AFRL-RV-PS-
TR-2022-0046

AFRL-RV-PS-
TR-2022-0046

# OPTIMAL PRN CODES AND RECEIVER DESIGN FOR MORE ROBUST AND SECURE SATELLITE NAVIGATION

**Grace Gao**

**Stanford University**
**496 Lomita Mall**
**Stanford, CA 94305**

**28 April 2022**

**Final Report**

**APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.**


**AIR FORCE RESEARCH LABORATORY**
**Space Vehicles Directorate**
**3550 Aberdeen Ave SE**
**AIR FORCE MATERIEL COMMAND**
**KIRTLAND AIR FORCE BASE, NM 87117-5776**

# DTIC COPY

# NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research which is exempt from public affairs security and policy review in accordance with AFI 61-201, paragraph 2.3.5.1. This report is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RV-PS-TR-2022-0046 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

| | |
|---|---|
| //SIGNED// | //SIGNED// |
| _____ | _____ |
| Benjamin J. Fogg | For: Erin N. Pettyjohn, Chief |
| Program Manager/AFRL/RVB | AFRL Geospace Technologies Division |

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

Approved for public release; distribution is unlimited.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

| **1. REPORT DATE** *(DD-MM-YYYY)* | **2. REPORT TYPE** | **3. DATES COVERED** *(From - To)* |
|---|---|---|
| 28-04-2022 | Final Report | 01 Jan 2020 – 31 Dec 2021 |

**4. TITLE AND SUBTITLE**

Optimal PRN Codes and Receiver Design for More Robust and Secure Satellite Navigation

**5a. CONTRACT NUMBER**
FA9453-20-1-0002

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**
63401F

**6. AUTHOR(S)**
Grace Gao

**5d. PROJECT NUMBER**
4846

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**
V1SD

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Stanford University
496 Lomita Mall
Stanford, CA 94305

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

Air Force Research Laboratory
Space Vehicles Directorate
3550 Aberdeen Avenue SE
Kirtland AFB, NM 87117-5776

**10. SPONSOR/MONITOR'S ACRONYM(S)**
AFRL/RVBYS

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**
AFRL-RV-PS-TR-2022-0046

**12. DISTRIBUTION / AVAILABILITY STATEMENT**
Approved for public release; distribution is unlimited (OPS-22-50555 dtd 11 May 2022).

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**
In this report, we present our work for more robust and secure satellite navigation: i) designing optimal Pseudo-Random Noise (PRN) codes; and receiver design using future Chimera Signals.
For optimal PRN code design, we developed a Gaussian policy gradient-based reinforcement learning algorithm which constructs high-quality families of spreading code sequences. We have demonstrated the ability of our algorithm to achieve better mean-squared auto- and cross-correlation than well-chosen families of equal-length Gold codes and Weil codes.
For receiver design using future Chimera Signals, we designed a method to provide continuous GPS signal verification between Chimera authentication times by using stochastic reachability analysis. We demonstrated that our spoofing detector probabilistically satisfies a user-defined false alarm requirement throughout the trajectory during nominal conditions, while demonstrating its ability to successfully detect spoofing during a simulated attack.

**15. SUBJECT TERMS**
satellite navigation, GNSS, optimal codes, receiver design

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON** |
|---|---|---|---|---|---|
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | | Benjamin J. Fogg |
| Unclassified | Unclassified | Unclassified | Unlimited | 18 | **19b. TELEPHONE NUMBER** *(include area code)* |

This page is intentionally left blank.

Approved for public release; distribution is unlimited.

## ACKNOWLEDGMENTS

This material is based on research sponsored by Air Force Research Laboratory under agreement number FA9453-20-1-0002. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

## DISCLAIMER

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the U.S. Government.

Approved for public release; distribution is unlimited.

# TABLE OF CONTENTS

# LIST OF FIGURES

**Figure** **Page**



Approved for public release; distribution is unlimited.

# 1. SUMMARY

In this report, we present our work for more robust and secure satellite navigation: i) designing optimal Pseudo-Random Noise (PRN) codes; and receiver design using future Chimera Signals.

For optimal PRN code design, we developed a Gaussian policy gradient-based reinforcement learning algorithm which constructs high-quality families of spreading code sequences. We have demonstrated the ability of our algorithm to achieve better mean-squared auto- and cross-correlation than well-chosen families of equal-length Gold codes and Weil codes.

