Wireless Pers Commun (2015) 83:1955–1970
DOI 10.1007/s11277-015-2497-9

Analysis of Single Frequency GPS Receiver Under Delay and Combining Spoofing Algorithm

A. R. Baziar[1] · **M. Moazedi**[1] · **M. R. Mosavi**[1]

Published online: 11 March 2015

Abstract Global position system (GPS) has become a satellite based critical international navigation and timing system. Navigation has a significant effect in our daily life. Hence, such a commonly used system is an interesting goal for criminal utilizing. Trusting GPS navigation, need spacious knowledge to inadvertent and intentional interferences. The position deviation in GPS, which is subject to spoofing, is analyzed in this paper. Serious research into spoofing has been carried out in recent years. One of the basic requirements and major challenges in designing anti-spoofing methods and evaluating a successful GPS spoofing countermeasure is collection of actual spoofing data used to verify the proposed protection algorithm. Since actual spoofing data is acquired through an expensive spoofer-receiver device, preparing genuine spoofing data without expensive spoofing devices, including extra software or hardware, can be helpful in the development of anti-spoofing studies. In this paper, after providing a refined assessment of existing approaches, a new practical and low-cost technique is proposed that helps to generate a set of spoofing data only with the employment of software receiver and a set of real GPS measurements. In this way, a new kind of spoofing data is resulted by utilizing delay and mixing procedure. This data will be generated in victim receiver antenna, if a spoofer-receiver device is used in practice. After explanation of the spoofing algorithm, its influence on the GPS receiver is studied in details, and then validation of proposed method is proved by appropriate tests.

Keywords Analysis · GPS receiver · Delay · Combining spoofing

✉ M. R. Mosavi
m_mosavi@iust.ac.ir

A. R. Baziar
amirrezabaziar@elec.iust.ac.ir

M. Moazedi
moazedi@elec.iust.ac.ir

[1] Department of Electrical Engineering, Iran University of Science and Technology, 16846-13114 Narmak, Tehran, Iran

1 Introduction

Over the last decades, positioning, navigation and GPS-dependent systems have enjoyed a tremendous attention. Therefore, security and integrity of these systems are very important. The target in designing secure systems is to fortify a system's weakest link against predictable attacks [1]. GPS is a modern technology, but not secure. Some unavoidable error sources such as clock errors and satellite circuit displacement, limits its precision [2]. In otherwise, GPS is vulnerable to interference due to some shortcomings. Mainly, it confronts by three main attacks: blocking, jamming and spoofing [3]. The conventional precision improvement approaches [4–7] can't encounter these attacks. Spoofing is more sinister than others, owing to the fact that the targeted receiver is unaware and so cannot warn users that its navigation solution is untrustworthy. Since, the adversary can emit signals identical to those sent by satellites and so mislead the receiver. In general, vulnerability of GPS is mainly owing to radio navigation system, weak GPS signal strength on the earth and openness of technical data of GPS, plus good stability and predictability of signal [8]. These problems provide specified opportunity for spoofers to generate and replace the counterfeit signals such that the targeted receiver cannot detect. However, the spoofing signal during the attack and after that makes some effects which can be detected and compensated by precisely investigating.

Because of different spoofing kinds, there are various countermeasures. In other words, each anti-spoofing technique has relevance to a special type of spoofing. As a result, it is necessary to go through the exercise of providing civil GPS spoofing. This allows researchers to explore the range of practical spoofing techniques, and so determine hard and easy aspects of spoofing to perform in real world. With this information, the difficulty of mounting a spoofing attack can be more accurately evaluated and receiver developers can prioritize their spoofing defenses by choosing countermeasures that are effective against easily-implementable spoofing techniques.

During past decade, numerous reports have been published for spoofing [9–16], detection [14–23] and mitigation of spoofing [14–18] approaches. In this paper, after studying different techniques a new spoofing scenario will be proposed. Section 2 reviews and explains former proposed spoofing techniques and practical samples of them. In the next section, the developed method will be reported. Section 4 relates simulations and test results to examine the suggested approach. Finally, Sect. 5 states the conclusion.

2 Review of Spoofers

Spoofing threats can be classified into three main groups: simplistic, intermediate and sophisticated spoofers. The discussion in the remainder of this section pertains to a complete review of spoofers.

2.1 Simplistic

This group encompasses a spoofer that simply attaches a power amplifier and an antenna to a GPS signal simulator and radiates the RF signal toward the target receiver. This can produce GPS signals, but cannot make them synchronize with the current broadcast GPS signals. However, if the adversary signals power be greater than the legitimate signals power, misleading commercial receivers would be possible [14].

Despite the ease of mounting a spoofing attack with a signal simulator, there are some drawbacks. One is cost and another is size. Hiding the simulator is another challenge [9]. The threat posed by a simulator-based spoofing attack is diminished by the fact that detecting such an attack appears to be easy, since synchronizing a simulator's output with the actual GPS signals in its vicinity is difficult. An unsynchronized attack may cause the victim receiver to lose lock and have to sustain a partial or complete reacquisition. Such a forced reacquisition would raise suspicion of a spoofing attack and nevertheless likely lead to an abrupt change in the victim receiver's GPS time estimate. The victim receiver could fag jumps of more than 100 ns, as evidence of possible spoofing. The presence of 100 s of counterfeit GPS signals may confuse the receiver's acquisition and hand off-to-track logic or may deny the receiver navigation entirely [15].

