETs is of the form of Vehicle-to-Vehicle communication (V2V) and Vehicle-to-Infrastructure (V2I) communication typically using Global Positioning System (GPS) to exchange
Messages with the RSU. In VANET, global navigation satellite systems like GPS are likely having the threat of being spoofed i.e. to get the false navigation results [1]. GPS system is having the significant impact on everyday life. The security and reliability of GPS system affects public safety in both military and civilian applications. Recently, a real world GPS spoofing attack was reported which demonstrated the vulnerability of the GPS signal to a spoofing attack. Therefore, such a widely used system increasingly becomes an attractive target for illicit exploitation by terrorists and hackers for various motives.

In the GPS spoofing, an attacker first takes the control over the original satellite signals and then transmits a powerful signal which is stronger than the GPS signal and the Vehicle or receiver gets the incorrect navigation results based on the signals of the spoofer. The spoofer is using GPS satellite simulator to generate signals that are stronger than those generated by the actual satellite system, an attacker can produce false readings in the GPS to deceive vehicles to think that they are in a different location. GPS spoofing attack is potentially more hazardous than jamming because the receiver is not aware of this threat and is still providing the navigation results which seems to be reliable but they are not knowing when they are being spoofed because in GPS the communication link is not being cut or jammed but the receiver or Vehicles are receiving the false navigation results and get diverted from their trajectory by GPS Spoofing attack. So these spoofing attacks that provide misleading navigation results of the receiver is difficult to detect because of signal infrastructure. Using trivial anti-spoofing algorithms in GPS receivers, spoofing attacks can be easily detected. So here we introduce the basic idea behind GPS spoofing detection, and provide some facts to describe various aspects of the GPS spoofing detection theory using two navigators.

II. RELATED WORK

Sebastian Bittl et al "Emerging Attacks on VANET Security based on GPS Time Spoofing" discusses the overview of Attacks on VANET Security based on GPS Time Spoofing. This paper show that by spoofing the GPS time signal, an attacker can break the non-repudiation property specified in current VANET standards. Furthermore, he can force targeted ITS-Ss to accept outdated messages and PSCs. Moreover, the attacker can perform a denial of service attack on parts of a VANET. These attacks are not limited to OBUs, but affect all kind of ITS-Ss (e.g., also road side units (RSUs) [2] .
Ali Jafarnia-Jahromi et al **"**GPS Vulnerability to Spoofing Threats and a Review of Anti-spoofing Techniques**"** showing the Classification of Spoofing Generation Techniques, GPS Vulnerability against the Spoofing Attack and the Classification of Anti-spoofing Techniques[3].
Zhenghao Zhang et al "Quickest Detection of GPS Spoofing Attack**"** uses the quickest detection method of GPS spoofing signals based carrier-signal-to-noise ratio (C/No) parameter of the signals to detect the GPS spoofing attack. Firstly, we propose a monopole-patch hybrid antenna connected to two independent low cost GPS receivers. The GPS signals from these two receiving paths are fed to two independent processing units. The differences of the carrier-signal-to-noise ratio(C/No) from these two receiving paths can be used as a statistic for the quickest detection algorithm [4].

Larisa Dobryakova et al "Design and analysis of spoofing detection algorithms for GNSS signals" describes a general approach to anti-spoofer design. We consider the algorithm of spoofing detection based on the analysis of the satellite signal for civilian use of Dual-Receiver. . A real-time method for detecting GNSS spoofing in a narrow-bandwidth civilian GNSS receiver is still being developed. The ability to detect a

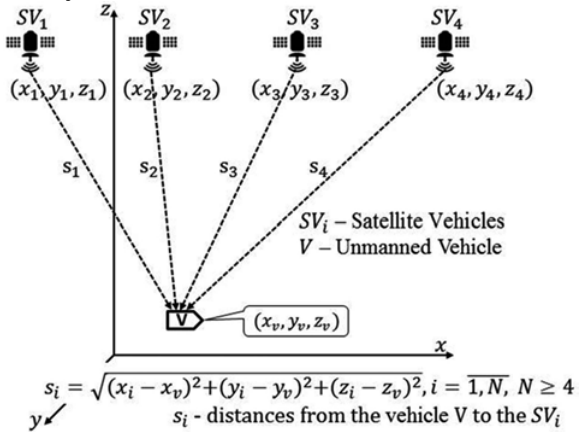
spoofing attack is important for reliability of systems ranging from cell-phone towers, the power grid, and commercial fishing monitors. It is used to characterize spoofing effects and to develop ways of defence against civilian spoofing [5].

