Secure Chaotic Spread Spectrum Systems

Jin Yu

WISELAB, ECE Department
Stevens Institute of Technology
Hoboken, NJ 07030

Outline

- Introduction
- Chaotic SS signals
- Security/LPI performance
  - Intercept receivers
    - Binary correlating detection
      - “Mismatch” problem
    - Particle-filtering based approach
    - Dual-antenna approach
  - Numerical results
- Conclusions

Introduction

- LPI/LPD-Secure/covert communications
- Spread-spectrum systems
  - Direct sequences
    - PN binary sequences
    - Chaotic sequences
  - Frequency hopping
  - Time hopping (UWB)
- Interceptors
  - likelihood-ratio test
  - Energy detector

Chaotic Signals

- Generate chaotic spreading sequences
  - Discrete Chaotic Map
    - Exponential Map, Triangular Map....
    - For Example: logistic map

$$x_{n+1} = \alpha x_n (1 - x_n) \quad 0 \le x_n \le 1,\ 0 \le \alpha \le 4$$

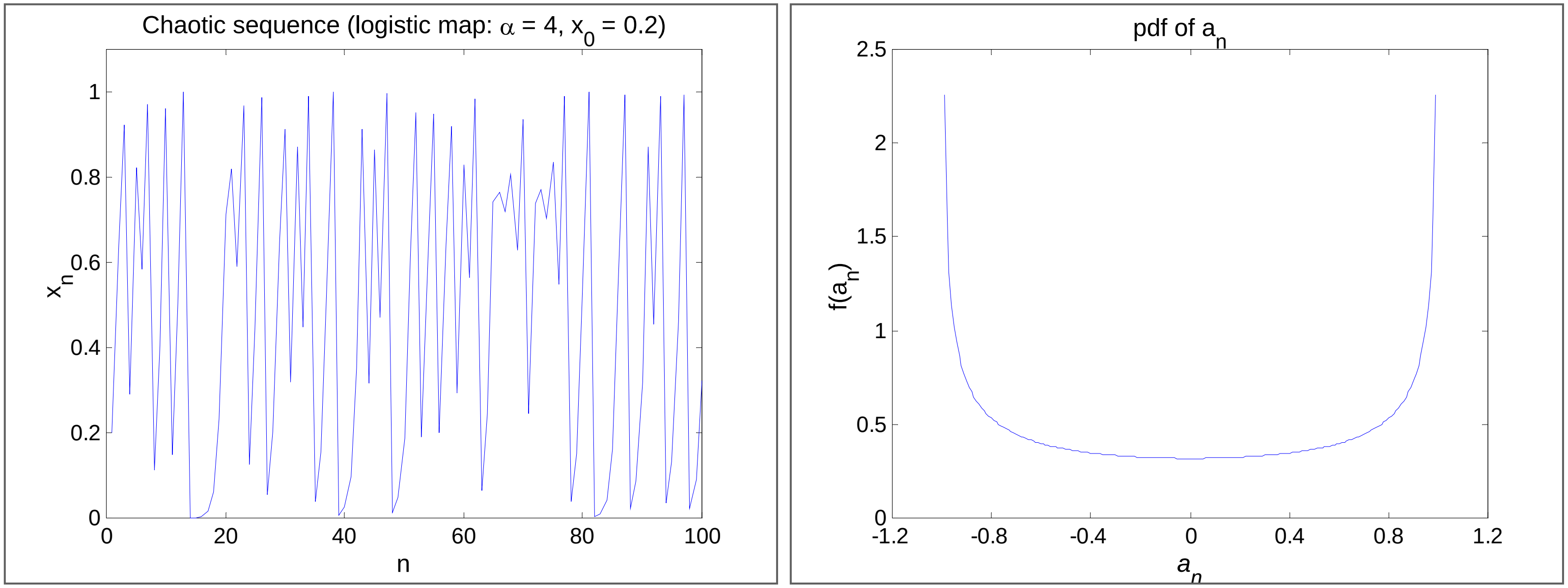
    - Bipolar signaling

$$a_n = 2x_n - 1$$

    - PDF of $\{a_n\}$

$$f(a_n) = \frac{1}{\pi \sqrt{1 - a_n^2}}, \quad -1 \le a_n \le 1$$

Properties of Chaotic Sequences



- Non-binary and non-periodic
- Random-like behaviors
- Good auto- and cross-correlation
- Large number of available spreading sequences for multiple-access applications

System Model

- Received Signals

$$r(t)=\begin{cases}\sqrt{2P}a(t)\cos(\omega_0 t+\phi)+n(t), & H_1 \\ n(t), & H_0\end{cases} \quad 0\le t\le T$$

where

$$a(t)=\sum_{n=-\infty}^{\infty} a_n p(t-nT_c-\tau T_c)$$

The chip epoch τT_c is modeled by r.v. τ, uniformly distributed in [0, 1).

Binary Correlating Method

- Likelihood ratio test (Optimum Intercept Receivers)
  - Synchronous coherent
  - Synchronous noncoherent
  - Asynchronous coherent
  - Asynchronous nonherent
- Gaussian approximation

$$\Lambda(r(t)) = \kappa_1 \mathrm{E}_{\varepsilon,\phi}\left\{ \prod_{n=0}^{N-1} \left[\sum_{q=0}^{Q-1} \exp\left(\frac{2\sqrt{2P}}{N_0} \int_{nT_c}^{(n+1)T_c} r_{\varepsilon,\phi}(t) b_q(t) \cos(\omega_0 t) dt \right) \right] \right\}$$