An extension to the traditional GPS signal simulator is a signal generator that transmits more GPS signals than the number that is expecting to see at the receiver's antenna. In opposition to the claimed low possibility of attacks that use simplistic spoofers, the ease of organizing such an attack, the abundance of information on GPS hardware and software signal simulators, besides the potential for navigation confusion or denial of navigation make this type of attack attractive to those whom wish to cause mischief or harm. Thus, this mode of attack can be described as one that generates navigation confusion or denial of navigation, depending on how the receiver deals with the multiplicity of signals. GPS signal simulators are decreasing in cost and becoming more available.

A successful experiment using this type of attack is described in Ref. [24] in 2002, by transmitting a sufficiently powerful signal that interferes with and obscures the GPS signals. The attacker has to first force the receiver to lose its lock on the satellite signals. This can be also achieved by jamming legitimate GPS signals. They placed the simulator, desktop PC and the computer monitor in the cab of a truck. The antenna was attached to the grill of the truck. If the equipment could broadcast a stronger signal, spoofing over a greater distance will be possible.

In summary, the ease of mounting an attack via GPS signal simulator makes this attack mode relatively relevant. However, the mere fact that a simplistic attack is easy to defend does not increase security. A gaping vulnerability will remain until civil GPS receivers at least are equipped with the elementary anti-spoofing techniques required to detect a simulator-type attack.

2.2 Intermediate

The second group synchronizes its counterfeit GPS signals with authentic ones, such that the fake signals can more-easily masquerade as genuine ones. The receiver-spoofer can be made small enough to be placed inconspicuously near the target receiver's antenna. The receiver component draws in legitimate GPS signals to estimate its own position, velocity, and time. Due to proximity, these apply to the victim antenna. Based on these estimates, the receiver-spoofer then generates counterfeit signals and generally orchestrates the spoofing attack. The receiverspoofer could even be placed rather distant from the target receiver if the target was stationary, and its position relative to the receiver-spoofer had been pre-surveyed.

One of the main challenges that must be overcome to carry out a successful spoofing attack is to gain position and velocity of the target receiver antenna. This knowledge is required to precisely position the counterfeit signals relative to the genuine signals at the target antenna. Without such information, a spoofing attack is easily recognized.

2.2.1 Replay/Meaconing

The simplest way to make an intermediate spoofing, tested in 2008 first time, is to receive legitimate GPS signals at one location and relays to another location without any modification [16]. This way the adversary can avoid detection if cryptography is employed, while it can "present" a victim with GPS signals that are not normally visible at the victim's location. The replay attack is characterized by two features: (1) the adversarial node capability to receive, record and replay GPS signals and (2) the delay between reception and retransmission of a signal. The spoofed signal can also be generated by manipulating and rebroadcasting actual signals, called meaconing.

2.2.2 Synchronized

As above mentioned, the primary difficulty in carrying out a spoofing attack is determining the 3-D vector to the target receiver's antenna. An attack via a receiver-spoofer overcomes this difficulty by construction. The receiver-spoofer is able to synchronize its signals to GPS time and align the counterfeit and genuine signals by virtue of its proximity to the target antenna. Agile control over signal amplitude, GPS timing, navigation data bits and code-phase alignment makes attacks by this receiver-spoofer difficult to detect. A practical sample of this attack is made by Humphreys and his colleagues in 2008 [15]. Indeed, this was extended of Cornell GRID receiver [25]. Each channel of the target receiver is brought under control of the receiver-spoofer. The counterfeit correlation peak is aligned with the peak corresponding to the genuine signal. The power of the counterfeit signal is then gradually increased. Eventually, the counterfeit signal gains control of the delay-lock-loop tracking points that track the correlation peak and consequently a false navigation solution is generated. An attack via portable receiver-spoofer could be more difficult to detect against than the simplistic spoofer. In addition, the electromagnetic radiation emitted from the spoofer's antenna can be targeted in a narrow beam, further complicating detection. Unsurprisingly, this fact along with the need for sub-cm-level knowledge of the target receiver's antenna location is challenging, make the likelihood of coordinated attacks with such a device relatively low [13–15].

2.3 Sophisticated

The third spoofer group is most sophisticated and effective one, which is the synchronous attack that coordinates not only its signals with the current broadcast signals, but also with the counterfeit GPS signals of other nearby spoofers. In other words, a sophisticated attacker contains several receiver-spoofer devices sharing a common reference oscillator and communication link, with each device mounted to one of the target receiver's antennas. It is worth to note that the angle-of-arrival defense fails under this attack scenario.

Naturally, this attack inherits nearly all challenges of mounting a single receiver-spoofer attack, with the additional expense of multiple receiver-spoofers and the additional complexity, since the perturbations to the incoming signals must be phase coordinated. However, carrier phase alignment and synchronizing the spoofing arrays is possible only for a bounded region around the target receiver. Moreover, physical limitations for placing the spoofer antenna toward the victim receiver made implementation of these attackers so hard and impossible in some cases because of target receiver's motion [13, 14].

3 Proposed Delay and Mixing Mechanism

In most cases to generate spoofing signals, complicated softwares and devices or not easily accessible simulators are used. Saving and delaying the authentic signal is earlier investigated [10]. By expanding this idea, counterfeit signal is generated from the collected data set. At the beginning, the input signal is sampled for a specific period and after delaying as a proper time, combined by the real signals. Actually, the delay and combine procedure construct the counterfeit signal by combining the main and delayed signal. However, in other spoofing scenarios the fake signal contains only one signal. The L1 signal, transmitted from GPS satellites is described in this equation [8]:

$$S_{L1}(t) = A_P P_i(t) W(t) D_i(t) \cos(\omega_{L1}(t + \Delta t) + \varphi_{L1}) + A_C C_i(t) D_i(t) \sin(\omega_{L1}(t + \Delta t) + \varphi_{L1}) \tag{1}$$

where A_P is amplitude of P code, $P_i(t)$ is the P code of i-th PRN, $W(t)$ is cryptographic code, $D_i(t)$ is the i-th PRN navigation message, ω_{L1} is the angular frequency of L1 signal, φ_{L1} is L1 signal phase, A_C is C/A code amplitude, $C_i(t)$ is i-th PRN C/A code and $\Delta t$is satellite signal spreading delay. As it can be noted that the first part of the equation is accessible only for military GPS receivers. Ignoring spreading delay, processed signal in civil GPS receivers can be written as follows:

$$S_{L1_{CA}}(t) = A_C C_i(t) D_i(t) \sin(\omega_{L1}(t) + \varphi_{L1}) \tag{2}$$

