Safety Assurance of Stochastic Systems

Yongxin Chen

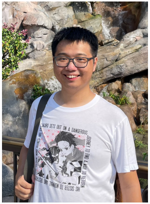
Georgia Institute of Technology

University of California San Diego

Mar, 2025

Collaborators

Saber Jafarpour
(CU Boulder)



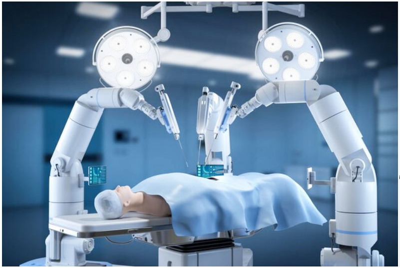
Zishun Liu
(Georgia Tech)

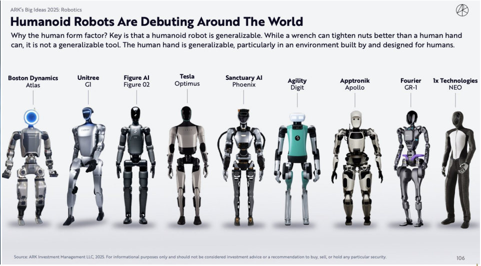
Liqian Ma
(Georgia Tech)

Papers

1. Jafarpour*, Liu*, Chen. *Probabilistic Reachability Analysis of Stochastic Control Systems*, 2024
2. Liu, Jafarpour, Chen. *Safety Verification of Nonlinear Stochastic Systems via Probabilistic Tube*, 2025

Safety-critical autonomous systems

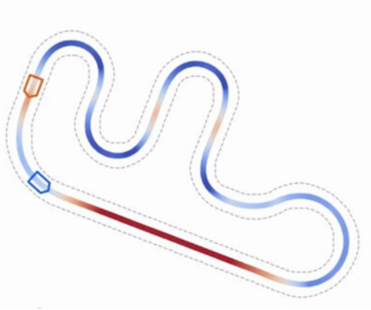


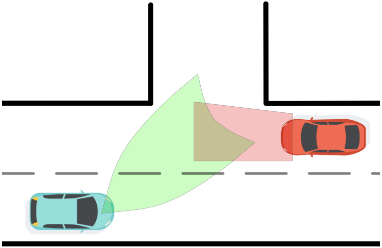


Control theory in safe autonomy

Barrier function:
Ensure safety by forcing the safe set to be a forward invariant set

Reachability analysis:
Ensure safety by certifying all the states the system can reach stay in the safe set





Challenges in safe autonomous systems

1. High-dimensional state, input and measurement spaces
2. Complex and highly nonlinear dynamics and environments
3. Uncertainties in the systems and environments

Safety verification under uncertainties

Deterministic uncertainty:

- worse case
- bounded
- unknown statistics
- robust control

Stochastic uncertainty:

- in average
- unbounded
- known statistics
- stochastic control

Goal: effective and scalable approach to safety assurance for general nonlinear systems under both deterministic and stochastic disturbances

System dynamics

$$dX_t = f(X_t, d_t, t)dt + g_t(X_t)dW_t$$

$$X_{t+1} = f(X_t, d_t, t) + w_t$$

Outline

1) Reachability Analysis of Stochastic Systems

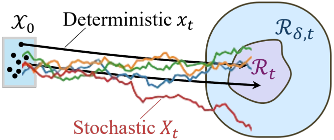
2) Safety Verification of Stochastic Systems via Probabilistic Tube

Reachability Analysis of Stochastic Systems

Probabilistic reachability

DRS: Given initial set $\mathcal{X}_0 \subseteq \mathbb{R}^n$ and disturbance set $\mathcal{D}$, the *deterministic reachable set* of $\dot{x}_t = f(x_t, d_t)$ at time t starting from $\mathcal{X}_0$ with disturbances in $\mathcal{D}$ is $\mathcal{R}_t = \{x_t \mid x_\tau, 0 \le \tau \le t \text{ is a trajectory with } x_0 \in \mathcal{X}_0, d_\tau \in \mathcal{D}\}$

DRS is too conservative for stochastic systems. Unbounded disturbance often result in trivial DRS, e.g., $\mathrm{d}X_t = \mathrm{d}W_t$



