Errata for Ph.D. Thesis "Towards Realistic Smart Meter Privacy against Bayesian Inference"

Ramana Reddy Avula

Acknowledgement

Page iii, Line 10 - change in grading committee after publication	
Before	"members Prof. Math Bollen, Prof. Simone Fischer-Hübner, and Assoc. Prof."
After	"members Prof. Simone Fischer-Hübner, Assoc. Prof. Isaac Skog, and Assoc. Prof."

Chapter 1: Control Strategies Against Controller-unaware Adversaries

§1.4.1, Page 7, Line 18 - data masking instead of data suppression	
Before	"-ing various methods, such as data swapping, data suppression, or data"
After	"-ing various methods, such as data swapping, data masking, or data"

Chapter 3: Control Strategies Against Controller-unaware Adversaries

§3.3.1, Page 32, Line 5 - wrong notation of vector sequence	
Before	"$[S_1^k, D_1^{k-1}, Y_{1:k-1}]$ denote the information available to the EMU at time-slot k."
After	"$[S_{1:k}, D_{1:k-1}, Y_{1:k-1}]$ denote the information available to the EMU at time-slot k."

§3.3.1.3, Page 36, Line 2-5, Sentence 2 - the complete sentence is to be removed	
Before	"We consider a utility-driven DSM scenario where the user receives a target demand signal from the grid, which is constant throughout the day. The target signal is generated by the grid operator using the historical demands of the user averaged during the day."
After	

§3.3.2, Page 38, Line 12 - wrong domain for $\boldsymbol{\beta}_k$	
Before	"-time controller, which can be characterized by a probability vector $P_{U_k} \in \Delta_{\lvert\mathcal{U}\rvert}$."
After	"-time controller, which can be characterized by a probability vector $P_{U_k} \in \Delta_{\lvert\mathcal{Y}\rvert}^{\lvert\mathcal{X}\rvert}$."

§3.3.2, Page 38, Line 13 - wrong notation of vector sequence	
Before	"Further, let $\underline{I}_k := [X_{1:k-1}, Z_1^k, D_1^{k-1}, Y_{1:k-1}]$ represent the information available"
After	"Further, let $\underline{I}_k := [X_{1:k-1}, Z_{1:k}, D_{1:k-1}, Y_{1:k-1}]$ represent the information available"

§3.3.2.1, Page 39, Line 14 - wrong domain for $\boldsymbol{\beta}_k$	
Before	"ESS state z_k, let $\boldsymbol{\mathcal{B}}(z_k) \subseteq \Delta_{\lvert\mathcal{U}\rvert}$ denote the feasible set of $\boldsymbol{\beta}_k$ satisfying the ESS"
After	"ESS state z_k, let $\boldsymbol{\mathcal{B}}(z_k) \subseteq \Delta_{\lvert\mathcal{Y}\rvert}^{\lvert\mathcal{X}\rvert}$ denote the feasible set of $\boldsymbol{\beta}_k$ satisfying the ESS"

§3.3.3, Page 43, Line 2 - wrong notation of vector sequence	
Before	"$\underline{I}_k := [X_{1:k-1}, Z_1^k, D_1^{k-1}, Y_{1:k-1}]$ represent the information available to the policy"
After	"$\underline{I}_k := [X_{1:k-1}, Z_{1:k}, D_{1:k-1}, Y_{1:k-1}]$ represent the information available to the policy"

§3.4.1.1, Page 51, Eq. 3.21 - conditional dependence of Y_k on $\tilde{r}_{k+1}$ in expectation is missing	
Before	$\tilde{r}_k(w_k) := \min_{y_k \in \mathcal{Y}} \left\{ r_k(w_k, y_k, \zeta_k^\dagger) + \mathbb{E}\left[\tilde{r}_{k+1}\left(W_{k+1}\right) \middle| W_k = w_k \right] \right\},$
After	$\tilde{r}_k(w_k) := \min_{y_k \in \mathcal{Y}} \left\{ r_k(w_k, y_k, \zeta_k^\dagger) + \mathbb{E}\left[\tilde{r}_{k+1}\left(W_{k+1}\right) \middle| W_k = w_k, Y_k = y_k \right] \right\},$

