

A Risk-Theoretical Approach to H₂-Optimal Control under Covert Attacks

Matias I. Müller,

Jezdimir Milošević, Henrik Sandberg and Cristian R. Rojas (e-mails: {mimr2, jezdimir, hsan, crro}@kth.se)

Department of Automatic Control, KTH Royal Institute of Technology, Stockholm, Sweden

57th IEEE Conference on Decision and Control December 18th, 2018



Setup R 000 C

Introduction

0000

Risk Theory C

CVaR Control Design

Example 00 Conclusions O

Introduction: Control Systems are Vulnerable

Introduction

0000

Introduction: Control Systems are Vulnerable

CVaR Control Design

Example

Conclusions

Risk Theory



Setup

Introduction Setup Risk Theory CVaR Control Design Example Conclusions 0000 **Introduction: Control Systems are Vulnerable** Control Center Inadequate protection against malware Network Network -Control Station Control Station - 11 : 111 ... Sensor-Actuator Sensor-Actuator Physical

Processes

Introduction

Setup

Risk Theory

0000 **Introduction: Control Systems are Vulnerable** Control Center Inadequate protection against malware Communication links are Network Network not encrypted Control Station Control Station : 11 ... Sensor-Actuator Sensor-Actuator Physical Processes

CVaR Control Design

Conclusions

Example



0000

Introduction Risk Theory CVaR Control Design Example Setup **Control System under Attack**

Conclusions









Introduction Setup Risk Theory CVaR Control Design Example Conclusions







Introduction Setup Risk Theory CVaR Control Design Example Conclusions



- The attacker corrupts measurements/control signals.
- It tries to remain stealthy.
- Presence of attack is revealed through alarm triggering.

Control System under Attack



- The attacker corrupts measurements/control signals.
- It tries to remain stealthy.
- Presence of attack is revealed through alarm triggering.

Our concern: Control design under attack

Introduction

Setup 000

am

Risk Theory

CVaR Control Design

Example 00 Conclusions O

Undetectable Attacks

R. S. Smith, "Covert misappropriation of networked control systems: Presenting a feedback structure," IEEE Control Systems, vol. 35, no. 1, pp. 82-92, Feb 2015.

 $\mu = (I - \Theta_{\tau} \Pi_s)^{-1} \Theta_{nt} \gamma_{nt},$ $\gamma = (I - \Theta_{\tau} \Pi_s)^{-1} \Pi_s \Theta_{nt} \gamma_{nt}.$

The covert controller is designed for reference tracking, with γ_{ref} as the reference input.

To see the consequences of the nested closed-loop systems in Figure 2, replace (3) by (5) and (2) by (6) and rearrange to get

 $y - y_n = (I - \Theta_\gamma \Pi_z)^{-1} \Theta_{nl} \Pi_z \gamma_{nl} - n$ (1)

and

 $y_n = SP_nC_{nf}y_{nf} + SP_nw + Sn + S(P_n - \Pi_n)\mu. \quad (1$

Note that in (11), the relative offset of the actual plant output y from that measured—and controlled—by the nominal controller y_0 is the output of the covert agent's $y_{u-refer$ ence tracking controller. This gives the covert agent theability to drive the actual plant output to a desired offset $with respect to its nominal controlled value <math>y_{u.t.}$

To examine the nominal controller's ability to detect the actions of the covert agent, the nominal controller's measurement y_w in the nominal case [given by (G)] is compared to the covert misappropriation strategy case [given by (I2)]. The only difference between these two appears to the nominal controller as an output disturbance Eurom, given by

 $w_{\text{constit}} = S (P_u - \Pi_u) (l - \Theta_\gamma \Pi_u)^{-1} \Theta_{nt} \gamma_{nt}.$ (13)

If the covert agent has perfect knowledge of the plant's input response, $\Pi_n = P_{\alpha_1}$ then $u_{mone} = 0$ and the covert misappropriation is undetectable. This case was studied in [11] as a particular case of a slightly more general parameterization of the covert agent. It is important to note that the covert agent needs no knowledge of the nominal controller to execute an undetectable misappropriation strategy.

Specifying the covert agent's actions via the feedback structure in Figure 2 ensures that the overt controller's plant input signal μ is appropriate for the plant. Any feedback or actuation ifmitations imposed by the plant are taken into account in the design of the $I_1 - 0^3$, feedback loop writin the covert agent and will limit the range of γ_{ac} offset values that the covert outroffset on effectively command. These limitations make no difference to the extent to which the covert corteller's actions are be detected.

It is more realistic to consider that the covert agent's knowledge of the plant is not perfect. In this case, define the covert agent's model error Δ via covert agent's point of view, band-limiting the frequency content of γ_{mi} to those frequencies where the network control system operates well will make the covert actions harder to detect.

 The size of the covert agent's model error Δ. The higher the quality of the covert agent's knowledge of the plant, the harder it will be to detect covert actions.

3) The covert agent's reference to actuation transfer function (I − θ_i, Π_i)⁻¹θ_m. This is a function of the design of the covert agent and can be used to further hide the covert action. For example, by designing the bandwidth of (I − θ_i, Π_i)⁻²θ_m, to be lower than that of T the frequency components of µ will be in the rance where S is small, reducine the size of favora.

The size of the covert offset command γ_{set}.