For receiver design using future Chimera Signals, we designed a method to provide continuous GPS signal verification between Chimera authentication times by using stochastic reachability analysis. We demonstrated that our spoofing detector probabilistically satisfies a user-defined false alarm requirement throughout the trajectory during nominal conditions, while demonstrating its ability to successfully detect spoofing during a simulated attack.

# 2. OPTIMAL PRN CODE DESIGN

## 2.1. INTRODUCTION

On January 13th of 2020, the U.S. Air Force 2nd Space Operations Squadron (2 SOPS) issued a statement that the first GPS III satellite was marked healthy and available for use [1]. This announcement officially marked the birth of the next-generation GPS constellation. In addition to broadcasting the new L1C signal, the modernized constellation is distinguished by its reprogrammable payload, which allows it to evolve with new technologies and changing mission needs. Furthermore, with the upcoming launch of the Navigation Technology Satellite-3 (NTS-3) testing platform in 2022 [2], the United States Air Force (USAF) seeks to explore technologies which will help shape future GPS constellations [3]. NTS-3 will demonstrate the agility of the next-generation satellite-based navigation architecture and the ability to rapidly deploy new technological advancements and capabilities via the reprogrammable nature of the upcoming GPS system. Indeed, this is the third Navigation Technology Satellite (NTS) mission, with the previous two, NTS-1 and NTS-2, developed in the 1970s in order to validate technologies, including the rubidium and cesium atomic clocks [4], that were integrated into the first generation of GPS satellites launched later that decade [5]. The NTS-3 program will further test several new technologies, including new signal designs for improved GPS security and interference mitigation [3]. According to a Request for Information announcement [6], the AFRL has expressed interest in exploring modifications to all layers of the GPS signal in order to enhance PNT resiliency and performance. We are indeed entering a new era of satellite navigation. However, many of the GPS spreading codes are based on linear shift feedback registers (LFSRs) [7], which were designed decades ago before personal computers. As a result, it is time to revisit the design methods of the GPS spreading code families.

## 2.2. METHODS, ASSUMPTIONS, AND PROCEDURES

In our work, we seek to explore using reinforcement learning techniques for the application of navigation spreading code design. To the best of our knowledge, this is the first work which explores using a machine learning approach for designing navigation spreading code signals. In particular, the key contributions of our work are the following:
1. We develop a policy gradient reinforcement learning algorithm which constructs high-quality families of spreading code sequences.
2. We utilize a Gaussian policy to represent a distribution over the action space which designs the binary codes.
3. We incorporate a baseline to reduce variance in the policy gradient estimate and to improve the agent's rate of learning.
4. We use a maximization evaluation metric to ensure the algorithm minimizes both the auto-correlation and crosscorrelation characteristics of the spreading codes simultaneously. With our algorithm, we demonstrate the ability to achieve low auto- and cross-correlation side peaks within the family of spreading codes. We further compare the correlation performance of the learned spreading codes with those of well-chosen families of equal-length Gold codes and Weil codes as well as with an analogous genetic algorithm implementation assigned the same code evaluation metric as our proposed algorithm.

### 2.2.1. Proposed Reinforcement Learning Framework

For the spreading code design application, the reinforcement learning agent is a code generator which takes in an initial set of spreading codes and follows its policy to output a modified code sequence. The resulting action is then evaluated and assigned a reward value by a code evaluator, which is utilized to update the policy parameters of the agent in order to improve its policy.

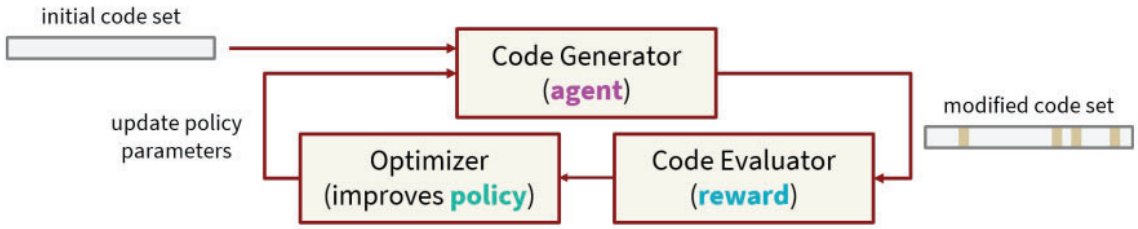



Figure 1. Proposed reinforcement learning framework for spreading code generation

### 2.2.2 GAUSSIAN POLICY FUNCTION REPRESENTATION

Using a neural network architecture, we represent the policy function as a distribution over the set of bits to toggle from the initial code set. Thus, the policy parameters correspond to the hidden layers of the network. As depicted in Fig. 2, for the agent to output a set of binary codes, it must sample from this toggle distribution provided by its currently learned policy function.

