GNSS Receiver Tracking Performance Analysis under Distance-Decreasing Attacks

Kewei Zhang and Panos Papadimitratos
Networked Systems Security Group
KTH Royal Institute of Technology, Stockholm, Sweden
Email: {kewei, papadim}@kth.se

***Abstract*—Numerous works have investigated the vulnerability of Global Navigation Satellite Systems (GNSS) against attacks. Upcoming systems make provisions for cryptographic civilian signal protection. However, this alone does not fully protect GNSS-based localization. In this paper, we show that attacks at the physical layer, without modification of navigation messages, can be severely effective. We analyze the influence of the, so called distance decreasing attacks, and we investigate their feasibility and we find that they can be practical and effective. Finally, we consider signal quality monitoring, but it can not readily serve as a countermeasure.**

***Keywords*—GNSS; Distance decreasing attacks; Tracking**

I. Introduction

Nowadays, numerous systems and applications rely on GNSS, with an ever-increasing importance of accurate positioning and clock synchronization. The broader the deployment and the higher the degree of reliance on GNSS, the more significant becomes the risk to attack and abuse the GNSS functionality. This can be critical for civilian applications, especially those with higher risk, exactly because GNSS are inherently vulnerable. In fact, this can render the GNSS-based positioning a weak link: for example, rather than hacking into a location-based mobile computing system (e.g., a truck fleet monitoring system), an attacker can forge or replay GNSS signals and dictate the location (and time offset) the GNSS receiver calculates [1–8].

Cryptographic protection has been proposed to secure against forgery of GNSS signals, i.e., *spoofing* attacks [9, 10]. This has led to the integration of security services for the upcoming Galileo system [11]. Assume now broadly available cryptographically protected civilian GNSS in the near future. This can significantly improve protection but it cannot eradicate the GNSS vulnerability. On the one hand, it remains possible to record and replay GNSS signals (without modifying them, to avoid their rejection after the cryptographic validation of the navigation messages). More interesting, it is possible for an attacker (adversary) to exploit the physical layer operation (again, without modifying the transmitted data), influence the ranging functionality and thus affect the calculated position. One special type of the attack, *distance decreasing (DD)* attacks, can modify the receiver's position by decreasing the pseudo-range estimation. Distance-decreasing attacks were first introduced in [12] and were later investigated in [13] and follow-up works for impulse radio ultra wide band (IR-UWB) ranging. Essentially, the attacker can decrease a distance up to the point that corresponds to a fraction of symbol duration.

978-1-4799-9858-6/15/$31.00

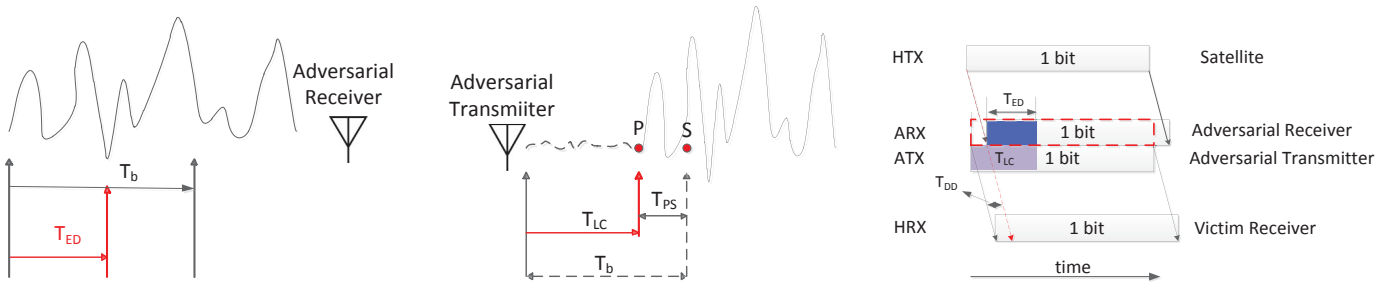
The mounting and the effectiveness of the attacks are physical layer specific. For GNSS, notably the Global Positioning System (GPS), a bit duration is 20ms, gives, in principle ample time to mount an effective attack. For example, the shortening of a pseudo-range by 15 km can be achieved by 0.05 ms time shift. The trade-off is, however, that the DD attack increases the probability of erroneous decoding at the victim (legitimate receiver). This implies that the attacker has to configure the attack to not only shorten the distance but also maintain the error probability very low. The induced errors were looked at in [14].