Even if the covert agent's howeledge of the plant is not perfect, the nominal controller still sees, and responds to, the actual measurement noise and the actual plant disturbances. Furthermore, the dynamics of the controlled plant appear unchanged from the rominal cases. The effect on the measured plant output is, of any mominal controller covtent is appearing. These features hinder the nominal controller cover the single state of the second controller is appearing. These features hinder the nominal controller cover the shallty to detect over actions through probeing signals, such as watermarks, or signal analysis, such as noise or disturbance statistics characterization.

A LINEAR FLOW CANAL CONTROL EXAMPLE

Nominal Model and Operation

To illustrate the action of the overt agent with an incorrect plott model, an impignor, cancel example, exigningly described in [12], is studied. The geographical separation in the application exploits the node of an archived acousted system of the and [37]. The irregularity systems in illustrated in Figure 3. A reserver's at fixed height feeds and how can althrough a controlled duke gale. The outlet flow of the revervis is properturbank to the gale height arc. The water flows through a narrow skoping cantol to a second duke gale with the ends of each can alt of the reserved acoust of the ends of each can alt are the measured variables and the couples of interest in the control probes.

This system can be modeled by two partial differential equations, known as the Saint-Venant equations. The simplified model used here can be found in [12]

FEBRUARY 2015 & IEEE CONTROL SYSTEMS MAGAZINE 85

Introduction

tion

Setup

am

Risk Theory

CVaR Control Design

Example 00 Conclusions O

Undetectable Attacks

R. S. Smith, "Covert misappropriation of networked control systems: Presenting a feedback structure," IEEE Control Systems, vol. 35, no. 1, pp. 82-92, Feb 2015.

 $\mu = (l - \Theta_{\gamma} \Pi_{s})^{-1} \Theta_{nt} \gamma_{nt},$ $\gamma = (l - \Theta_{\gamma} \Pi_{s})^{-1} \Pi_{s} \Theta_{nt} \gamma_{nt}.$

The covert controller is designed for reference tracking, with γ_{ref} as the reference input.

To see the consequences of the nested closed-loop systems in Figure 2, replace (3) by (5) and (2) by (6) and rearrange to get

 $y - y_n = (I - \Theta_\gamma \Pi_n)^{-1} \Theta_{nd} \Pi_n \gamma_{nd} - n$ (1)

and

 $y_n = SP_nC_{nd}y_{nd} + SP_nw + Sn + S(P_n - \Pi_n)\mu.$ (12)

Note that in (11), the relative offset of the actual plant output y from that measured—and controlled—by the nominal controller y, is the output of the covert agent's y_ar-reference tracking controller. This gives the covert agent the ability to drive the actual plant output to a desired offset with respect to its nominal controlled value y_u.

To examine the nominal controller's ability to detect the actions of the covert agent, the nominal controller's measurement y_w in the nominal case [given by (4)] is compared to the covert misappropriation strategy case [given by (12)]. The only difference between these two appears to the peminal controller as an output disturbance meaning given by

 $w_{\text{conset}} = S(P_u - \Pi_u)(l - \Theta_r \Pi_u)^{-1}\Theta_{\text{ref}} T_{\text{ref}}$

If the covert agent has perfect knowledge of the plant's input response, $\Pi_{ie} = P_{oe}$ then $u_{tower} = 0$ and the covert misappropriation is undetectable. This case was studied in [11] as a particular case of a slightly more general parame-

covert agent needs no knowledge of the nominal controller to execute an undetectable misappropriation strategy.

Specifying the cover agent's actions via the feedback structure in Figure 2 ensures that the covert controller's plant input signal μ is appropriate for the plant. Any feedback or actuation limitations imposed by the plant and taken into account in the design of the Π_{-} -0, feedback loop within the covert agent and will limit the range of τ_{ac} offset values that the covert controller on effective command. These limitations make no difference to the extent to which the covert controller's actions and be detected.

It is more realistic to consider that the covert agent's knowledge of the plant is not perfect. In this case, define the covert agent's model error Δ via covert agent's point of view, band-limiting the frequency content of γ_{ret} to those frequencies where the network control system operates well will make the covert actions harder to detect.

 The size of the covert agent's model error Δ. The higher the quality of the covert agent's state log of the plant, the harder it will be to detect covert action

3) The covert agent's reference to actuate enough function (I ~ Θ, II, 3⁻¹Θ,... This is function of the design of the covert agent are Can be used to arthore hide the covert action. For canample, by designing the bandwidth of (I ~ Θ M, a⁻¹Θ_m to be lower than that of T the frequency components of µ will be in the range where 5 journal, reducing the size of itomax. The size of theovert offset command γ_m.

There is the operatory appet's location of the plane is not perform the operatory appet of the plane is not perform the plane is not perform the operatory of the actual plane distance. The thermore, the dynamics of the controlled plane is appeared in the plane is of the promised plane is appeared in the plane is of the plane is the plane of the plane is plane is the plane is the

LINEAR FLOW CANAL CONTROL EXAMPLE

ominal Model and Operation

Illustrate the action of the covert agent with an incorrect model, an implicit course along the end of the second interpletation explaints the node for a model segmention in the application explaints the node for a model segment of the protein ST and ST. The implicit segments are set of the figure 3. At reserves at a fixed height theorem 4. How each through a controlled duke gath. The outlet flow of the reserver's reporteriorization to the gath height are second and through a controlled duke gath. The outlet flow of the reserver's reporteriorization of the model of the second through a narrow skeping canal to a second duke gath with the rest of each canad are the measured variables and the couples of interest in the control problem.

