TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 13
Number 3
September 2019
DOI: 10.12716/1001.13.03.14

Logistic Map-encrypted Chaotic Ranging Code as a Proposed Alternative to GNSS PRN Pseudorange Code

M. Filić & F. Dimc
University of Ljubljana, Ljubljana, Slovenia

ABSTRACT: Pseudo-Random Noise (PRN) Gold code was selected for utilisation as the Global Navigation Satellite System (GNSS) pseudo-range measurement code sequence. Recent studies revealed a potential security vulnerability issue due to the Gold PRN code utilisation in a GNSS-related cyber-attack known as GNSS spoofing. Here a PRN code construction method based on chaotic-form logistic map is proposed as an alternative to the existing Gold code practice. Dubbed Chaotic Ranging Code (CRC), is a PRN code generation method that generates ranging code with orthogonal properties as good as, if not better, then those of the Gold PRN code, while assuming the encryption embedded in the proposed CRC code provides improved GNSS information security.

1 INTRODUCTION

Satellite navigation is one of a handful of technologies that lie the foundations of modern civilisation. Being technology-driven, every Global Navigation Satellite System (GNSS) shortcoming or vulnerability immediately affects a growing number of GNSS-enabled technology and socio-economic systems and their services (HM Government Office for Science, 2018). GNSS uses Pseudo-Random Noise (PRN) Gold codes in signals transmitted by satellites as they allow for (GPS Directorate, 2013): (i) precise GNSS pseudorange measurements, used in position estimation process, (ii) unambiguous identification of related satellite signals (every GNSS satellite uses its own unique Gold code), (iii) efficient radio spectrum management through the application of spread-spectrum Code Division Multiple Access (CDMA), achieved through lack of cross-correlation between the orthogonal Gold code. Ability of GNSS receiver to replicate the PRN code's waveform is one of the essential requirements for a successful GNSS position estimation (Petrovski, Tsujii, 2012). As an example, the US Global Positioning System, one of the GNSSs, utilises the Coarse Acquisition (C/A) PRN code aimed for civil users of the 1023 bits length. Additionally, implementation of PRN codes ensures essentially a level of information security through hiding data from the plane sight, the encryption embedded in that manner is considered an intrinsic feature of a PRN code (Roeck, 2009), (Yang, Xiao-Jun, 2012). PRN Gold codes are generated deterministically and in a transparent manner using shift-register arithmetic (GPS Directorate, 2013), an approach suitable for early GPS receivers with limited computing capacity.

Recent studies revealed a range of potential issues with Gold code implementation. Increasing demand for a limited spectrum requires more efficient codes, with autocorrelation effects minimised even better than in the case of Gold code. A tendency has emerged to minimise the exposure of code generation, as an information security measure. Finally, a security threat has been identified in

utilisation of PRN Gold codes for GNSS pseudorange measurements, an essential input for GNSS position estimation process. It has been shown that the flaw may be exploited in cyber-attacks against GNSS, known as GNSS spoofing (Tippenhauer et al, 2011), (Filić, 2018).

A novel approach in GNSS ranging PRN code generation has been proposed as a counter-measure to the rising GNSS spoofing threats. Chaotic processes have been identified as a potential class of ranging signal sources that may tame GNSS spoofing problem (Petrovski, Tsujii, 2012), (Yang, Xiao-Jun, 2012). In addition, chaotically-driven ranging PRN codes allows for fast synchronisation as an advantage for GNSS receivers, due to embedded chaotic system properties (Pecora, Carroll, 2015).

Logistic map has been a simple and popular model of biological population growth by Pierre Francois Verhulst in 1838, and has gained even more popularity after (May, 1976) it was disclosed its unusual behaviour for specifically configured map, capable of extending a chaotic behaviour (Kanso, Smaoui, 2009). Research revealed the onset of chaos for its control parameter in the (3.6, 4) interval of values. Since then, the chaotic behaviour of the logistic map has been used in numerous applications, including communications-related encryption methods (Yang, 2004), (Mitra, 2007), (Kanso, Smaoui, 2009).