Assuming this equation as authentic signal, constructed counterfeit signal by delay and combination procedure can be written as:

$$\begin{aligned} C_{L1_{CA}}(t) = {} & A_C^A C_i^A(t) D_i^A(\mathrm{t}) \sin\left(\omega_{L1}(\mathrm{t} - \Delta t_A) + \varphi_{L1}^A\right) \\ & + A_C^D C_i^D(\mathrm{t}) D_i^D(\mathrm{t}) \sin\left(\omega_{L1}(\mathrm{t} - \Delta t_D) + \varphi_{L1}^D\right) \end{aligned} \tag{3}$$

where the A and D footers respectively present the authentic and delayed signal. The Eq. (3) is indeed spreading signal as spoofing. For generating this signal we need to save the authentic signal. Then, this signal that demonstrates as delayed one will be combined with the authentic one. After providing and transmitting the fake signal, the received signal by the victim receiver can be expressed as:

$$R_{L1_{CA}}(t) = S_{L1_{CA}}(t) + C_{L1_{CA}}(t) \tag{4}$$

For negating the authentic signal in the GPS receiver, the power of the constructed counterfeit signal can be increased [15, 22]. Neglecting Δt_A the Eq. (4) can be corrected as:

$$R_{L1_{CA}}(t) \approx C_{L1_{CA}} \tag{5}$$

As mentioned above, spoofing signal power is adjusted greater than the authentic one in order to successfully mislead the target receiver [12]. Since power of received GPS signal is low on the surface of the Earth [8], spoofing signal power can be simply adjusted higher than the authentic one in order to prevent easy detection [21]. In summary, spoofing data is generated in four steps:

Step 1: Saving the authentic GPS signal as a delayed signal and estimating its power level.

Step 2: Combining the delayed and authentic signal.

Step 3: Adjusting the combined signal power proportional to estimated power level in step 1.
Step 4: Spreading the constructed counterfeit signal toward the target receiver.

We suppose that the counterfeit signal is the dominant term in the input signal and the victim receiver tracks only the spoofing signals. The block diagram of the total implemented system is demonstrated in Fig. 1. In fact, the spoofing scenario causes to change the preamble bits at beginning of the navigation message sub-frame. So, the sub-frames are changed and a new navigation bits are generated. This lead to variation of TOW and satellite clocks correction, so the satellite's pseudo-range and position are changed extremely. As can be shown in Fig. 2, the geometry position of the target receiver is deviated in this way. Updating rate of HOW every 6 s is the main reason of excessive satellite position deviation. As it is known, HOW is the first 17 bits of TOW [26].

4 Performance Analysis and Test Results

In the delay and combine procedure, two parameters are effective: delay time and amplitude of delayed signal. For validation of the proposed algorithm, four different data sets are investigated. Changing the delay time and amplitude of counterfeit signal conduces to different data sets. This section presents some test scenarios that have been used for evaluating the performance of suggested algorithm.

At first, we saved the authentic signal during a specified time used in each test. After some preprocessing, it is combined by the authentic signals in different delays. Then, the mixed signal transmits to the target receiver. Preprocessing concludes adjusting the delayed signal amplitude proportional to the current scale in each scenario to combine signals.

Also, it is worth to note that difference between the authentic and delayed signal in every two continuous sample is approximately 17 ms. In other words, if in the n-th sample difference between the authentic and delayed signal is 1 s, in the (n+1)-th sample the delay will be 1 s and 17 ms. In all tests, the received spoofing signal in the target receiver and its counterpart authentic signal were analyzed in personal computer by Matlab software [26]. Finally, the position errors due to spoofing are reported in details.