This system can be modeled by two partial differential equations, known as the Saint-Venant equations. The simplified model used here can be found in [12]

FEBRUARY 2015 & IEEE CONTROL SYSTEMS MAGAZINE 85

"If the covert agent has perfect knowledge of the plant's input response then the covert misappropriation is undetectable [to the controller]."

A Risk-Theoretical Approach to H_2 -Optimal Control under Covert Attacks

Introduction

tion

Setup

am

Risk Theory

CVaR Control Design

Example 00 Conclusions O

Undetectable Attacks

R. S. Smith, "Covert misappropriation of networked control systems: Presenting a feedback structure," IEEE Control Systems, vol. 35, no. 1, pp. 82-92, Feb 2015.

 $\mu = (I - \Theta_{\gamma} \Pi_{s})^{-1} \Theta_{nl} \gamma_{nl},$ $\gamma = (I - \Theta_{\gamma} \Pi_{s})^{-1} \Pi_{s} \Theta_{nl} \gamma_{nl}.$

The covert controller is designed for reference tracking, with $\gamma_{\rm ref}$ as the reference input.

To see the consequences of the nested closed-loop systems in Figure 2, replace (3) by (5) and (2) by (6) and rearrange to get

 $y - y_n = (I - \Theta_\gamma \Pi_n)^{-1} \Theta_{nd} \Pi_n \gamma_{nd} - n$ (1)

and

 $y_n = SP_nC_{nd}y_{nd} + SP_nw + Sn + S(P_n - \Pi_n)\mu.$ (12)

Note that in (11), the relative offset of the actual plant output y from that measured—and controlled—by the nominal controller y, is the output of the covert agent's y_ar-reference tracking controller. This gives the covert agent the ability to drive the actual plant output to a desired offset with respect to its nominal controlled value y_u.

To examine the nominal controller's ability to detect the actions of the covert agent, the nominal controller's measurement y_w in the nominal case [given by (4)] is compared to the covert misappropriation strategy case [given by (12)]. The only difference between these two appears to the peminal controller as an output disturbance meaning given by

 $w_{\text{const}} = S(P_u - \Pi_u)(l - \Theta_{\gamma}\Pi_u)^{-1}\Theta_{nt}\gamma_{nt}$

If the covert agent has perfect knowledge of the plant's input response, $\Pi_{k} = P_{\alpha}$, then $u_{\text{covert}} = 0$ and the covert misappropriation is undetectable. This case was studied in [11] as a particular case of a slightly more general parame-

covert agent needs no knowledge of the nominal controller to execute an undetectable misappropriation strategy.

Specifying the cover agent's actions via the feedback structure in Figure 2 ensures that the covert controller's plant input signal μ is appropriate for the plant. Any feedback or actuation limitations imposed by the plant and taken into account in the design of the Π_{-} -0, feedback loop within the covert agent and will limit the range of τ_{ac} offset values that the covert controller on effective command. These limitations make no difference to the extent to which the covert controller's actions and be detected.

It is more realistic to consider that the covert agent's knowledge of the plant is not perfect. In this case, define the covert agent's model error Δ via covert agent's point of view, band-limiting the frequency content of γ_{rot} to those frequencies where the network control system operates well will make the covert actions harder to detect.

 The size of the covert agent's model error Δ. The higher the quality of the covert agent's state log of the plant, the harder it will be to detect covert action

3) The covert agent's reference to actuate enough function (I ~ Θ, II, 3⁻¹Θ,... This is function of the design of the covert agent are Can be used to arthore hide the covert action. For canample, by designing the bandwidth of (I ~ Θ M, a⁻¹Θ_m to be lower than that of T the frequency components of µ will be in the range where 5 journal, reducing the size of itomax. The size of theovert offset command γ_m.

There is the correspondence of the plane is not perfect, the organic correction of the second second perfect, the organic correction end was and the second bases. For hermerse, the dynamics correct correction appears for the second for second seco

LINEAR FLOW CANAL CONTROL EXAMPLE

ominal Model and Operation

Illustrate the action of the covert agent with an incoverte int model, an implicitor, canal county, exigning eorganisms of the standard fragment of the standard integration and exignition the need for a structured accented system of the standard fragment of the structure fragment A reserves at a fixed height free structure of the structure of the structure of the structure of the structure through a controlled balaice gate. The structure flows of the reversite sproperiments and from the structure as second actions, the structure of the structure the structure of the structu

This system can be modeled by two partial differential equations, known as the Saint-Venant equations. The simplified model used here can be found in [12] "If the covert agent has perfect knowledge of the plant's input response then the covert misappropriation is undetectable [to the controller]."

The controller cannot compensate for these attacks either!

FEBFUARY 2015 & IEEE CONTROL SYSTEMS MAGAZINE 85





• Inaccurate/Outdated model



- Inaccurate/Outdated model
- Fictitious uncertainty (multiplicative watermarking, Teixeira'18)



- Inaccurate/Outdated model
- Fictitious uncertainty (multiplicative watermarking, Teixeira'18)

Condition: covert attack + partial knowledge of the attacker:



- Inaccurate/Outdated model
- Fictitious uncertainty (multiplicative watermarking, Teixeira'18)

Condition: covert attack + partial knowledge of the attacker:

How to design a controller that performs well in most of the feasible attacker scenarios?



