Por que Precisamos de Redes Inteligentes de Abastecimento e Distribuição com Segurança e Privacidade?

SBPC 2018

Dr.-Ing. Fábio Borges de Oliveira

Laboratório Nacional de Computação Científica (LNCC)
Coordenação de Tecnologia da Informação e Comunicação (CoTIC)

Tópicos

Laboratório Nacional de Computação Científica

Redes de Fornecimento (*Smart Grids*)

Por que Precisamos?

O Problema da Eletricidade

Rede Antiga

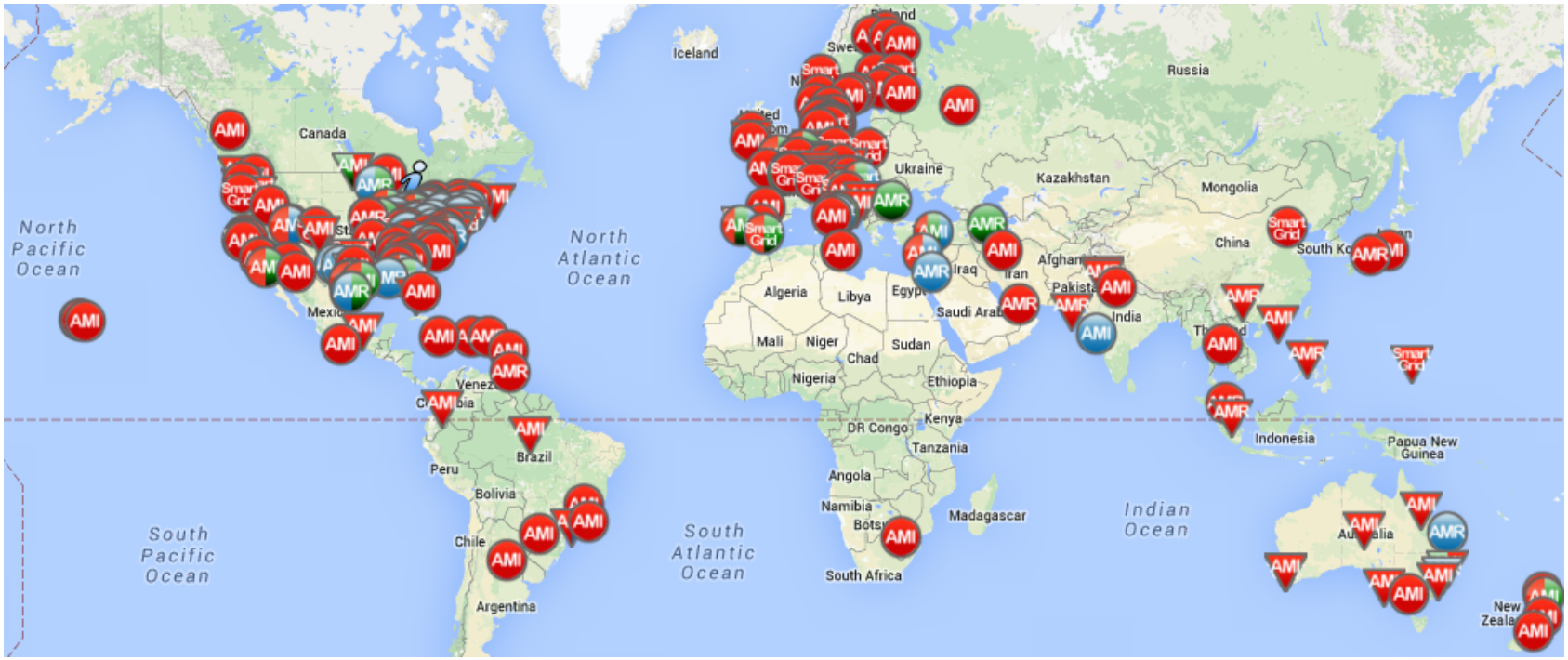
Rede Inteligente

Segurança e Privacidade

Conclusões

Smart Metering Projects Map

Google Maps



Pipelines for Goods

Transportes automatizados de mercadorias