Case A. $A_C^D = A_C^A$

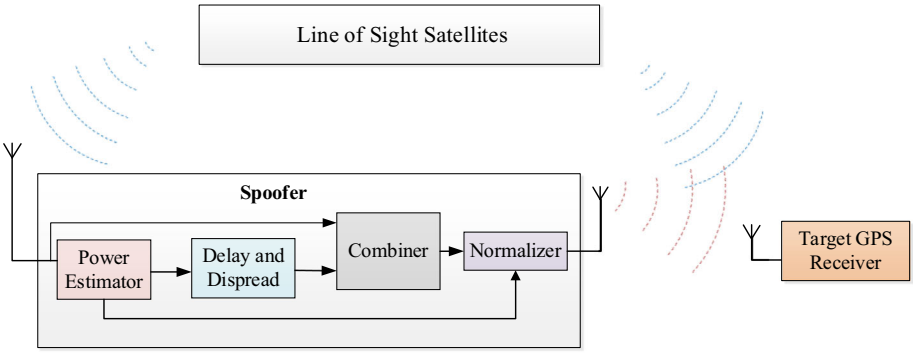

Fig. 1 Total implemented system

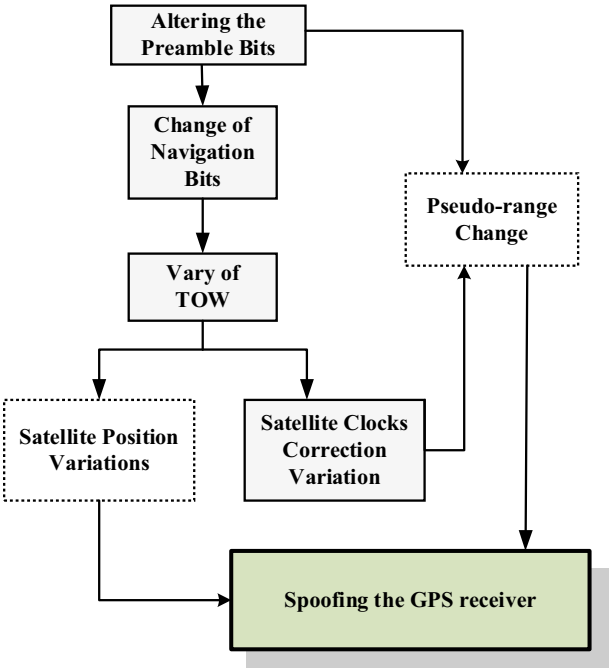

Fig. 2 Effects of spoofing signal

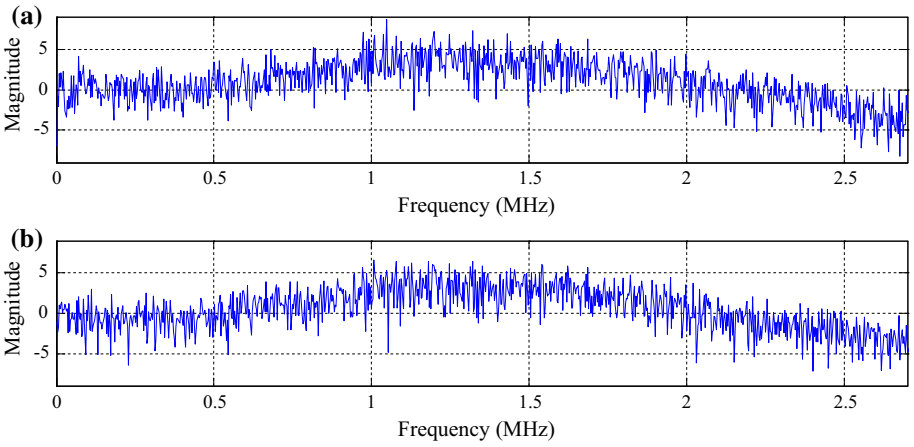

Fig. 3 Frequency domain: **a** authentic signal and **b** spoofing signal

In this scenario, amplitude of authentic and delayed signals is equal. At first, we inspected spoofing and real signals at frequency domain. According to Fig. 3, there is no observable difference in frequency domain of two signals. The Fig. 4 shows acquisition result of one sample of constructed signal. As it is observed, four satellites of the spoofing signal are common with the authentic one; PRN18 is added and PRN14 is omitted.

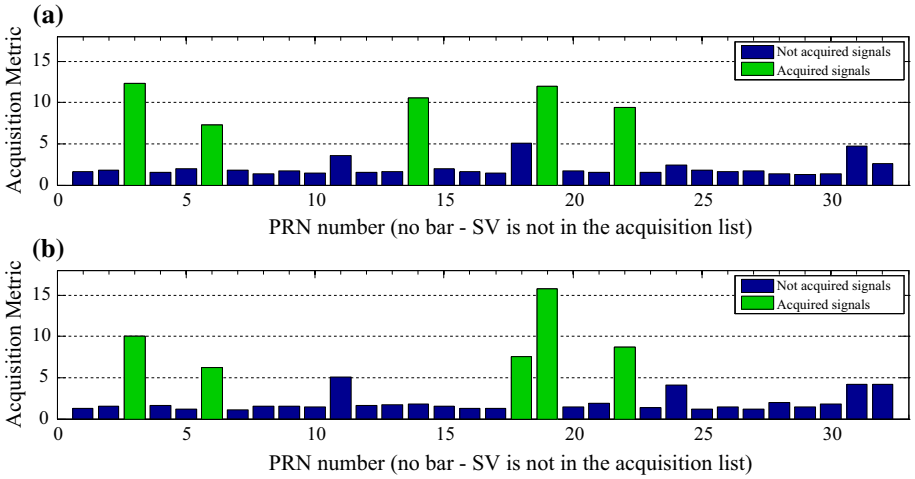

Fig. 4 Acquisition result: **a** authentic signal and **b** spoofing signal

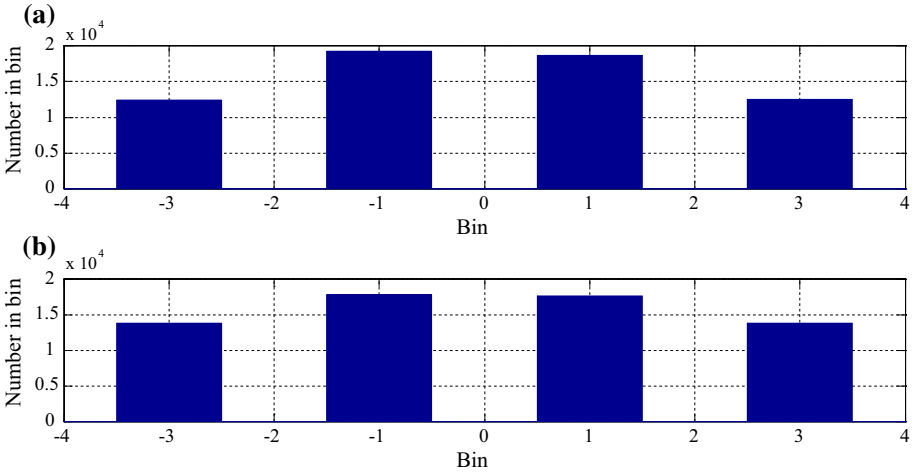

Fig. 5 Histogram: **a** authentic signal and **b** spoofing signal

Operation of this signal is finished in this step, since the extracted navigation message from tracking segment can't solve the navigation equations. Indeed, the constructed signal contains no preamble bits. None of more than 2500 sample of these tests with variant delay times reaches a reasonable answer.