- Inaccurate/Outdated model
- Fictitious uncertainty (multiplicative watermarking, Teixeira'18)

Condition: covert attack + partial knowledge of the attacker:

How to design a controller that performs well in most of the feasible attacker scenarios?

Modeling the lack of knowledge of the attacker as uncertainty



- Inaccurate/Outdated model
- Fictitious uncertainty (multiplicative watermarking, Teixeira'18)

Condition: covert attack + partial knowledge of the attacker:

How to design a controller that performs well in most of the feasible attacker scenarios?

Modeling the lack of knowledge of the attacker as uncertainty



Models the attacker might potentially pocess













 $J_C := \|y_{\text{ref}} - y\|_2^2$





A Risk-Theoretical Approach to H2-Optimal Control under Covert Attacks



$$\boldsymbol{J}_{C} := \left\| \left(1 - \frac{[G - \Pi_{0}] C}{1 + GC} \right) \frac{GSK_{0}}{1 + K_{0}\Pi_{0}} \right\|_{2}^{2} + \left\| \left(1 - \frac{GC}{1 + GC} \right) R \right\|_{2}^{2} + \left\| \frac{HGC}{1 + GC} \right\|_{2}^{2}$$

A Risk-Theoretical Approach to H_2 -Optimal Control under Covert Attacks



$$\boldsymbol{J}_{C} := \left\| \left(1 - \frac{[G - \Pi_{0}] C}{1 + GC} \right) \frac{GSK_{0}}{1 + K_{0}\Pi_{0}} \right\|_{2}^{2} + \left\| \left(1 - \frac{GC}{1 + GC} \right) R \right\|_{2}^{2} + \left\| \frac{HGC}{1 + GC} \right\|_{2}^{2}$$

Matias Müller

A Risk-Theoretical Approach to \mathcal{H}_2 -Optimal Control under Covert Attacks



A Risk-Theoretical Approach to H_2 -Optimal Control under Covert Attacks



Matias Müller

A Risk-Theoretical Approach to H2-Optimal Control under Covert Attacks

Introduction

Setup

000

Problem Formulation

CVaR Control Design

Example

Conclusions

Problem 1: H2RCA (\mathcal{H}_2 -optimal Risk control under Covert Attacks)

Risk Theory

$$\begin{split} \min_{C \in \mathcal{H}_2} \mathcal{R}(\boldsymbol{J}_C) \\ \boldsymbol{J}_C(\theta) &= \left\| \left(1 - \frac{[G - \Pi_\theta] C}{1 + GC} \right) \frac{GSK_\theta}{1 + K_\theta \Pi_\theta} \right\|_2^2 \\ &+ \left\| \left(1 - \frac{GC}{1 + GC} \right) R \right\|_2^2 + \left\| \frac{HGC}{1 + GC} \right\|_2^2 \end{split}$$


Risk Theory

Setup

000

CVaR Control Design

Example 00

Conclusions O

Problem Formulation

Problem 1: H2RCA (\mathcal{H}_2 -optimal Risk control under Covert Attacks)

$$\begin{split} \min_{C \in \mathcal{H}_2} \mathcal{R}(\boldsymbol{J}_C) \\ \boldsymbol{J}_C(\theta) &= \left\| \left(1 - \frac{[G - \Pi_\theta] C}{1 + GC} \right) \frac{GSK_\theta}{1 + K_\theta \Pi_\theta} \right\|_2^2 \\ &+ \left\| \left(1 - \frac{GC}{1 + GC} \right) R \right\|_2^2 + \left\| \frac{HGC}{1 + GC} \right\|_2^2 \end{split}$$

Contribution:

1 How to choose $\mathcal{R}()$



Risk Theory

Setup

000

CVaR Control Design

Example 00

Conclusions O

Problem Formulation

Problem 1: H2RCA (\mathcal{H}_2 -optimal Risk control under Covert Attacks)

$$\begin{split} \min_{C \in \mathcal{H}_2} \mathcal{R}(\boldsymbol{J}_C) \\ \boldsymbol{J}_C(\theta) &= \left\| \left(1 - \frac{[G - \Pi_\theta] C}{1 + GC} \right) \frac{GSK_\theta}{1 + K_\theta \Pi_\theta} \right\|_2^2 \\ &+ \left\| \left(1 - \frac{GC}{1 + GC} \right) R \right\|_2^2 + \left\| \frac{HGC}{1 + GC} \right\|_2^2 \end{split}$$

Contribution:

- **1** How to choose $\mathcal{R}()$
- 2 Risk theoretic framework for attack resilient controller design



Risk Theory

Setup 000 CVaR Control Design

Example 00

Conclusions O

Problem Formulation

Problem 1: H2RCA (\mathcal{H}_2 -optimal Risk control under Covert Attacks)

$$\begin{split} \min_{C \in \mathcal{H}_2} \mathcal{R}(\boldsymbol{J}_C) \\ \boldsymbol{J}_C(\theta) &= \left\| \left(1 - \frac{[G - \Pi_\theta] C}{1 + GC} \right) \frac{GSK_\theta}{1 + K_\theta \Pi_\theta} \right\|_2^2 \\ &+ \left\| \left(1 - \frac{GC}{1 + GC} \right) R \right\|_2^2 + \left\| \frac{HGC}{1 + GC} \right\|_2^2 \end{split}$$