Laboratório Nacional de Computação Científica

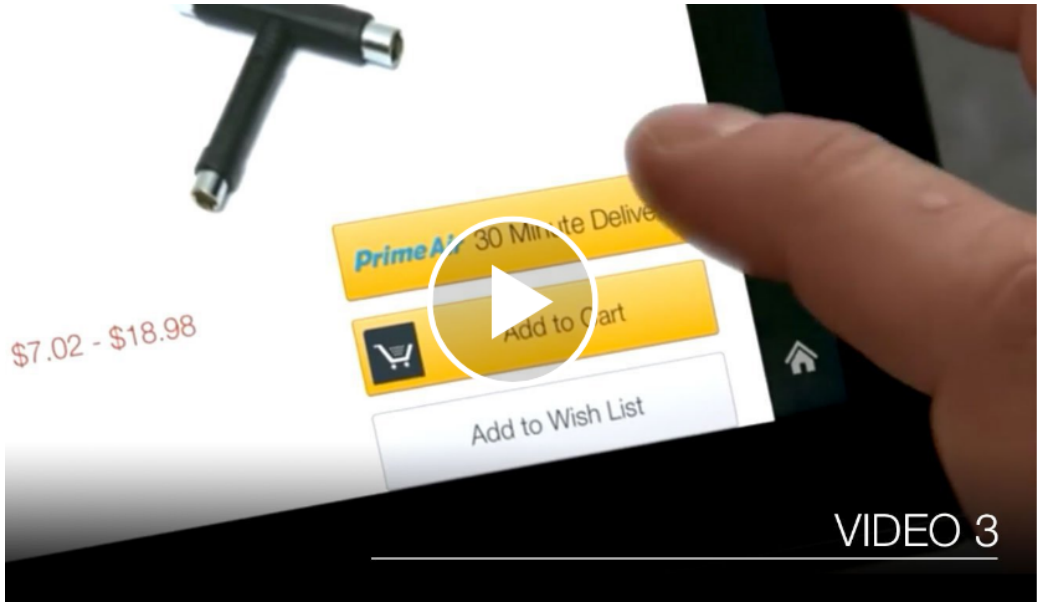
Transportes automatizados

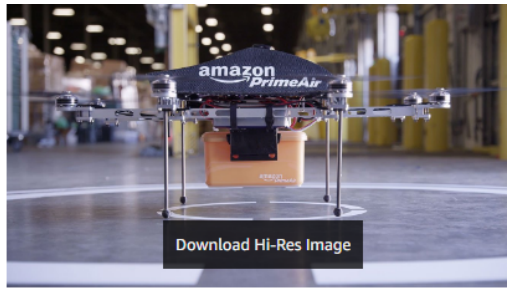
Terrestres

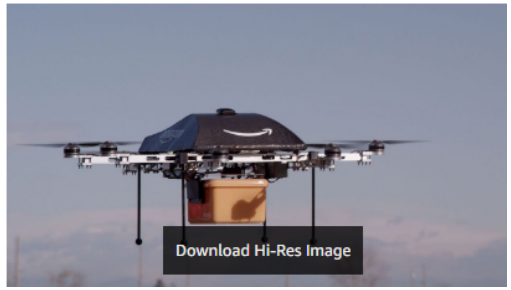
Transportes automatizados

Aéreos

Laboratório Nacional de Computação Científica







Tópicos

Notícias no Caos em Maio de 2018

Desabastecimento

- Dia 24, Greve de caminhoneiros gera desabastecimento pelo Brasil

Notícias no Caos em Maio de 2018

Desabastecimento

- Dia 24, Greve de caminhoneiros gera desabastecimento pelo Brasil
- 28 às 12:35, Abastecida por trem, Bauru tem gasolina e diesel