Guangteng Fan et al "A Spoofing Detection Method for Motion Receiver using Single Antenna" is using is using the Spoofing detection method for motion receivers using single antenna. The direction of arrival (DOA) technique is the most effective mean of spoofing detection, but it is high hardware complexity and cannot be applied to motion vectors. This method uses the difference of distance between GPS satellites and spoofers to the receivers, and makes the detection by carrier phase double-difference which only needs single antenna [6].

Larisa Dobryakova et al **"**The main scenarios of Gnss spoofing and corresponding spoofing detection algorithms" represents the various GPS Spoofing scenarios and the corresponding Detection Algorithm. Many civil GNSS (Global Navigation Satellite System) applications need secure, assured information for asset tracking, fleet management and the like. But there is also a growing demand for geo-security location based services. Unfortunately, GNSS is vulnerable to malicious intrusion and spoofing. A spoofer can transmit its counterfeit signals from a stand-off distance of several hundred meters, or it can be co-located with its victim. The paper also considers the algorithm of spoofing detection based on the analysis of the satellite signal for civilian use of Dual-Receiver . During the operation, the algorithm compares the distance of received signals from two receivers [7].

III. THE BASIC IDEA OF NAVIGATION

GPS positioning is based on the process of determining absolute or relative locations of vehicles or person by measurement of distances, using the geometry of circles, spheres or triangles. At a minimum this process requires 3 ranges to 3 known points but here GPS positioning uses the 4 "pseudo ranges" to 4 satellites to get more accurate results. The Navigation Message includes a broadcast ephemeris from which the receiver can compute satellite coordinates (X,Y,Z) as shown in fig(1). These are Cartesian coordinates in a geocentric system, which has its origin at the Earth centre of mass, Z axis pointing towards the North Pole, X pointing towards the Prime Meridian (which crosses Greenwich) and Y at right angles to X and Z to form a right-handed orthogonal coordinate system [8-9].



Fig(1)

The Time at which the signal is transmitted from the satellite is encoded on the signal, using the time according to an atomic clock onboard the satellite. Time of signal reception is recorded by receiver using an atomic clock. The real range Si from the Satellite Vehicles SVi to the vehicle S is

$$s_i = ct_i,\ i = 0\text{-}N-1 \quad (1)$$

Where c is the speed of light (in a vacuum) = 299.792 458 km/s, ti — real time of GPS signal propagation from the SVi to the vehicle S, which is unknown. A receiver measures pseudo range Si from the Satellite Vehicles SVi to the vehicle S as:

$$\rho i = c\,(T_{\downarrow i} - T_{\uparrow i} + \Delta t),\ i = 0,\ N-1 \quad (2)$$

Where $T\uparrow i$ — is the reading of the Satellite Vehicles SVi clock when the signal was transmitted; $T\downarrow i$ — is the known reading of the receiver clock when signal of SVi is received; Δt – the receiver clock bias (error in the measurement of time aboard vehicle S).

From Pythagoras Theorem, we can write the range from the SVi to the vehicle V as

$$\sqrt{(xi - xv)2 + (yi - yv)2 + (zi - zv)2} = c\,(T_{\downarrow i} - T_{\uparrow i} + \Delta t),\ i = 0\text{-}N-1 \quad (3)$$

