Secure Discrete-Time Linear-Quadratic Mean-Field Games

Muhammad Aneeq uz Zaman, Sujay Bhatt & Tamer Başar

October 29, 2020

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Agent Model & Objective

Agent Model & Objective

Secure n-agent Linear Quadratic (LQ) game

- Large population game, to solve a *consensus problem*, each agent aims to align with aggregate behavior.

Agent Model & Objective

Secure n-agent Linear Quadratic (LQ) game

- Large population game, to solve a *consensus problem*, each agent aims to align with aggregate behavior.
- An agent comprised of a sensor and a controller, connected through a noise-less channel.

Agent Model & Objective

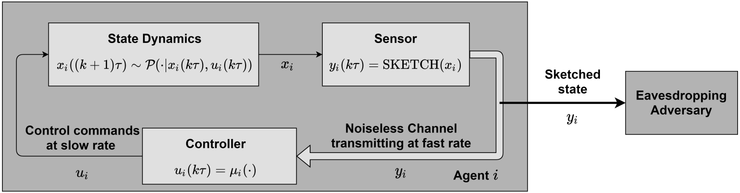
Secure n-agent Linear Quadratic (LQ) game

- Large population game, to solve a *consensus problem*, each agent aims to align with aggregate behavior.
- An agent comprised of a sensor and a controller, connected through a noise-less channel.
- The channel is susceptible to eavesdropping by adversaries.

Agent Model & Objective

Secure n-agent Linear Quadratic (LQ) game

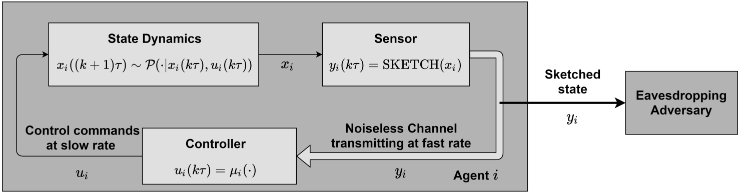
- Large population game, to solve a *consensus problem*, each agent aims to align with aggregate behavior.
- An agent comprised of a sensor and a controller, connected through a noise-less channel.
- The channel is susceptible to eavesdropping by adversaries.



Agent Model & Objective

Secure *n*-agent Linear Quadratic (LQ) game

- Large population game, to solve a *consensus problem*, each agent aims to align with aggregate behavior.
- An agent comprised of a sensor and a controller, connected through a noise-less channel.
- The channel is susceptible to eavesdropping by adversaries.

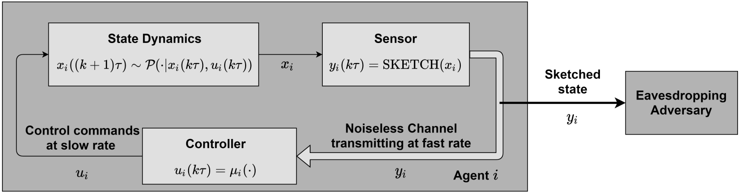


- State sketched using private key.

Agent Model & Objective

Secure n-agent Linear Quadratic (LQ) game

- Large population game, to solve a *consensus problem*, each agent aims to align with aggregate behavior.
- An agent comprised of a sensor and a controller, connected through a noise-less channel.
- The channel is susceptible to eavesdropping by adversaries.



- State sketched using private key.
- Adversary is non-strategic.

Main Results & Organization

Main Results & Organization

- We introduce the Secure n-agent Linear Quadratic (LQ) game and counterpart Secure LQ-MFG (SLQ-MFG).

Main Results & Organization

- We introduce the Secure n-agent Linear Quadratic (LQ) game and counterpart Secure LQ-MFG (SLQ-MFG).
- We propose a secure communication (Sketching & Reconstruction) mechanism.