In this paper, we explore the distance decreasing attack (Sec. II) and formulate analytically its effectiveness (Sec. III). Then, with the help of simulations, the attack effect on a single pseudo-range and the resultant perceived displacement of the victim receiver are illustrated (Sec. III). Moreover, we simulate the tracking performance of an *honest receiver (HRX)* under DD attack in different setups and find that it is hardly detectable with signal quality monitoring (Sec. IV).

II. Distance-Decreasing (DD) Attacks

Consider, without loss of generality, an *honest transmitter (HTX)* and an *honest receiver (HRX)* representing a satellite and a legitimate receiver respectively. The *adversarial receiver (ARX)* and the *adversarial transmitter (ATX)* are deployed by the adversary to receive and relay the signals. The attack comprises two phases: the *early detect (ED)* and the *late commit (LC)*, implemented at the ARX and ATX respectively. Basically, the ARX does not decode a received bit at the end of its duration but rather attempts to do so prematurely (early), based on a fraction of the received symbol (bit) within some time $T_{ED} < T_b$, where T_b is the bit duration (length) (see Fig. 1a). At the same time, the ATX, in sync with ARX, performs a late commit: rather than initiating a bit transmission once it has the bit relayed by the ARX, the ATX starts with a near-noise transmission for some time $T_{LC} < T_b$; once it receives the value of the bit decoded (early) by the ARX, the ATX transmits the corresponding signal for the remaining part of the bit (see Fig. 1b).

The overall attack is presented in Fig. 1c: if the ATX late-committed transmission is successfully decoded by the HRX, then the perceived beginning of the bit (black arrow) is earlier than the beginning of the reception of the actual HTX signal, had it propagated to the HRX (red dotted arrow). This difference is shown as T_{DD}. Essentially, the gained time is proportional to the chosen values T_{ED}, T_{LC}, in fact, their difference: $T_{DD} = T_{LC} - T_{ED}$. Nonetheless, the



(a) Early detect at the ARX.

(b) Late commit at the ATX.

(c) Effect of the distance decreasing attack.

Fig. 1: Principle of distance decreasing attack.

lower T_{ED} the more likely it is that the ARX decodes the bit erroneously. Similarly, the higher T_{LC} the more likely it is that HRX decodes the adversarial transmission erroneously. This implies that the adversary should configure its attack, choosing the targeted T_{DD} and thus the distance decrease, so that the resultant bit error rate (BER) remains low.

The value of T_{DD} of course depends on how fast the ARX can communicate with the ATX; in the above exposition, for the sake of simplicity, we considered this negligible. But, actually, $T_{DD} = T_{LC} - T_{ED} - T_{delay}$, with T_{delay} the processing ARX-ATX communication latency. ARX and ATX need to be appropriately equipped to keep T_{delay} low. Given the significant length of the GPS bits, this is not a hard requirement to meet. As it will be made clear in the rest of the paper, it is easy to achieve T_{DD} in the order of $1ms$ and thus distance (pseudo-range) shortening in the order of tens or hundreds of km.

III. Analysis Results

The bit error rate (BER) at an honest receiver, after demodulation, is [15]:

$$P_b = \frac{1}{2} erfc\left(\sqrt{\frac{C/N_0}{R_b}}\right) = \frac{1}{2} erfc\left(\sqrt{\frac{C}{N_0} T_b}\right), \quad (1)$$

where T_b is the symbol length, R_b is the data rate and $erfc(x) = \frac{2}{\sqrt{\pi}} \int_{t=x}^{\infty} e^{-t^2} dt$ is the complementary error function.

The distance decreasing attack, both ED and LC, increase the BER because of the increased uncertainty about the transmitted symbol. Eq. (1) assumes that the BER is determined based on all symbol samples. However, the ARX determines the symbol based on samples over T_{ED}, thus the probability of error with early detection is :

$$P_{ED} = \frac{1}{2} erfc\left(\sqrt{\frac{C}{N_0} T_{ED}}\right). \quad (2)$$

When the attacker implements only the late commit phase, the symbol transmission by the ATX is essentially in two parts (Fig. 1c): the first, for T_{LC}, before knowing the symbol value, and the second, based on the detection result (based on whole symbol length, assuming no early detection were attempted). The question is what ATX can transmit during the first part of its late-committing transmission. There can be different strategies: for example, if the ATX transmits practically noise, then the first T_{LC} part of the symbol will make no contribution the HRX demodulation. Thus, the probability of error introduced by the late commit phase is:

$$P_{LC} = P_b + (1 - P_b) \times \frac{1}{2} erfc\left(\sqrt{\frac{C}{N_0}(T_b - T_{LC})}\right), \quad (3)$$

where P_b is the BER for the detection based on the entire symbol (bit) energy ((1)).