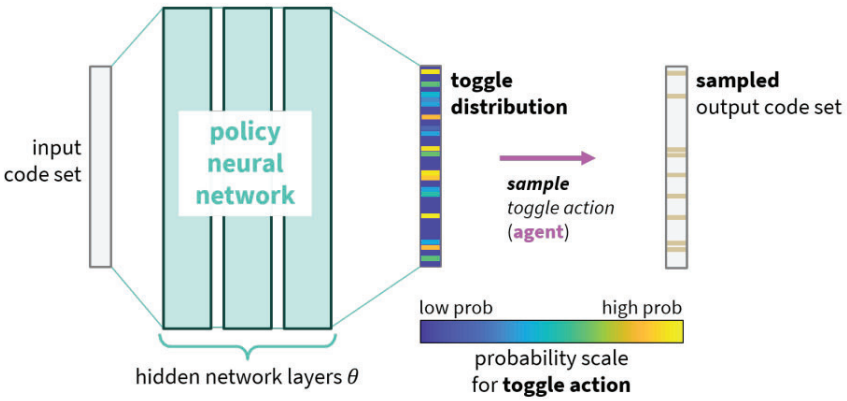



Figure 2. Illustration of policy network representation

### 2.2.3 SPREADING CODE EVALUATION METRIC

In order to learn a useful set of spreading codes, the agent must learn to minimize both the auto-correlation and cross-correlation characteristics of the generated code set. The evaluation metric provides the agent feedback to improve its policy function for code generation. We utilize the mean-square non-central auto-correlation and the mean-square cross-correlation as the two objectives to minimize.

## 2.3. RESULTS AND DISCUSSION

We validate the ability of our algorithm to devise low-correlation spreading code sequences and further compare its performance with that of well-chosen families of equal-length Gold codes and Weil codes. We compare the performance of our algorithm with Gold codes of length-63, 127, and 511. Similarly, since Weil codes only exist for sequence lengths that correspond to a prime number length, we compare our algorithm with Weil codes of length-67, 127, 257, and 521. From our policy gradient method, we generate sequences for family sizes of 3 codes up to 31 codes. We additionally compare our proposed algorithm with the best performing code set across 10, 000 sampled families of Gold codes and Weil codes. In few of the sample runs of Gold and Weil codes, we observed a large deviation in the auto- and cross-correlation cost components which frequently leads to worse performance on the overall objective. In these instances, we would resample the conventional code families, leading to an improvement in the performance metric of the Gold and Weil codes.

Fig. 3 shows the converged normalized mean-square auto- and cross-correlation performance of our policy gradient algorithm after training, comparing it with the best equal-length Gold and Weil code families of equal-length. We plot the final performance as a function of the code family size, with the normalized auto-correlation component RAC represented by the dashed lines and the normalized cross-correlation component RCC indicated by the solid lines. Because we conducted the experiments on a laptop with 16 GB of RAM, for sequences of greater than 500 bits in length, we only conducted tests for family sizes of up to 15 codes. However, by porting this algorithm on a system with more extensive computational resources, with access to GPU devices and increased RAM, we would be able to perform optimization for larger code

family sizes. Indeed, for each of the conducted tests, we observe in Fig. 3 that for all code lengths, the proposed policy gradient method in violet outperforms the best Gold code (in gold) and Weil code (in blue) families for both the auto- and cross-correlation objectives. We additionally observe in Fig. 3 that to perform well on the reward function, the policy gradient method learns to equalize the auto- and cross-correlation objectives, in order to avoid compromising one objective for the other and perform better on the overall maximization objective.