Or if N=4 we can write

$$\begin{aligned}
&\sqrt{(X0 - Xv)2 + (Y0 - Yv)2 + (Z0 - Zv)2} = c(T_{\downarrow 0} - T_{\uparrow 0} + \Delta t)\\
&\sqrt{(X1 - Xv)2 + (Y1 - Yv)2 + (Z1 - Zv)2} = c(T_{\downarrow 1} - T_{\uparrow 1} + \Delta t)\\
&\sqrt{(X2 - Xv)2 + (Y2 - Yv)2 + (Z0 - Zv)2} = c(T_{\downarrow 0} - T_{\uparrow 0} + \Delta t)\\
&\sqrt{(X3 - Xv)2 + (Y3 - Yv)2 + (Z3 - Zv)2} = c(T_{\downarrow 0} - T_{\uparrow 0} + \Delta t) \quad (4)
\end{aligned}$$

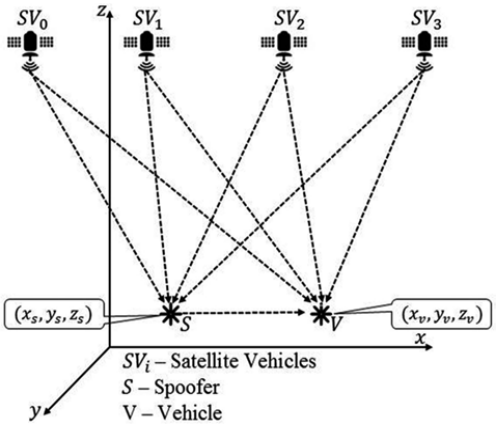
Processor of GPS navigator solves the system of equations (4), compute the position of the vehicle (x_v, y_v, z_v) and error in the measurement of time aboard vehicle Δt, that to use it as a clock correction of the GPS navigator [8-9].

IV. THE MAIN SCENARIO OF GPS SPOOFING

Spoofer receives signals from the SVi, introduces additional delays τi, amplifies signals and sends this signals by the transmitting antenna in the direction of the vehicle S (in the direction of the victim) as shown in fig(2). In this case, the system takes the form

$$\begin{aligned}
&\sqrt{(X0 - Xv)2 + (Y0 - Yv)2 + (Z0 - Zv)2} = c(T^{s}_{\downarrow 0} - T_{\uparrow 0} + \Delta t)\\
&\sqrt{(X1 - Xv)2 + (Y1 - Yv)2 + (Z1 - Zv)2} = c(T^{s}_{\downarrow 1} - T_{\uparrow 1} + \Delta t)\\
&\sqrt{(X2 - Xv)2 + (Y2 - Yv)2 + (Z0 - Zv)2} = c(T^{s}_{\downarrow 0} - T_{\uparrow 0} + \Delta t)\\
&\sqrt{(X3 - Xv)2 + (Y3 - Yv)2 + (Z3 - Zv)2} = c(T_{\downarrow 0} - T_{\uparrow 0} + \Delta t) \quad (5)
\end{aligned}$$

Where $T{\downarrow}is{=}T{\downarrow}i{+}\ \tau i$, i = 0-3 is the known reading of the receiver clock when signal of spoofer is received.
Processor of GNSS navigator solves the system of equations (5), compute the false position of the vehicle (x_v,y_v,z_v) and error in the measurement of time aboard vehicle Δt.



Fig(2)

V. THE SPOOFING DETECTING USING TWO NAVIGATORS

Assume that navigator $N1$ located at a distance $D1$ from the spoofer and processor of navigator $N1$ solves the system of equations (5), compute the false position of the vehicle $(x_1{}^f,y_1{}^f,z_1{}^f)$ and error in the measurement of time aboard vehicle Δt. Assume also that navigator $N2$ located at a distance $D2$ from the spoofer and processor of navigator $N2$ solves the system of equations (5), compute also the false position of the vehicle $(x_2{}^f,y_2{}^f,z_2{}^f)$ and error in the measurement of time aboard vehicle Δt. If we designate