Main Results & Organization

- We introduce the Secure n-agent Linear Quadratic (LQ) game and counterpart Secure LQ-MFG (SLQ-MFG).
- We propose a secure communication (Sketching & Reconstruction) mechanism.
- We prove that the MFE of the (vanilla) LQ-MFG is an ϵ-MFE of the SLQ-MFG (in linear controllers).

Main Results & Organization

- We introduce the Secure *n*-agent Linear Quadratic (LQ) game and counterpart Secure LQ-MFG (SLQ-MFG).
- We propose a secure communication (Sketching & Reconstruction) mechanism.
- We prove that the MFE of the (vanilla) LQ-MFG is an ϵ-MFE of the SLQ-MFG (in linear controllers).
- Furthermore, we show that the MFE of the LQ-MFG is an $(\epsilon + \varepsilon)$-NE of the finite agent game.

Main Results & Organization

- We introduce the Secure *n*-agent Linear Quadratic (LQ) game and counterpart Secure LQ-MFG (SLQ-MFG).
- We propose a secure communication (Sketching & Reconstruction) mechanism.
- We prove that the MFE of the (vanilla) LQ-MFG is an ϵ-MFE of the SLQ-MFG (in linear controllers).
- Furthermore, we show that the MFE of the LQ-MFG is an $(\epsilon + \varepsilon)$-NE of the finite agent game.
- Finally, we empirically investigate the performance of the $(\epsilon + \varepsilon)$-NE.

Secure n-agent Linear Quadratic (LQ) game

Secure *n*-agent Linear Quadratic (LQ) game

- Consider an n-agent game, each agent $i \in \{1, 2, \cdots, n\}$ has linear dynamics,

$$\begin{aligned} x_i(k\tau + (j+1)\Delta) &= Ax_i(k\tau + j\Delta) + Bu_i(k\tau) + \tilde{w}_i(k\tau + j\Delta), \\ y_i(k\tau + j\Delta) &= \text{SKETCH}(x_i(k\tau + j\Delta)) = C_i x_i(k\tau + j\Delta), \end{aligned}$$

Secure n-agent Linear Quadratic (LQ) game

- Consider an n-agent game, each agent $i \in \{1, 2, \cdots, n\}$ has linear dynamics,

$$\begin{aligned} x_i(k\tau + (j+1)\Delta) &= Ax_i(k\tau + j\Delta) + Bu_i(k\tau) + \tilde{w}_i(k\tau + j\Delta), \\ y_i(k\tau + j\Delta) &= \mathrm{SKETCH}(x_i(k\tau + j\Delta)) = C_i x_i(k\tau + j\Delta), \end{aligned}$$

- Observations generated at fast rate $1/\Delta$ and control at slow rate $1/\tau$, s.t. $\tau = N\Delta$.

Secure *n*-agent Linear Quadratic (LQ) game

- Consider an n-agent game, each agent $i \in \{1, 2, \cdots, n\}$ has linear dynamics,

$$x_i(k\tau + (j+1)\Delta) = Ax_i(k\tau + j\Delta) + Bu_i(k\tau) + \tilde{w}_i(k\tau + j\Delta),$$
$$y_i(k\tau + j\Delta) = \text{SKETCH}(x_i(k\tau + j\Delta)) = C_i x_i(k\tau + j\Delta),$$

- Observations generated at fast rate $1/\Delta$ and control at slow rate $1/\tau$, s.t. $\tau = N\Delta$.
- $x_i(0)$ and $\tilde{w}_i$ are generated i.i.d., second order distribution.