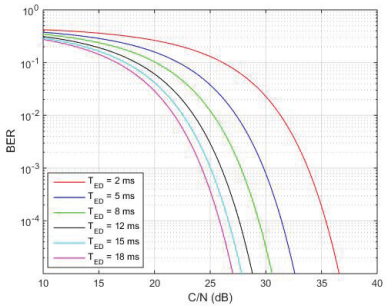
When LC is combined with ED, compared to (3), the only difference would be the time used for symbol detection. Thus, the BER is :

$$P_{DD} = P_{ED} + (1 - P_{ED}) \times \frac{1}{2} erfc\left(\sqrt{\frac{C}{N_0}(T_b - T_{LC})}\right), \quad (4)$$

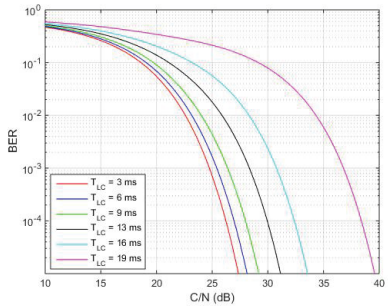
where P_{ED} is obtained by (2).

Figs. 2a-2c show that, indeed, the longer the early detection time, T_{ED}, the lower the BER will be. The closer to T_b, the more the ARX resembles to an honest receiver. On the other hand, the longer the late commit time, T_{LC}, the higher the BER will be (in extremis, $T_{LC} \to T_b$ implies no actual signal). We do not vary T_{LC} in Fig. 2c but rather fix $T_{DD} = T_{LC} - T_{ED}$ to a value ($1ms$). Increasing T_{ED} will reduce BER, but high T_{ED} implies T_{LC} grow too, which pushes BER high. For instance, in Fig. 2c, BER for $T_{ED} = 18ms$ is higher than that for $5ms$. Thus the meaningful ATX transmission will be limited in duration accordingly.

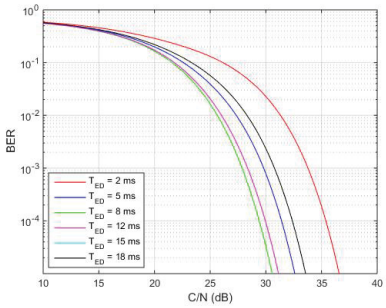
Now we assume that a distance decreasing attack is mounted to modify one pseudo-range. Consider constellations based on data obtained from [16] as shown in Fig. 3. Then, depending on the relative position of the victim and the attacked (ith satellite-receiver) communication, the displacement changes, shown in Fig. 4, this in the order of hundreds of km, commensurate with the extend of shortening $T_{DD} = 1ms$ ($300km$). In Fig. 3, we see that satellite 3 has the biggest elevation angle and satellite 16 has the smallest one oppositely. As a result, in Fig. 4, the effect of position shift by changing ρ_3 is much more pronounced than that for changing ρ_{16}.



(a) BER for early detect, P_{ED}.



(b) BER for late commit, P_{LC}.



(c) BER, P_{DD}, for targeted $T_{DD} = 1ms$, assuming same noise conditions for ARX and HRX.

Fig. 2: BER for different DD attack scenarios.

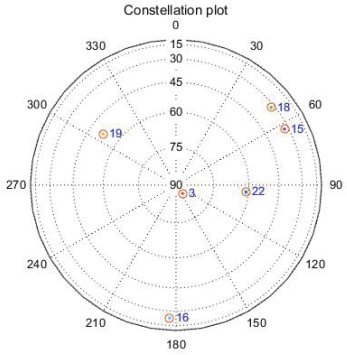


Fig. 3: Constellation of 6 available satellites.