Synchronous Coherent Case

- Using Gaussian approximation, we obtain

$$m_\lambda = N(N_0 T_c)(0.5 + \gamma_c C \delta_{k,1})$$

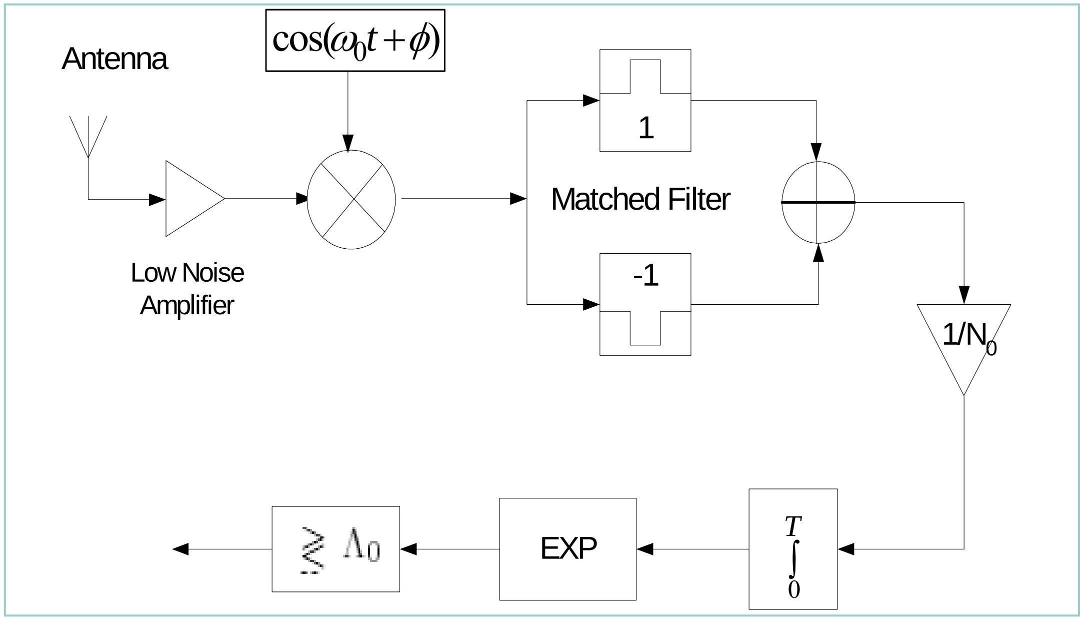
$$\sigma_\lambda^2 = N(N_0 T_c)^2 (0.5 + (2C\gamma_c + D\gamma_c^2)\delta_{k,1})$$

$$P_D = Q\left(\frac{Q^{-1}(P_{FA}) - \sqrt{2N\gamma_c C}}{\sqrt{1 + 4C\gamma_c + 2D\gamma_c^2}}\right)$$

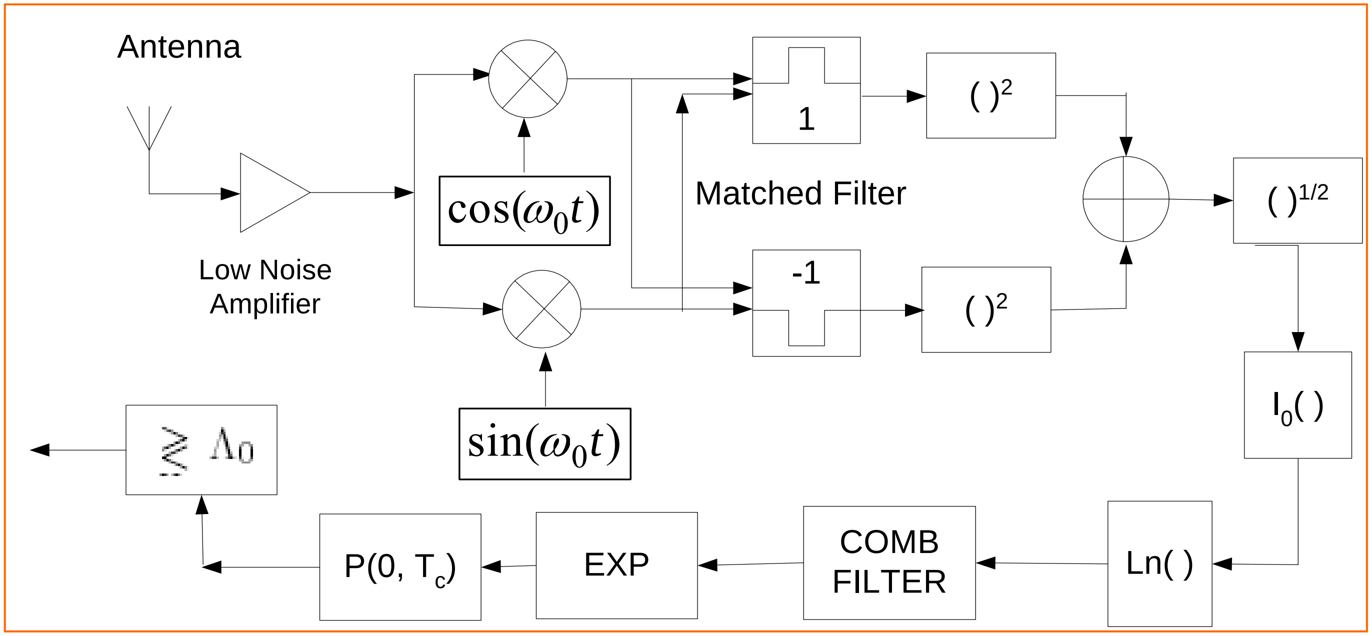
$$C = \frac{E[a^2]}{E[|a|]}$$

$$D = \frac{Var(a^2)}{E^2[|a|]}$$

(a) Binary Synchronous Coherent Detector



Synchronous Noncoherent Case



The mean and variance of λ is

$$m_\lambda = N(N_0 T_c)(1+\gamma_c C\delta_{k,1})$$

$$\sigma_\lambda^2 = N(N_0 T_c)^2(1+(2C\gamma_c + 0.5D\gamma_c^2)\delta_{k,1})$$

$$\Rightarrow P_D = Q\left(\frac{Q^{-1}(P_{FA}) - \sqrt{N}\gamma_c C}{\sqrt{1+2C\gamma_c + 0.5D\gamma_c^2}}\right)$$

Asynchronous Cases

- Assume chip epoch is U[0, T_c)
  - Coherent case

$$P_D(\lambda/\tau) = Q\left(\frac{Q^{-1}(P_{FA}) - \sqrt{2N}C(1-2\tau+2\tau^2)\gamma_c}{\sqrt{1+4C\gamma_c}}\right)$$

$$\Rightarrow \overline{P}_D = \int_0^1 Q\left(\frac{Q^{-1}(P_{FA}) - \sqrt{2N}C(1-2\tau+2\tau^2)\gamma_c}{\sqrt{1+4C\gamma_c}}\right)d\tau$$