Case B. $A_C^D = 2A_C^A$

In this scenario, delayed signal amplitude is twice that of the authentic signal. In the first step, more than 2500 samples by different delay times were examined. In 21 samples, successful spoofing signal was created. Histogram, frequency domain and acquisition output are shown in Figs. 5, 6 and 7, respectively, for one of them. As can be seen, there is

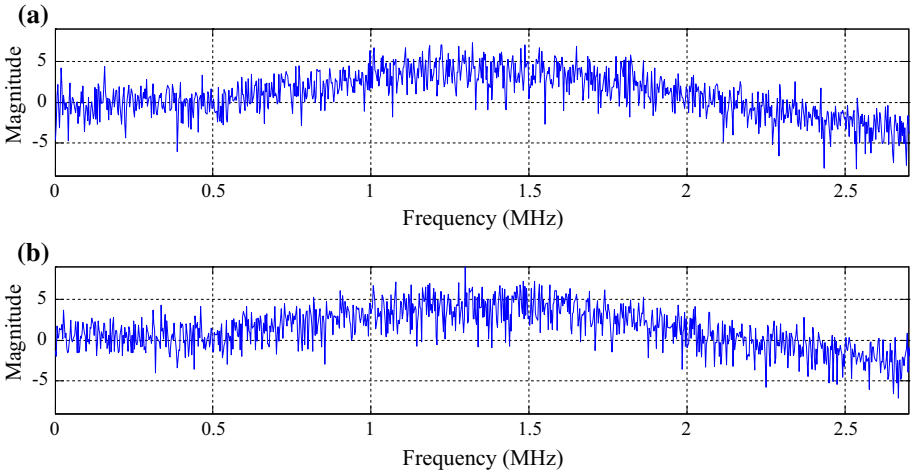

Fig. 6 Power density: **a** authentic signal and **b** spoofing signal

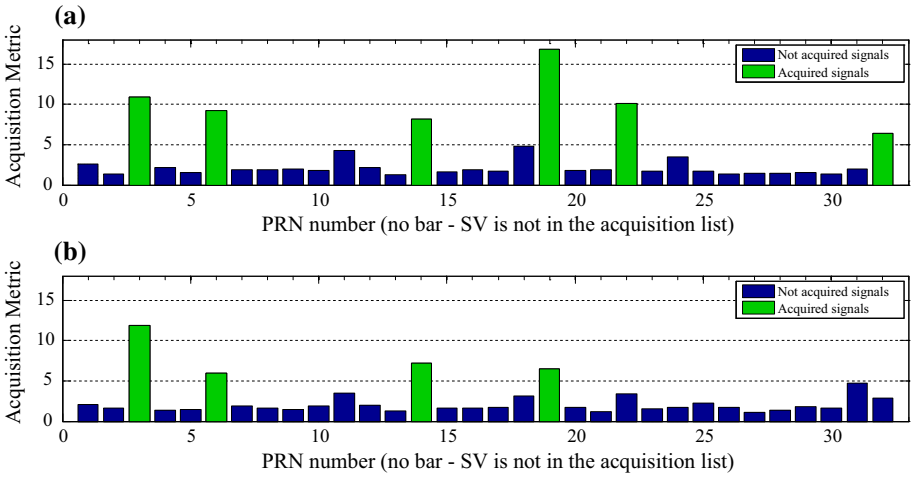

Fig. 7 Acquisition result: **a** authentic signal and **b** spoofing signal

no obvious difference between features of two signals. Moreover, statistical distribution and frequency domain of two signals are similar.

The spoofing signal contains four satellites of authentic signal and prevents the other two satellites to pass the tracking segment. Spoofing error is also specified separately in East, North and Up (ENU) coordinates. More details of produced spoofing data sets are reported in Table 1. As can be seen in the Table, this data set can spoof the victim single frequency GPS receiver from 96 to 1900 m.

Furthermore, Fig. 8 shows spoofing error versus delay time. It is obvious that there isn't a definite relation between delay time and position error. However, it can be extracted that number of successful spoofing data sets in small delay times are more than those with big delay time. However, larger position errors due to spoofing occurred in big delay times.

Table 1 Details of spoofing error at first scenario

Delay time [ms]	ΔE [m]	ΔN [m]	ΔU [m]	Position error [m]
35	9	34	142	146
70	29	63	154	169
105	31	30	115	123
210	32	53	116	131
245	40	42	121	134
420	72	45	342	352
490	39	48	102	119
525	36	35	139	148
700	46	186	724	749
2625	72	65	331	345
2905	88	48	154	184
2940	71	40	120	145
4830	29	39	83	96
5530	34	109	133	175
5828	110	41	155	194
12,250	498	526	1757	1900
17,972	62	39	131	150
24,815	27	66	80	107
28,367	97	38	143	177
37,590	27	76	83	116
43,330	473	523	1661	1804