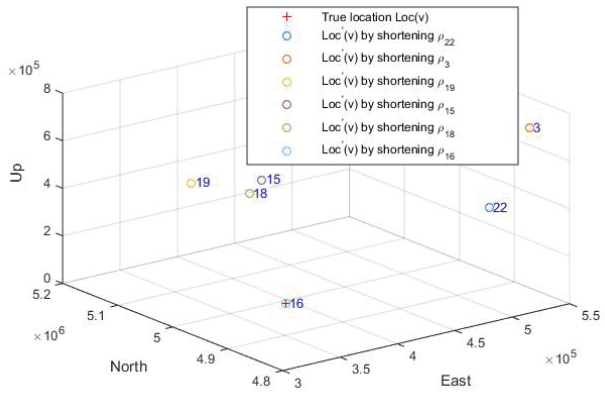


Fig. 4: Distance decreasing (DD) attack effect for $T_{DD} = 1ms$: actual HRX position (red '+'), and induced position through a DD attack on the pseudo-range estimate for one satellite ('o' labeled for the corresponding satellite).

IV. Tracking Performance Evaluation

Assuming HRX is in cold-start mode, or having lost lock on the HTX signals after being jammed by the adversary, we experiment with DD attacks and the resultant signals at the HRX. The ARX front-end has, as a generic GNSS receiver, bandpass filters (BPF), amplifiers, a local oscillator and an analog-to-digital converter (ADC). The ARX does common acquisition to obtain coarse signal frequency and code phase, and hereafter implements ED and LC during the signal tracking. Consider signal tracking at the ARX: as Fig. 5a shows, generic GNSS receivers utilize 20 ms (20 CA codes) to determine the bit value, and continuously calculate phase error and code error with 1 ms (CA code) interval with help of previous errors, till end of processing. However, the ARX, as shown in Fig. 5b, conveys the bit detection result, including current carrier and code phases, to ATX at end of the T_{ED}. During $\{T_b - T_{ED}\}$, the ARX continuously estimates phase and code errors; and the next bit uses these estimation to enable continuous bit detection. Two parts of signal transmitted by the ATX are shown in Fig. 6: T_{LC}, which is built on the previous bit detection result, and $\{T_b - T_{LC}\}$, which is built on the current bit detection result. Therefore the junction of these two components could have different tracking effects at the HRX based on different equipment setups.

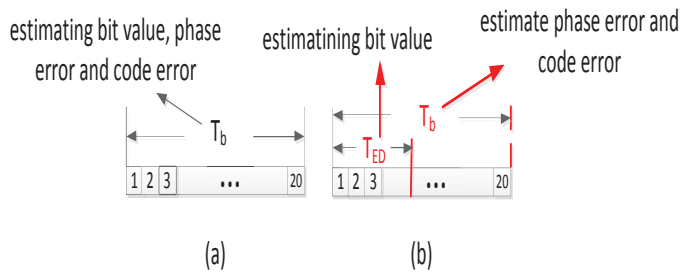


Fig. 5: *Early detection* details on tracking, (a) shows generic receiver; (b) shows ARX; $1, 2, \ldots, 20$ represents ms.

Carrier Phase Tracking: As described before, the signal arriving at the HRX is a bit in Fig. 6 plus noise. The received signal bit at the HRX can be modeled with

$$S(t) = n(t) + \begin{cases} CA(t)B(t-\tau_1(t))cos(2\pi ft + \theta_1(t)) & 0 \le t < \frac{T_{LC}}{2} \\ CA(t)\left(-B(t-\tau_1(t))\right)cos(2\pi ft + \theta_1(t)) & \frac{T_{LC}}{2} \le t < T_{LC} \\ CA(t)B(t-\tau_2(t))cos(2\pi ft + \theta_2(t)) & T_{LC} \le t \le T_b \end{cases}, \quad (5)$$

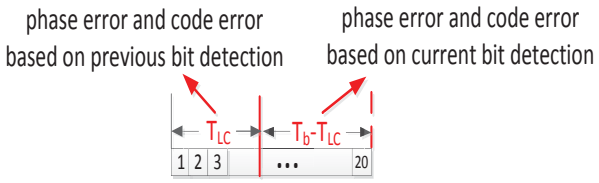


Fig. 6: *Late commit* details, bit structure on ATX.

where $n(t)$ is noise, $CA(t)$ is CA code, $B(t)$ is the bit value$\{\pm 1\}$, $\tau_{\{1,2\}}$ and $\theta_{\{1,2\}}$ are signal code delay and phase corresponding to T_{LC} and $\{T_b - T_{LC}\}$ in Fig. 6. We split T_{LC} into two equal intervals ($\frac{T_{LC}}{2}$), transmitting two values $\{\pm 1\}$ (instead of noise). Then, after signal integration at the HRX, the energy of the first two parts of $S(t)$ will be eliminated to zero approximately. However, these two parts will contribute to the code and phase estimation.