Here utilisation of Chaotic Ranging Code (CRC), an alternative ranging PRN code for GNSS pseudorange measurement, is proposed, based on utilisation of the chaotic-behaving configuration of the logistic map. Methodology for the CRC construction is presented in Section 2, along with description of code performance examination methodology. Practical realisation results are presented in Section 3. Characteristics and related performance of the proposed alternative GNSS logistic map-encrypted PRN code are discussed in Section 4. Manuscripts concludes with the research results, CRC performance and potential shortcomings summary, and a proposal for further research subjects in Section 5.

2 METHOD FOR CHAOTIC RANGING CODE GENERATION

2.1 *Alternative chaotically-behaving logistic map-based CRC construction*

Logistic map is a simple mathematical expression that may generate a chaotically behaving dynamics, depending on its control parameter r, and the initial condition x_0 (Figures 1, 2, 3). Logistic map is defined as in Eq (1).

$$x[k+1] := r \cdot x[k]\left(1 - x[k]\right) \; for x \in (0,1), r \in \mathbb{R} \quad (1)$$

The chaotically-behaving logistic map-based PRN code alternative proposed here was constructed using the logistic PRN binary data LOGMAP1 algorithm suggested by (Kanso, Smaoui, 2009). The algorithm reads as follows (Algorithm 1).

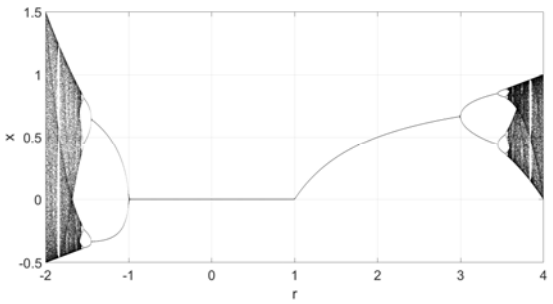

Figure 1. Bifurcation diagram of logistic map (May, 1976) for control parameter *r* in *[-2, 4]*

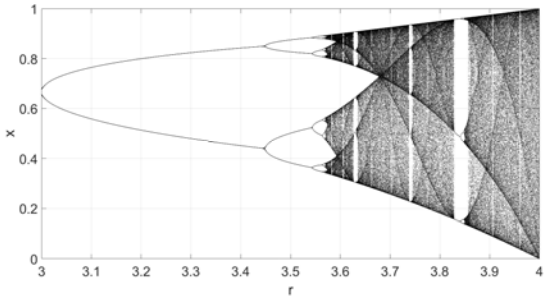

Figure 2. Bifurcation diagram of logistic map (May, 1976) for control parameter r in [3, 4]

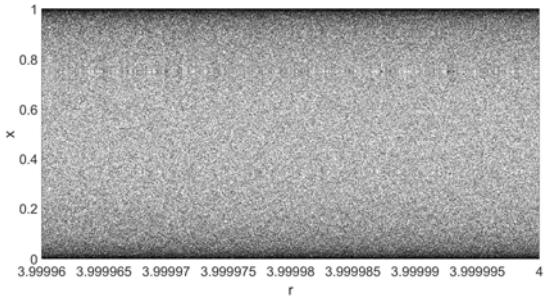

Figure 3. Bifurcation diagram of logistic map (May, 1976) for control parameter *r* in *[3.99996, 4]*

2.2 *Performance assessment*

(Kanso, Smaoui, 2009) proved randomness of the PRN sequence *a,* resulting from implementation of Algorithm 1, and examined other statistical properties of their proposed method, but did not examine either orthogonality or potential communications applications. They presented the rationale for setting threshold level at the 0.5 value, and selection of the *r* control parameter from the interval (3.99996, 4) (Figure 3) in order to obtain pseudo-random noise codes.