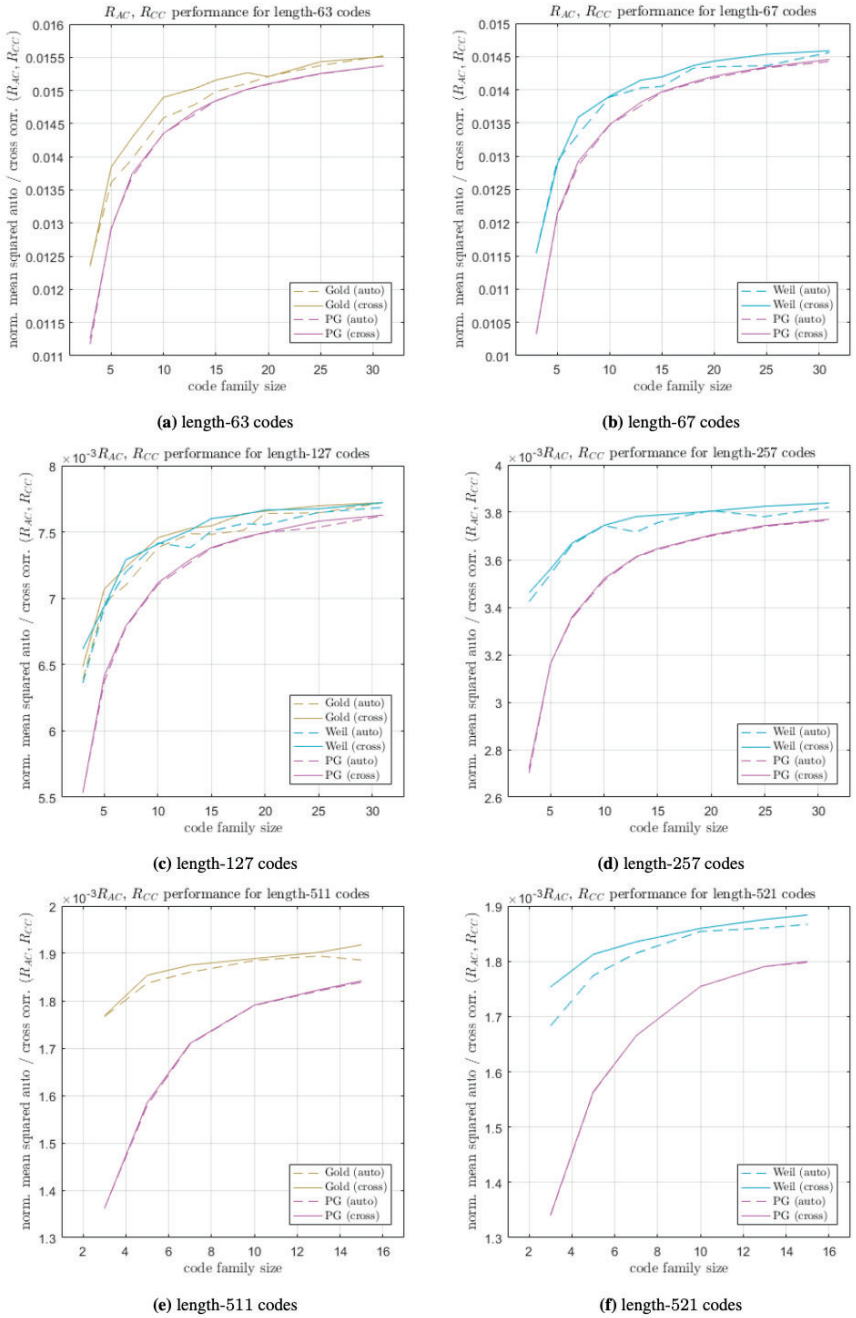



Figure 3. Comparison of the proposed policy gradient method with that of well-chosen Gold and Weil code families