For carrier tracking, the Costas loop is the phase locked loop (PLL) in GNSS receivers as it is insensitive to phase transitions due to navigation bits [16]. Therefore the first two parts of (5) could be merged when analyzing phase tracking errors. Several common Costas loop discriminators are described in [15]; here we use the arctangent discriminator $ATAN(Q_p/I_p)$ in our simulation to detect the phase error. The closed Costas loop is presented in Fig. 7, when feeding $S(t)$ to this Costas loop, the Q arm yields (assuming the code replica is perfectly aligned):

$$\begin{aligned} &sin(2\pi ft+\Delta)cos(2\pi ft+\theta_1(t))\,[u(t)-u(t-T_{LC})]+\\ &sin(2\pi ft+\Delta)cos(2\pi ft+\theta_2(t))\,[u(t-T_{LC})-u(t-T_b)]\\ &=\frac{1}{2}\left[sin(\Delta-\theta_1(t))+\frac{1}{2}sin(2\pi 2ft+\Delta+\theta_1(t))\right]\times\\ &\quad[u(t)-u(t-T_{LC})]+\\ &\quad\frac{1}{2}\left[sin(\Delta-\theta_2(t))+sin(2\pi 2ft+\Delta+\theta_2(t))\right]\times\\ &\quad[u(t-T_{LC})-u(t-T_b)]\,, \end{aligned} \tag{6}$$

where $u(t)$ is step function and Δ is the local carrier phase. The I arm gives:

$$\begin{aligned} &cos(2\pi ft+\Delta)cos(2\pi ft+\theta_1(t))\,[u(t)-u(t-T_{LC})]+\\ &cos(2\pi ft+\Delta)cos(2\pi ft+\theta_2(t))\,[u(t-T_{LC})-u(t-T_b)]\\ &=\frac{1}{2}\left[cos(\Delta-\theta_1(t))+\frac{1}{2}cos(2\pi 2ft+\Delta+\theta_1(t))\right]\times\\ &\quad[u(t)-u(t-T_{LC})]+\\ &\quad\frac{1}{2}\left[cos(\Delta-\theta_2(t))+cos(2\pi 2ft+\Delta+\theta_2(t))\right]\times\\ &\quad[u(t-T_{LC})-u(t-T_b)]\,. \end{aligned} \tag{7}$$

When the I and Q signals are lowpass-filtered, with the high frequency terms eliminated, the remaining signals are:

$$Q=\begin{cases} 1/2sin(\Delta-\theta_1(t)) & 0\le t\le T_{LC}\\ 1/2sin(\Delta-\theta_2(t)) & T_{LC}<t\le T_b \end{cases} \tag{8}$$

and

$$I=\begin{cases} 1/2cos(\Delta-\theta_1(t)) & 0\le t\le T_{LC}\\ 1/2cos(\Delta-\theta_2(t)) & T_{LC}<t\le T_b \end{cases}. \tag{9}$$

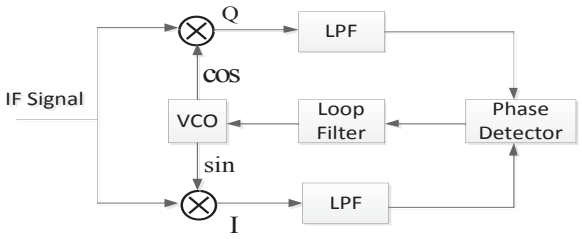


Fig. 7: Closed Costas loop for carrier tracking.

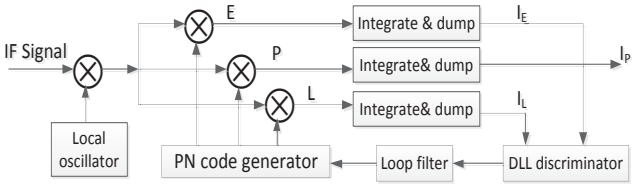


Fig. 8: I arm of non-coherent delay-lock loop.