Secure *n*-agent Linear Quadratic (LQ) game

- Consider an n-agent game, each agent $i \in \{1, 2, \cdots, n\}$ has linear dynamics,

$$\begin{aligned} x_i(k\tau + (j+1)\Delta) &= Ax_i(k\tau + j\Delta) + Bu_i(k\tau) + \tilde{w}_i(k\tau + j\Delta), \\ y_i(k\tau + j\Delta) &= \mathrm{SKETCH}(x_i(k\tau + j\Delta)) = C_i x_i(k\tau + j\Delta), \end{aligned}$$

- Observations generated at fast rate $1/\Delta$ and control at slow rate $1/\tau$, s.t. $\tau = N\Delta$.
- $x_i(0)$ and $\tilde{w}_i$ are generated i.i.d., second order distribution.
- C_i (private key) chosen uniformly from set of private keys

$$\mathcal{C} = \{C_i | i \in \{1, 2, \ldots, M\}, M < \infty, C_i \in \mathbb{R}^{q \times m}, N > Obs(A, C_i)\}.$$

Secure n-agent Linear Quadratic (LQ) game (contd.)

Secure n-agent Linear Quadratic (LQ) game (contd.)

- C_i is singular, multi-rate setup used to reconstruct state.

Secure n-agent Linear Quadratic (LQ) game (contd.)

- C_i is singular, multi-rate setup used to reconstruct state.
- Each agent aims to minimize its cost

$$J_i^n = \limsup_{T\to\infty} \frac{1}{T}\mathbb{E}\Big\{ \sum_{k=0}^{T-1} \Big\| x_i(k\tau) - \frac{1}{n-1}\sum_{j\neq i} x_j(k\tau) \Big\|_Q^2 + ||u_i(k\tau)||_R^2 \Big\},$$

Secure *n*-agent Linear Quadratic (LQ) game (contd.)

- C_i is singular, multi-rate setup used to reconstruct state.
- Each agent aims to minimize its cost

$$J_i^n = \limsup_{T\to\infty} \frac{1}{T}\mathbb{E}\Big\{ \sum_{k=0}^{T-1} \Big\| x_i(k\tau) - \frac{1}{n-1}\sum_{j\neq i} x_j(k\tau) \Big\|_Q^2 + ||u_i(k\tau)||_R^2 \Big\},$$

- The solution concept used is that of *Nash Equilibrium*.

Secure Linear Quadratic Mean-Field Game (SLQ-MFG)

Secure Linear Quadratic Mean-Field Game (SLQ-MFG)

- Consider the limiting case where $n \to \infty$.

Secure Linear Quadratic Mean-Field Game (SLQ-MFG)

- Consider the limiting case where $n \to \infty$.
- We focus on a generic agent whose dynamics are

$$x(k\tau + (j+1)\Delta) = Ax(k\tau + j\Delta) + Bu(k\tau) + \tilde{w}(k\tau + j\Delta),$$
$$y(k\tau + j\Delta) = Cx(k\tau + j\Delta).$$

Secure Linear Quadratic Mean-Field Game (SLQ-MFG)

- Consider the limiting case where $n \to \infty$.
- We focus on a generic agent whose dynamics are

$$x(k\tau + (j+1)\Delta) = Ax(k\tau + j\Delta) + Bu(k\tau) + \tilde{w}(k\tau + j\Delta),$$
$$y(k\tau + j\Delta) = Cx(k\tau + j\Delta).$$

- The cost function of the generic agent given the mean-field trajectory $\bar{x}$ is

$$J(\mu, \bar{x}) = \limsup_{T\to\infty} \frac{1}{T}\mathbb{E}\Big\{ \sum_{k=0}^{T-1} ||x(k\tau) - \bar{x}(k\tau)||_Q^2 + ||u(k\tau)||_R^2 \Big\}.$$

Secure Linear Quadratic Mean-Field Game (SLQ-MFG) (contd.)

Secure Linear Quadratic Mean-Field Game (SLQ-MFG) (contd.)

- We use the solution concept of mean-field equilibrium (MFE).

Secure Linear Quadratic Mean-Field Game (SLQ-MFG) (contd.)

- We use the solution concept of mean-field equilibrium (MFE).
- First define operator $\Lambda : \mathcal{M} \to \ell^{\infty}$, generates a mean-field trajectory $\bar{x}$ generated by a control law μ.

Secure Linear Quadratic Mean-Field Game (SLQ-MFG) (contd.)

