TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 06/10 pp599-605
Volume 18, Number 6, December 2013

Intermediate Spoofing Strategies and Countermeasures

Yang Gao, Hong Li*, Mingquan Lu, and Zhenming Feng

Abstract: Intermediate spoofing can impact most off-the-shelf Global Navigation Satellite Systems (GNSS) receivers, therefore low cost detection of such spoofing is very important to protect the reliability of the GNSS receivers used in critical safety and financial applications. This paper presents two strategies to analyze attacks by intermediate spoofing attackers to identify the weaknesses of such attacks. The analyses lead to a code and carrier phase consistency detection method with simulation results showing that this method can indicate the receiver when spoofing has occurred. The method can be used by most receivers, is inexpensive, and requires only a small software upgrade.

Key words: intermediate spoofing; dragging code phase strategy; low cost countermeasures; code and carrier phase consistency

1 Introduction

Global Navigation Satellite Systems (GNSS) signals are vulnerable to interference, jamming, and spoofing due to their low power and open signal structure, which means that navigation and timing services can be easily interrupted by high power noise or mislead by counterfeit signals. Spoofing is even more hazardous than jamming, since it can lead the receiver to the wrong position or the wrong time without the receiver being aware of the problem so that the navigation and timing results are still trusted by the user. These attacks are not only dangerous to critical safety and financial application but also to the location-based security services such as geo-encryption and position attestation[1].

Spoofing attacks can be divided into simplistic attacks, intermediate attacks, and sophisticated attacks[2]. Simplistic attacks are implemented by connecting a signal generator to an antenna, but this will not likely synchronize to the real satellite signal. To deceive the receiver, a high power Radio Frequency (RF) noise must first be transmitted to force the receiver to lose its lock to the genuine signal, followed by the counterfeit signal with a much higher power level than the real signal. This kind of spoofing can be easily detected because both the lost of the lock and the abnormally high SNR will alert the receiver, but most current civilian GPS receivers can not detect this and successful attacks have already been demonstrated[3].

Intermediate spoofing is an attack via a receiver-spoofer, which is composed of a GNSS receiver and a signal generator. The receiver tracks satellite signals to accurately synchronize with the satellite time and emphasis with estimates of the Doppler frequencies and code phases of every satellite signal tracked by the victim receiver. Then the signal generator uses this information to generate counterfeit signals synchronized to the genuine signal. The receiver-spoofer adjusts the code phase and the carrier frequency of the fake signal to align with the genuine signal and then increases the power a little to control the correlation peak so as to lead the correlation peak away from the genuine peak. This kind of spoofing can deceive a receiver without breaking the tracking state, which is hard to detect by receivers except for the

• Yang Gao, Hong Li, Mingquan Lu, and Zhenming Feng are with the Department of Electronic Engineering, Tsinghua University, Beijing 100084, China. E-mail: gaoy03@mails.tsinghua.edu.cn; lihongee@tsinghua.edu.cn.
∗ To whom correspondence should be addressed.
Manuscript received: 2012-07-15; revised: 2013-04-02; accepted: 2013-04-03

multi-antenna receivers. The receiver-spoofer has been demonstrated by Humphreys et al.[2]

Sophisticated spoofing is similar to the intermediate spoofing but with additional synchronization equipments to transmit signals with a coordinated carrier phase, which can even deceive multi-antenna receivers. However, sophisticated attacks are very expensive and no successful implementations have been reported so far.

The detection of intermediate and sophisticated spoofing is very important to prevent furtive invasions, and has attracted much attention in recent years. Bit latency detection[1,2] requires the spoofer to predict an unpredictable data bit, but this method usually needs an additional clock. Signal parameter estimation[4] treats the counterfeit signal as a multipath signal, but requires a tracking loop structure change. Vestige Signal Detection (VSD) methods including Ratio test, Early-Late Phase Metric, and Signal Quality Monitoring[2,5,6] are low cost, but have high false alarm rates due to the multipath influence[7]. Other methods such as monitoring of the signal power and bounding and comparing of range rates[8] have been suggested, but no simulations or tests have yet been given.

Though a receiver-spoofer has been developed that can launch an intermediate attack, spoofing strategies that can successfully and safely drag the tracking peak have not yet been investigated. This study analyzes strategies a spoofer could use to deceive a receiver and weaknesses in these strategies with ways to detect these strategies.