Then the arctangent discriminator outputs:

$$\arctan\frac{Q}{I}=\begin{cases} \Delta-\theta_1(t) & 0\le t\le T_{LC}\\ \Delta-\theta_2(t) & T_{LC}<t\le T_b \end{cases}. \tag{10}$$

Eq. (10) shows there is a phase jitter, $|\theta_2(T_{LC})-\theta_1(T_{LC})|$, at the junction of T_{LC} and $\{T_b - T_{LC}\}$. However, this phase jitter could not serve as evidence to detect the existence of the DD signal. Because $\theta_1(t)$ and $\theta_2(t)$, corresponding to $\{T_{LC}\}$ and $\{T_b - T_{LC}\}$ in Fig. 6, are based on continuous detection results. Therefore $\theta_1(t)$, $\theta_2(t)$ will have the same variance if ARX does not loose track.

Code Tracking: The code tracking loop of a GNSS receiver is a delay locked loop (DLL), also called early-late tracking loop. The basic idea is to correlate the incoming signal with three replicas of CA code, shown in Fig. 8 (only I arm). The characteristics for different discriminators for common delay lock loops are analyzed in [15]; among those $\frac{1}{2}\frac{(I_E^2+Q_E^2)-(I_L^2+Q_L^2)}{(I_E^2+Q_E^2)+(I_L^2+Q_L^2)}$ is chosen here because it is independent of the PLL performance as it uses both the I and Q arms [16].

Similar to the carrier phase tracking, because of the continuous bit estimation, the code phase at the ATX will be a good estimation of signal at the ARX, if ARX can smoothly track the signals. As a result, the performance of tracking output about code phase at the HRX will show a similar trend, except for the first bit.

A. Discriminators Output Results

In our simulation, civilian GPS signals were analyzed. Signal-to-noise ratio (SNR) is calculated by typical values in an L1 Coarse/Acquisition (C/A) code receiver, carrier-to-noise ratio (C/N_0) $\sim$ 37 to 45 dB-Hz, with 4MHz front-end bandwidth $SNR = C/N_0 - BW \sim$ -29dB to -21dB [17]. Consider the analytical result in Fig. 2: in our simulation choosing $C/N_0 = 41$dB-Hz at ARX results into $SNR = -25$dB. This indeed gives extremely low BER in the simulation too, thus

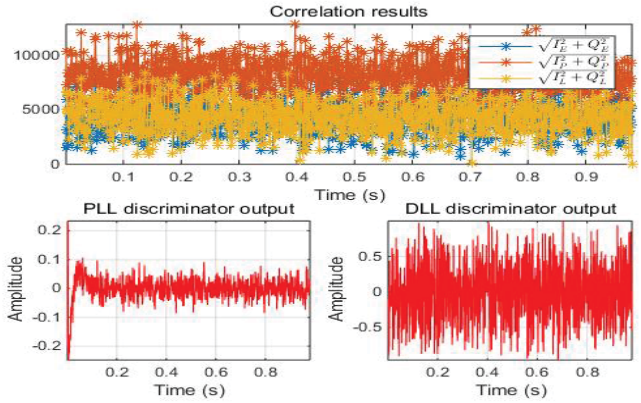


Fig. 9: Tracking performance at HRX when both ARX and ATX are implemented, with $SNR = -25$dB and $T_{ED} = 13$ms, $T_{LC} = 14$ms; variance of DLL discriminator output is 0.0725 and variance of PLL discriminator output is 0.0017.

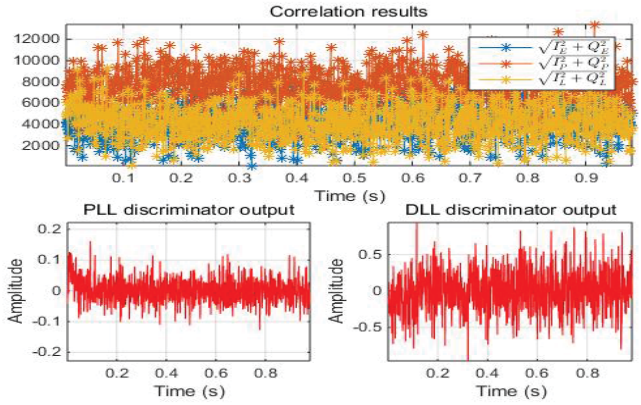


Fig. 10: Tracking performance at HRX with legitimate signal when $SNR = -25$dB; variance of DLL discriminator output is 0.0737 and variance of PLL discriminator output is 0.0016.

we examine the receiver tracking outputs, instead of BER. The adversary can control the SNR between the ATX and HRX (e.g. changing the transmission power). In our simulation, we assume the same SNR at the HRX too (e.g., choice of good placement of ATX with respect to HRX).

