Analysis and Application of Distributed Navigation Spoofers

Chao Ma¹, Jun Yang¹* and Chao Zhou¹

¹ College of Intelligence Science and Technology, National University of Defense Technology, Changsha, 410073, China

*mcmtwjyy@gmail.com

Abstract. As a typical aerospace technology application, Global Satellite Navigation System (GNSS) affects the national Positioning Navigation Timing (PNT) service. However, not all users are making good use of GNSS. In recent years, the most prominent phenomenon is the Unmanned Aerial Vehicle (UAV) “black flight”, which seriously affects the normal operation of civil aviation. To solve such problem, navigation spoofing can be used as an effective method to disrupt the flight of malicious UAVs. Currently, a centralized antenna is the most common way to transmit false navigation signals, but when the target receiver contains two receiving antennas or spatial filtering technology, this spoofing method is ineffective. Therefore, we aim at the distributed spoofers that each antenna emits a false navigation signal, and point out that this sophisticated attack will become the development trend of navigation spoofing in the future.

1. Introduction

The low power and openness of civil navigation signals make them vulnerable to interference or spoofing. In 2002, Warner and Johnston conducted the first GPS spoofing experiment by using a navigation signal simulator [1]. This test has shown that a hand-held GPS civilian receiver inside a truck can be kept locked on false navigation signals at a distance of no more than 30 feet. In 2008, Prof. Todd modified the GRID receiver to design a real navigation spoofer [2], and conducted spoofing experiment [3-5]. In 2006, Mark and Todd systematically concluded the types and methods of navigation spoofing [6].

Navigation spoofer can be divided into three categories: simplistic, intermediate and sophisticated. Among them, intermediate spoofer is the most widely used. The characteristic is the “Receiver-Spooper” structure. The function of Receiver is to transmit the space-time system of real navigation satellites to the spoofer by a commercial navigation chip, and the spoofer uses an antenna to transmit the simulated constellation to the target receiver. However, this type of spoofer can be effectively detected by spatial filtering methods such as antenna array [7]. So it is necessary to design sophisticated spoofer to solve this problem. The sophisticated spoofer is based on distributed antennas, so we regard this spoofer as distributed navigation spoofer.

The next section covers navigation basics and three types of distributed navigation spoofer. Section 3 discusses key technologies and considerations. Section 4 simulates distributed navigation spoofers and gives some conclusions.
2. Navigation, spoofing and sophisticated spoofer design

2.1. Satellite navigation basics
The navigation signal belongs to the spread spectrum signal, which is divided into three signal levels: carrier, pseudo-code and date code. The data code and pseudo-code perform an exclusive or operation to realize spread spectrum. The combined code then modulates the carrier through Binary Phase Shift Keying (BPSK). Taking Global Positioning System (GPS) as an example \[8\], without considering P(Y) code, the navigation signal issued by卫星 can be expressed as

\[
s^{(i)}(t) = A(x^{(i)}(t)D^{(i)}(t))\sin(2\pi ft + \theta)
\]

(1)

Where \(A\) is the signal amplitude. \(x^{(i)}(t)\) is the C/A code of satellite \(i\). \(D^{(i)}(t)\) is the data code. \(f\) and \(\theta\) are carrier frequency and initial phase respectively.

The target receiver calculates the pseudorange and satellite position from the navigation signal, and obtains the self-position and time results by solving the following four-element nonlinear equations \[8\]:

\[
\sqrt{(x^{(1)} - x)^2 + (y^{(1)} - y)^2 + (z^{(1)} - z)^2} + \delta t_u = \rho_c^{(1)}
\]

\[
\sqrt{(x^{(2)} - x)^2 + (y^{(2)} - y)^2 + (z^{(2)} - z)^2} + \delta t_u = \rho_c^{(2)}
\]

\[
\vdots
\]

\[
\sqrt{(x^{(N)} - x)^2 + (y^{(N)} - y)^2 + (z^{(N)} - z)^2} + \delta t_u = \rho_c^{(N)}
\]

(2)

Where \([x, y, z]^T\) is the coordinate vector of the target receiver. \([x^{(i)}, y^{(i)}, z^{(i)}]^T\) is the coordinate vector of the satellite \(i\). \(\rho_c^{(i)}\) the pseudorange after correction. \(\delta t_u\) is the clock error. Changing user positioning results can be realized by changing satellite positions or pseudoranges, and the common part of pseudoranges affects timing results.