δ-PRS: Given initial set $\mathcal{X}_0 \subseteq \mathbb{R}^n$, disturbance set $\mathcal{D}$, and $\delta \in (0,1)$, $\mathcal{R}_{\delta,t} \subseteq \mathbb{R}^n$ is a *δ-probabilistic reachable* set of $\mathrm{d}X_t = f(X_t, d_t)\mathrm{d}t + g(X_t)\mathrm{d}W_t$ at time t if for any $x_0 \in \mathcal{X}_0$ and piecewise continuous d_τ in $\mathcal{D}$, $\mathbb{P}\left(X_t \in \mathcal{R}_{\delta,t}\right) \ge 1 - \delta$

Separation strategy and stochastic deviation

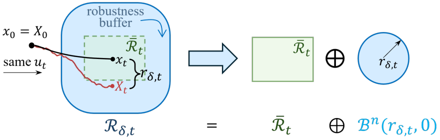
Associated trajectories: X_t ($\mathrm{d}X_t = f(X_t, d_t)\mathrm{d}t + g(X_t)\mathrm{d}W_t$), x_t ($\dot{x}_t = f(x_t, d_t)$) start from the same initial condition $X_0 = x_0$ and driven by the same d_τ

Separation strategy: Let $\overline{\mathcal{R}}_t$ be an over-approximation of DRS and

$$\mathbb{P}\left(\|X_t - x_t\| \le r_{\delta,t}\right) \ge 1 - \delta$$

for some $r_{\delta,t}$, then $\overline{\mathcal{R}}_t \oplus \mathcal{B}^n(r_{\delta,t}, 0)$ is a δ-PRS

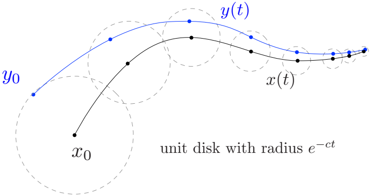
Problem: Establish a tight probabilistic bound $r_{\delta,t}$ of the stochastic deviation $\|X_t - x_t\|$ for associated trajectories X_t, x_t



Contraction theory

Matrix measure of $A \in \mathbb{R}^{n\times n}$

$$\mu(A) = \lim_{\epsilon \to 0^+} \frac{\|I_n + \epsilon A\| - 1}{\epsilon}$$



Equivalent assumption for $\dot{x}_t = f(x_t, d_t)$

1. $\mu(D_x f(x,d)) \le c$
2. $(x-y)^\top (f(x,d) - f(y,d)) \le c\|x-y\|^2$

Distance between any two trajectories satisfies

$$\|x_t - y_t\| \le e^{ct}\|x_0 - y_0\|$$

- energy function $V_t = \|x_t - y_t\|^2$

$$\frac{\mathrm{d}V_t}{\mathrm{d}t} = 2(x_t - y_t)^\top (f(x_t, d_t) - f(y_t, d_t)) \le 2cV_t$$

$$\Longrightarrow \|x_t - y_t\|^2 = V_t \le e^{2ct} V_0 = e^{2ct}\|x_0 - y_0\|^2$$

Contraction analysis for stochastic deviation

Assumption: For stochastic system $\mathrm{d}X_t = f(X_t, d_t)\mathrm{d}t + g(X_t)\mathrm{d}W_t$

1. $\mu(D_x f(x,d)) \leq c$
2. $g(x)g(x)^\top \preceq \sigma^2 I_n$

- (Pham et al 09) $V_t = \|X_t - x_t\|^2$ for associated trajectories X_t, x_t

$$\begin{aligned}\frac{\mathrm{d}\mathbb{E}(V_t)}{\mathrm{d}t} =& 2\mathbb{E}[(X_t - x_t)^\top (f(X_t, d_t) - f(x_t, d_t))] + \mathbb{E}[\mathrm{tr}(g(X_t)^\top g(X_t))] \\ \leq& 2c\,\mathbb{E}(V_t) + n\sigma^2, \quad V_0 = 0\end{aligned}$$

$$\Longrightarrow \mathbb{E}(\|X_t - x_t\|^2) = \mathbb{E}(V_t) \leq \tfrac{n\sigma^2}{2c}(e^{2ct} - 1)$$

Markov inequality

$$\mathbb{P}\left(\|X_t - x_t\| \leq \sqrt{\tfrac{n\sigma^2}{2c\delta}(e^{2ct} - 1)}\right) = \mathbb{P}\left(V_t \leq \tfrac{n\sigma^2}{2c\delta}(e^{2ct} - 1)\right) \geq 1 - \delta$$