Mathematical models of a spoofer strategies are given with simulation results which show that both strategies will cause abnormal changes in the receiver states. A countermeasure strategy is given which monitors the Code and Carrier Phase Consistency (CCPC), including a mathematical model and simulation results. This research shows that intermediate spoofing can be detected if more receiver states are monitored, which will increase the spoofing difficulty.

2 Intermediate Spoofing

Intermediate spoofing can deceive most off-the-shelf receivers without them being aware. The spoofing process of the receiver-spoofer can be divided into the following steps[2].

Step 1 The receiver-spoofer tracks the genuine signals and estimates the code phase and the carrier frequency of the signals that the victim receiver tracks.

Step 2 The receiver-spoofer generates the fake signal at a lower power and several code chips away from the genuine one tracked by the victim receiver.

Step 3 The receiver-spoofer gradually adjusts the code phase to align with the genuine signal, acting like a multipath signal, and then increases the signal power to control the tracking points.

Step 4 The receiver-spoofer adjusts the code phase to drag the correlation peak away from the genuine signal to then completely control the receiver.

The process is illustrated in Fig. 1.

In Steps 1-3, the fake signal will have very low power, just like a multipath signal, to avoid detection. The weakest part of the spoofing is Step 4 due to its higher power and the competition with the genuine signal, so this is also the best time for the receiver to detect the spoofing. After a receiver-spoofer was demonstrated in 2008, the device was tested on four kinds of receivers. All the receivers were cheated and kept tracking the "satellite signal" without losing the signal lock or activating an alarm[9].

3 Spoofing Strategies Analysis

3.1 Two spoofing strategies

The strategy of dragging code phase is very important to keep the victim receiver tracking and to avoid detection. Two strategies are shown in Figs. 2 and 3.

Strategy 1 shown in Fig. 2 maintains the consistency between the carrier phase (Doppler) and the code phase

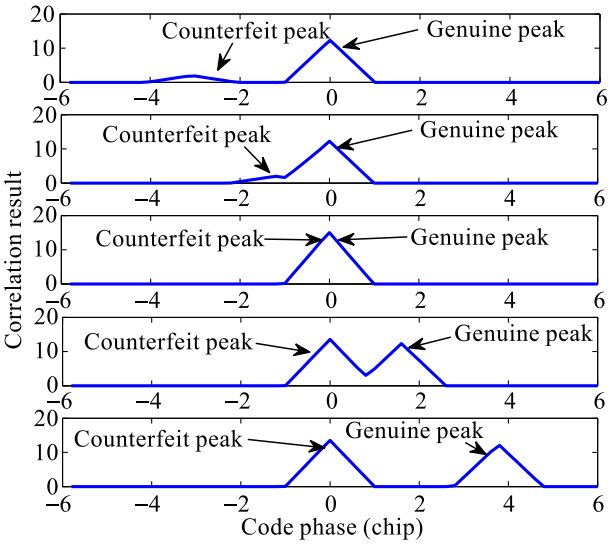

Fig. 1 The steps for intermediate spoofing.

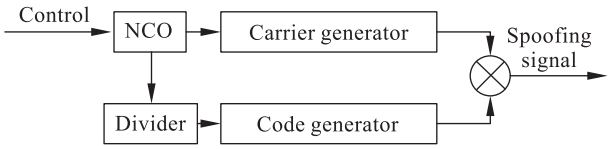

Fig. 2 Strategy 1: Adjust the code phase consistent with the carrier phase.

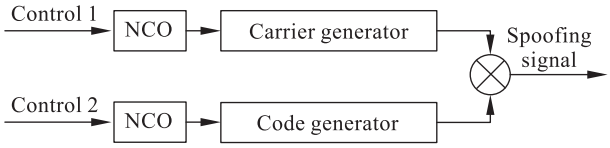

Fig. 3 Strategy 2: Adjust the code phase independent of the carrier phase.

(Doppler) via a Numerical Control Oscillator (NCO), which is true in real signals where the code Doppler is proportional to the carrier Doppler, because the Doppler effect is caused by the motion between the satellite and the receiver. Consider an L1 C/A signal as an example, the relationship between the code Doppler ($f_{\text{Doppler}}^{\text{code}}$) and the carrier Doppler ($f_{\text{Doppler}}^{\text{carrrier}}$) can typically be expressed as $f_{\text{Doppler}}^{\text{code}} = f_{\text{Doppler}}^{\text{carrier}}/1540$.