Contribution:

- **1** How to choose $\mathcal{R}()$
- 2 Risk theoretic framework for attack resilient controller design
- 3 Comparison between different measures of risk

,	Introduction	Setup	Risk Theory	CVaR Control Design	Example	Conclusions			
KTH %	0000	000	●00	00000	00	O			
VETENSKAP	Risk Theory								

200 Carlo Carlo

KTH vetenskap	Introduction 0000	Setup 000	Risk Theory ●00	CVaR Control Design 00000	Example 00	Conclusions O	
	Risk Theory						

 $\theta \sim p(\theta)$

Random variable



Random variable

Decision



Random variable

Decision

Cost (pdf)





















Matias Müller



Matias Müller



Common choices of $\mathcal{R}()$ are $\mathbb{E}\{\}$,







Definition (Conditional value-at-risk)

$$CVaR_{\alpha}(Y) := \frac{1}{1-\alpha} \int_{y:P\{Y \le y\} \ge \alpha} yp(y) dy$$



Definition (Conditional value-at-risk)

$$CVaR_{\alpha}(Y) := \frac{1}{1-\alpha} \int_{y:P\{Y \le y\} \ge \alpha} y p(y) dy$$





Definition (Conditional value-at-risk)

$$CVaR_{\alpha}(Y) := \frac{1}{1-\alpha} \int_{y:P\{Y \le y\} \ge \alpha} yp(y) dy$$





Definition (Conditional value-at-risk)

$$CVaR_{\alpha}(Y) := \frac{1}{1-\alpha} \int_{y:P\{Y \le y\} \ge \alpha} yp(y) dy$$





Definition (Conditional value-at-risk)

$$\operatorname{CVaR}_{\alpha}(Y) := \frac{1}{1-\alpha} \int_{y: \operatorname{P}\{Y \le y\} \ge \alpha} y p(y) dy = \mathbb{E}\left\{Y | Y \ge \operatorname{VaR}_{\alpha}(Y)\right\}$$





Definition (Conditional value-at-risk)

For $\alpha \in [0, 1]$:

$$CVaR_{\alpha}(Y) := \frac{1}{1-\alpha} \int_{y:P\{Y \le y\} \ge \alpha} yp(y) dy = \mathbb{E}\left\{Y|Y \ge VaR_{\alpha}(Y)\right\}$$



CVaR is convex \rightarrow easy to optimize



An alternative expression for CVaR

Conclusions



Remark

By considering the dual problem (Rockafellar and Uryasev, 2000):



Remark

By considering the dual problem (Rockafellar and Uryasev, 2000):

$$\operatorname{CVaR}_{\alpha}(\boldsymbol{J}_{C}) = \min_{\mu \in \mathbb{R}} \mu + \frac{1}{1 - \alpha} \mathbb{E}\left\{ [\boldsymbol{J}_{C} - \mu]_{+} \right\}$$

â	
KTH &	
R VETENSKAP	

Introduction	Setup	Risk Theory	CVaR Control Design	Example	Conclusions		
0000	000	000	●0000	00	O		
CVaR Control Design							

KTH vetenskap

Introduction Setup Risk Theory CVaR Control Design Example Conclusions CVaR Control Design •••••• •••••• ••••• ••••• ••••• ••••• ••••• ••••• ••••• ••••• ••••• ••••• ••••• ••••• ••• <td

ф КТН ¥	Introduction 0000	Setup 000	Risk Theory 000	CVaR Control Design ●0000	Example 00	Conclusions O		
CH KONST	CVaR Control Design							
1 Reparametrize the cost function: Youla Parameter								

Let $Q := \frac{C}{1+GC} \iff C = \frac{Q}{1-CQ}$. Then

KTH VETENSKAP OCH KONST

CVaR Control Design

1 Reparametrize the cost function: Youla Parameter Let $Q := \frac{C}{1+GC} \iff C = \frac{Q}{1-CQ}$. Then

$$\boldsymbol{J}_{C}(\theta) = \left\| \left(1 - \frac{\left[G - \Pi_{\theta}\right]C}{1 + GC} \right) \frac{GSK_{\theta}}{1 + K_{\theta}\Pi_{\theta}} \right\|_{2}^{2} + \left\| \left(1 - \frac{GC}{1 + GC} \right)R \right\|_{2}^{2} + \left\| \frac{HGC}{1 + GC} \right\|_{2}^{2}$$

KTH vetenskap och konst

Introduction

CVaR Control Design

CVaR Control Design

00000

1 Reparametrize the cost function: Youla Parameter

Risk Theory

Let
$$Q := \frac{C}{1+GC} \iff C = \frac{Q}{1-CQ}$$
. Then

Setup

$$\boldsymbol{J}_{C}(\theta) = \left\| \left(1 - \frac{[G - \Pi_{\theta}]C}{1 + GC} \frac{GSK_{\theta}}{1 + K_{\theta}\Pi_{\theta}} \right\|_{2}^{2} + \left\| \left(1 - \frac{GC}{1 + GC} \right)R \right\|_{2}^{2} + \left\| \frac{HGC}{1 + GC} \right\|_{2}^{2} \right\|_{2}^{2}$$