$$\Delta D{=}D1{-}D2 \qquad (6)$$

The system of equations (5) for navigator N2 can be written as

$$\begin{aligned}
&\sqrt{(\mathrm{X0}-\mathrm{Xv})2+(\mathrm{Y0}-\mathrm{Yv})2+(\mathrm{Z0}-\mathrm{Zv})2} = c(T^{s}{}_{\downarrow 0}-T_{\uparrow 0}+\Delta t+\Delta D/c)\\
&\sqrt{(\mathrm{X1}-\mathrm{Xv})2+(\mathrm{Y1}-\mathrm{Yv})2+(\mathrm{Z1}-\mathrm{Zv})2} = c(T^{s}{}_{\downarrow 1}-T_{\uparrow 1}+\Delta t+\Delta D/c)\\
&\sqrt{(\mathrm{X2}-\mathrm{Xv})2+(\mathrm{Y2}-\mathrm{Yv})2+(\mathrm{Z0}-\mathrm{Zv})2} = c(T^{s}{}_{\downarrow 0}-T_{\uparrow 0}+\Delta t+\Delta D/c)\\
&\sqrt{(\mathrm{X3}-\mathrm{Xv})2+(\mathrm{Y3}-\mathrm{Yv})2+(\mathrm{Z3}-\mathrm{Zv})2} = c(T_{\downarrow 0}-T_{\uparrow 0}+\Delta t+\Delta D/c) \qquad (7)
\end{aligned}$$

In this case, the processor of navigator $N2$ solves the system of equations (6), compute the false position of the vehicle $(x_2{}^f,y_2{}^f,z_2{}^f)$ $=(x_1{}^f,y_1{}^f,z_1{}^f)$ and error in the measurement of time aboard vehicle $\Delta t+\Delta D/c$.
Comparing (4), (5) and (7), we can write

$$(x_v,y_v,z_v)= (x_2{}^f,y_2{}^f,z_2{}^f) = (x_1{}^f,y_1{}^f,z_1{}^f)$$

And it means that all GNSS navigation systems, which are under the influence of signals from the spoofer, determine the same false coordinates and therefore the measured distance between the navigators should approach zero

$$\Delta D_{1\text{-}2}= ((x_1{}^f-x_2{}^f)^2+(y_1{}^f-y_2{}^f)^2+(z_1{}^f-z_2{}^f)^2)^{1/2} \approx 0$$

This property is the basis of the decision rule system for GPS spoofing detection.

VI. CONCLUSION

Since there are various methods of spoofing detection, here in this approach we are using two navigators on a single vehicle and there are two processors for these navigators to solve the various equations of navigation based on the distance between the two navigators and the various satellites. Based on this property we are able to make decision whether the signals are spoofed or original signals. This method helps us to detect the spoofing attack if present in that particular are and hence provide the safety in the transportation of the VANET.

VII. REFERENCES

[1]. Bariah, L., Shehada, D. Salahat, E., & Yeun, C. Y. (2015). Recent Advances in VANET Security: A Survey.

[2]. Bittl, S., Gonzalez, A. A., & Myrtus, M. (2015). Emerging Attacks on VANET Security based on GPS Time Spoofing, 344–352.

[3]. Jafarnia-jahromi, A., Broumandan, A., & Nielsen, J. (2012). GPS Vulnerability to Spoofing Threats and Review of Anti-spoofing Techniques, 2012.

[4]. Zhenghao Zhang, Matthew Trinkle, Lijun Qian, and Husheng Li (2013). Quickest Detection of GPS Spoofing Attack, 1-6.

[5]. Dobryakova, L., Lemieszewski, Ł., & Ochin, E. (2014). Zeszyty Naukowe Design and analysis of spoofing detection algorithms for GNSS signals, 40(112), 47–52.

[6]. Fan, G., Huang, Y., Zhang, G., Nie, J., & Sun, G. (2015). A Spoofing Detection Method for Motion Receiver Using Single Antenna, (Iccsnt), 1433–1436.

[7] Conference, T., Systems, T., Dobryakova, L., & Ochin, E. (2013). The main scenarios of gnss spoofing and corresponding spoofing detection algorithms, 1–10.

[8] B. W. Parkinson and J. J. Spiker Jr., 1996, Global Positioning System: Theory and Applications, American Institute of Aeronautics and Astronautics, Inc.

[9] B.Hofmann-Wellenhof, H. Lichtenegger and J. Collins, GPS Theory and Practice, fifth edition, SpringerWien New York, 2001.