Fig. 9 and Fig. 10 illustrate the tracking outputs at the HRX: in the presence of the DD attack (lock on the adversarial signal) (Fig. 9) and only for the legitimate signal (Fig. 10). One might consider the PLL discriminator output for the first bit of the DD attack signal. However, whether this could serve to detect the attack is not clear: it depends on whether the HRX has already locked on some legitimate signal prior to onset of the attack and we have no conclusive evidence it would effectively differentiate DD signals.

We plotted these two figures based on $T_{ED} = 13$ms and $T_{LC} = 14$ms, and we also examined the results for the cases of $T_{ED} = 3$ms, $T_{LC} = 4$ms and $T_{ED} = 7$ms, $T_{LC} = 8$ms listed in Tab. 1 always maintaining $T_{DD} = 1ms$. It shows that there is no obvious difference for different configurations. The reason is that in our simulation the result of acquisition is

TABLE 1: Variance of DLL and PLL discriminators with different configuration

SNR = -25 dB			
Parameters (ms)	$T_{ED} = 3$ $T_{LC} = 4$	$T_{ED} = 7$ $T_{LC} = 8$	$T_{ED} = 13$ $T_{LC} = 14$
$\mathbf{Var_{pll}}$	0.0017	0.0016	0.0017
$\mathbf{Var_{dll}}$	0.0758	0.0697	0.0725

pretty good and it needs very short time to track carrier phase and code phase. For actual receivers, acquisition can be much worse than in the idealized simulation, thus leading to more pronounced variances for different setups.

B. Signal Quality Monitoring

Signal quality monitoring (SQM) has been developed to test degraded or incorrect GPS signals in safety-of-life navigation or positioning, for instance civil aviation [18, 19]. In US, the Wide-Area Augmentation System (WAAS) and Local-Area Augmentation System (LAAS) report such failure information to users. The decision process, for instance the Neyman-Pearson lemma, on a failure or success is implemented with statistical hypothesis tests. Two common SQM detection tests are the delta test (Δ-*test*) and ratio test [20]. The Δ-test measures the differences between the early and late correlator outputs, normalized by the prompt correlator output to identify asymmetric correlation peaks:

$$\Delta = \frac{\tilde{I}_{early} - \tilde{I}_{late}}{2\tilde{I}_{prompt}}, \tag{11}$$

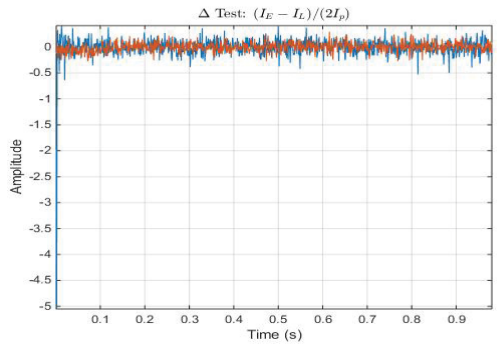
where I indicates in-phase samples. The ratio test is defined to monitor flat correlation peaks and abnormally sharp or elevated correlation peaks:

$$R = \frac{\tilde{I}_{early} + \tilde{I}_{late}}{2\tilde{I}_{prompt}}. \tag{12}$$

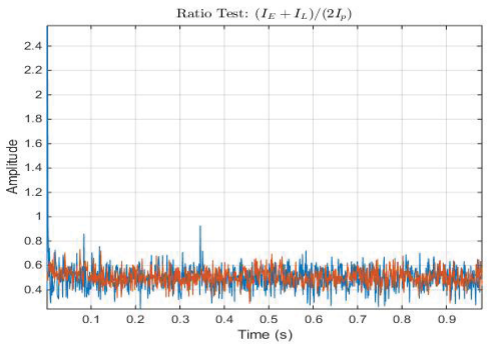
These two tests assume the carrier loop is completely phase-locked. We implemented them to see whether they can identify the relay signal at the HRX (Fig. 11). There are no flat correlation peaks or sharp correlation peaks when feeding both signals to the HRX. An abnormal correlation peak only occurs at the beginning of the signal (the first bit). Same as discriminator outputs, we do not have conclusive evidence on whether the forged signal exists or not.