Conclusions

Example

Setup

Risk Theory

CVaR Control Design

Example 00

Conclusions O

CVaR Control Design

1 Reparametrize the cost function: Youla Parameter Let $Q := \frac{C}{1+GC} \iff C = \frac{Q}{1-CO}$. Then

$$J_{C}(\theta) = \left\| \left(1 - \frac{[G - \Pi_{\theta}]C}{1 + GC} \frac{GSK_{\theta}}{1 + K_{\theta}\Pi_{\theta}} \right\|_{2}^{2} + \left\| \left(1 - \frac{GC}{1 + GC} \right)R \right\|_{2}^{2} + \left\| \frac{HGC}{1 + GC} \right\|_{2}^{2} \\ = \left\| (1 - [G - \Pi_{\theta}]Q) \frac{GSK_{\theta}}{1 + K_{\theta}\Pi_{\theta}} \right\|_{2}^{2} + \left\| (1 - GQ)R \right\|_{2}^{2} + \left\| HGQ \right\|_{2}^{2}$$

CVaR Control Design

CVaR Control Design

00000

Example

Conclusions

Risk Theory

Setup

1 Reparametrize the cost function: Youla Parameter Let $Q := \frac{C}{1+GC} \iff C = \frac{Q}{1-CQ}$. Then $J_{C}(\theta) = \left\| \left(1 - \frac{[G - \Pi_{\theta}]C}{1+GC} \right) \frac{GSK_{\theta}}{1+K_{\theta}\Pi_{\theta}} \right\|_{2}^{2} + \left\| \left(1 - \frac{GC}{1+GC} \right)R \right\|_{2}^{2} + \left\| \frac{HGC}{1+GC} \right\|_{2}^{2}$ $= \left\| (1 - [G - \Pi_{\theta}]Q) \frac{GSK_{\theta}}{1+K_{\theta}\Pi_{\theta}} \right\|_{2}^{2} + \left\| (1 - GQ)R \right\|_{2}^{2} + \left\| HGQ \right\|_{2}^{2}$ $=: V_{Q}(\theta)$

Risk Theory

Setup

CVaR Control Design

Example 00

Conclusions

CVaR Control Design

1 Reparametrize the cost function: Youla Parameter Let $Q := \frac{C}{1+GC} \iff C = \frac{Q}{1-CQ}$. Then

$$J_{C}(\theta) = \left\| \left(1 - \frac{[G - \Pi_{\theta}]C}{1 + GC} \frac{GSK_{\theta}}{1 + K_{\theta}\Pi_{\theta}} \right\|_{2}^{2} + \left\| \left(1 - \frac{GC}{1 + GC} R \right\|_{2}^{2} + \left\| \frac{HGC}{1 + GC} \right\|_{2}^{2} \right) \\ = \left\| (1 - [G - \Pi_{\theta}]Q) \frac{GSK_{\theta}}{1 + K_{\theta}\Pi_{\theta}} \right\|_{2}^{2} + \left\| (1 - GQ)R \right\|_{2}^{2} + \left\| HGQ \right\|_{2}^{2} \right\|_{2}^{2}$$

 $=: V_{\mathcal{Q}}(\theta)$

H2RCA is then equivalent to

 $\min_{Q\in\mathcal{H}_2} \operatorname{CVaR}_{\alpha}(V_Q)$

KTH vetenskap och konst

CVaR Control Design

CVaR Control Design

00000

Risk Theory

2 Approximate the feasible set \mathcal{H}_2 in

Setup

Introduction

 $\min_{\mathcal{Q}\in\mathcal{H}_2}\mathrm{CVaR}_\alpha(\mathbf{V}_{\mathcal{Q}})$

Conclusions

Example

KTH vetenskap

CVaR Control Design

CVaR Control Design

Example

Conclusions

Risk Theory

2 Approximate the feasible set \mathcal{H}_2 in

Setup

Introduction

 $\min_{Q \in \mathcal{H}_2} \operatorname{CVaR}_{\alpha}(V_Q) \approx \min_{Q \in \mathcal{Q}_L} \operatorname{CVaR}_{\alpha}(V_Q)$
KTH vetenskap och konst

CVaR Control Design

CVaR Control Design

00000

Example

Conclusions

2 Approximate the feasible set \mathcal{H}_2 in

Setup

Introduction

 $\min_{Q \in \mathcal{H}_2} \operatorname{CVaR}_{\alpha}(V_Q) \approx \min_{Q \in \mathcal{Q}_L} \operatorname{CVaR}_{\alpha}(V_Q)$ with $\mathcal{Q}_L = \{Q \colon Q(z) = \sum_{k=0}^L x_k z^{-k}, x_0, \dots, x_L \in \mathbb{R}\}.$

Risk Theory

KTH vetenskap och konst

CVaR Control Design

Risk Theory

2 Approximate the feasible set \mathcal{H}_2 in

Setup

 $\min_{Q \in \mathcal{H}_2} \operatorname{CVaR}_{\alpha}(V_Q) \approx \min_{Q \in \mathcal{Q}_L} \operatorname{CVaR}_{\alpha}(V_Q)$ with $\mathcal{Q}_L = \{ Q \colon Q(z) = \sum_{k=0}^L x_k z^{-k}, x_0, \dots, x_L \in \mathbb{R} \}.$