# 3 CHIMERA RECEIVER DESIGN

## 3.1. INTRODUCTION

To provide secure navigation for civilian GPS users, the Air Force Research Lab (AFRL) has developed the Chips-Message Robust Authentication (Chimera) [8] signal enhancement for the GPS L1C signal [9]. Chimera inserts an encrypted signature within both the navigation message and the pilot channels of L1C to allow civilian users to jointly authenticate both components of the signal [10]. Furthermore, the AFRL will broadcast and test this signal enhancement on the upcoming Navigation Technology Satellite-3 (NTS-3) experimental platform, which will be launched in 2023 [11, 12]. If incorporated within the GPS L1C signal, the Chimera enhancement will be the first GPS signal encryption scheme available for civilian users, thereby enabling secure navigation for all future GPS users. To ensure the GPS signal cannot be forged by a malicious attacker, the Chimera-enhanced satellite segment will only publish the encryption key to the user segment after the subsequent key has already been updated. Users with access to only the GPS L1C signal receive the slow channel encryption key every 3 minutes within the GPS L1Cnavigation message, while users with access to secure out-of-band channels receive the fast channel encryption key every 6 seconds. With these encryption keys, users can authenticate their received GPS signal periodically at the rate of key reception. However, in either case, the Chimera signal authentication feature is not continuously available. In particular, even fast-channel users will experience a 6-second latency in signal authentication, whereas GPS position update rates for moving receivers, such as autonomous vehicles, typically occur at 5-20 Hz. To address this challenge, the present work develops a method to provide continuously available, authenticated navigation solutions using the Chimera signal. We utilize measurements from another self-contained sensor on-board the vehicle, such as an IMU, in order to validate the received GPS signal, while accounting for measurement uncertainties and unknown, bounded biases in the self-contained sensor and GPS measurements during authentic conditions.

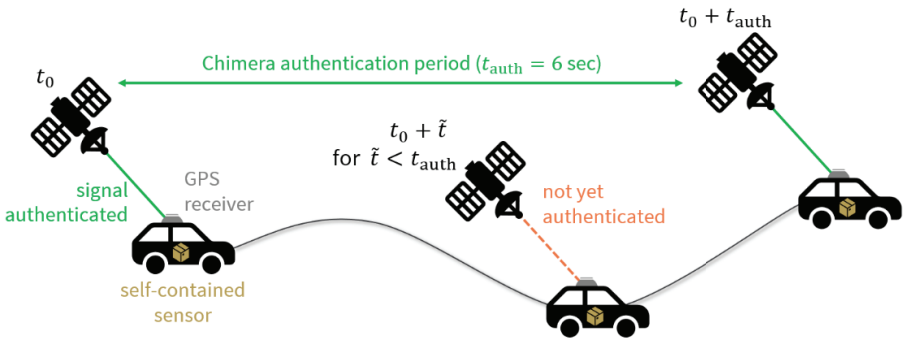
## 3.2. METHODS, ASSUMPTIONS, AND PROCEDURES

We propose a spoofing detector to provide continuous GPS signal verification between Chimera authentication times using stochastic reachability analysis inspired by recent methods such as [13–16]. We derive our spoofing detector and state estimator for a generic linear or nonlinear self-contained sensor model and with GPS positioning measurements. To experimentally validate our technique, we implement our algorithm for a ground receiver paired with (1) a linear sensor model of two-dimensional acceleration inputs in the navigation frame of reference, as well as (2) an on-board IMU sensor. At each time instant when the receiver position is updated, our formal verification method leverages the previously authenticated set of Chimera measurements in combination with known bounds on the measurement drift rates of the IMU sensor to ensure the detector meets a user-defined false alarm threshold on declaring a spoofing event.

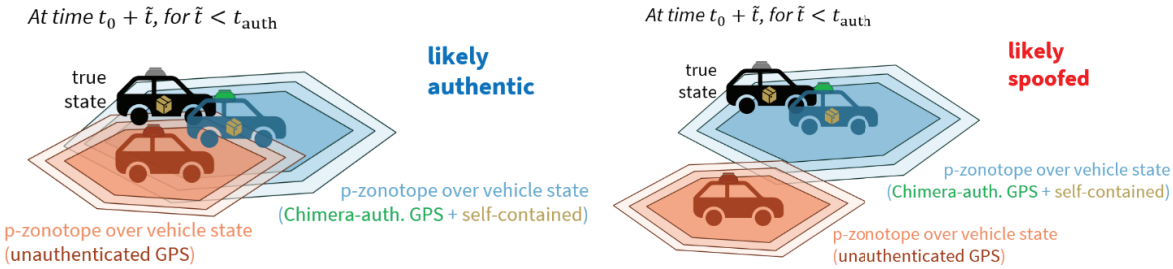
To address the challenges of point-valued spoofing detection methods and leverage the Chimera signal enhancement, our proposed formal verification technique:

1. enables continuous GPS signal verification between Chimera authentication times by validating the received signal against local, self-contained sensors;
2. provides a probabilistic overbound on the set of possible vehicle states for navigation, in the presence of both stochastic uncertainties and bounded measurement biases for the self-contained sensor and the GPS sensor during authentic conditions; and
3. evaluates a spoofing detection statistic that satisfies a user-defined false alarm metric, while accounting for potential biases in the self-contained sensor and GPS measurements during nominal, unspoofed operation.