2.2. Definition and Goal of navigation spoofing
Navigation spoofing refers to the process that makes errors in the position or time information of the target receiver by false navigation signal of replaying or self-generating. From the view of application, the goal of navigation spoofing can be divided into two types:

- \(G1\): The accuracy of the receiver positioning (or timing) is reduced by navigation spoofing. Standard Positioning Service (SPS) cannot be satisfied.
- \(G2\): The receiver positioning (or timing) is mistakenly locked to the designated point. When the receiver is installed in a vehicle such as UAV, the goal of navigation spoofing can also be defined that the vehicle is mistakenly lured to the designated area.

2.3. Design of distributed navigation spoofer
The distributed navigation spoofer takes “Receiver-spoof” structure as the basic unit. The platform such as UAV, hot air balloon, base station or low-orbit satellite can be used as carrier to realize the false constellation design in figure 1. Different platform equipped with basic unit is called as a node. Three distributed navigation spoofers are proposed based on this structure.

- Independent: node \(i\) uses the C/A code of real satellite \(j\), and the navigation messages are filled according to the own simulated satellite motion. It can be seen that this kind of spoofer is treated as an independent navigation constellation for spoofing.
- Hybrid: node \(i\) uses the C/A code and the navigation messages of real satellite \(j\).
- Duplicated: node \(i\) uses the C/A code and the navigation messages of real satellite \(j\), and compensates pseudorange. Compared with Hybrid spoofer, the duplicated spoofer only treats the node
as a relay station. For the target receiver, the node is basically transparent. The characteristics of different spoofers are illustrated in table 1.

![Sophisticated spoofer structure](image)

**Figure 1.** Sophisticated spoofer structure.

**Table 1.** Comparison of three distributed navigation spoofers.

|                         | Independent | Hybrid  | Duplicated |
|-------------------------|-------------|---------|------------|
| Implementation complexity| Intermediate| Low     | High       |
| Spoofing goal           | $G1, G2$    | $G1$    | $G1, G2$   |
| Detection probability   | Easy        | Hard    | Intermediate|
| Dilution of precision (DOP)| Decided by nodes | Decided by real satellites | Decided by real satellites |
| Recommended carrier     | Low-orbit satellites or high-speed aircraft | none       | Low-speed stabilized platform |

3. Key technologies and considerations of distributed navigation spoofer

3.1. **Compensation for pseudorange and doppler frequency**

Depending on the different spoofer types, the node needs to decide whether to do pseudorange or Doppler frequency compensation. We arrange them as shown in table 2.

**Table 2.** Compensation for pseudorange and doppler frequency.

|                         | Independent | Hybrid  | Duplicated |
|-------------------------|-------------|---------|------------|
| Pseudorange compensation| ×           | ×       | √          |
| Doppler compensation    | ×           | √       | √          |

Pseudorange offset is compensated by delay filter [9] or ephemeris modification [10]. The offset value $\Delta D$ can be expressed as

\[ \Delta D = r_{AC} - r_{BC} - c \cdot \Delta T_B \] (3)
Where $r_{AC}$ and $r_{BC}$ are the geometric distances between AC and BC respectively in figure 1. $c$ is the speed of light. $\Delta T_b$ is the transmission delay required for each node to transmit, receive and process.

Doppler frequency offset is compensated by Numerically Controlled Oscillator (NCO). The offset value $\Delta f$ can be expressed as

$$\Delta f = \frac{f_{L1}}{c} \left( (v_A - v_c) \cdot \hat{I}_{AC} - (v_A - v_b) \cdot \hat{I}_{AB} - (v_b - v_c) \cdot \hat{I}_{BC} \right) \quad (4)$$

Where $f_{L1}$ is the carrier frequency. $(v_i - v_j) \cdot \hat{I}_o$ is the vector projection of the velocities of $i$ and $j$ point along the line of $ij$. $c$ is the speed of light.

### 3.2. Influence factors on the spoofing accuracy of the target receiver

For the target receiver, the positioning/timing accuracy can be expressed as the product of DOP factor and User-Equivalent Range Error (UERE). DOP is determined by the geometric relationship between satellites and the receiver. UERE is the equivalent error of different errors in space. Under the condition of the distributed navigation spoofer, UERE will be greatly affected by time synchronization between nodes.

#### 3.2.1. The effect of time synchronization between nodes

Compared with the real navigation constellation, each node of the distributed navigation spoofer does not have a unified time system because there is no highly stable atomic clock. And this factor will seriously affect the spoofing accuracy.