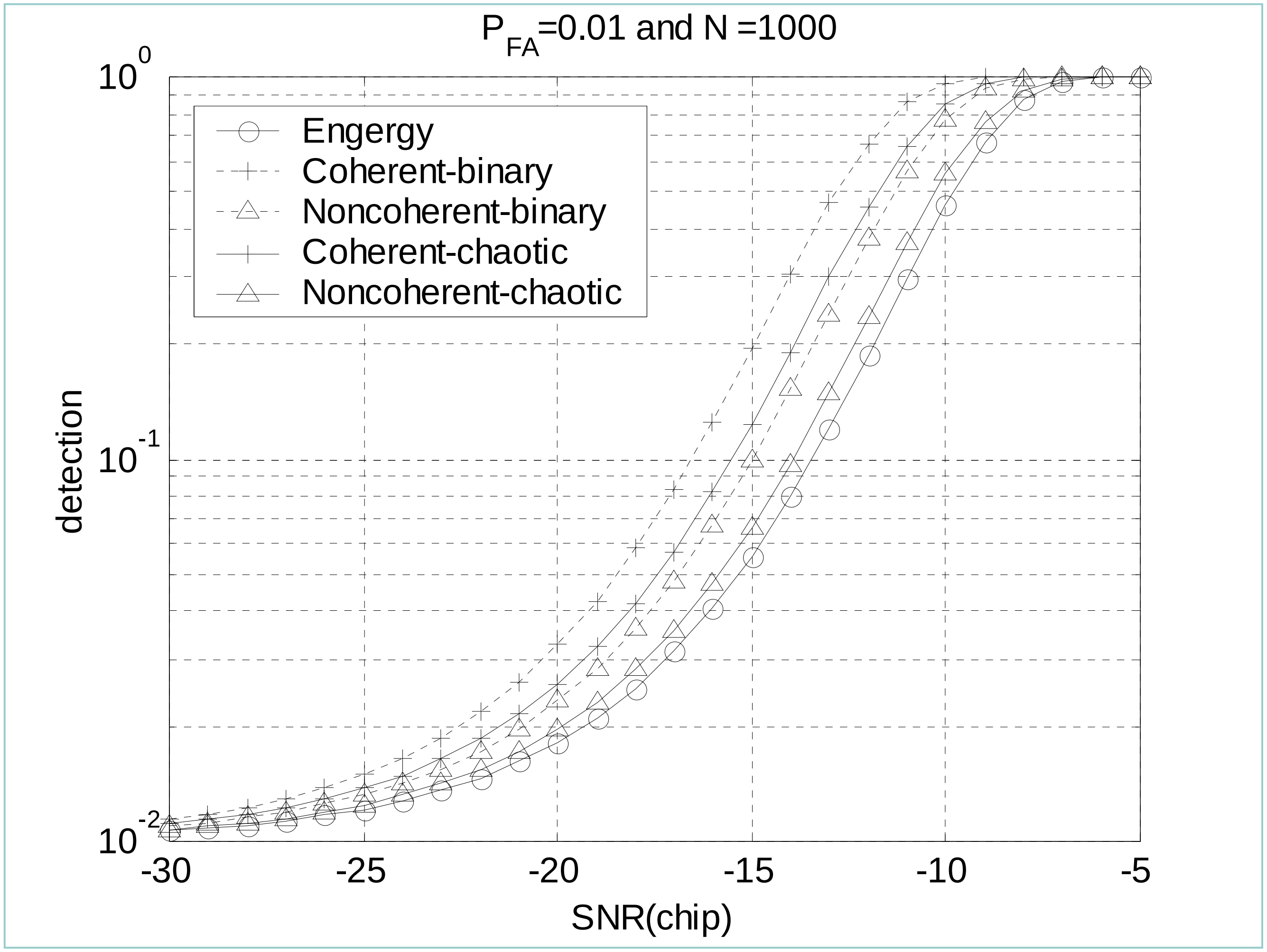
  - Noncoherent case

$$P_D(\lambda/\tau) = Q\left(\frac{Q^{-1}(P_{FA}) - \sqrt{N}C(1-\tau+\tau^2)\gamma_c}{\sqrt{1+2C\gamma_c}}\right)$$

$$\Rightarrow \overline{P}_D = \int_0^1 Q\left(\frac{Q^{-1}(P_{FA}) - \sqrt{N}C(1-\tau+\tau^2)\gamma_c}{\sqrt{1+2C\gamma_c}}\right)d\tau$$

Performance Comparison

Chaotic vs. Binary PN (Sync)



Particle-Filtering Based Detector

- Uncertainties in Chaotic Signals
  - Amplitude uncertainty (mismatch problems)
    - For all detection scenarios with chaotic signals
  - Phase uncertainty
    - Noncoherent detections
  - Delay uncertainty
    - Asynchronous detections

Particle-Filtering Based Detector

- Design particle sets
  - approximate the unknown random variables
  - select the most likely particle statistically
  - combat the impact due to uncertainties
- Reduce computational complexity
  - Updated particles for each iteration
  - Fixed particles for each iteration

Particle-Filtering Based Detector

- LRT function with particle filtering

$$\Lambda(r(t)) = \frac{p(\mathbf{r}_I \mid H_1)}{p(\mathbf{r}_I \mid H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \Lambda_0$$

← Coherent detection

$$\Lambda(r(t)) = \frac{\prod_{i=1}^{N} \left(\sum_{j=1}^{L_a} p(\mathbf{r}_{I,i} \mid a_i(j)) \right)}{L_a^N \prod_{n=1}^{N} p(\mathbf{r}_{I,n})}$$