The core idea of our proposed method is as follows, with an illustration of our method shown in Fig. 4 and the high-level architecture depicted in Fig. 4. Recall that, during the 6 second Chimera authentication period, the receiver obtains a series of unauthenticated GPS measurements, as shown in Fig. 4(a). Between the Chimera authentication times, we maintain a pair of receiver position state estimates, one of which is based on the unauthenticated GPS positioning measurements and the other which is initialized according to the previous Chimera-authenticated GPS measurements, then updated according to trusted, local, self-contained sensor, such as an Inertial Measurement Unit (IMU). We similarly maintain a pair of probabilistic zonotopes (p-zonotopes) on the receiver state error, one based on the variance and bounded biases from the unauthenticated GPS positioning measurements during authentic conditions, and the other which is computed via a stochastic reachability-based state estimation Kalman Filter (KF) using the self-contained sensor information. From the two stochastic reachable sets, we find the probabilistic set, or EPH, of expected errors between the estimators, under nominal, unspoofed conditions. To detect spoofing, we test if the current error between the estimators has sufficiently high likelihood within this EPH with respect to a user-defined false alarm condition, as shown in the final detector block in Fig. 5. Intuitively, if the received GPS signal is likely authentic, then we should observe significant overlap between the two p-zonotopes on the state estimate, as depicted in Fig 4(b). However, if the p-zonotope based on the unauthenticated GPS measurements is not sufficiently consistent with the p-zonotope based on the self-contained sensor information, as depicted in Fig. 4(c), then we declare the received GPS measurements as being likely spoofed. As depicted in Fig. 5, the output stochastic reachable state estimation takes in the detector decision as an input. While the detector outputs an “authentic” decision, the output stochastic reachability (SR) state estimator outputs the fused state estimate, based on the self-contained sensor measurement and the GPS measurements. Once the detector outputs a “spoofed” decision, the output SR state estimator switches to rely on the self-contained sensor filter untilit can reauthenticate the received GPS measurements via the Chimera enhancement.




**(a)** Illustration of problem statement applied to a ground vehicle model, over one Chimera fast channel epoch of $t_{\text{auth}} = 6$ seconds.




**(b) Likely authentic** scenario, at time step $t_0 + \tilde{t}$

**(c) Likely spoofed** scenario, at time step $t_0 + \tilde{t}$

Figure 4. Core idea and illustration of our Chimera receiver method

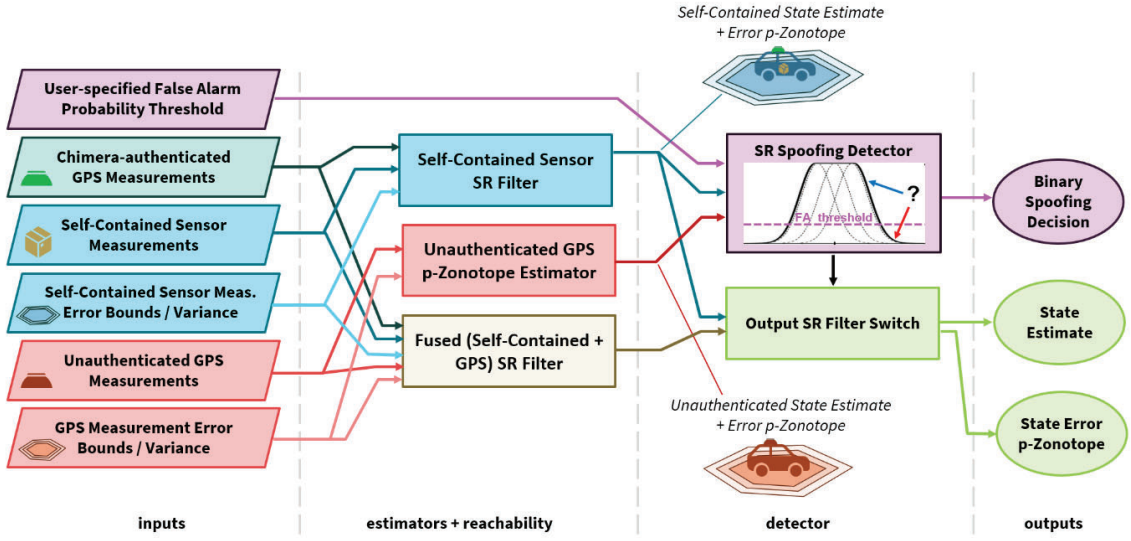
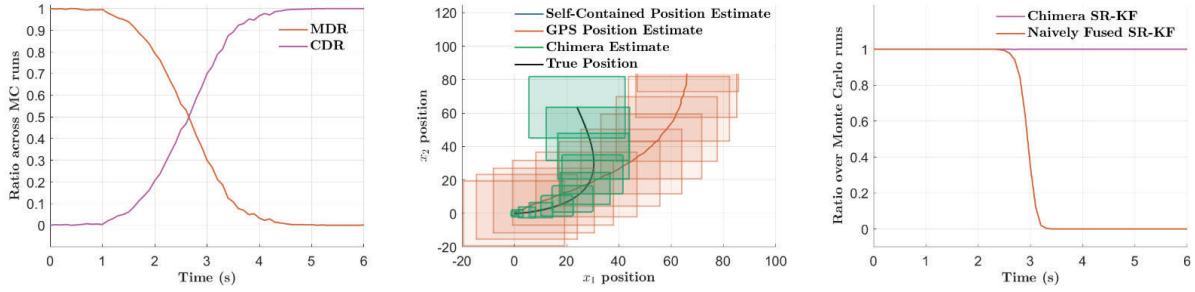