Gap between linear and nonlinear analysis

Linear dynamics

$$\begin{aligned} \mathrm{d}X_t &= (cX_t + d_t)\mathrm{d}t + \sigma \mathrm{d}W_t \\ \dot{x}_t &= cx_t + d_t \end{aligned}$$

Nonlinear analysis

$$\mathbb{P}\left(\|X_t - x_t\| \leq \sqrt{\frac{\sigma^2}{2c}(e^{2ct} - 1)}\sqrt{n/\delta} \right) \geq 1 - \delta$$

Gaussian state X_t with covariance

$$\mathrm{cov}(X_t) = \int_0^t \sigma^2 e^{c(t-\tau)} e^{c(t-\tau)} d\tau = \tfrac{\sigma^2}{2c}(e^{2ct} - 1)\, I_n$$

Gaussian concentration

$$\mathbb{P}\left(\|X_t - x_t\| \leq \sqrt{\frac{\sigma^2}{2c}(e^{2ct} - 1)}(4\sqrt{n} + 2\sqrt{2\log(1/\delta)}) \right) \geq 1 - \delta$$

$$\boxed{\sqrt{1/\delta} \text{ vs } \sqrt{\log(1/\delta)}}$$

$$\boxed{10^5 \text{ vs } 4.8 \text{ when } \delta = 10^{-10}}$$

Georgia Tech

Sub-Gaussian norm concentration

Definition: A random vector $X \in \mathbb{R}^n$ is said to be sub-Gaussian with variance proxy ϑ^2, denoted as $X \sim subG(\vartheta^2)$, if

$$\mathbb{E}_X\left(e^{\lambda\langle \ell, X\rangle}\right) \leq e^{\frac{\lambda^2\vartheta^2}{2}},\ \forall\lambda \in \mathbb{R},\ \forall \ell \in \mathcal{S}^{n-1}$$

Lemma (Liu, C. 25): Let $X \sim subG(\vartheta^2)$, then for any $\delta \in (0,1)$ and any $\varepsilon \in (0,1)$

$$\|X\| \leq \vartheta\sqrt{\varepsilon_1 n + \varepsilon_2 \log(1/\delta)}$$

holds with probability at least $1-\delta$, where

$$\varepsilon_1 = \frac{\log(1/(1-\varepsilon^2))}{\varepsilon^2},\ \varepsilon_2 = \frac{2}{\varepsilon^2}$$

$X_t - x_t$ is not sub-Gaussian

Average moment generating function (AMGF)

Average exponential function over unit sphere $\mathcal{S}^{n-1}$

$$\Phi_{n,\lambda}(x) = \mathbb{E}_{\ell \sim \mathcal{S}^{n-1}} \left(e^{\lambda \langle \ell, x \rangle} \right)$$

Average moment generating function

$$\mathbb{E}_X \left(\Phi_{n,\lambda}(X) \right) = \mathbb{E}_X \left(\mathbb{E}_{\ell \sim \mathcal{S}^{n-1}} (e^{\lambda \langle \ell, X \rangle}) \right)$$

Lemma (Altschuler, Talwar. 22): If a random variable $X \in \mathbb{R}^n$ satisfies $\mathbb{E}_X \left(\Phi_{n,\lambda}(X) \right) \leq e^{\frac{\lambda^2 \vartheta^2}{2}}$, $\forall \lambda \in \mathbb{R}$, then for any $\delta \in (0,1)$ and any $\varepsilon \in (0,1)$

$$\|X\| \leq \vartheta \sqrt{\varepsilon_1 n + \varepsilon_2 \log(1/\delta)}$$

holds with probability at least $1 - \delta$

Concentration of stochastic deviation

Theorem (Jafarpour, Liu, C. 24): With probability at least $1-\delta$:

$$\|X_t - x_t\| \le \sqrt{\frac{\sigma^2(e^{2ct}-1)}{2c}(\varepsilon_1 n + \varepsilon_2 \log(1/\delta))}$$

same dependence as Gaussian concentration: $\sqrt{n}$, $\sqrt{\log(1/\delta)}$

Sketch of proof: bound $\mathbb{E}(\Phi_{n,\lambda}(X_t - x_t))$

- when $c = 0$, $h_t = \mathbb{E}(\Phi_{n,\lambda}(X_t - x_t))$ satisfies

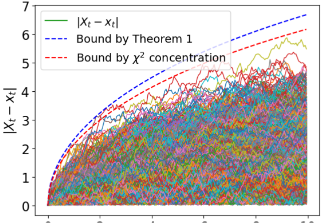
$$\frac{\mathrm{d}h_t}{\mathrm{d}t} \le \frac{\lambda^2\sigma^2}{2} h_t,\ \ h_0 = 1 \implies \mathbb{E}(\Phi_{n,\lambda}(X_t - x_t)) \le e^{\frac{\lambda^2\sigma^2 t}{2}}$$