Notícias no Caos em Maio de 2018

Desabastecimento

- Dia 24, Greve de caminhoneiros gera desabastecimento pelo Brasil
- 28 às 12:35, Abastecida por trem, Bauru tem gasolina e diesel
- 28 às 21:02, Mesmo abastecida por trens, Bauru tem falta de combustível por alta procura

Notícias no Caos em Maio de 2018

Desabastecimento

- Dia 24, Greve de caminhoneiros gera desabastecimento pelo Brasil
- 28 às 12:35, Abastecida por trem, Bauru tem gasolina e diesel
- 28 às 21:02, Mesmo abastecida por trens, Bauru tem falta de combustível por alta procura
- 29, 15:38, Trem com combustível descarrila e polícia investiga sabotagem em Bauru

Notícias no Caos em Maio de 2018

Desabastecimento

- Dia 24, Greve de caminhoneiros gera desabastecimento pelo Brasil
- 28 às 12:35, Abastecida por trem, Bauru tem gasolina e diesel
- 28 às 21:02, Mesmo abastecida por trens, Bauru tem falta de combustível por alta procura
- 29, 15:38, Trem com combustível descarrila e polícia investiga sabotagem em Bauru
- 30, Fornecimento de gás natural não foi afetado pela greve dos caminhoneiros, em SC

Notícias no Caos em Maio de 2018

Desabastecimento

- Dia 24, Greve de caminhoneiros gera desabastecimento pelo Brasil
- 28 às 12:35, Abastecida por trem, Bauru tem gasolina e diesel
- 28 às 21:02, Mesmo abastecida por trens, Bauru tem falta de combustível por alta procura
- 29, 15:38, Trem com combustível descarrila e polícia investiga sabotagem em Bauru
- 30, Fornecimento de gás natural não foi afetado pela greve dos caminhoneiros, em SC
- Jun. 1, Preço alto de combustíveis e greve turbinam conversão para gás veicular (+50% de Kit Gás)