(Mitra, 2007) presented a methodology for the assessment of the PRN code orthogonality through the examination of auto-correlation function, given as in Eq (2).

$$r_{i,j}(\tau) = \frac{1}{N} \sum_{\tau=1-N}^{N-1} c_i(n) c_j(n+\tau) \quad (2)$$

Algorithm 1: LOGMAP1 (Kanso, Smaoui, 2009)

Data: Vector of chaotically-behaving logistic map's initial conditions (encryption secret key) *ic* = (*x0, r*), with *x0* as the initial value, and *r* as the logistic map control parameter; requested PRN code length (*N*); threshold parameter (*t)*
Result: A binary sequence of chaotically-encrypted PRN code *a*

1 set x[0] := x0, y[0] := 0; t := 0.5; a[0] := 0;
2 **for** i
3
4 $y[i+1] = \sum_{k}^{i} x[k] (mod 1);$
5 if(x[i+1] < 0.5) {z[i+1] := 0} else {z[i+1] := 0};
6 if(y[i+1] < 0.5) {w[i+1] := 0} else {w[i+1] := 0};
7 a[i+1] := w[i+1] XOR z[i+1];
8 **end;**

(Mitra, 2007) proposed a Figure of Merit (*FoM*) parameter, as a quantitative measure of frequency suitability of the PRN code for CDMA (Eq (3)), *FoM* is defined for a sequence $x_i(n)$, of the length *N*, and with the auto-correlation function $r_i(\tau)$ given. (Mitra, 2007) also suggested the rule of thumb for estimation of encryption strength from *FoM*, when larger *FoM* values refer to larger bandwidth and stronger encryption using the PRN code constructed. Finally, (Mitra, 2007) presented the Gold code assessment auto-correlation results, used here for reference, but did not disclose numerical results of the Gold code in the study.

$$FoM(x) = \frac{r_{i,i}^2(0)}{\sum_{r \neq 0} \left| r_{i,i}^2(\tau)^2 \right|} \quad (3)$$

(Huang et al, 1998) gave an independent and more general discussion on orthogonality assessment.

3 PRACTICAL REALISATION

The CRC code generation was performed based on the methodology and approach given by (Mitre, 2007). Practical realisation of the proposed CRC, based on chaotically-behaving logistic map, was conducted in the R open-source programming framework for statistical computing. Sets of length 100 and 1023 were constructed for every scenario with different logistic map parameters, as presented in Table 1.

Table 1. Scenario description

Scenario	value (logistic map control parameter)	x0 (initial value)	PRN code length
A	3.99997	0.4	100
B	3.99997	0.4	1023
C	3.99998	0.4	100
D	3.99998	0.4	1023

Table 2 FoMs for scenarios considered

Scenario	FoM
A	-2.66685
B	-2.582446
C	0.5498525
D	14.86747

The CRC sequences constructed within Scenarios A, B, C, and D, respectively, were examined for their auto-correlation functions to address the spectrum utilisation efficiency and orthogonality. This research did not examined the encryption strength in more details that was given in (Mitra, 2007) methodology, adopting the hypothesis of FoM as a single descriptor of both bandwidth and encryption strength.

Results of the analysis are depicted in Figures 4, 5, 6, and 7, respectively. Figure 8 presents the PRN code resulted from Scenario D. The cross-correlation function of two independent PRN codes with the same code length, constructed within Scenarios B and D, respectively, were examined from the inter-operability perspective, and depicted in Figure 9.