CVaR Control Design

00000

Example

Conclusions

Introduction

KTH vetenskap

	Introduction 0000	Setup 000	Risk Theory 000	CVaR Control Design	Example 00	Conclusions O
	CVaR Control Design					
3 We approximate $\text{CVaR}_{\alpha}(V_Q(\theta))$:						

Introduction Setup Risk Theory CVaR Control Design Example Conclusions

3 We approximate
$$\text{CVaR}_{\alpha}(V_Q(\theta))$$
:

$$\operatorname{CVaR}_{\alpha}(V_{\mathcal{Q}}) = \min_{\mu \in \mathbb{R}} \mu + \frac{1}{1 - \alpha} \mathbb{E}\left\{ [V_{\mathcal{Q}} - \mu]_{+} \right\}$$

(

 Introduction
 Setup
 Risk Theory
 CVaR Control Design
 Example
 Conclusions

 KTH
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000
 000

3 We approximate $\text{CVaR}_{\alpha}(V_Q(\theta))$:

$$\operatorname{CVaR}_{\alpha}(V_{Q}) = \min_{\mu \in \mathbb{R}} \mu + \frac{1}{1 - \alpha} \underbrace{\mathbb{E}\left\{ [V_{Q} - \mu]_{+} \right\}}_{\text{hard to compute!}}$$



We approximate
$$\text{CVaR}_{\alpha}(V_Q(\theta))$$
:

$$\operatorname{CVaR}_{\alpha}(V_{Q}) = \min_{\mu \in \mathbb{R}} \mu + \frac{1}{1 - \alpha} \underbrace{\mathbb{E}\left\{ [V_{Q} - \mu]_{+} \right\}}_{\text{hard to compute!}}$$

$$\{\theta_i\}_{i=1}^N$$
: *N* iid samples from $p(\theta)$

 Introduction
 Setup
 Risk Theory
 CVaR Control Design
 Example

 VETENSAR
 000
 000
 000
 000
 000

 VETENSAR
 CVaR Control Design
 00
 00

3 We approximate
$$\text{CVaR}_{\alpha}(V_Q(\theta))$$
:

$$CVaR_{\alpha}(V_{Q}) = \min_{\mu \in \mathbb{R}} \mu + \frac{1}{1 - \alpha} \underbrace{\mathbb{E}\left\{ [V_{Q} - \mu]_{+} \right\}}_{\text{hard to compute!}}$$
$$\approx \min_{\mu \in \mathbb{R}} \mu + \frac{1}{1 - \alpha} \frac{1}{N} \sum_{i=1}^{N} [V_{Q}(\theta_{i}) - \mu]_{+}$$

 $\{\theta_i\}_{i=1}^N$: *N* iid samples from $p(\theta)$

(

Conclusions

 Introduction
 Setup
 Risk Theory
 CVaR Control Design
 Example

 VETENSAR
 000
 000
 000
 000
 00

 VETENSAR
 CVaR Control Design
 Example
 00

 CVaR Control Design
 CVaR Control Design
 Example

3 We approximate $\text{CVaR}_{\alpha}(V_Q(\theta))$:

$$CVaR_{\alpha}(V_{Q}) = \min_{\mu \in \mathbb{R}} \mu + \frac{1}{1 - \alpha} \underbrace{\mathbb{E}\left\{ [V_{Q} - \mu]_{+} \right\}}_{\text{hard to compute!}}$$
$$\approx \min_{\mu \in \mathbb{R}} \mu + \frac{1}{1 - \alpha} \frac{1}{N} \sum_{i=1}^{N} [V_{Q}(\theta_{i}) - \mu]_{+}$$
$$=: \overline{CVaR}_{\alpha}(\{V_{Q}(\theta_{i})\}_{i=1}^{N})$$
$$\{\theta_{i}\}_{i=1}^{N}: N \text{ iid samples from } p(\theta)$$

Conclusions

 Introduction
 Setup
 Risk Theory
 CVaR Control Design
 Example

 VETENSAR
 000
 000
 000
 000
 00

 VETENSAR
 CVaR Control Design
 Example
 00

 VOLUCION
 CVaR Control Design
 00

(a) We approximate
$$\operatorname{CVaR}_{\alpha}(V_{\mathcal{Q}}(\theta))$$
:

$$\operatorname{CVaR}_{\alpha}(V_{\mathcal{Q}}) = \min_{\mu \in \mathbb{R}} \mu + \frac{1}{1 - \alpha} \underbrace{\mathbb{E}\left\{ [V_{\mathcal{Q}} - \mu]_{+} \right\}}_{\text{hard to compute!}}$$

$$\approx \min_{\mu \in \mathbb{R}} \mu + \frac{1}{1 - \alpha} \frac{1}{N} \sum_{i=1}^{N} [V_{\mathcal{Q}}(\theta_{i}) - \mu]_{+}$$

$$=: \overline{\operatorname{CVaR}}_{\alpha}(\{V_{\mathcal{Q}}(\theta_{i})\}_{i=1}^{N})$$

 $\{\theta_i\}_{i=1}^N$: *N* iid samples from $p(\theta)$

Problem 2:

$$\min_{Q \in \mathcal{H}_2} \operatorname{CVaR}_{\alpha}(V_Q) \approx \min_{Q \in \mathcal{Q}_L} \overline{\operatorname{CVaR}_{\alpha}(\{V_Q(\theta_i)\}_{i=1}^N)}$$