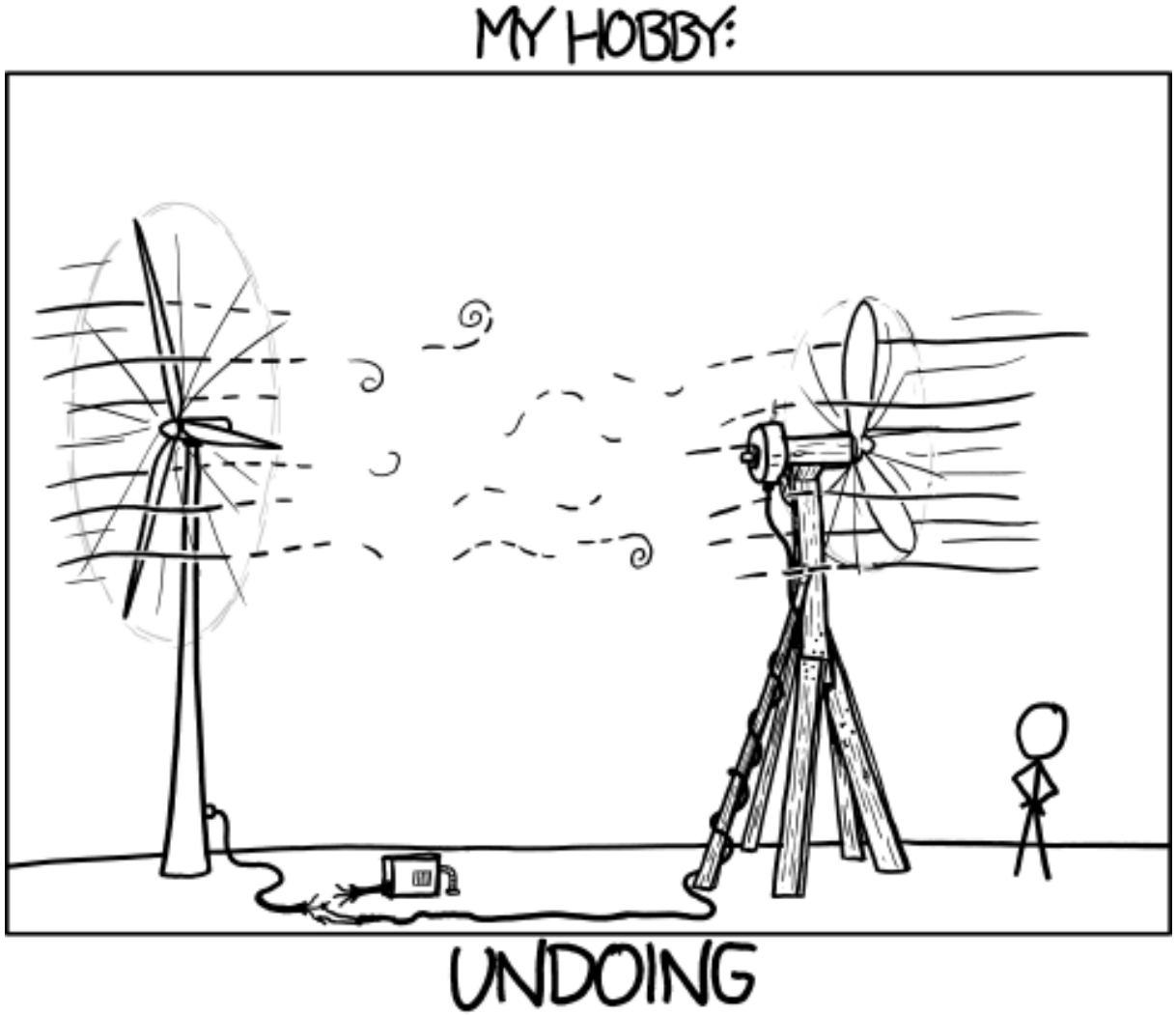
Notícias no Caos em Maio de 2018

Desabastecimento

- Dia 24, Greve de caminhoneiros gera desabastecimento pelo Brasil
- 28 às 12:35, Abastecida por trem, Bauru tem gasolina e diesel
- 28 às 21:02, Mesmo abastecida por trens, Bauru tem falta de combustível por alta procura
- 29, 15:38, Trem com combustível descarrila e polícia investiga sabotagem em Bauru
- 30, Fornecimento de gás natural não foi afetado pela greve dos caminhoneiros, em SC
- Jun. 1, Preço alto de combustíveis e greve turbinam conversão para gás veicular (+50% de Kit Gás)
- Jun. 5, Consumo de GNV cresce em maio com greve dos caminhoneiros, diz Abegás

Tópicos

Desfazendo



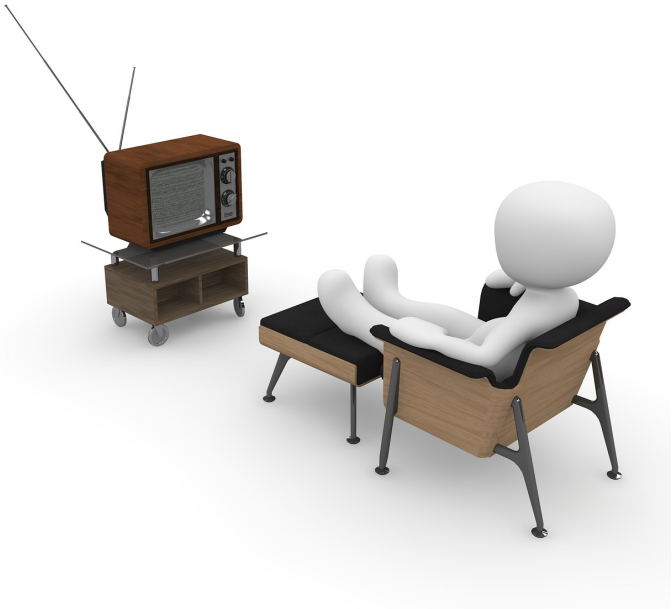
[xkcd]