The typical UERE budget for a single frequency receiver is shown in table 3 [8]. Different types of distributed navigation spoofer will introduce new errors. For example, each node of the independent spoofer uses navigation chip to complete positioning and timing, so the positioning result affects the broadcast ephemeris, and the timing result affects the broadcast clock in table 3. The positioning/timing errors of the hybrid/duplicated spoofer can be expressed by the equivalent range error to join in table 3. It is worth mentioning that the timing accuracy of commercial receiver is about 20 ns at present, and it can reach 10 ns with timing receivers. When we adopt Real-Time Kinematic (RTK) or Precise Point Positioning (PPP) technology, the timing accuracy can reach 2-5 ns.

#### Table 3. GPS Standard Positioning Service typical UERE budget.

| Segment Source | Error Source | $\sigma$ Error (m) |
|----------------|--------------|--------------------|
|                | Broadcast clock | 1.1 (Independent) |
| Space/control  | L1 P(Y) - L1 C/A group delay | 0.3 |
|                | Broadcast ephemeris | 0.8 (Independent) |
|                | Ionospheric delay | 7.0 |
|                | Tropospheric delay | 0.2 |
| User           | Receiver noise and resolution | 0.1 |
|                | Multipath | 0.2 |
|                | Equivalent range error | Hybrid, Duplicated |
| System UERE    | Total (RSS) | 7.1 |

#### 3.2.2. DOP selection

The independent spoofer as an standalone system, DOP can be determined by itself. The nodes’ constellation can be arranged by numerical analysis or intelligent algorithm [11-13]. For the hybrid and duplicated spoofer, DOP is determined by the real navigation constellation. When the number of nodes is not consistent with the number of visible satellites, an exhaustive method or k-means clustering algorithm [14] can be adopted to select visible satellites to ensure the DOP does not decrease obviously.
3.2.3. Isolation of reception and transmission. A serious problem faced by the “Receiver-Spoofing” structure in the practical application is the isolation of receiving and transmitting navigation signals. Each node must ensure that it does not affect the reception of real navigation signals while emitting spoofing signals. The isolation technologies mainly include:

- Time division of reception and transmission: the receiving and transmitting time of each node is completely independent. Because the receiving time of real satellite signals is generally within a few minutes, it is feasible to apply this method.
- Reducing receiving sensitivity and transmitting power control: since the distributed navigation spoofer is usually in the air, reducing the sensitivity of the receiving of each node will not improve the missed detection rate obviously, and the transmitting power can be appropriately reduced according to the specific scene.
- Space isolation technology: Spiral or horn antenna is used to improve antenna directivity, or physical isolation medium is added to reduce antenna coupling.

4. Simulation analysis and conclusion
Using the Satellite Tool Kit (STK) and MATLAB, three distributed navigation spoofer are simulated in typical scenarios. A typical scenario:
- Time: 8 a.m. on July 3, 2019.
- The effective coverage area for target receivers: 1×1 km². The longitude and latitude coordinate of the center: 112.997620, 28.217295.
- The antenna elevation angle of target receivers: 30°. The number of visible satellites is 8.

4.1 The independent spoofer
The orbital elements of real satellite are modified to make it conform the low-orbit satellite motion. Using dual-frequency commercial or timing receiver applies on each node [15-16], UERE budget is obtained as shown in table 4. The positioning errors in the coverage area are shown in figure 2. If the spoofer can make the target coincide with the real position, it would be feasible to get the target anywhere by reasonably varying pseudoranges. So the positioning errors are the differences between the spoofing positioning results and the real target positions. This type of spoofer can achieve navigation spoofing for multiple targets. However, the spoofing accuracy is lower than SPS because the positioning/timing accuracy of each node is limited.

| Table 4. UERE budget of the independent spoofer. |
|------------------------------------------------|
| Segment Source                  | Error Source               | 1σ Error (m) | 1σ Error (m) |
|---------------------------------|-----------------------------|--------------|--------------|
| Space/control                   | Broadcast clock             | 6.1          | 3.2          |
|                                 | L1 P(Y) - L1 C/A group delay| 0.3          | 0.3          |
|                                 | Broadcast ephemeris         | 3.1          | 2.1          |
| User                            | Ionospheric delay           | 0.2          | 0.2          |
|                                 | Tropospheric delay          | 0.2          | 0.2          |
|                                 | Receiver noise and resolution| 0.1          | 0.1          |
|                                 | Multipath                   | 0.2          | 0.2          |
| System UERE                    | Total (RSS)                 | 6.860        | 3.856        |
4.2 The hybrid spoofer
UERE budget is expressed as shown in table 5, and the positioning errors in the coverage area are shown in figure 3. It can be seen that hybrid spoofer can only implement spoofing goal $G_1$, and the spoofing accuracy generates overall deviation within the coverage area. This is mainly determined by the relative position of each node, each satellite and the target receiver. The effect of UERE on positioning results is basically negligible.