Strategy 2 shown in Fig. 3 breaks this consistency with the code Doppler no longer related to the carrier Doppler, which is an abnormal situation.

Both strategies could be used to drag the tracking points off in theory, but the responses of the receiver will be quite different.

3.2 Mathematical model of intermediate spoofing

During the attack, the composite signal in the antenna can be expressed as

$$S(t) = S_{\text{S}}(t) + S_{\text{A}}(t) \tag{1}$$

where $S_{\text{A}}(t)$ represents authentication (genuine) signal and $S_{\text{S}}(t)$ represents the spoofing (counterfeit) signal, with these two signals are given as

$$S_{\text{A}}(t) = \sqrt{2P_{\text{A}}} \cdot c[f_{\text{nom}}^{\text{code}} t + f_{\text{Doppler}}^{\text{code}} t - \Phi] \cdot \sin[2\pi(f_{\text{nom}}^{\text{carrier}} + f_{\text{Doppler}}^{\text{carrier}})t + \psi] \tag{2}$$

$$S_{\text{S}}(t) = \sqrt{2P_{\text{S}}} \cdot c[f_{\text{nom}}^{\text{code}} t + \hat{f}_{\text{Doppler}}^{\text{code}} t - \hat{\Phi} + \Delta f_{\text{spoof}}^{\text{code}} t] \cdot \sin[2\pi(f_{\text{nom}}^{\text{carrier}} + \hat{f}_{\text{Doppler}}^{\text{carrier}} + \Delta f_{\text{spoof}}^{\text{carrier}})t + \hat{\psi}] \tag{3}$$

where P_{A} and P_{S} are the powers of the authentication and the spoofing signals. $c[\cdot]$ is the function that maps the code phase to the code square wave. $f_{\text{nom}}^{\text{code}}$ is the nominal code frequency. $f_{\text{Doppler}}^{\text{code}}$ is the code Doppler shift due to the relative motion. $f_{\text{nom}}^{\text{carrier}}$ is the nominal carrier frequency. $f_{\text{Doppler}}^{\text{carrier}}$ is the carrier Doppler frequency. Φ and ψ are the code phase delay and carrier phase delay due to the propagation from the satellite to the receiver. $\hat{f}_{\text{Doppler}}^{\text{code}}$, $\hat{\Phi}$, $\hat{f}_{\text{Dopper}}^{\text{carrier}}$, and $\hat{\psi}$ are the parameters that the spoofer estimates and uses to generate the fake signal. $\Delta f_{\text{spoof}}^{\text{carrier}}$ and $\Delta f_{\text{spoof}}^{\text{code}}$ are the carrier and code frequencies the spoofer adds to the fake signal to drag the code phase.

The composite signal can also be written as

$$S(t) = \frac{(\sqrt{2P_{\text{S}}} - \sqrt{2P_{\text{A}}})}{\sqrt{2P_{\text{S}}}} S_{\text{S}}(t) + \sqrt{2P_{\text{A}}} \cdot \left[\frac{S_{\text{A}}(t)}{\sqrt{2P_{\text{A}}}} + \frac{S_{\text{S}}(t)}{\sqrt{2P_{\text{S}}}} \right] \tag{4}$$

When the spoofer aligns with the code phase, the following assumptions can be made: $\hat{f}_{\text{Doppler}}^{\text{carrier}} \approx f_{\text{Doppler}}^{\text{carrier}}$, $\hat{f}_{\text{Doppler}}^{\text{code}} \approx f_{\text{Doppler}}^{\text{code}}$, $\hat{\Phi} \approx \Phi$, and $\hat{\psi} \neq \psi$.