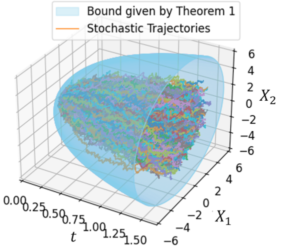
- when $c \neq 0$, convert to $c = 0$ through $\tilde{X}_t = e^{-ct}X_t$, $\tilde{x}_t = e^{-ct}x_t$

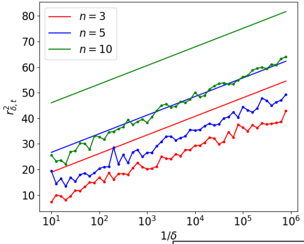
Georgia Tech

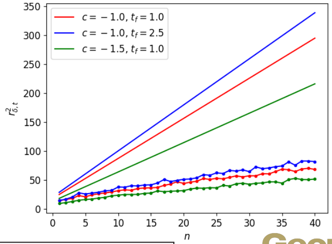
Tight probabilistic bound

- linear dynamics $\mathrm{d}X_t = c\,X_t \mathrm{d}t + \sigma \mathrm{d}W_t$









tight dependence: $\sqrt{n}$, $\sqrt{\log(1/\delta)}$

Probabilistic reachability with deterministic methods

Theorem (Jafarpour, Liu, C. 24): Let $\overline{\mathcal{R}}_t$ be an over-approximation of the DRS of deterministic system $\dot{x}_t = f(x_t, d_t)$. Then, for any probability level $\delta \in (0,1)$, a δ-PRS of $\mathrm{d}X_t = f(X_t, d_t)\mathrm{d}t + g(X_t)\mathrm{d}W_t$ is

$$\mathcal{R}_{\delta,t} = \overline{\mathcal{R}}_t \oplus \mathcal{B}^n\left(r_{\delta,t}, 0\right)$$

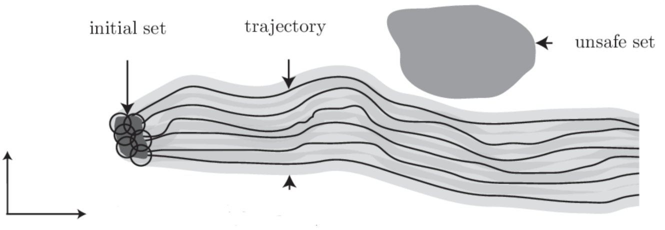
where $r_{\delta,t} = \sqrt{\frac{\sigma^2}{2c}(e^{2ct}-1)(\varepsilon_1 n + \varepsilon_2 \log(1/\delta))}$

$\overline{\mathcal{R}}_t$: computed with any deterministic reachability analysis methods

- Contraction-based, interval-based for scalability
- HJB-based, set-propagation for accuracy

Safety Verification of Stochastic Systems via Probabilistic Tube

Safety verification of stochastic systems



probabilistic reachability is not enough

stochastic trajectories should avoid unsafe set with high probability

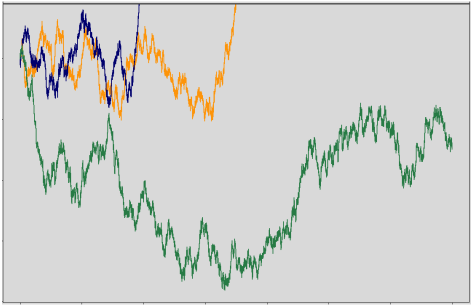
Martingale inequality

nonnegative supermartingale

$$M_s \geq \mathbb{E}[M_t \mid \mathcal{F}_s], \quad s < t$$

Ville's martingale inequality

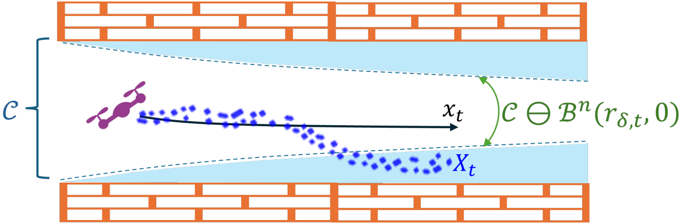
$$\mathbb{P}\left(\sup_{t \geq 0} M_t \geq C\right) \leq \frac{\mathbb{E}[M_0]}{C}$$