Table 5. UERE budget of the hybrid spoofer.

| Segment Source | Error Source                  | Error (m) | Error (m) |
|----------------|-------------------------------|-----------|-----------|
| Space/control  | Broadcast clock               | 1.1       | 1.1       |
|                | L1 P(Y) - L1 C/A group delay  | 0.3       | 0.3       |
|                | Broadcast ephemeris           | 0.8       | 0.8       |
| User           | Ionospheric delay            | 0.2       | 0.2       |
|                | Tropospheric delay           | 0.2       | 0.2       |
|                | Receiver noise and resolution| 0.1       | 0.1       |
|                | Multipath                    | 0.2       | 0.2       |
|                | Equivalent range error       | 6.7       | 3.6       |
| System UERE    | Total (RSS)                  | 6.853     | 3.877     |

Figure 2. The spoofing accuracy under different UERE budget (independent).

Figure 3. The spoofing accuracy under different UERE budget (hybrid).
4.3 The duplicated spoofer

UERE budget is the same as table 5. The positioning errors in the coverage area are shown in figure 4. The pseudorange compensation can improve the spoofing accuracy, but at the same time, this type spoofer can only keep a target receiver with high spoofing accuracy. With the increasing of the relative offset to the specified target, the spoofing accuracy decreases continuously. We should be flexible in selecting distributed navigation spoofer based on specific scenarios.

![Figure 4. The spoofing accuracy under different UERE budget (duplicated).](image-url)

**References**

[1] J. S. Warner and R. G. Johnston. (2002) *A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing*. The Journal of Security Administration

[2] Humphreys TE, Ledvina BM, Tech V, et al. (2009) *Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer*.

[3] Shepard DP, Bhatti JA, Humphreys TE, Fansler AA. (2012) *Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks*.

[4] Bhatti J, Humphreys T E. (2017) *Hostile Control of Ships via False GPS Signals: Demonstration and Detection*. Navigation, 64(1):51-66.

[5] Shepard DP, Bhatti JA, Humphreys TE, Fansler AA. (2012) *Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks*.

[6] Psiaki, M. L., & Humphreys, T. E. (2016). GNSS Spoofing and Detection. Proceedings of the IEEE, 104(6), 1258-1270.

[7] Jafarnia-Jahromi A., Broumandan A., Nielsen J. and Lachapelle Gerard. (2012) *GPS vulnerability to spoofing threats and a review of antSpoofing techniques*. International Journal of Navigation & Observation.

[8] Kaplan, D. (1996) *Understanding GPS: Principles and Applications*. Artech House Publishers, Norwood.

[9] Yang, J., Chen, J. Y., Zhong, X. P., & Ming, D. X.. (2010) *High Precision Delay Satellite Navigation Signal Generation Theory and Application In Navigation Satellite Simulation Test // CSNC 2010*.

[10] Chao M., Jun Y., Jianyun C. and Yinyin T.. (2018) *Indoor and outdoor positioning system based on navigation signal simulator and pseudolites*. Advances in Space Research.

[11] BlancoDelgado, Nunes and SecoGranados. (2011) *Relation between GDOP and the geometry of the satellite constellation*. International Conference on Localization & Gnss. IEEE.

[12] Nielsen R. O.. (1997) *Relationship between dilution of precision for point positioning and for relative positioning with GPS*. IEEE Transactions on Aerospace & Electronic Systems, 33(1), 333-338.
[13] Chien-Sheng Chen. (2015) Weighted geometric dilation of precision calculations with matrix multiplication. Sensors, 15, 803-817.

[14] Kanungo T., Mount D. M., Netanyahu N. S., Piatko C. D., Silverman R. and Wu A. Y. (2002) An efficient k-means clustering algorithm: analysis and implementation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(7), 0-892.

[15] http://www.unicorecomm.com/product/content_972.html

[16] http://www.septentrio.com/products