Figure 5. High-level architecture of our spoofing detector and stochastic reachability estimator for continuous Chimera-enhanced GPS signal verification

### 3.3. RESULTS AND DISCUSSION

During the simulated spoofing attack, we observe in 6(a) a low correct detection rate (CDR) in the initial part of the trajectory, when the bias is too small with respect to the expected, nominal GPS measurement errors and the self-contained sensor errors to be detected. Correspondingly, we observe a high missed detection rate (MDR) in the initial part of the trajectory. Once the bias is large enough, the CDR increases to1and the MDR decreases to 0. Once a spoofing event is detected, the Chimera SR-KF switches from using the fused state estimates and error p-zonotopes to the self-contained state estimates and error p-zonotopes. When the GPS measurement bias is small, the fused state estimate and3σerror zonotope bound the true state. As the bias grows, the spoofing attack is detected by our proposed approach, and eventually the fused state estimate and 3σ zonotopes no longer bound the true state. In this case, the Chimera SR-KF switches to using the state estimates and error p-zonotopes of the self-contained SR filter, and we observe in Fig. 6(c) that the Chimera SR-KF continues to bound the true state during this spoofing scenario over the 1000 Monte Carlo trajectories.




**(a)** Ratio of MDR and CDR. **(b)** Bird's eye view of the trajectory. **(c)** Ratio of states bound by $3\sigma$ error zonotopes.

Figure 6. Monte Carlo validation of the Chimera SR-KF estimator and detector during spoofed conditions for the linear, double-integrator system

## 4. CONCLUSIONS

For the optimal PRN code design work, we developed a reinforcement learning framework to devise a family of high-performing spreading code sequences which achieve low mean-square periodic auto- and cross-correlation objectives. We utilize a Gaussian policy gradient method to directly optimize the agent's bit-toggling reinforcement learning policy, and we believe this is the first work to develop a machine learning method to design navigation spreading code signals. We further demonstrated the ability of our algorithm to construct higher performing codes than well-chosen conventional codes, including Gold codes and Weil codes, as well as the spreading sequences obtained from a genetic algorithm with incorporated elitism. In particular, we observe that the policy gradient method outperforms these code sequences in both the auto- and cross-correlation objectives across various sequence lengths and code family sizes.

For the Chimera receiver work, we derived a stochastic reachability-based filter and spoofing detector to provide continuously authenticated navigation solutions between Chimera authentication times. In particular, we derived the detector to satisfy a user-defined false alarm requirement in nominal GPS operation while operating with stochastic errors and unknown, bounded biases in the measurements from the GPS and self-contained sensor measurements. We

further extended our state estimation filter and spoofing detector for a nonlinear propagation model by conservatively modeling the linearization error in the state propagation. We empirically validated, via Monte Carlo simulations, that our Chimera SR-KF and SR-EKF detectors satisfy the user-defined false alarm requirement, while detecting spoofing during simulated trajectory-drifting spoofing attacks. Additionally, we demonstrated that our Chimera SR-KF and SR-EKF estimators successfully bound the vehicle state during both authentic and spoofing conditions.