Tesla X

CRT

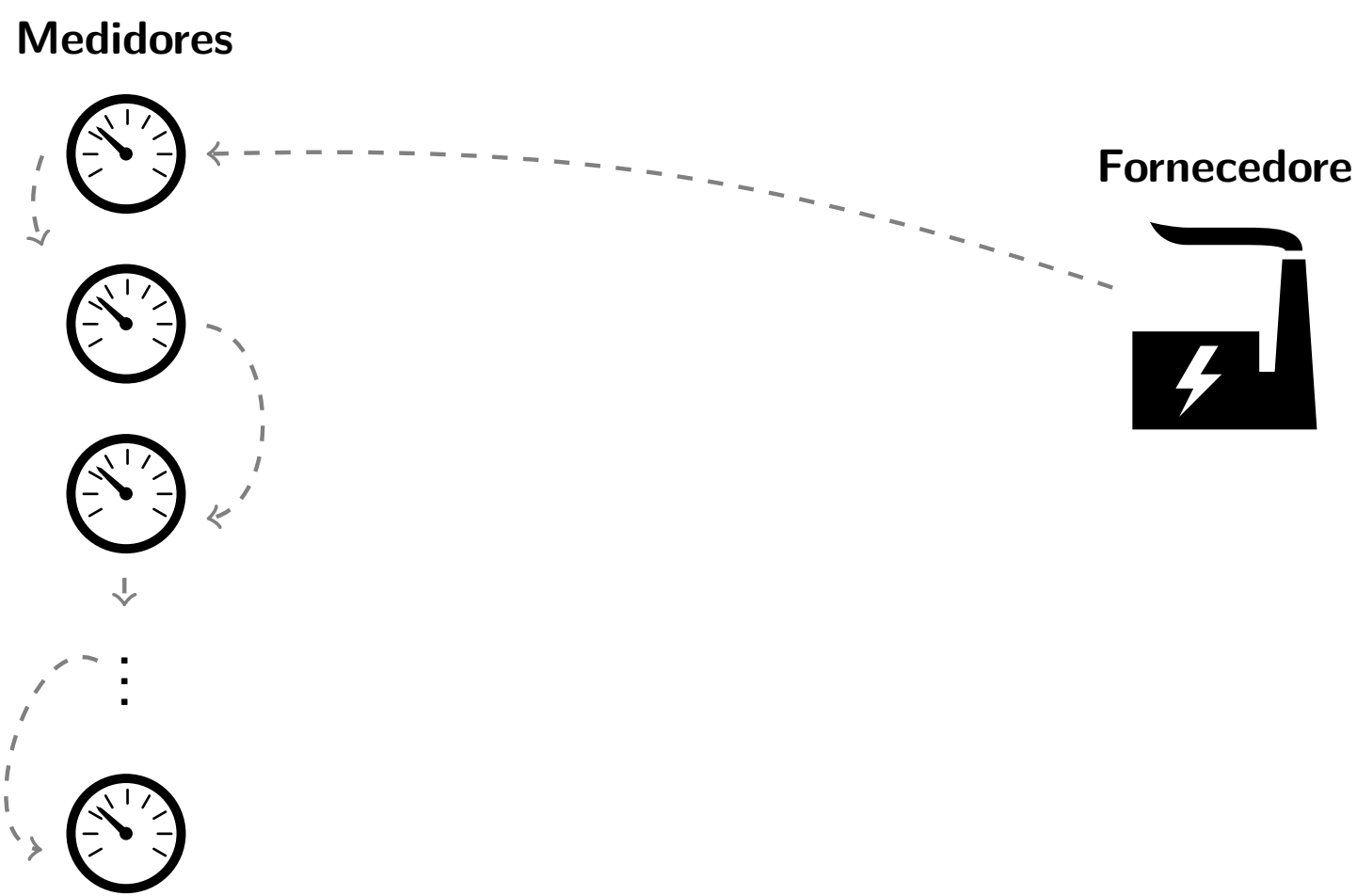

eMeeting
Product Roadmap