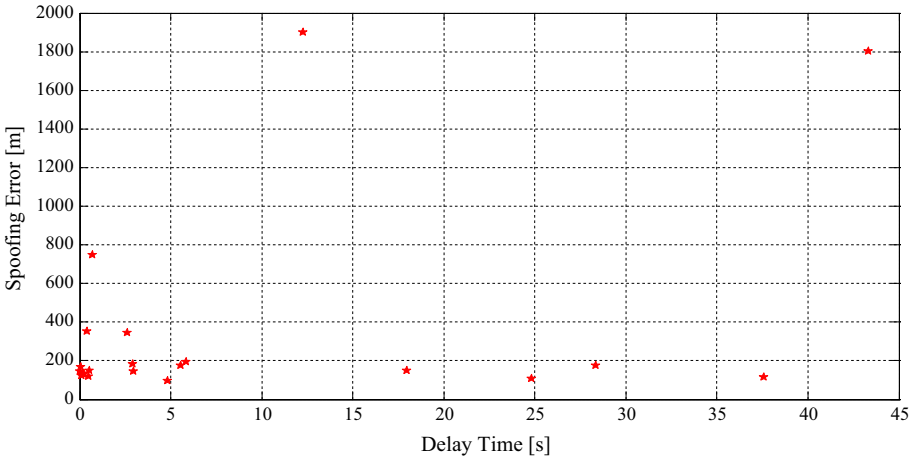

Fig. 8 Spoofing error versus delay time at first data set

To assurance of yield results, the test was repeated two other times. In the second epoch, 20 successful results gathered. Table 2 and Fig. 9 show details of these samples. In this test, 54 and 1758 m are respectively minimum and maximum RMS errors in position. In the next epoch, more than 750 samples with different delays were investigated. We

Table 2 Details of spoofing error at second scenario

Delay time [ms]	ΔE [m]	ΔN [m]	ΔU [m]	Position error [m]
35	27	24	74	82
105	19	25	49	58
140	30	37	98	109
175	37	50	94	113
210	39	42	91	108
245	49	74	90	126
385	40	63	74	105
490	30	30	93	102
560	51	65	99	129
595	21	38	32	54
665	57	60	30	88
910	42	52	91	113
2065	42	67	72	107
2975	56	82	143	174
3010	75	63	285	301
3605	41	73	25	87
4550	71	55	279	293
9293	24	23	95	101
11,392	462	506	1619	1758
24,622	40	57	50	86

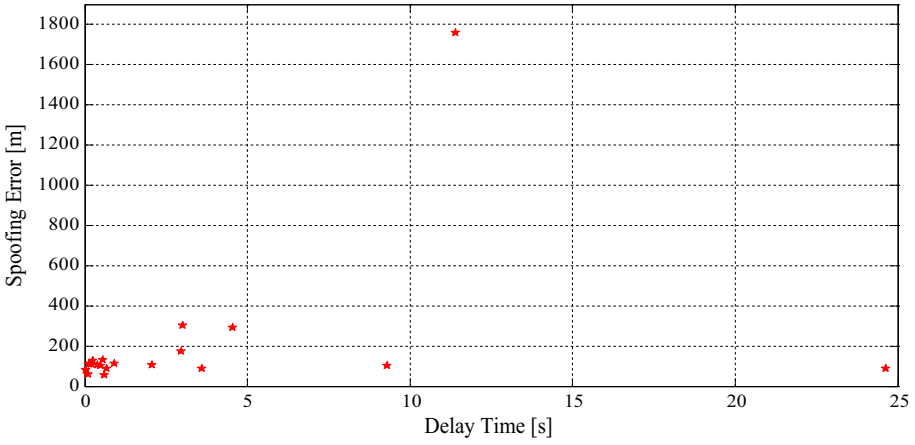

Fig. 9 Spoofing error versus delay time at second data set

produced 19 effective spoofing data sets, by 90 and 1795 m as minimum and maximum amount of them. More aspects of them can be seen in Table 3 and Fig. 10.

Another issue that is receiving more attention in the Tables 1, 2 and 3 is that effect of spoofing signal in three coordinates is not similar. The position error in U axis is more than others. In other words, the counterfeit signal affects the height of the target receiver

Table 3 Details of spoofing error at third scenario

Delay time [ms]	ΔE [m]	ΔN [m]	ΔU [m]	Position error [m]
70	70	29	99	125
105	32	40	102	114
140	28	37	77	90
175	43	52	95	117
280	59	48	272	282
315	35	47	93	110
350	43	35	125	137
420	42	25	99	110
560	35	41	88	103
630	35	42	127	138
665	37	47	90	108
735	29	29	89	98
1050	24	159	659	678
2135	62	35	92	116
2905	59	76	125	158
4620	48	73	93	128
4935	471	511	1655	1795
6055	32	29	102	111
13,825	435	472	1530	1659

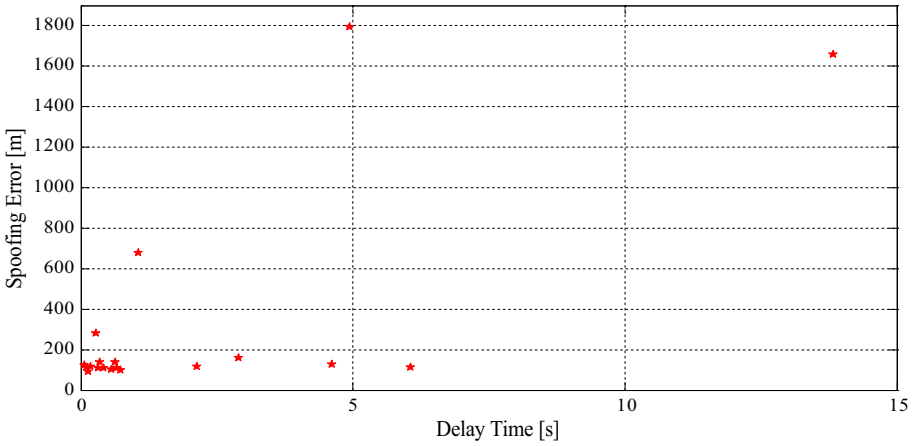

Fig. 10 Spoofing error versus delay time at third data set

majorly. The successful samples of three scenarios are collected in Fig. 11. It is obvious that distribution of successful spoofing signals decreases sharply after 5 s delay time.