Then, the spoofer begins to adjust the code phase by adding $\Delta f_{\text{spoof}}^{\text{carrier}}$ and $\Delta f_{\text{spoof}}^{\text{code}}$ to the signal generator. Thus at the beginning of dragging, when $t \approx 0$ and $\Delta f_{\text{spoof}}^{\text{code}} t \approx 0$, Eq. (4) can be approximated as

$$S(t) = \frac{(\sqrt{2P_{\text{S}}} - \sqrt{2P_{\text{A}}})}{\sqrt{2P_{\text{S}}}} S_{\text{S}}(t) + S_{\text{A}}(t) \cos[\pi \Delta f_{\text{spoof}}^{\text{carrier}} t + (\psi - \hat{\psi})/2] \tag{5}$$

In Strategy 1, to keep the consistency between the code phase and the carrier phase in the L1 C/A case, the frequency offsets should be related as $\Delta f_{\text{spoof}}^{\text{carrier}} = 1540 \cdot \Delta f_{\text{spoof}}^{\text{code}}$. Test[10] had shown that counterfeit signal should not be too strong. When the power ratio $P_{\text{S}}/P_{\text{A}} \approx 1.2$, spoofing can be successful, thus Eq. (5) can be approximated as

$$S(t) \approx 0.046 S_{\text{S}}(t) + S_{\text{A}}(t) \cos[\pi \Delta f_{\text{spoof}}^{\text{carrier}} t + (\psi - \hat{\psi})/2] \tag{6}$$

Equation (6) shows that the power of composite signal will quickly fade due to $\Delta f_{\text{spoof}}^{\text{carrier}}$ during the dragging procedure, which will increase the probability of the victim receiver losing its lock. Thus, the spoofer must increase the power ratio to avoid alerting the victim receiver, which increases the risk of detection by a signal power monitor.

In Strategy 2, the spoofer can avoid the power fading, by setting $\Delta f_{\text{spoof}}^{\text{carrier}} = 0$, which was the strategy by Humphreys et al.[2] The composite signal can then be expressed as

$$S(t) \approx \frac{(\sqrt{2P_{\text{S}}} - \sqrt{2P_{\text{A}}})}{\sqrt{2P_{\text{S}}}} S_{\text{S}}(t) + S_{\text{A}}(t) \cos[(\psi - \hat{\psi})/2] \tag{7}$$

Only the code phase is adjusted when the spoofer drags the correlation peak, while the carrier phase (Doppler) of the fake signal remains consistent with that of the genuine signal until the code phase has been dragged away for more than one code chip.

3.3 Simulations of the two strategies

Simulations were made to validate the conclusions using the process shown in Fig. 4.

The simulations were made at the signal parameter level with the code phases and the carrier phases of the genuine and counterfeit signals generated by calculating the Doppler and nominal frequency. Then the receiver tracks the "signal" described by the parameters to estimate the code phase and the carrier phase[10]. The tracking states and tracking results are stored and compared with the input parameters. The simulation process can be described as follows.

(1) At $t = 0$ s, the counterfeit signal is about four code chips away from the genuine signal and at very low power, the counterfeit signal gradually approaches the genuine peak as shown in the first and second parts of Fig. 1.

(2) At $t = 60$ s, the counterfeit signal exactly aligns with the code phase of the genuine signal and increases the power to control the tracking loop, as shown in the third part of Fig. 1.

(3) At $t = 65$ s, the spoofer begins to drag the tracking point away from the genuine point for more than one chip, as the fourth and fifth parts of Fig. 1 show.

The CN0 (carrier-power to noise-density ratio) is 46 dB·Hz and the power ratio of the counterfeit signal and the genuine signal is $P_S/P_A = 1.2$. The simulation results of spoofing Strategy 1 are shown in Figs. 5-7. The simulation results of spoofing Strategy 2 are shown in Figs. 8-10.

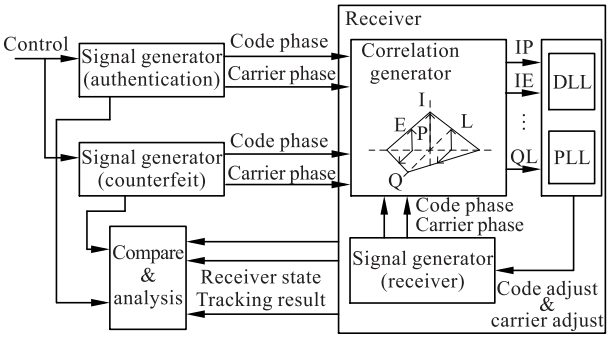

Fig. 4 Simulation descriptions.