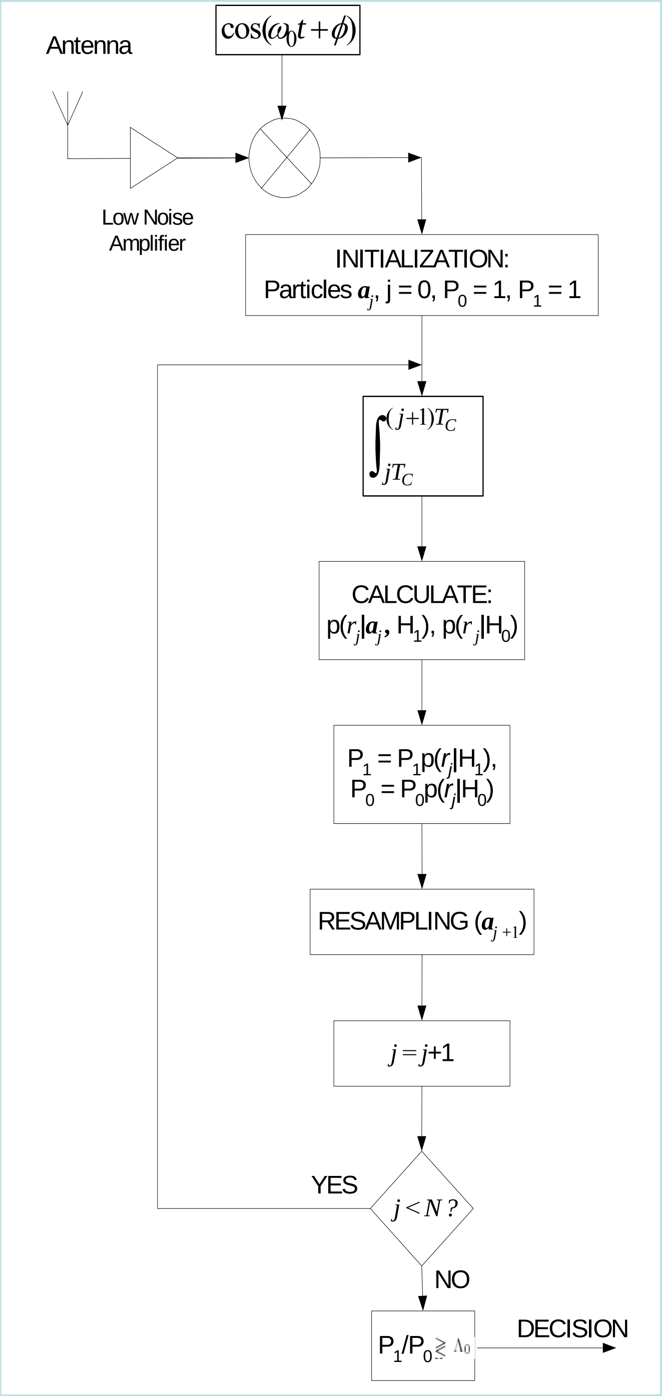
$$\Lambda(r(t)) = \frac{p(\mathbf{r}_I, \mathbf{r}_Q \mid H_1)}{p(\mathbf{r}_I, \mathbf{r}_Q \mid H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \Lambda_0$$

← Noncoherent detection

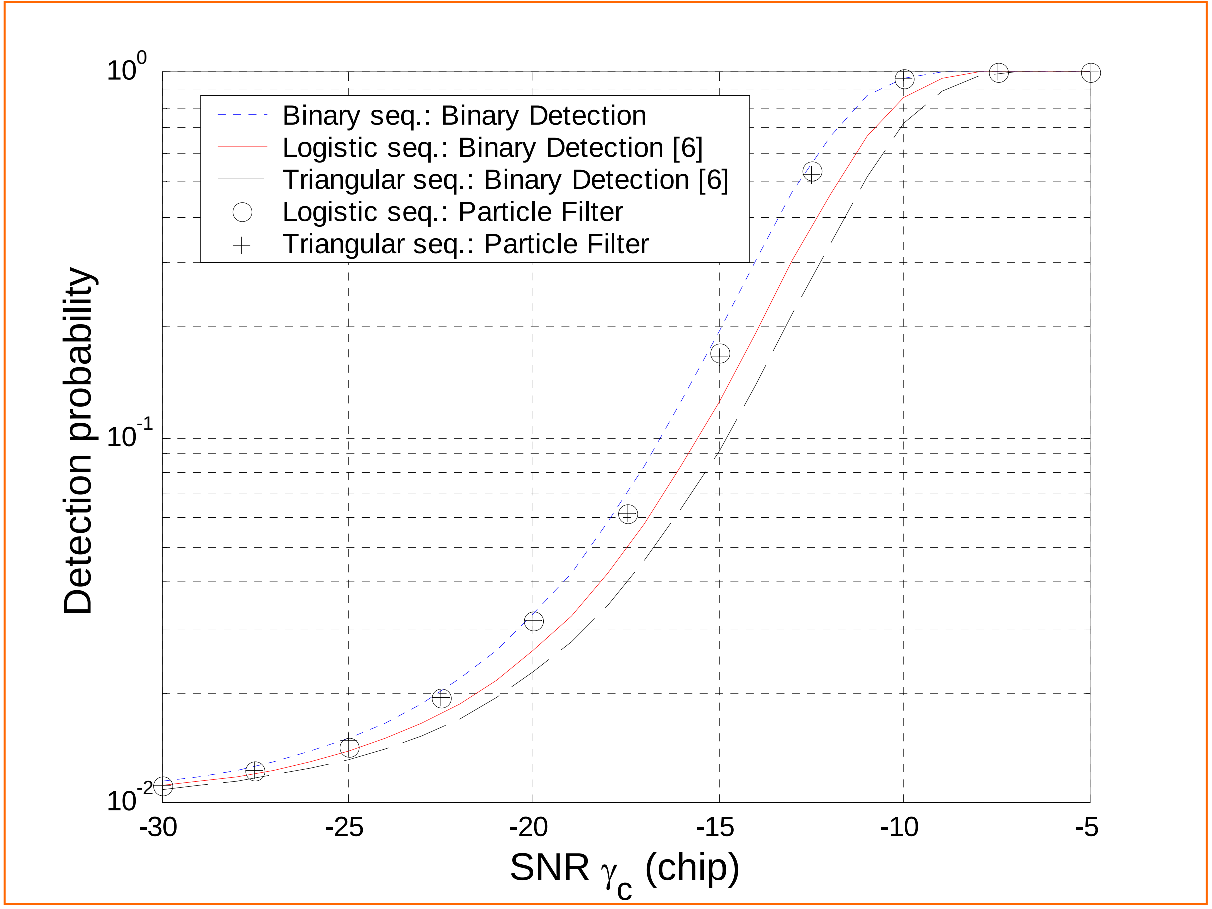
$$\Lambda(r(t)) = \frac{\prod_{i=1}^{N} \left(\sum_{j=1}^{L_a} \sum_{p=1}^{L_p} p(\mathbf{r}_{I,i}, \mathbf{r}_{Q,i} \mid a_i(j), \phi_i(p)) \right)}{L_a^N L_p^N \prod_{n=1}^{N} p(\mathbf{r}_{I,n}, \mathbf{r}_{Q,n})}$$

Notice: probability density functions p(•) is used to select ***the particles*** $a_i(j)$ and $\phi_i(p)$ which are mostly close to the actual amplitude and phase.