Case C. $A_C^D = 3A_C^A$

In this scenario, amplitude ratio of spoofing signal to authentic signal is 3. About 1150 instances are tested and 996 samples of them are effective spoofing signal by position error between 2 and 2139 m. Successful examples are shown in Fig. 12. As can be seen,

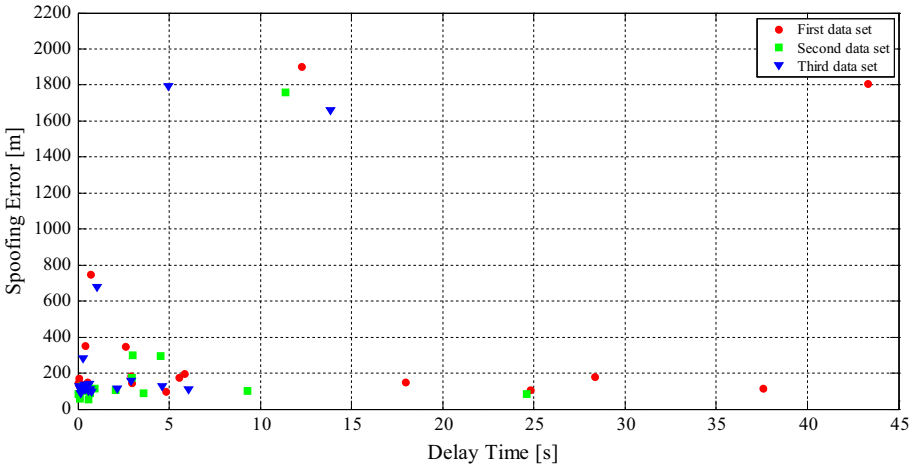

Fig. 11 Spoofing error versus delay time at three data sets

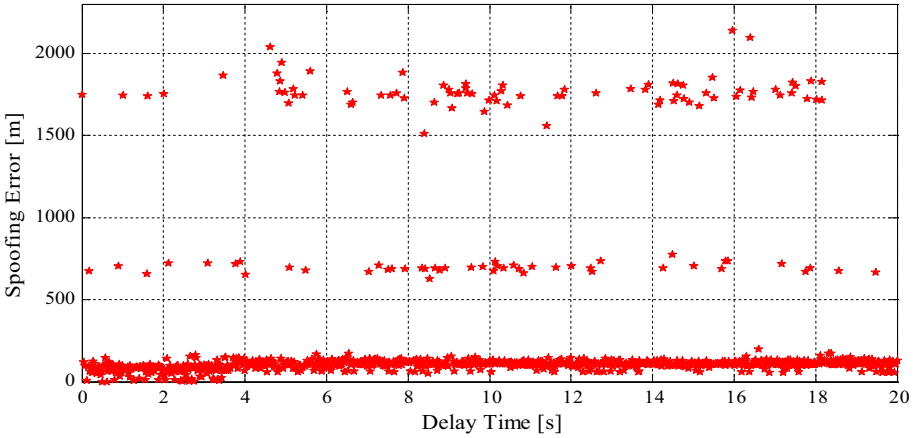

Fig. 12 Spoofing error versus delay time at third scenario

distribution of spoofing versus delay time is approximately uniform and most of examples have small spoofing meters. In other words, density of distribution is sparse in large spoofing values.

5 Conclusion

In this article, we proposed a new methodology for spoofing generation. In that, delay and combination procedure deviate the position of target receiver. In other words, unlike the previously suggested scenarios, the fake signal in this algorithm is combined of two GPS signal. Whereas, in former spoofing attacks, the counterfeit signal was a single GPS signal. Investigating more than 1000 successful samples terminated in that pseudo-range deviation seems as decreasing and extravagant satellite position deviation. However, pseudo-range

variance is about 100 times more than satellite position deviation. Salient change of pseudo-range is a reasonable argument for extremely variation of the target GPS receiver height. These two factors redound to position error due to spoofing. On the other hand, difference of GPS signal features as doppler frequency is less than 2 % relative to authentic signal. As a result, this scenario is less expensive and more difficult to detect and resist in competition with simplistic spoofer, since it has a power normalizer and a lower hardware complexity and size. Moreover, spoofing signal is approximately synchrone with the authentic one, so there is no need to lose the target receiver lock and reacquisition. In summary, we could made changes in navigation bits and then deviate the receiver position. Indeed, this algorithm caused decreasing pseudo-range and excessive satellite position deviation without much hardware equipment.