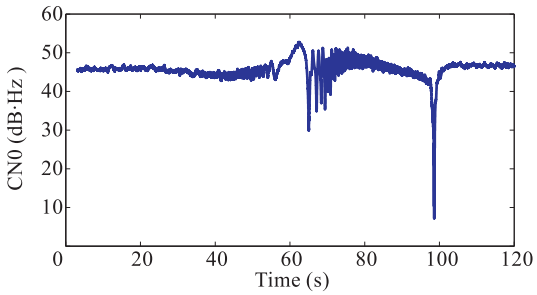

Fig. 5 CN0 variation during spoofing, Strategy 1.

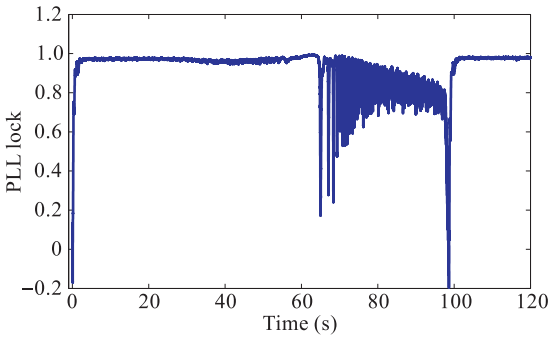

Fig. 6 PLL lock variation during spoofing, Strategy 1.

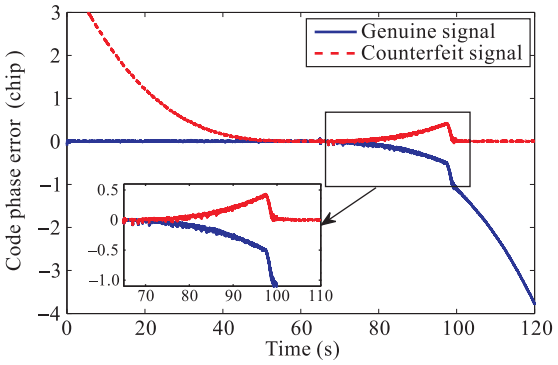

Fig. 7 Tracking phase errors of the genuine and counterfeit signals for Strategy 1.

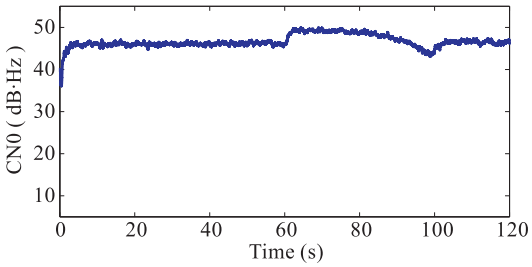

Fig. 8 CN0 variation during spoofing, Strategy 2.

Figures 7 and 10 show the code phase errors between the code phase estimated by receiver and the true input code phase (including the genuine signal and the counterfeit signal).

The code phase error between the receiver and the genuine signal is approximately zero from $t = 0$ s to

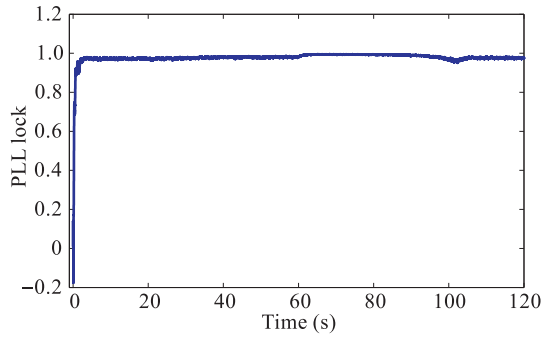

Fig. 9 PLL lock variation during spoofing, Strategy 2.

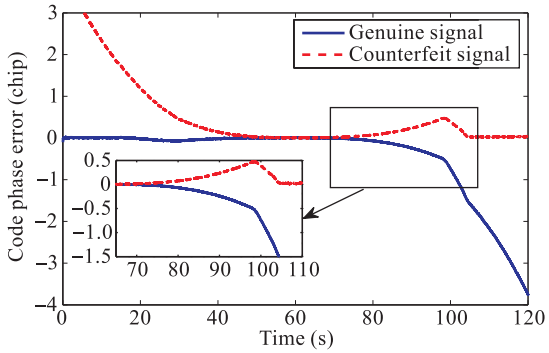

Fig. 10 Tracking phase errors of the genuine and counterfeit signals for Strategy 2.