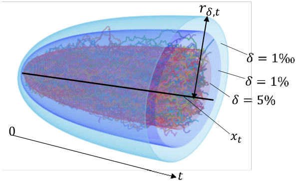
foundation of stochastic barrier methods

Set-erosion and probabilistic tube

Set-erosion: certify the safety of $\dot{x}_t = f(x_t, d_t)$ over an eroded safe set



Probabilistic tube: a tube in which stochastic trajectories stay with high probability



> Problem: Given a finite time horizon $[0,\ T]$, establish a tight probabilistic tube for $\mathrm{d}X_t = f(X_t, d_t)\mathrm{d}t + g(X_t)\mathrm{d}W_t$

Georgia Tech

Affine martingale for probabilistic tube

Definition: For a stochastic process v_t, a nonnegative function $M(v,t) : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}_{\geq 0}$ is said to be an affine martingale of v_t if there exist $a_t, b_t \in \mathbb{R}$ such that

$$\frac{\mathbb{E}(M(v_{t+\mathrm{d}t}, t+\mathrm{d}t)|v_t) - M(v_t,t)}{\mathrm{d}t} \leq a_t M(v_t,t) + b_t$$

Affine martingale can be converted to a supermartingale:
$\widetilde{M}(v_t,t) = M(v_t,t)\psi_t + \int_t^T b_\tau \psi_\tau \mathrm{d}\tau$ with $\psi_t = e^{\int_t^T a_\tau \mathrm{d}\tau}$

Given any $\overline{M} > 0$ and $\mathcal{V}_t = \{v : \widetilde{M}(v,t) \leq \overline{M}\}$, it holds that

$$\mathbb{P}\left(v_t \in \mathcal{V}_t, \forall t \leq T\right) \geq 1 - \frac{M(v_0,0)\psi_0 + \int_0^T b_\tau \psi_\tau \mathrm{d}\tau}{\overline{M}}$$

Martingale for probabilistic tube

Average moment generating function induces affine martingale

$$M(X_t - x_t, t) = \Phi_{n,\lambda}(X_t - x_t) = \mathbb{E}_{\ell \sim \mathcal{S}^{n-1}}\left(e^{\lambda \langle \ell, X_t - x_t \rangle}\right)$$

is an affine martingale over $X_t - x_t$ when $c = 0$

$$\frac{\mathbb{E}(\Phi_{n,\lambda}(X_{t+\mathrm{d}t} - x_{t+\mathrm{d}t})|X_t - x_t) - \Phi_{n,\lambda}(X_t - x_t)}{\mathrm{d}t} \leq \frac{\lambda^2\sigma^2}{2}\Phi_{n,\lambda}(X_t - x_t)$$

Theorem (Liu, Jafarpour, C. 25):

$$\mathbb{P}\left(\|X_t - x_t\| \leq r_{\delta,t},\ \forall t \leq T\right) \geq 1 - \delta$$

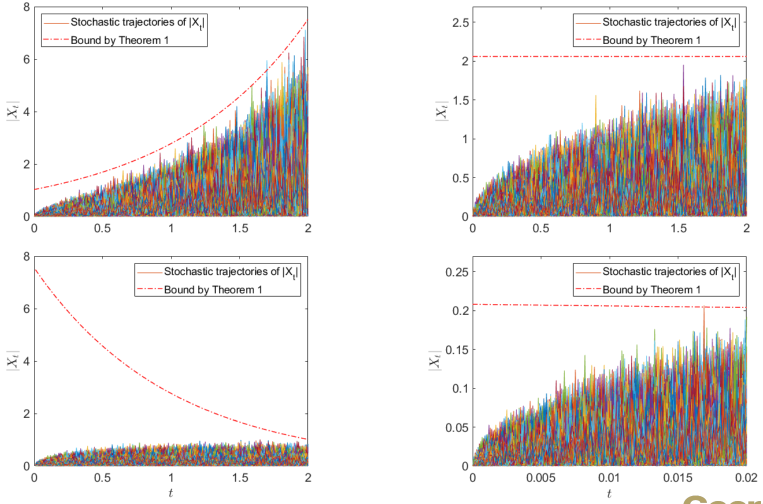
where

$$r_{\delta,t} = e^{ct}\sigma\sqrt{\frac{1 - e^{-2cT}}{2c}(\varepsilon_1 n + \varepsilon_2 \log(1/\delta))}$$