References

1. Ferguson, N., & Schneier, B. (2003). *Practical cryptography*. New York: Wiley.
2. Mosavi, M. R. (2006) "Frequency domain modeling of GPS positioning errors", *Proceedings of the 8th International Conference on Signal Processing*, Vol. 4, (pp. 1–4).
3. Warner, J. S., & Johnston, R. G. (2003). *GPS spoofing countermeasures* (Vol. 10, pp. 22–30). Los Alamos National Laboratory: Vulnerability Assessment Team.
4. Mosavi, M. R. (2006). Comparing DGPS corrections prediction using neural network, fuzzy neural network and Kalman filter. *Journal of GPS Solutions, 10*(2), 97–107.
5. Mosavi, M. R., & EmamGholipour, I. (2013). De-noising of GPS receivers positioning data using wavelet transform and bilateral filtering. *Journal of Wireless Personal Communications, 71*(3), 2295–2312.
6. Mosavi, M. R., Azad, M. S., & EmamGholipour, I. (2013). Position estimation in single-frequency GPS receivers using Kalman filter with pseudo-range and carrier phase measurements. *Journal of Wireless Personal Communications, 72*(4), 2563–2576.
7. Mosavi, M. R., Nabavi, H., & Nakhaei, A. (2014). Neural technologies for precise timing in electric power systems with a single-frequency GPS receiver. *Journal of Wireless Personal Communications, 75*(2), 925–941.
8. Cheng, X. J., Cao, K. J., Xu, J. N., & Li, B. (2009) "Analysis on forgery patterns for GPS civil spoofing signals", *Proceedings of the 4th International Conference on Computer Sciences and Convergence Information Technology*, (pp. 353–356).
9. Warner, J. S. & Johnston, R. G. (2002) "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing". *Journal of Security Administration, 25*, 19–28.
10. Tippenhauer, N. O., Popper, C., Rasmussen K. B., & Capkun S. (2011) "On the requirements for successful GPS spoofing attacks", *Proceedings of the 18th ACM Conference on Computer and Communications Security*, (pp. 75–86).
11. Nighswander, T., Ledvina, B. Diamond, J. Brumley, R., & Brumley, D. (2012). GPS software attacks. In *Proceedings of the 2012 ACM conference on Computer and communications networks-securityand protection* (pp. 450–461).
12. Ledvina, B. M., Bencze, W. J., Galusha, B. & Miller, I. (2012) "An in-line anti-spoofing device for legacy civil GPS receivers", *Proceedings of the 23rd International Technical Meeting of the Satellite Division of The Institute of Navigation*, (pp. 689–712).
13. Montgomery, P. Y., Humphreys, T. E., & Ledvina, B. M. (2009) "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer", *Institute of International Technical Meeting of the Institute of Navigation*, (pp. 1–7).
14. Jahromi, A. J., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012) "GPS vulnerability to spoofing threats and a review of anti-spoofing techniques". *International Journal of Navigation and Observation, 2012*, 1–16.
15. Humphreys, T. E., Ledvina, B. M., Psiaki, M. L., O'Hanlon, B. W., & Kintner, P. M. (2008) "Assessing the spoofing threat: Development of a portable GPS civilian spoofer", *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation*, (pp. 2314–2325).
16. Papadimitratos, P., & Jovanovic, A. (2008). GNSS-based positioning: Attacks and countermeasures. *IEEE Military Communications Conference*, 1–8.
17. Jahromi, A. J., Lin, T., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012) "Detection and mitigation of spoofing attacks on a vector-based tracking GPS receiver", *International Technical Meeting of The Institute of Navigation*, (pp. 3–8).

18. Nielsen, J., Broumandan A., & Lachapelle, G. (2010). Spoofing detection and mitigation with a moving handheld receiver. *GPS World Magazine, 21*(9), 27–33.
19. White, N. A., Maybeck, P. S., & DeVilbiss, S. L. (1998). Detection of interference/jamming and spoofing in a DCPS-aided inertial system. *IEEE Transactions on Aerospace and Electronic Systems, 34*(4), 1208–1217.
20. Shepard, D. P., & Humphrey, T. E. (2010). Characterization of receiver response to spoofing attacks. *GPS World, 21*(9), 27–33.
21. Jahromi, A. J., Broumandan, A., Nielsen, J., & Lachapelle, G. (2012). GPS spoofer countermeasure effectiveness based on signal strength, noise power and C/No observables. *International Journal of Satellite Communications and Networking, 30*(4), 181–191.
22. Wen, H., Huang, P. Y. R., Dyer, J., Archinal A., & Fagan, J., "Countermeasures for GPS signal spoofing", *Proceedings of the 18th International Technical Meeting of the Satellite Division of The Institute of Navigation*, (pp. 1285–1290).
23. Cavaleri, A., Motella, B., Pini M., & Fantino, M. (2012) "Detection of Spoofed GPS signals at code and carrier tracking level", *Proceedings of the 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing*, (pp. 1–6).
24. Scott, L. (2007). Location assurance. *GPS World, 18*(7), 14–18.
25. Humphreys, T. E., Psiaki, M. L., Kintner, P. M., & Ledvina, B. M., (2006) "GNSS receiver implementation on a DSP: Status, challenges and prospects", *Proceedings of the 19th International Technical Meeting of the Satellite Division of The Institute of Navigation*, (pp. 1–13).
26. Borre, K., Akos, D. M., Bertelsen, N., Rinder, P., & Jensen, S. H. (2007). *A software-defined GPS and Galileo receiver: A Single-frequency approach*. Boston: Birkhäuser.

A. R. Baziar received his B.S. and M.S. degree in Electronic Engineering from respectively Shahid Rajaee Teacher Training University in 2011 and Iran University of Science and Technology (IUST) in 2013, Tehran, Iran. His current research interests include GPS signal processing and de-noising.

M. Moazedi received her B.S. and M.S. degrees in Electronic Engineering from IUST, Tehran, Iran in 2008 and 2011, respectively. She is currently Ph.D. student of IUST Department of Electrical Engineering. Her research interests in the area of analog and mixed signal integrated circuits, GPS security and integrity.

M. R. Mosavi received his B.S., M.S. and Ph.D. degrees in Electronic Engineering from IUST, Tehran, Iran in 1997, 1998 and 2004, respectively. He is currently faculty member of Department of Electrical Engineering of IUST as professor. He is the author of more than 200 scientific publications on journals and international conferences. His research interests include circuits and systems design.