## REFERENCES


[1] T. Cozzens, (2020) First GPS III satellite now available, accessed: 4 September 2020. [Online] Available: https://www.gpsworld.com/first-gps-iii-satellite-now-available/.

[2] AFRL U.S. Air Force, (2020) Navigation Technology Satellite - 3 (NTS-3, accessed: 5 September 2020. [Online] Available: https://afresearchlab.com/technology/space-vehicles/successstories/nts-3#:~:text=Set%20to%20launch%20in%202022,architecture%20for%20satellite%20navigation%20technology.

[3] D. Chapman, J. Hinks, and J. Anderson, "Way, way out in front – Navigation Technology Satellite-3: The vanguard for space-based PNT," Inside GNSS, vol. 15, no. 4, 2020.

[4] B. W. Parkinson and S. T. Powers, "Part 1: The origins of GPS, and the pioneers who launched the system," GPS World, 2010, accessed: 7 September 2020. [Online] Available: https://www.gpsworld.com/origins-gps-part-1/.

[5] S. Erwin, "Air Force experiment NTS-3 could point the way to the next generation of GPS," SpaceNews, 2019, accessed: 7 September 2020. [Online] Available: https://spacenews.com/air-force-experiment-nts-3-could-point-the-way-to-the-next-generation-of-gps/.

[6] Department of the Air Force, Air Force Materiel Command, "Navigation Technology Satellite-3," 2016, Request for Information (RFI–RVKVE-NTS-3), accessed: 5 September 2020. [Online] Available: http: //www.fbodaily.com/archive/2016/03-March/24-Mar-2016/FBO-04057628.htm.

[7] S. W. Golomb, et al., Shift register sequences, Aegean Park Press, Walnut Creek, CA, 1967.

[8]. M. Anderson, K. L. Carroll, N. P. DeVilbiss, J. T. Gillis, J. C. Hinks, B. W. O'Hanlon, J. J. Rushanan, L. Scott, and R. A. Yazdi, "Chips-message robust authentication (Chimera) for GPS civilian signals," in Proceedings of the 30th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+2017), 2017, pp. 2388–2416.

[9] GPS Directorate, "Navstar gps space segment/user segment l1c interfaces," IS-GPS-800G, 14 May 2020.

[10] Air Force Research Laboratory (AFRL) Space Vehicles Directorate, Advanced GPS Technology, "Chips Message Robust Authentication (Chimera) Enhancement for the L1C Signal: Space Segment/User SegmentInterface,"IS-AGT-100, April 2019.

[11] D. A. Davis, "New Chimera Signal Enhancement Could Spoof-Proof GPS Receivers," Inside GNSS, 2019.

[12] T. Cozzens, "NTS-3 mission progresses toward launch in 2023," GPS World, June 2021.

[13]. Bhamidipati and G. X. Gao, “Integrity-Driven Landmark Attention for GPS-Vision Navigation via Stochastic Reachability,” in Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation, ION GNSS+ 2020, 2020, pp. 2311–2326.

[14] M. Althoff, “Reachability analysis and its application to the safety assessment of autonomous cars,” Ph.D. Dissertation, Technische Universität München, 2010.

[15]. Bhamidipati and G. X. Gao, “GPS Spoofing Mitigation and Timing Risk Analysis in Networked PMUs via Stochastic Reachability,” in Proceedings of the 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation, ION GNSS+ 2020, 2020, pp. 3920–3937.

[16] M. Althoff, O. Stursberg, and M. Buss, “Safety assessment for stochastic linear systems using enclosing hulls of probability density functions,” in 2009 European Control Conference (ECC), IEEE, 2009, pp. 625–630.

## DISTRIBUTION LIST

DTIC/OCP
8725 John J. Kingman Rd, Suite 0944
Ft Belvoir, VA 22060-6218 1 cy

AFRL/RVIL
Kirtland AFB, NM 87117-5776 1 cy

Official Record Copy
AFRL/RVB/Benjamin J. Fogg 1 cy