Georgia Tech

Analysis of martingale-based probabilistic tube

- linear dynamics $\mathrm{d}X_t = c\,X_t\mathrm{d}t + \sigma\mathrm{d}W_t$



Modified probabilistic tube for contractive dynamics

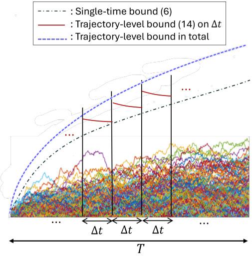
$\boxed{\text{union bound} + \text{martingale}}$

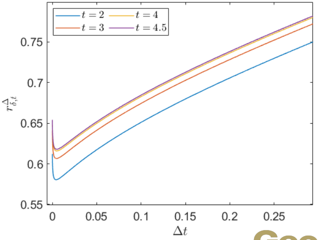
Theorem (Liu, Jafarpour, C. 25): When $c < 0$

$$\mathbb{P}\left(\|X_t - x_t\| \le r_{\delta,t},\ \forall t \le T\right) \ge 1 - \delta$$

where

$$r_{\delta,t} = \frac{\sigma\left(\sqrt{1 - e^{2ct}} + \sqrt{e^{-2c\Delta t} - 1}\right)}{\sqrt{-2c}} \sqrt{\varepsilon_1 n + \varepsilon_2 \log \frac{2T}{\delta \Delta t}}$$





Georgia Tech

Safety verification via probabilistic tube

Theorem (Liu, Jafarpour, C. 25): Given a safe set $\mathcal{C} \in \mathbb{R}^n$, an initial state set $\mathcal{X}_0 \subseteq \mathcal{C}$ and a probability level $\delta \in (0,1)$, the stochastic system $\mathrm{d}X_t = f(X_t, d_t)\mathrm{d}t + g(X_t)\mathrm{d}W_t$ can be verified to be safe with $1-\delta$ guarantee on the time horizon $[0,T]$ if the deterministic system $\dot{x}_t = f(x_t, d_t)$ satisfies

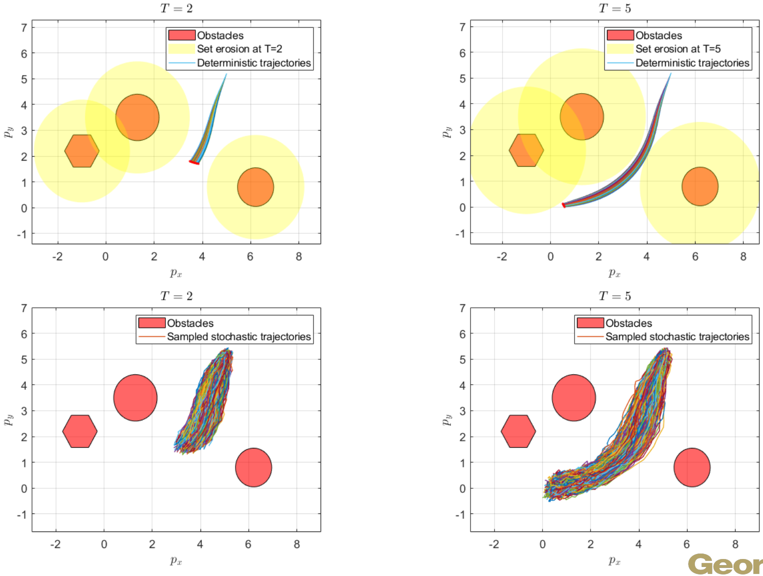
$$x_0 \in \mathcal{X}_0 \Rightarrow x_t \in \mathcal{C} \ominus \mathcal{B}^n\left(r_{\delta,t}, 0\right), \quad \forall d_\tau \in \mathcal{D},\ \forall t \le T$$

where

$$r_{\delta,t} = \begin{cases} e^{ct}\sigma\sqrt{\frac{1-e^{-2cT}}{2c}\left(\varepsilon_1 n + \varepsilon_2 \log(1/\delta)\right)} & c \ge 0 \\ \frac{\sigma\left(\sqrt{1-e^{2ct}}+\sqrt{e^{-2c\Delta t}-1}\right)}{\sqrt{-2c}}\sqrt{\varepsilon_1 n + \varepsilon_2 \log\frac{2T}{\delta\Delta t}} & c < 0 \end{cases}$$