CRT vs LCD

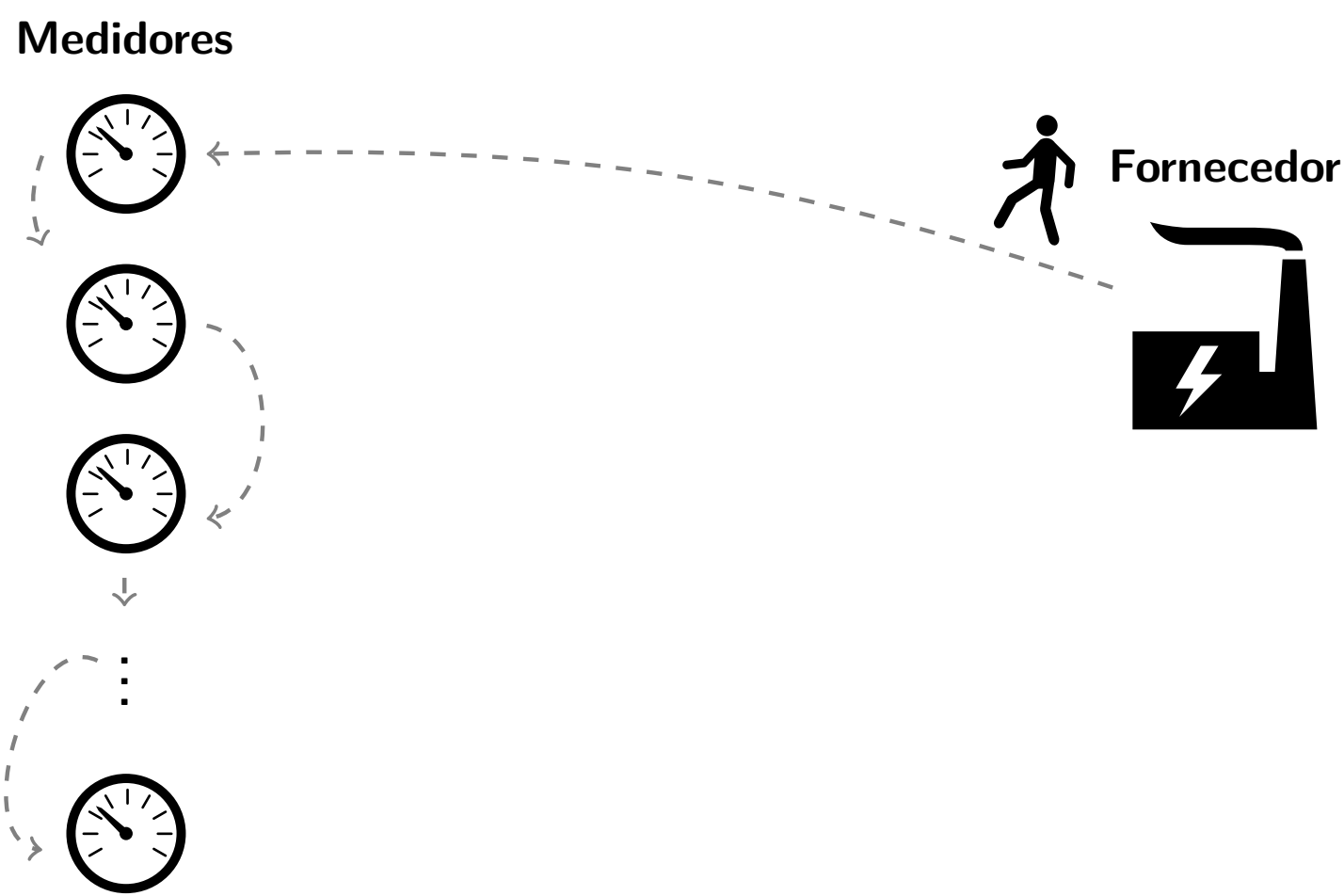


Tópicos

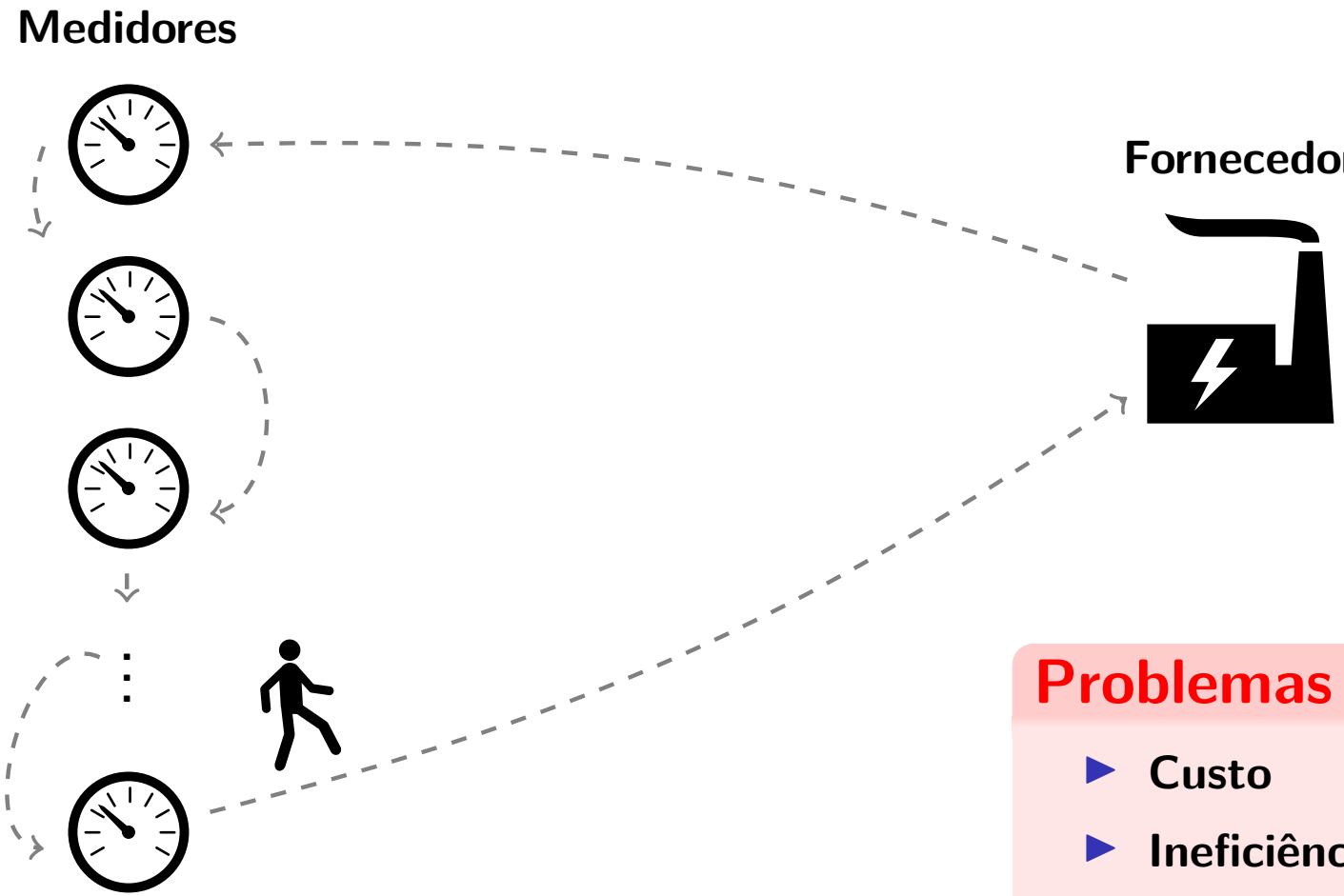