- We use the solution concept of mean-field equilibrium (MFE).
- First define operator $\Lambda : \mathcal{M} \to \ell^\infty$, generates a mean-field trajectory $\bar{x}$ generated by a control law μ.

Definition

The tuple $(\mu^*, \bar{x}^*) \in \mathcal{M} \times \ell^\infty$ is an MFE if $\bar{x}^* = \Lambda(\mu^*)$ and

$$J(\mu^*, \bar{x}^*) \leq J(\mu, \bar{x}^*), \;\; \forall \mu \in \mathcal{M}$$

Secure Linear Quadratic Mean-Field Game (SLQ-MFG) (contd.)

- We use the solution concept of mean-field equilibrium (MFE).
- First define operator $\Lambda : \mathcal{M} \to \ell^\infty$, generates a mean-field trajectory $\bar{x}$ generated by a control law μ.

Definition

The tuple $(\mu^*, \bar{x}^*) \in \mathcal{M} \times \ell^\infty$ is an MFE if $\bar{x}^* = \Lambda(\mu^*)$ and

$$J(\mu^*, \bar{x}^*) \le J(\mu, \bar{x}^*), \;\; \forall \mu \in \mathcal{M}$$

- MFE is analog to Nash Equilibrium.

State Reconstruction using Multi-Rate Output Sampling

State Reconstruction using Multi-Rate Output Sampling

- If we denote $y_{[k]} := [y^T((k-1)\tau), \ldots, y^T((k-1)\tau + (N-1)\Delta)]^T$, then

$$y_{[k+1]} = C_0 x(k\tau) + D_0 u(k\tau) + C_d w_{[k]}$$

State Reconstruction using Multi-Rate Output Sampling

- If we denote $y_{[k]} := [y^T((k-1)\tau), \ldots, y^T((k-1)\tau + (N-1)\Delta)]^T$, then

$$y_{[k+1]} = C_0 x(k\tau) + D_0 u(k\tau) + C_d w_{[k]}$$

- Thus the state $x(k\tau)$ can be expressed as,

$$x(k\tau) = L_y y_{[k]} + L_u u((k-1)\tau) + w(k\tau)$$

State Reconstruction using Multi-Rate Output Sampling

- If we denote $y_{[k]} := [y^T((k-1)\tau), \ldots, y^T((k-1)\tau + (N-1)\Delta)]^T$, then

$$y_{[k+1]} = C_0 x(k\tau) + D_0 u(k\tau) + C_d w_{[k]}$$

- Thus the state $x(k\tau)$ can be expressed as,

$$x(k\tau) = L_y y_{[k]} + L_u u((k-1)\tau) + w(k\tau)$$

- The controller reconstructs the state as,

$$\hat{x}(k\tau) = L_y y_{[k]} + L_u u((k-1)\tau)$$

State Reconstruction using Multi-Rate Output Sampling

- If we denote $y_{[k]} := [y^T((k-1)\tau), \ldots, y^T((k-1)\tau + (N-1)\Delta)]^T$, then

$$y_{[k+1]} = C_0 x(k\tau) + D_0 u(k\tau) + C_d w_{[k]}$$

- Thus the state $x(k\tau)$ can be expressed as,

$$x(k\tau) = L_y y_{[k]} + L_u u((k-1)\tau) + w(k\tau)$$

- The controller reconstructs the state as,

$$\hat{x}(k\tau) = L_y y_{[k]} + L_u u((k-1)\tau)$$

- Estimation error $w(k\tau)$ is a zero mean random vector with covariance matrix Σ_C. Define set $\mathcal{E}_C := \{\Sigma_C : C \in \mathcal{C}\}$.

MFE of the SLQ-MFG

MFE of the SLQ-MFG

- We show that the MFE of SLQ-MFG doesn't exist in class of linear controllers.