Particle-Filtering Based Detector



Synchronous coherent receivers with $P_{FA} = 0.01$, L_a = 50, and N = 1000



Asynchronous Detection: Multiple sampling

- Obtain multiple observations by multiple sampling at τ_n (combat delay uncertainty)

$$\mathbf{R}_I = \begin{pmatrix} r_{I,1}^{1} & r_{I,2}^{1} & \cdots & r_{I,N}^{1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{I,1}^{N_d} & r_{I,1}^{N_d} & \cdots & r_{I,N}^{N_d} \end{pmatrix} \qquad \mathbf{R}_Q = \begin{pmatrix} r_{Q,1}^{1} & r_{Q,2}^{1} & \cdots & r_{Q,N}^{1} \\ \vdots & \vdots & \ddots & \vdots \\ r_{Q,1}^{N_d} & r_{Q,1}^{N_d} & \cdots & r_{Q,N}^{N_d} \end{pmatrix}$$

$$\mathbf{N}_I = \begin{pmatrix} n_{I,1}^{1} & n_{I,2}^{1} & \cdots & n_{I,N}^{1} \\ \vdots & \vdots & \ddots & \vdots \\ n_{I,1}^{N_d} & n_{I,1}^{N_d} & \cdots & n_{I,N}^{N_d} \end{pmatrix} \qquad \mathbf{N}_Q = \begin{pmatrix} n_{Q,1}^{1} & n_{Q,2}^{1} & \cdots & n_{Q,N}^{1} \\ \vdots & \vdots & \ddots & \vdots \\ n_{Q,1}^{N_d} & n_{Q,1}^{N_d} & \cdots & n_{Q,N}^{N_d} \end{pmatrix}$$

Parallel Detection Algorithm

- LRT function

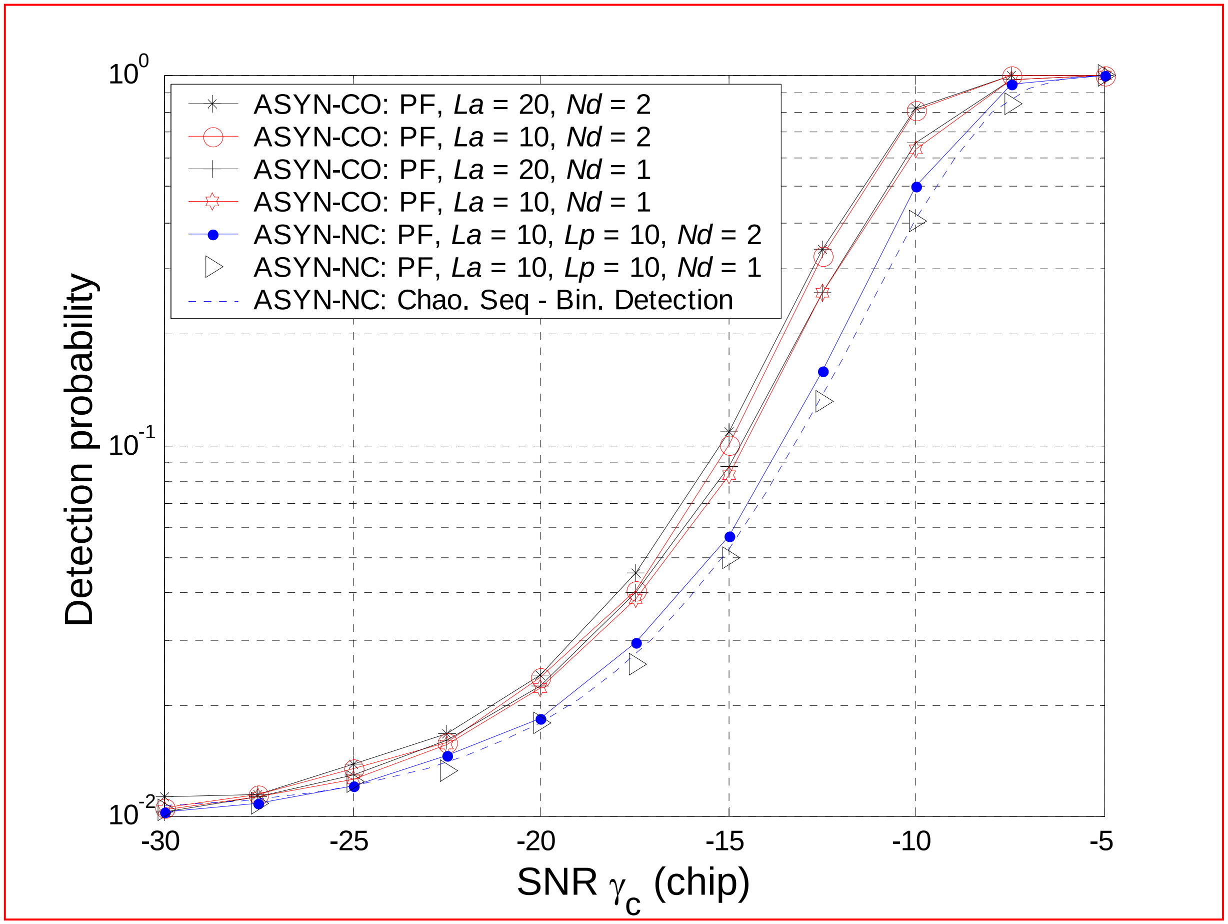
$$\Lambda(r(t)) = \max_{n}\left\{\frac{p(\mathbf{r}_I^n \mid H_1)}{p(\mathbf{r}_I^n \mid H_0)}, n = 1,2,\ldots,N_d\right\} \underset{H_0}{\overset{H_1}{\gtrless}} \Lambda_0$$

$$\Lambda(r(t)) = \max_{n}\left\{\frac{p(\mathbf{r}_I^n, \mathbf{r}_Q^n \mid H_1)}{p(\mathbf{r}_I^n, \mathbf{r}_Q^n \mid H_0)}, n = 1,2,\ldots,N_d\right\} \underset{H_0}{\overset{H_1}{\gtrless}} \Lambda_0$$