V. Discussion and Conclusion

Constructing a counterfeit signal with local carrier replicas and spreading code replicas, the adversary needs a precise clock (oscillator) to reproduce the carrier frequency and code phases; to perfectly align with the authentic signals not to introduce additional clock errors to the HRX clock. Moreover, the adversary needs to know approximately the velocity of the victim, in order to manipulate the Doppler effect. Without jamming at the beginning of (prior to) the DD attack, the adversary sends a relatively low-power signal to disguise itself as multi-path at the HRX; when it is aligned with the authentic signals, the adversary gradually increases its transmission power to hijack the tracking process at the HRX (and eventually take over the lock from the satellite(s)) [1].



(a) Delta test.



(b) Ratio test.

Fig. 11: Red lines indicate authentic signal; blue lines are results of combination of relay and authentic signals.

We investigated the effect and practicality of distance decreasing attacks (DD) against civilian GPS signals. The attacker's ability to significantly affect positioning remains a threat even if the navigation message is authenticated. It is interesting to investigate in future work if spreading code authentication can thwart DD attacks; or if a variant of the attack could be devised. Another item of our future work is to investigate the cumulative effect of DD attacks on multiple signals and on imposing a sought position (or trajectory) on the victim (HRX).

REFERENCES

[1] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr, "Assessing the Spoofing Threat," *GPS World*, vol. 20, no. 1, pp. 28–38, 2009.

[2] T.-H. Kim, C. S. Sin, and S. Lee, "Analysis of effect of spoofing signal in GPS receiver," *IEEE ICCAS*, Jeju, 2012.

[3] P. Papadimitratos and A. Jovanovic, "Protection and fundamental vulnerability of GNSS," *IEEE IWSSC*, Toulouse, France, 2008.

[4] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," *ION International Technical Meeting*, Savannah, GA, 2009.

[5] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS Signal Spoofing," *ION GNSS*, Long Beach, CA, 2005.

[6] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," *ACM CCS*, Chicago, IL, 2011.

[7] P. Papadimitratos and A. Jovanovic, "GNSS-based Positioning: Attacks and Countermeasures," *IEEE MILCOM*, San Diego, CA, 2008.

[8] A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen, and G. Lachapelle, "GNSS spoofing detection in handheld receivers based on signal spatial correlation," *IEEE/ION PLANS*, US-SC, 2012.

[9] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-Time GPS Spoofing Detection via Correlation of Encrypted Signals," *Journal of ION*, vol. 60, no. 4, pp. 267–278, 2013.

[10] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *Journal of ION*, vol. 59, no. 3, pp. 177–193, 2012.

[11] J. T. Curran, M. Paonni, and J. Bishop, "Securing the Open-Service: A Candidate Navigation Message Authentication Scheme for Galileo E1 OS," *European Navigation Conference*, Rotterdam, Netherlands, 2014.

[12] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, "So near and yet so far: Distance-bounding attacks in wireless networks," *ACM SASN*, Alexandria, VA, 2006.

[13] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "Effectiveness of distance-decreasing attacks against impulse radio ranging," *ACM Wisec*, Hoboken, NJ, 2010.

[14] D. H. Arze Pando, "Distance-decreasing attack in global navivation satellite system," http://secowinetcourse.epfl.ch/previous/09/ArzePando. DanieHoracio/Final_Report.pdf.

[15] E. Kaplan and C. Hegarty, *Understanding GPS: principles and applications*. Artech House, 2005.

[16] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, *A software-defined GPS and Galileo receiver: a single-frequency approach*. Springer Science & Business Media, 2007.

[17] A. Joseph, "GNSS Solutions: Measuring GNSS Signal Strength," *Journal of Inside GNSS on Engineering Solutions for the GNSS Community*, vol. 5, no. 8, pp. 20–25, 2010.

[18] R. E. Phelts, D. M. Akos, and P. Enge, "Robust Signal Quality Monitoring and Detection of Evil Waveforms," *ION International Technical Meeting*, Salt Lake City, UT, 2000.

[19] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, "An in-line anti-spoofing device for legacy civil gps receivers," *ION International Technical Meeting*, San Diego, CA, 2010.

[20] R. E. Phelts, "Multicorrelator techniques for robust mitigation of threats to gps signal quality," Ph.D. dissertation, Stanford University, 2001.