$t = 70$ s, and code phase error between the receiver and the counterfeit signal is larger than 1 chip during $t = 0$ s to $t = 20$ s, which means that the receiver initially tracks the genuine signal.

After $t = 80$ s, the code phase error between the receiver and the genuine signal keeps increasing, while that between the receiver and the counterfeit signal remains less than 0.5 chip, which means that the counterfeit signal successfully controls the receiver.

Although, both strategies result in successful spoofing attacks, the receiver states are quite different. Comparing Figs. 5 and 6 with Figs. 8 and 9 shows that for a receiver with Phase Locked Loop (PLL), when the spoofer in Strategy 1 began to drag the correlation peak, the PLL lock varied greatly, with value even below 0.2 for some time intervals and the CN0 also fell below 10 dB·Hz, both of which indicate loss of the lock to the receiver. In Strategy 2, the PLL lock value remains reasonable during the spoofing process, with very small variations and the CN0 remains high, which means that the spoofing was harder to detect.

4 Countermeasures

As indicated, Strategy 2 is the better choice for the spoofer to more discretely drag the correlation peak. However, the consistency between the carrier phase and the pseudo range (code phase) will be broken. Thus, the receiver should monitor the CCPC to detect the spoofing.

4.1 CCPC mathematical model

Let $P(t)$ represent the pseudo range between the satellite and the antenna at time t. Then the increment of $P(t)$ between t_1 and t_2 can be expressed as

$$\Delta P = P(t_1) - P(t_2) = \int_{t_1}^{t_2} v_{\mathrm{r}}(t)\mathrm{d}t \tag{8}$$

where $v_{\mathrm{r}}(t)$ represents the relative radial velocity between the satellite and the antenna. The range increment can be measured for both the code and the carrier[11, 12] as

$$\Delta P_{\mathrm{code}} = \int_{t_1}^{t_2} c \cdot [f_{\mathrm{Doppler}}^{\mathrm{code}}(t)/f_{\mathrm{nom}}^{\mathrm{code}}]\mathrm{d}t \tag{9}$$

$$\Delta P_{\mathrm{carrier}} = \int_{t_1}^{t_2} c \cdot [f_{\mathrm{Doppler}}^{\mathrm{carrier}}(t)/f_{\mathrm{nom}}^{\mathrm{carrier}}]\mathrm{d}t \tag{10}$$

where ΔP_{code} represents the range increment measured in the code, $\Delta P_{\mathrm{carrier}}$ represents that measured in the carrier, and c represents the light speed. The two should be the same without spoofing. CCPC statistics can be defined as

$$I_{\mathrm{CCPC}} = \Delta P_{\mathrm{carrier}} - \Delta P_{\mathrm{code}} \tag{11}$$

I_{CCPC} can be calculated by the receiver as

$$I_{\mathrm{CCPC}} = c \cdot [f_{\mathrm{NCO}}^{\mathrm{carrier}}(t_2 - t_1)/f_{\mathrm{nom}}^{\mathrm{carrier}} - f_{\mathrm{NCO}}^{\mathrm{code}}(t_2 - t_1)/f_{\mathrm{nom}}^{\mathrm{code}}] \tag{12}$$

or

$$I_{\mathrm{CCPC}} = c \cdot [\Delta\psi_{\mathrm{carrier}}/(2\pi f_{\mathrm{nom}}^{\mathrm{carrier}}) - \Delta\Phi_{\mathrm{code}}/f_{\mathrm{nom}}^{\mathrm{code}}] \tag{13}$$

where $f_{\mathrm{NCO}}^{\mathrm{carrier}}$ and $f_{\mathrm{NCO}}^{\mathrm{carrier}}$ represent the frequencies of the carrier and code NCOs in receiver (only contains the doppler frequency, the nominal frequency is ignored), and $\Delta\psi_{\mathrm{carrier}}$ and $\Delta\Phi_{\mathrm{code}}$ represent the increments of the carrier phase and the code phase measured in the receiver.