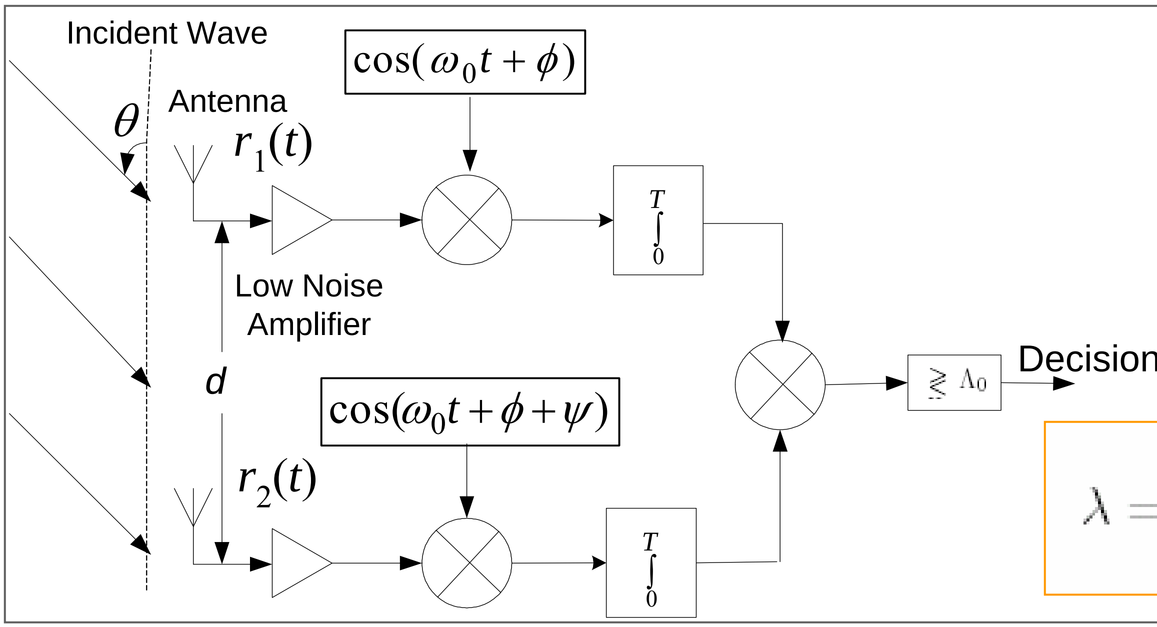
Notice: The row having the minimum delay is automatically selected by probability density functions p(•) to detect the presence of radio signals.

Numerical Results

Asynchronous detectors with various N_d, $P_{FA} = 0.01$, $N = 1000$, and parallel detection algorithm.



Dual-Antenna Approach: Synchronous coherent case



$$\Delta = d\cos\theta / c$$

$$\psi = 2\pi d\cos\theta / \lambda_0$$

$$\lambda = \sum_{j=1}^{N} r_{1,j} r_{2,j} \underset{H_0}{\overset{H_1}{\gtrless}} \Lambda_0$$