§3.4.2.1, Page 55, Eq. 3.26 - wrong notation for optimal causal MAP detection strategy	
Before	$\zeta_k^{\#}(y_{k-1:k}, \hat{\pi}_{k-1}) = \underset{\hat{\boldsymbol{h}}_k \in \boldsymbol{\mathcal{H}}}{\operatorname{argmax}} \left\{ \hat{r}_k(y_{k-1:k}, \hat{\pi}_{k-1}, \hat{\boldsymbol{h}}_k) \right\},$
After	$\bar{\zeta}^*(y_{k-1:k}, \hat{\pi}_{k-1}) = \underset{\hat{\boldsymbol{h}}_k \in \boldsymbol{\mathcal{H}}}{\operatorname{argmax}} \left\{ \hat{r}_k(y_{k-1:k}, \hat{\pi}_{k-1}, \hat{\boldsymbol{h}}_k) \right\},$

§3.4.2.1, Page 56, Eq. 3.28 - wrong notation for Bayesian risk and conditional dependence of Y_k on $\tilde{r}_{k+1}$ in expectation is missing	
Before	$\tilde{r}_k(\boldsymbol{a}_k, \pi_k, \hat{\pi}_{k-1}) = \min_{y_k \in \mathcal{Y}_k(\boldsymbol{a}_k)} \Big\{ c_k(\boldsymbol{a}_k, \pi_k, \hat{\pi}_{k-1}, y_k) + \mathbb{E}\left[\tilde{r}_{k+1}(\boldsymbol{A}_{k+1}, \mathit{\Pi}_{k+1}, \hat{\mathit{\Pi}}_k) \middle| \boldsymbol{A}_k = \boldsymbol{a}_k \right] \Big\},$
After	$\tilde{r}_k(\boldsymbol{a}_k, \pi_k, \hat{\pi}_{k-1}) = \min_{y_k \in \mathcal{Y}_k(\boldsymbol{a}_k)} \Big\{ r_k(\boldsymbol{a}_k, \pi_k, \hat{\pi}_{k-1}, y_k) + \mathbb{E}\left[\tilde{r}_{k+1}(\boldsymbol{A}_{k+1}, \mathit{\Pi}_{k+1}, \hat{\mathit{\Pi}}_k) \middle| \boldsymbol{A}_k = \boldsymbol{a}_k, Y_k = y_k \right] \Big\},$

§3.4.2.1, Page 56, Line 13-16 - typeset error for subscripts in variables	
Before	"where $\mathcal{Y}k(\boldsymbol{a}k)$ is the set of valid control actions given by the ESS model; $\tilde{r}k$ is the expected risk over $[k, \ldots, N]$ due to the optimal strategy $\mu k : N^*$; and the recursion is initialized by a terminal cost function $\tilde{r}N + 1$. Note that (3.28) needs to be solved over continuous spaces of the belief states π_k and $\hat{\pi}k - 1$. In the following, we have"
After	"where $\mathcal{Y}_k(\boldsymbol{a}_k)$ is the set of valid control actions given by the ESS model; $\tilde{r}_k$ is the expected risk over $[k, \ldots, N]$ due to the optimal strategy $\mu^*_{k:N}$; and the recursion is initialized by a terminal cost function $\tilde{r}_{N+1}$. Note that (3.28) needs to be solved over continuous spaces of the belief states π_k and $\hat{\pi}_{k-1}$. In the following, we have"

§3.4.2.1, Page 56, Proposition 3.3, Line 4 - error in the statement	
Before	"the minimum expected cumulative Bayesian risk equivalent to the optimal strategy"
After	"an upper bound to the minimum expected cumulative Bayesian risk achievable by the optimal strategy"

§3.4.2.1, Page 56, Line 23 - should be "approximate optimal" instead of "optimal strategy"	
Before	"to $\hat{\pi}_{k-1}$, the optimal strategy $\tilde{\mu}^*_k$ can be obtained using the simplex partitioning"
After	"to $\hat{\pi}_{k-1}$, the approximate optimal strategy $\tilde{\mu}^*_k$ can be obtained using the simplex partitioning"

References

Page 116, Ref. 106 - missing volume and wrong page numbers	
Before	“R. R. Avula, J.-X. Chin, T. J. Oechtering, G. Hug, and D. Månsson, "Design framework for privacy-aware demand-side management with realistic energy storage model," IEEE Transactions on Smart Grid, pp. 1-1, 2021.”
After	“R. R. Avula, J.-X. Chin, T. J. Oechtering, G. Hug, and D. Månsson, "Design framework for privacy-aware demand-side management with realistic energy storage model," IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3503-3513, 2021.”