MFE of the SLQ-MFG

- We show that the MFE of SLQ-MFG doesn't exist in class of linear controllers.
- Define augmented state $z(k\tau) = [x^T(k\tau), \bar{x}^T(k\tau)]^T$. MF trajectory $\bar{x}$ is defined by matrix F.

MFE of the SLQ-MFG

- We show that the MFE of SLQ-MFG doesn't exist in class of linear controllers.
- Define augmented state $z(k\tau) = [x^T(k\tau), \bar{x}^T(k\tau)]^T$. MF trajectory $\bar{x}$ is defined by matrix F.
- Dynamics of augmented state is

$$z((k+1)\tau) = \bar{A}z(k\tau) + \bar{B}u(k\tau) + \bar{w}(k\tau)$$

$$\bar{A} = \begin{bmatrix} A_0 & 0 \\ 0 & F \end{bmatrix}, \bar{B} = \begin{bmatrix} B_0 \\ 0 \end{bmatrix}, \bar{w}(k\tau) = \begin{bmatrix} w^0(k\tau) \\ 0 \end{bmatrix}$$

MFE of the SLQ-MFG

MFE of the SLQ-MFG

- Cost of generic agent under control law K, $u(k\tau) = -K(\hat{x}^T(k\tau), \bar{x}^T(k\tau))$

$$J(K, F) = \limsup_{T \to \infty} \frac{1}{T} \mathbb{E}\Big\{ \sum_{k=0}^{T-1} \|z(k\tau)\|_Q^2 + \|u(k\tau)\|_R^2 \Big\}.$$

MFE of the SLQ-MFG

- Cost of generic agent under control law K, $u(k\tau) = -K(\hat{x}^T(k\tau), \bar{x}^T(k\tau))$

$$J(K, F) = \limsup_{T \to \infty} \frac{1}{T} \mathbb{E}\Big\{ \sum_{k=0}^{T-1} \|z(k\tau)\|_Q^2 + \|u(k\tau)\|_R^2 \Big\}.$$

- The controller $\hat{K}_F$ which minimizes $J(K, F)$ for any stable F is

$$\hat{K}_F = (\bar{B}^T \hat{P} \bar{B} + R)^{-1} \bar{B}^T \hat{P} \bar{A}(I - \hat{\Sigma}_C \Sigma_{\hat{K}_F}^{-1})$$

where $\hat{P}$ is the solution to a Lyapunov equation.

MFE of the SLQ-MFG

- Cost of generic agent under control law K, $u(k\tau) = -K(\hat{x}^T(k\tau), \bar{x}^T(k\tau))$

$$J(K, F) = \limsup_{T\to\infty} \frac{1}{T}\mathbb{E}\Big\{\sum_{k=0}^{T-1} \|z(k\tau)\|_Q^2 + \|u(k\tau)\|_R^2\Big\}.$$

- The controller $\hat{K}_F$ which minimizes $J(K, F)$ for any stable F is

$$\hat{K}_F = (\bar{B}^T\hat{P}\bar{B} + R)^{-1}\bar{B}^T\hat{P}\bar{A}(I - \hat{\Sigma}_C\Sigma_{\hat{K}_F}^{-1})$$

where $\hat{P}$ is the solution to a Lyapunov equation.

- $\Sigma_{\hat{K}_F}$ is the covariance matrix of stationary distribution and is shown to be singular. Hence $\hat{K}_F$ does not exist.

ϵ-MFE of the SLQ-MFG

ϵ-MFE of the SLQ-MFG

Definition

The tuple $(K', F') \in \mathbb{R}^{p\times 2m} \times \mathbb{R}^{m\times m}$ is an ϵ-MFE if $F' = \Lambda(K')$ and

$$J(K', F') \leq J(K, F') + \epsilon, \ \ \forall K \in \mathbb{R}^{p\times 2m}, \epsilon > 0$$