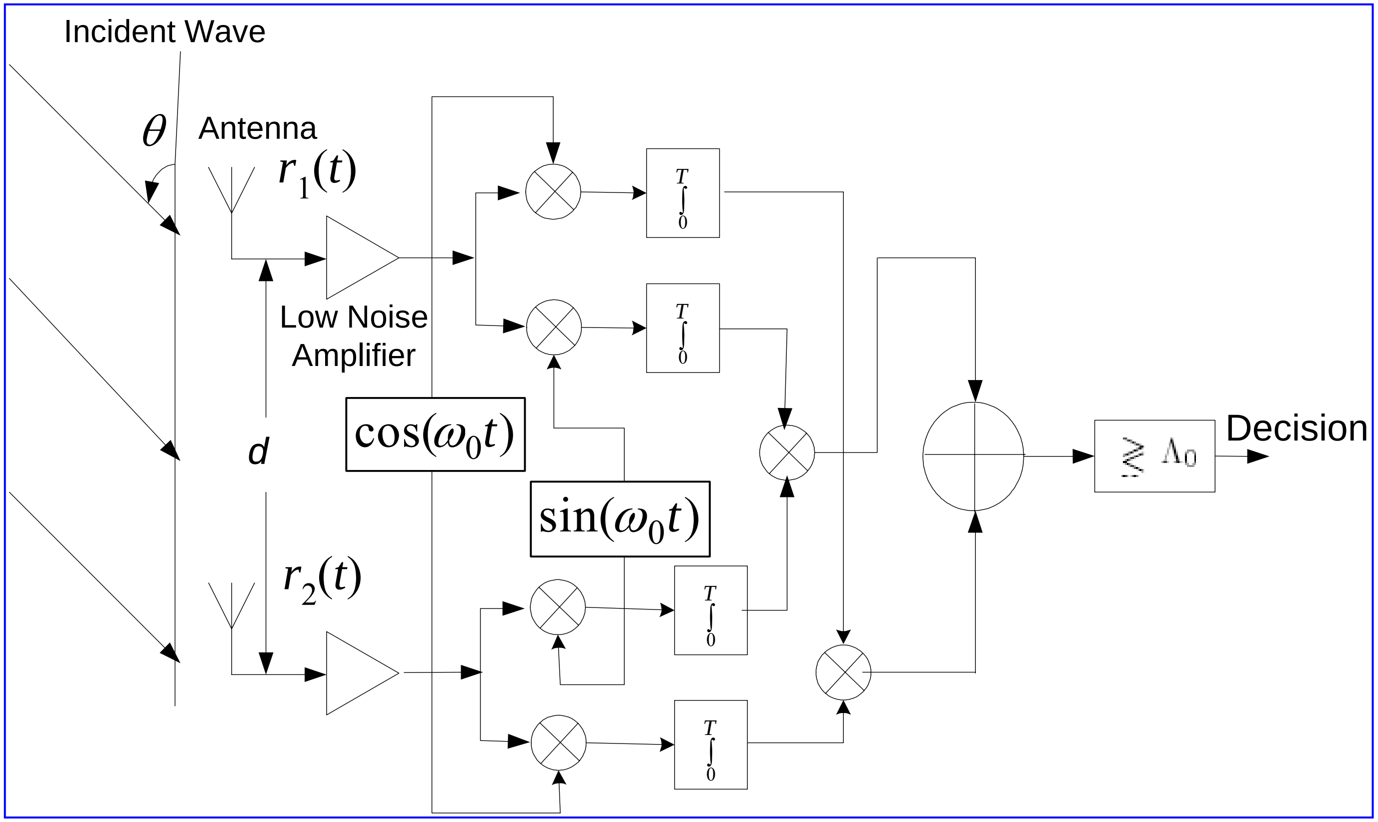
Signal Model

$$\begin{cases} r_1(t) = \sqrt{2P}a(t)\cos(\omega_0 t + \phi) + n_1(t) \\ r_2(t) = \sqrt{2P}a(t)\cos(\omega_0 t + \phi + \psi) + n_2(t) \end{cases}$$

Detection Probability

$$P_D = Q\left(\frac{Q^{-1}(P_{FA}) - 2\sqrt{N}\gamma_c}{\sqrt{1 + 4\gamma_c}} \right)$$

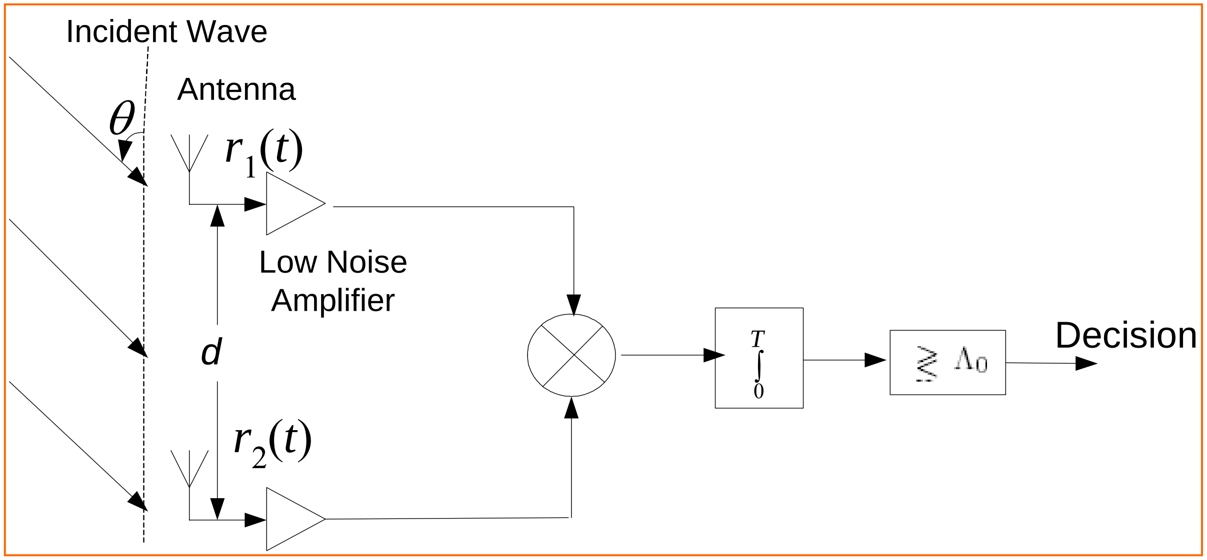
Dual-Antenna Approach: Synchronous noncoherent case



$$\lambda = \sum_{j=1}^{N} \left(r_{I,1,j} r_{I,2,j} + r_{Q,1,j} r_{Q,2,j} \right) \underset{H_0}{\overset{H_1}{\gtrless}} \Lambda_0$$

$$P_{D|\theta} = Q\left(\frac{Q^{-1}(P_{FA}) - \sqrt{2N}\,\Omega(\theta)\gamma_c}{\sqrt{1+2\gamma_c}} \right)$$

Dual-Antenna Approach: Asynchronous case



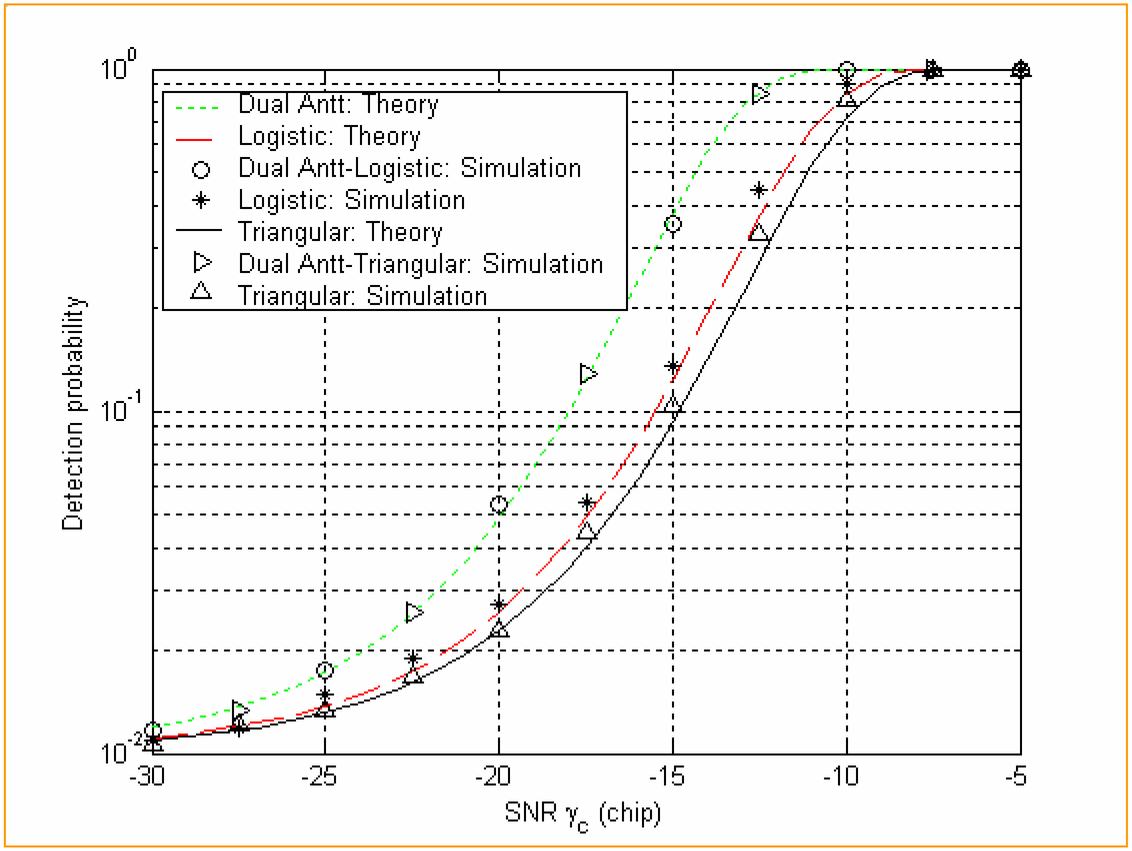
$$\lambda = \int_0^T r_1(t) r_2(t) dt \underset{H_0}{\overset{H_1}{\gtrless}} \Lambda_0$$