4.2 CCPC simulation

Figures 11-13 show simulation results for a spoofing free scenario, spoofing using Strategy 1 and spoofing using Strategy 2, where the spoofing occurred at $t = 60$ s and controlled the receiver after $t = 100$ s. The simulation methodology is the same as that in Section

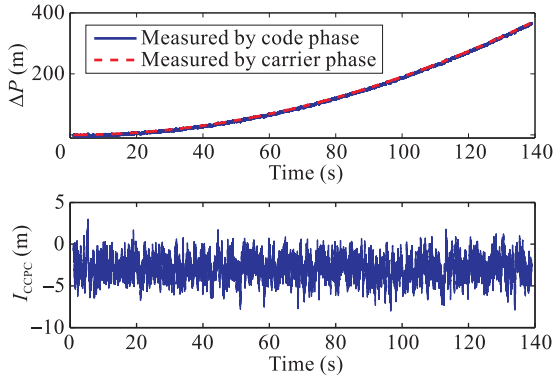

Fig. 11 Range increment and I_{CCPC} without spoofing.

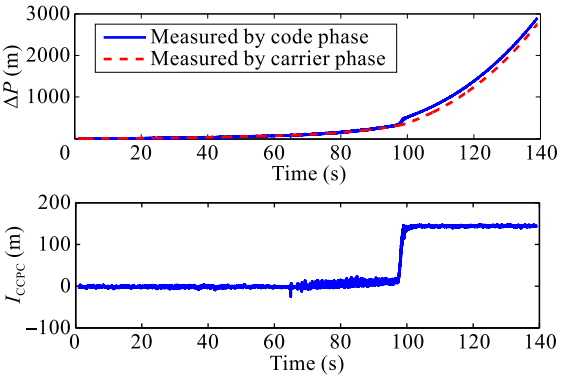

Fig. 12 Range increment and I_{CCPC} for Strategy 1 spoofing.

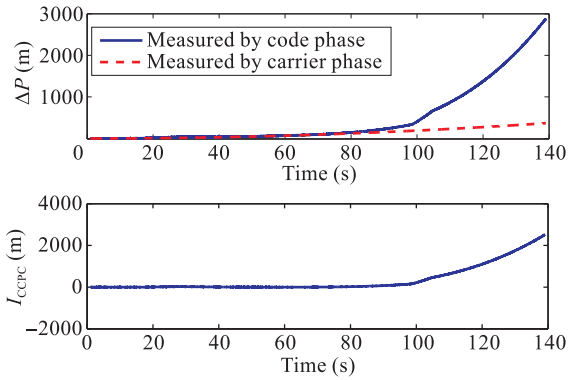

Fig. 13 Range increment and I_{CCPC} for Strategy 2 spoofing.

3. The first part shows ΔP_{code} and $\Delta P_{carrier}$ while the second part shows the I_{CCPC}.

As Figs. 11-13 show, for the spoofing free condition, I_{CCPC} remains very small throughout the whole process; with the Strategy 1 spoofing, during the dragging period, I_{CCPC} increases to more than 100 meters and then remains nearly constant after the successful dragging, which is large enough to alert the receiver that something is wrong; and with the Strategy 2 spoofing, I_{CCPC} keeps increasing during the code phase dragging to more than 1000 meters, which is a very obvious indicator that the receiver is tracking a counterfeit signal.

5 Conclusions and Future Directions

Though intermediate spoofing can successfully deceive most off-the-shelf GNSS receivers without breaking the tracking or alerting the user, some receiver states are still abnormal which can indicate the receiver that an attack is occurring.

Two spoofing strategies were analyzed to identify the abnormal signal variations in the receiver. Strategy 1 breaks the receiver tracking states; while Strategy 2 breaks the consistency between the carrier phase and the code phase, but in a manner less likely to alert the receiver. Strategy 2 would be more successful for most receivers.

The weakness of Strategy 2 is exploited for a spoofing detection method based on checking the consistency between the carrier phase and the code phase. Simulations show that I_{CCPC} varies great when spoofing occurs for both strategies compared to that in the spoofing free situation. This detection method proposed in this paper does not need additional hardware, but can be implemented through only a simple software upgrade.

Future research will investigate the appropriated threshold and the related detection and false alarm rates of this method, especially in multipath environments, which can also result in inconsistencies between the code phase and carrier phase, but with smaller variations.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (No. 61101070).