ϵ-MFE of the SLQ-MFG

Definition

The tuple $(K', F') \in \mathbb{R}^{p\times 2m} \times \mathbb{R}^{m\times m}$ is an ϵ-MFE if $F' = \Lambda(K')$ and

$$J(K', F') \leq J(K, F') + \epsilon, \ \ \forall K \in \mathbb{R}^{p\times 2m}, \epsilon > 0$$

Assumption

With P given as the unique positive definite solution to the DARE,

$$P = A_0^T P A_0 + Q - A_0^T P B_0 (R + B_0^T P B_0)^{-1} B_0^T P A_0$$

and furthermore that $G_P := -(R + B_0^T P B_0)^{-1} B_0^T$ and $H_P := A_0^T (I + P B_0 G_P)$, we have $\|H_P\|_2 + \frac{\|B_0 G_P\|_2 \|Q\|_2}{(1 - \|H_P\|_2)^2} < 1$

ϵ-MFE of the SLQ-MFG (contd.)

ϵ-MFE of the SLQ-MFG (contd.)

Theorem

Under above given Assumption, the MFE of LQ-MFG (K^*, F^*) is also the ϵ-MFE of the SLQ-MFG where $\epsilon = \mathcal{O}(\mathrm{tr}(\Sigma_C))$.

ϵ-MFE of the SLQ-MFG (contd.)

Theorem

Under above given Assumption, the MFE of LQ-MFG (K^*, F^*) is also the ϵ-MFE of the SLQ-MFG where $\epsilon = \mathcal{O}(\text{tr}(\Sigma_C))$.

- ϵ is dependent on the estimation error

ϵ-MFE of the SLQ-MFG (contd.)

Theorem

Under above given Assumption, the MFE of LQ-MFG (K^*, F^*) is also the ϵ-MFE of the SLQ-MFG where $\epsilon = \mathcal{O}(\mathrm{tr}(\Sigma_C))$.

- ϵ is dependent on the estimation error
- $\mathrm{tr}(\Sigma_C) \to 0 \implies \epsilon \to 0.$

$(\epsilon + \varepsilon)$-Nash Equilibrium of the secure n-agent LQ game

$(\epsilon + \varepsilon)$-Nash Equilibrium of the secure n-agent LQ game

Theorem

Under above given Assumption, let the cost of secure n-agent LQ game under controller μ^* *be* $J_i^n(\mu^{*i}, \mu^{*-i})$*, then*

$$J_i^n(\mu^{*i}, \mu^{*-i}) - \inf_{\pi^i \in \Pi_K^i} J_i^n(\pi^i, \mu^{*-i}) < \epsilon + \varepsilon$$

where $\epsilon = \mathcal{O}(\sigma_{max})$ *and* $\sigma_{max} := \max_{\Sigma_C \in \mathcal{E}_C} \mathrm{tr}(\Sigma_C)$ *and* $\varepsilon = \mathcal{O}(\sigma_{max}/\sqrt{n-1})$.

$(\epsilon + \varepsilon)$-Nash Equilibrium of the secure n-agent LQ game

Theorem

Under above given Assumption, let the cost of secure n-agent LQ game under controller μ^* be $J_i^n(\mu^{*i}, \mu^{*-i})$, then

$$J_i^n(\mu^{*i}, \mu^{*-i}) - \inf_{\pi^i \in \Pi_K^i} J_i^n(\pi^i, \mu^{*-i}) < \epsilon + \varepsilon$$

where $\epsilon = \mathcal{O}(\sigma_{max})$ and $\sigma_{max} := \max_{\Sigma_C \in \mathcal{E}_C} \mathrm{tr}(\Sigma_C)$ and $\varepsilon = \mathcal{O}(\sigma_{max}/\sqrt{n-1})$.

- If $\mathrm{tr}(\sigma_{max}) \to 0$ and $n \to \infty$ then $(\epsilon + \varepsilon) \to 0$.