Numerical Examples

Safety verification of autonomous vehicles

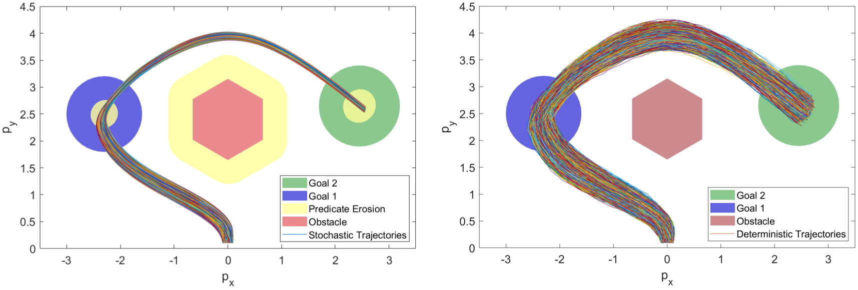


Safety verification under STL specifications

Signal temporal logic formula

$$\varphi = (\Box_{[0,T]}\pi_{\text{obs}}) \wedge (\Diamond_{[0,T]}\pi_{\text{goal}_2}) \wedge (\neg\pi_{\text{goal}_2}\mathcal{U}_{[0,T]}\pi_{\text{goal}_1})$$

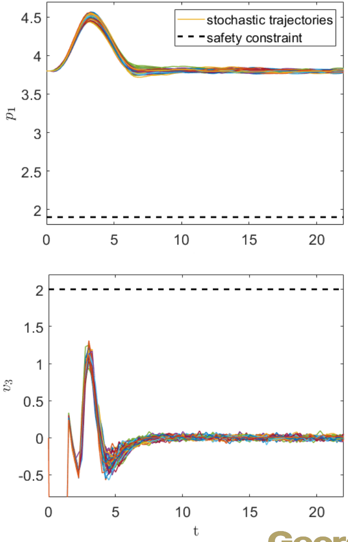
$\Box_{[0,T]}$: *globally* $\Diamond_{[0,T]}$: *eventually* $\mathcal{U}_{[0,T]}$: *until*



Safe stochastic MPC

Deterministic MPC over an eroded safe set $\mathcal{C} \ominus \mathcal{B}_{i|k}$

$$
\begin{aligned}
\min_{u_{k:k+N-1|k}} \quad & J_N(x_{k:k+N|k}, u_{k:k+N-1|k}) \\
\text{s.t.} \quad & x_{k|k} = X_k \\
& x_{i+1|k} = f(x_{i|k}, u_{i|k}) \\
& x_{i+1|k} \in \mathcal{C} \ominus \mathcal{B}_{i|k} \\
& i = k, \ldots, k+N-1
\end{aligned}
$$



Takeaway

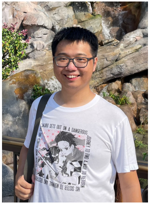
1. A scalable framework of safety assurance for stochastic systems
2. Separation strategy reduces stochastic problems into deterministic problems
3. A new set of tools to analyze fluctuations of stochastic dynamics

Papers

1. Probabilistic Reachability Analysis of Stochastic Control Systems
2. Safety Verification of Nonlinear Stochastic Systems via Probabilistic Tube
3. Probabilistic Reachability of Discrete-Time Nonlinear Stochastic Systems
4. Safety Verification of Stochastic Systems: A Set-Erosion Approach
5. Safety Verification of Stochastic Systems under Signal Temporal Logic Specifications
6. Probabilistic Reachability of Stochastic Systems with Neural Network Controllers
7. A New Proof of Sub-Gaussian Norm Concentration Inequality
8. Trajectory Optimization of Stochastic Systems under Chance Constraints via Set Erosion

Georgia Tech

Acknowledgment

Thank you for your attention!