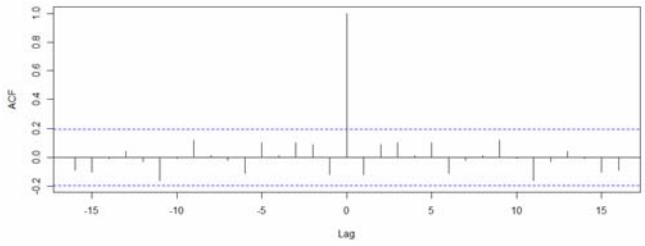

Figure 4. Auto-correlation function of the PRN code constructed under Scenario A

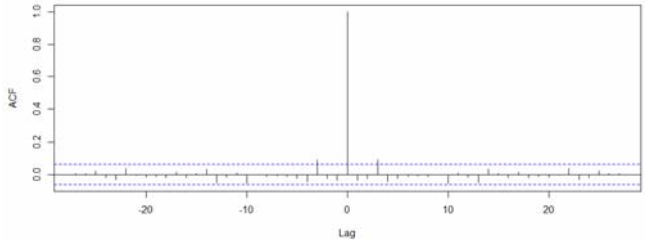

Figure 5. Auto-correlation function of the PRN code constructed under Scenario B

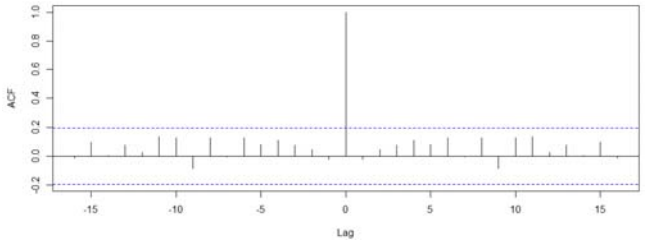

Figure 6. Auto-correlation function of the PRN code constructed under Scenario C

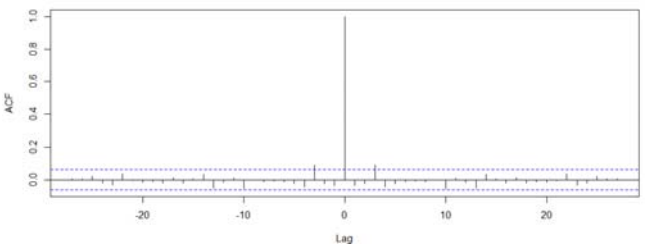

Figure 7. Auto-correlation function of the PRN code constructed under Scenario D

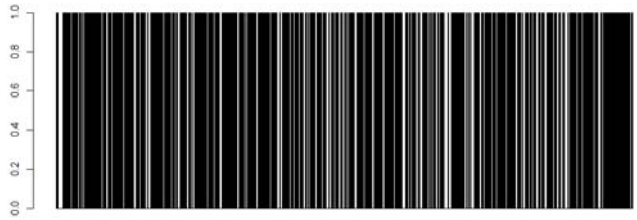

Figure 8. A PRN code sequence *a*, of length 1023, constructed within Scenario D

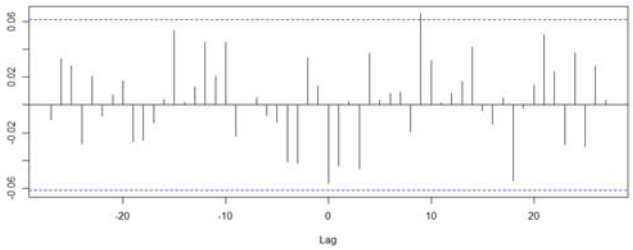

Figure 9. Cross-correlation function of two alternative PRN codes, constructed within Scenarios B and D, respectively

4 DISCUSSION AND CONCLUSION

Shortcomings of the currently deployed Gold code for GNSS pseudorange measurements are addressed in research presented in this manuscript. Construction of Chaotic Ranging Code (CRC), an alternative logistic map-based ranging PRN code for satellite positioning, was considered in this research, and resulting code assessed for its performance, as a potential candidate for the GNSS pseudorange measurement code. The alternative CRC code performance was compared with Gold code ones, based on methodology and Gold code assessment presented by (Mitra, 2007). Research was focused on spectrum efficiency and code orthogonality issues, as well as as with transparency of the process, with the quality of encryption marginally concerned in accordance with the guiding methodology adopted.