Performance sensitivity w.r.t. sampling rate

Performance sensitivity w.r.t. sampling rate

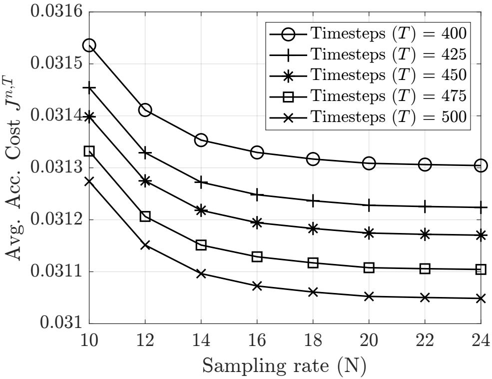


Figure: Average accumulated cost w.r.t. change in sampling rate N.

Performance sensitivity w.r.t. model parameters

Performance sensitivity w.r.t. model parameters

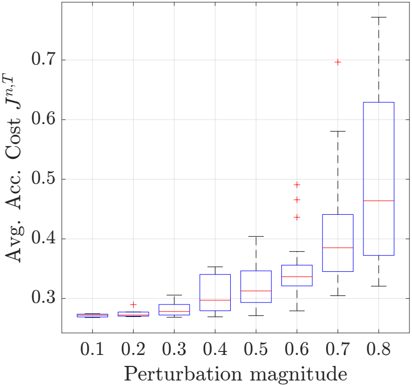


Figure: Average accumulated cost w.r.t. perturbation of the A and B matrices.

Performance sensitivity w.r.t. private keys

Performance sensitivity w.r.t. private keys

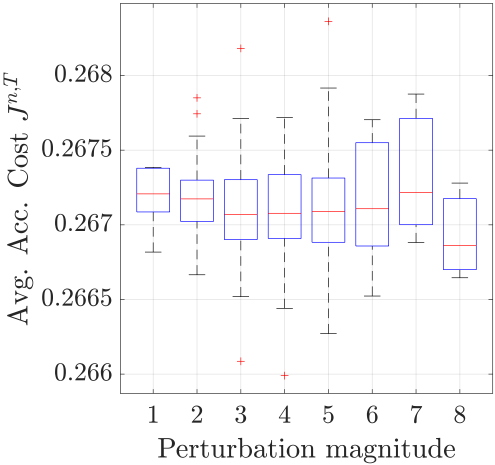


Figure: Average accumulated cost w.r.t. perturbation of the set of keys $\mathcal{C}$.

Conclusion

Conclusion

- We proposed a multi-rate sensor output sampling mechanism to reconstruct the state with some estimation error.

Conclusion

- We proposed a multi-rate sensor output sampling mechanism to reconstruct the state with some estimation error.
- We showed that estimation error results in non-existence of the Mean-Field Equilibrium (MFE) of the SLQ-MFG for the class of linear controllers

Conclusion

- We proposed a multi-rate sensor output sampling mechanism to reconstruct the state with some estimation error.
- We showed that estimation error results in non-existence of the Mean-Field Equilibrium (MFE) of the SLQ-MFG for the class of linear controllers
- We established that MFE of (standard) LQ-MFG, corresponds to ϵ-MFE of the SLQ-MFG, and an $(\epsilon + \varepsilon)$-Nash equilibrium for the secure $n-$agent dynamic game.

Conclusion

- We proposed a multi-rate sensor output sampling mechanism to reconstruct the state with some estimation error.
- We showed that estimation error results in non-existence of the Mean-Field Equilibrium (MFE) of the SLQ-MFG for the class of linear controllers
- We established that MFE of (standard) LQ-MFG, corresponds to ϵ-MFE of the SLQ-MFG, and an $(\epsilon + \varepsilon)$-Nash equilibrium for the secure $n-$agent dynamic game.
- We empirically demonstrated that performance of the $(\epsilon + \varepsilon)$-Nash equilibrium improves with increasing sampling rate N, deteriorates with variations in model parameters (A, B), and is insensitive to small perturbations in the set of private keys $\mathcal{C}$.