References

[1] C. J. Wullems, A spoofing detection method for civilian L1 GPS and the E1-B galileo safety of life service, *IEEE Transactions on Aerospace and Electronic Systems,* vol. 48, no. 4, pp. 2849-2864, Oct. 2012.

[2] T. E. Humphreys, B. M. Ledviana, M. L. Psiaki, B. W. o'Hanlon, and P. M. Kintner, Assessing the spoofing threat: Development of a portable GPS civilian spoofer, in *Proc. 21st International Technical Meeting of the Satellite Division of the Institute of Navigation*, Savannah GA, US, 2008, pp. 2314-2325.

[3] J. S. Warner and R. G. Johnston, A simple demonstration that the Global Positioning System (GPS) is vulnerable to spoofing, *Journal of Security Administration,* vol. 25, pp. 19-28, 2002.

[4] F. Dovis, X. Chen, A. Cavaleri, K. Ali, and M. Pini, Detection of spoofing threats by means of signal parameters estimation, in *Proc. 24th International Technical Meeting of the Satellite Division of the Institute of Navigation*, Portland, OR, US, 2010, pp. 416-422.

[5] M. Pini, M. Fantion, A. Cavaleri, S. Ugazio, and L. L. Presti, Signal quality monitoring applied to spoofing detection, in *Proc. 24th International Technical Meeting of the Satellite Division of the Institute of Navigation*, Portland, OR, US, 2010, pp. 1888-1897.

[6] A. Cavaleri, B. Motella, M. Pini, and M. Fantino, Detection of spoofed GPS signal at code and carrier tracking level, in *Proc. 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal*, Noordwijk, Netherlands, 2010, pp. 1-6.

[7] K. D. Wesson, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, An evaluation of the vestigial signal defense for civil GPS anti-spoofing, in *Proc. 24th International Technical Meeting of the Satellite Division of the Institute of Navigation*, Portland, OR, US, 2010, pp. 2646-2657.

[8] P. Papadimitratos and A. Jovanovic, Protection and fundamental vulnerability of GNSS, in *Proc. Satellite and Space Communication 2008*, Toulouse, France, 2008, pp. 167-171.

[9] D. P. Shepard and T. E. Humphreys, Characterization of receiver response to spoofing attacks, in *Proc. 24th International Technical Meeting of the Satellite Division of the Institute of Navigation*, Portland, OR, US, 2010, pp. 2608-2619.

[10] J. M. Kelly, M. S. Braasch, and M. F. DiBennedetto, Characterization of the effects of high multipath phase rates in GPS, *GPS Solutions,* vol. 7, no. 1, pp. 5-15, 2003.

[11] P. Axelrad and R. G. Brown, GPS navigation algorithms, in *Global Positioning System: Theory and Applications*, B. W. Parkinson and J. J. Spilke, Ed. Washington DC: American Institute of Aeronautics and Astronautics, 1996, pp. 409-433.

[12] E. D. Kaplan and C. J. Hegarty, *Understanding GPS: Principles and Applications, Second Edition*. Boston, USA: Artech House, 2005.

Yang Gao received his BEng degree in electronic and information engineering from Tsinghua University, Beijing, China, in 2007. He is currently a PhD candidate of information and communication engineering at the Department of Electronic Engineering, Tsinghua University. His research interests include satellite positioning and statistical signal processing.

Hong Li received his BS degree in electronic engineering from Sichuan University, Chengdu, China, in 2004, and received his PhD degree in electronic engineering from Tsinghua University, Beijing, China, in 2009. His current interests include signal processing and satellite positioning and navigation.

Mingquan Lu received his MS degree in electronic engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 1993. He joined the Department of Electronic Engineering of Tsinghua University, Beijing, China, in 2003 and is currently a professor at the Institude of High-speed Signal Processing and Network Transmission, Tsinghua University. His research interests include signal processing, simulation of satellite navigation system, and local area navigation system.

Zhenming Feng received his BEng and MEng degrees in electronic engineering from Tsinghua University, Beijing, China, in 1970 and 1981, respectively. He has been with the Department of Electronic Engineering, Tsinghua University, since 1970, where he became a professor in 2000. Before 1990, his research direction was radar signal processing. Now his research interests include broadband access networks, satellite positioning and navigation, and wireless communications.