Scenarios A, B, C, and D (Table 1) presented the CRC sequences with different performance levels. Their auto-correlation functions performed well, allowing for acceptable orthogonality, and therefore a proper inter-operability, allowing for simultaneous utilisation of the same spectrum by a constellation of GNSS satellites. Lattices are suppressed sufficiently, with several scenarios performing even better than the standard GNSS Gold code PRN (Mitra, 2007). However, FoM values vary largely. As it is expected, larger codes and wider spread brings more robust encryption and wider bandwidth. Still, the selection of particular configuration of a logistic map may have significant impact on the *FoM* for particular logistic map-encrypted PRN code.

In summary, a framework for construction of a ranging code alternative to the GNSS Gold code for pseudorange measurement was assembled, in compliance with requirements for GNSS ranging code performance and based on utilisation of chaotically-behaving logistic map. The CRC generation algorithm developed by (Kanso, Smaoui, 2009) was configured and assessed for performance using methodology developed by (Mitra, 2007) to compare its quality with the existing GNSS PRN Gold code. Four variants of the CRCs were generated, and their performances assessed. The interpretation of research results revealed variations in encryption robustness depending on logistic map configuration, and confirmed importance of construction of long PRN codes. Future research will address a wider set of logistic map configurations across the range of configuration parameters, development and utilisation of more exact measures of encryption strength for PRN code assessment based on methodological approach outlined in (Roeck, 2009) and (Yang, Xiao-Jun, 2012), and CRC field validation in simulated scenarios of GNSS spoofing cyber-attacks.

REFERENCE

Filić, M. (2018). Foundations of GNSS spoofing detection and mitigation with distributed GNSS SDR receiver. *TransNav*, 12(4), 649-656.

GPS Directorate. (2013). Global Positioning Systems Directorate Systems Engineering and Integration Interface Specification IS-GPS-200J. Washington, DC. Available at: https://bit.ly/2R6MkSF

HM Government Office for Science. (2018). Satellite-Derived Time and Position: A Study of Critical Dependencies. HM Government of the UK and NI. Available at: https://bit.ly/2E2STnd

Huang, N E et al. (1998). The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis. *Proc R Soc Lond*, 454, 903-995.

Kanso, A, Smaoui. (2009). Logistic chaotic maps for binary numbers generations. *Ch, Sol and Fract*, 40, 2557-2568. Available at: https://bit.ly/2RY2Xku

May, R M. (1976). Simple mathematical models with very complicated dynamics. *Nature*, 261, 459-467.

Mitra, A. (2007). On Pseudo-Random and Orthogonal Binary Spreading Sequences. *Int J of Inf Tech*, 4(2), 137-144.

Pecora, L M, Carroll, T L. (2015). Synchronization of chaotic systems. *Chaos*, 25, 097611. doi: 10.1063/1.4917383

Petrovski, I, Tsujii, T. (2012). Digital Satellite Navigation and Geophysics: A Practical Guide with GNSS Signal Simulator and Receiver Laboratory. Cambridge University Press. Cambridge, UK.

Roeck, A. (2009). Quantifying Studies of (Pseudo) Random Number Generation for Cryptography (PhD thesis). L'Ecole Polytechnique. Palaiseau, France. Available at: https://bit.ly/2WRBEdv

Tippenhauer, N O, Poepper, C, Rasmussen, K B, and Čapkun, S. (2011). On the Requirements for Successful GPS Spoofing Attacks. Proc of the 18 th ACM conference on Computer and communications security, 75-86. Chicago, IL.

Yang, L, Xiao-Jun, T. (2012). A new pseudorandom number generator based on complex number chaotic equation.. Chyn Phys B, 21(9), 090506.

Yang, T. (2004). A survey of chaotic secure communication systems. *Int J of Comp Cogn*, 2(2), 81-130. Available at: https://bit.ly/2LiGImY