$$P_{D|\theta} = Q\left(\frac{Q^{-1}(P_{FA}) - \Omega(\theta)\sqrt{N}\gamma_c}{\sqrt{1+2\gamma_c}} \right)$$

$$\Omega(\theta) = \cos(2\pi d \cos\theta / \lambda_0)$$

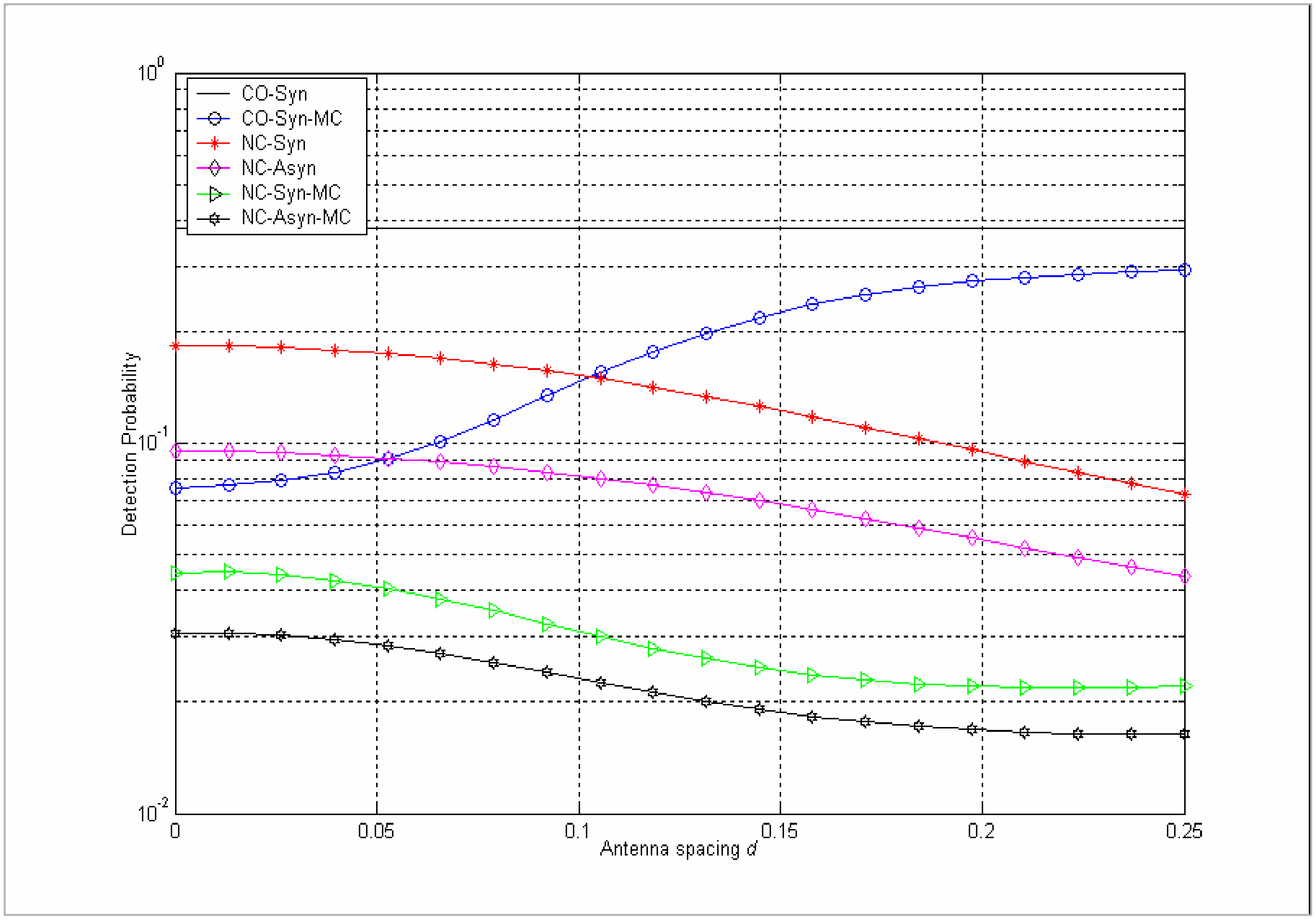
Numerical Results

LPI performance of chaotic DS SS signals with $N = 1000$ and $P_{FA} =$ 0.01 for synchronous coherent detectors.



Numerical Results

LPI performance of chaotic DS SS signals with various *d*, *N* = 1000, and chip SNR = -15 dB. MC: Mutual coupling.



Conclusions

- The mismatch between chaotic sequences and binary detection results in the LPI performance improvement;
- Particle-filtering based approach can be used to combat the uncertainties and then improve the detection performance;
- Dual antenna approach can also suppress the uncertainties; however, it is subject to mutual coupling.

Thank You!

Any Questions?