Conclusions



Introduction

CVaR Control Design

CVaR Control Design

Example

Conclusions

Lemma (Convergence of cost functions)

Setup

Let N = # iid samples from $p(\theta)$, and L = length of the FIR filter:

Risk Theory



Lemma (Convergence of cost functions)

Let N = # iid samples from $p(\theta)$, and L = length of the FIR filter:

 $\lim_{N,L\to\infty} \min_{Q\in\mathcal{Q}_L} \overline{\mathrm{CVaR}_{\alpha}}(\{V_Q(\theta_i)\}_{i=1}^N) = \min_{Q\in\mathcal{H}_2} \mathrm{CVaR}_{\alpha}(V_Q)$



Let N = # iid samples from $p(\theta)$, and L = length of the FIR filter.



Let N = # iid samples from $p(\theta)$, and L = length of the FIR filter. Then $Q^* := \arg \min_{Q \in Q_L} \overline{\text{CVaR}}_{\alpha}(\{V_Q(\theta_i)\}_{i=1}^N) = \sum_{k=0}^L x_k^* z^{-k},$



Let N = # iid samples from $p(\theta)$, and L = length of the FIR filter. Then $Q^* := \arg\min_{Q \in Q_L} \overline{\text{CVaR}}_{\alpha}(\{V_Q(\theta_i)\}_{i=1}^N) = \sum_{k=0}^L x_k^* z^{-k},$ $x^* := [x_0^* \quad x_1^* \quad \dots \quad x_L^*],$



Let N = # iid samples from $p(\theta)$, and L = length of the FIR filter. Then $Q^{\star} := \arg \min_{Q \in Q_L} \overline{\text{CVaR}}_{\alpha}(\{V_Q(\theta_i)\}_{i=1}^N) = \sum_{k=0}^L x_k^{\star} z^{-k},$ $x^{\star} := [x_0^{\star} \quad x_1^{\star} \quad \dots \quad x_L^{\star}], \text{ where}$

$$\begin{bmatrix} \mathbf{x}^{\star} & \mu^{\star} & \mathbf{t}^{\star} \end{bmatrix}^{\top} := \underset{[\mathbf{x} & \mu}{\operatorname{arg\,min}} \underset{\mathbf{t}]^{\top} \in \mathbb{R}^{L+N+2}}{\operatorname{arg\,min}} \mu + \frac{1}{N(1-\alpha)} \mathbf{1}_{N}^{\top} \mathbf{t}$$

subject to
$$t_{i} \ge k(\theta_{i}) + \mathbf{x}^{\top} \mathbf{M}(\theta_{i}) \mathbf{x} - 2\mathbf{c}^{\top}(\theta_{i}) \mathbf{x} - \mu,$$

$$t_{i} \ge 0, \quad i = 1, \dots, N$$



Let N = # iid samples from $p(\theta)$, and L = length of the FIR filter. Then $Q^{\star} := \arg \min_{Q \in Q_L} \overline{\text{CVaR}}_{\alpha}(\{V_Q(\theta_i)\}_{i=1}^N) = \sum_{k=0}^L x_k^{\star} z^{-k},$ $x^{\star} := [x_0^{\star} \quad x_1^{\star} \quad \dots \quad x_L^{\star}], \text{ where}$

$$\begin{bmatrix} \mathbf{x}^{\star} & \mu^{\star} & \mathbf{t}^{\star} \end{bmatrix}^{\top} := \underset{[\mathbf{x} & \mu & \mathbf{t} \end{bmatrix}^{\top} \in \mathbb{R}^{L+N+2}}{\operatorname{arg\,min}} \mu + \frac{1}{N(1-\alpha)} \mathbf{1}_{N}^{\top} \mathbf{t}$$

subject to
$$t_{i} \geq k(\theta_{i}) + \mathbf{x}^{\top} \mathbf{M}(\theta_{i}) \mathbf{x} - 2\mathbf{c}^{\top}(\theta_{i}) \mathbf{x} - \mu,$$

$$t_{i} \geq 0, \quad i = 1, \dots, N$$

H2RCA \approx Problem 2 \rightarrow QCLP (easy to solve)



A Risk-Theoretical Approach to H2-Optimal Control under Covert Attacks







• Link between Control Design and Financial Theory of Risk



- Link between Control Design and Financial Theory of Risk
- When $\mathcal{R} = \text{CVaR}_{\alpha}$, a QLCP approximates the solution



- Link between Control Design and Financial Theory of Risk
- When $\mathcal{R} = \text{CVaR}_{\alpha}$, a QLCP approximates the solution
- Better control performance by using $p(\theta)$



A Risk-Theoretical Approach to H₂-Optimal Control under Covert Attacks

Matias I. Müller,

Jezdimir Milošević, Henrik Sandberg and Cristian R. Rojas (e-mails: {mimr2, jezdimir, hsan, crro}@kth.se)

Department of Automatic Control, KTH Royal Institute of Technology, Stockholm, Sweden

57th IEEE Conference on Decision and Control December 18th, 2018



CVaR Properties





CVaR Properties



A Risk-Theoretical Approach to \mathcal{H}_2 -Optimal Control under Covert Attacks