Non-smart Grid



Non-smart Grid



Non-smart Grid



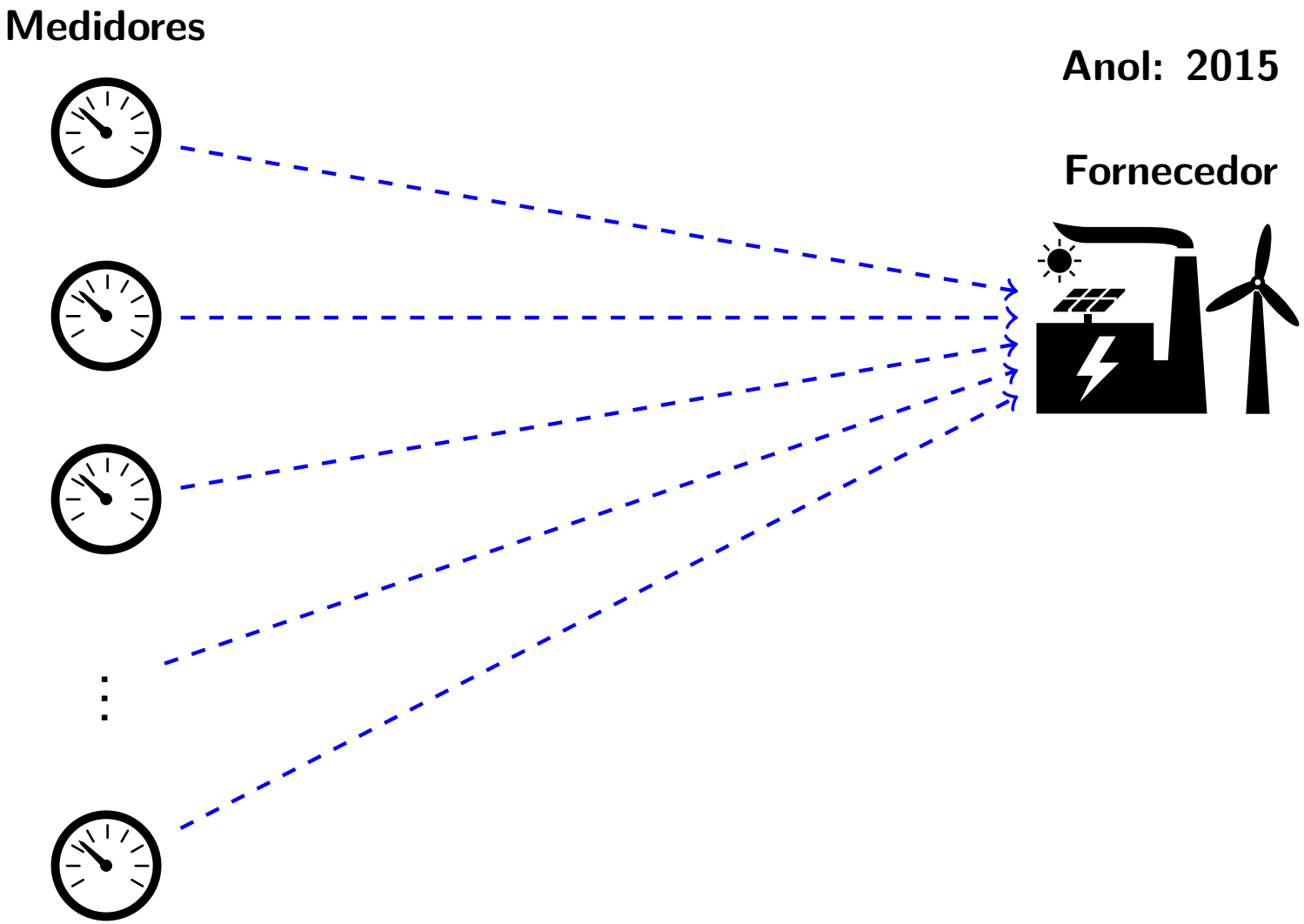
Problemas

- Custo
- Ineficiência
- Fraude

Tópicos

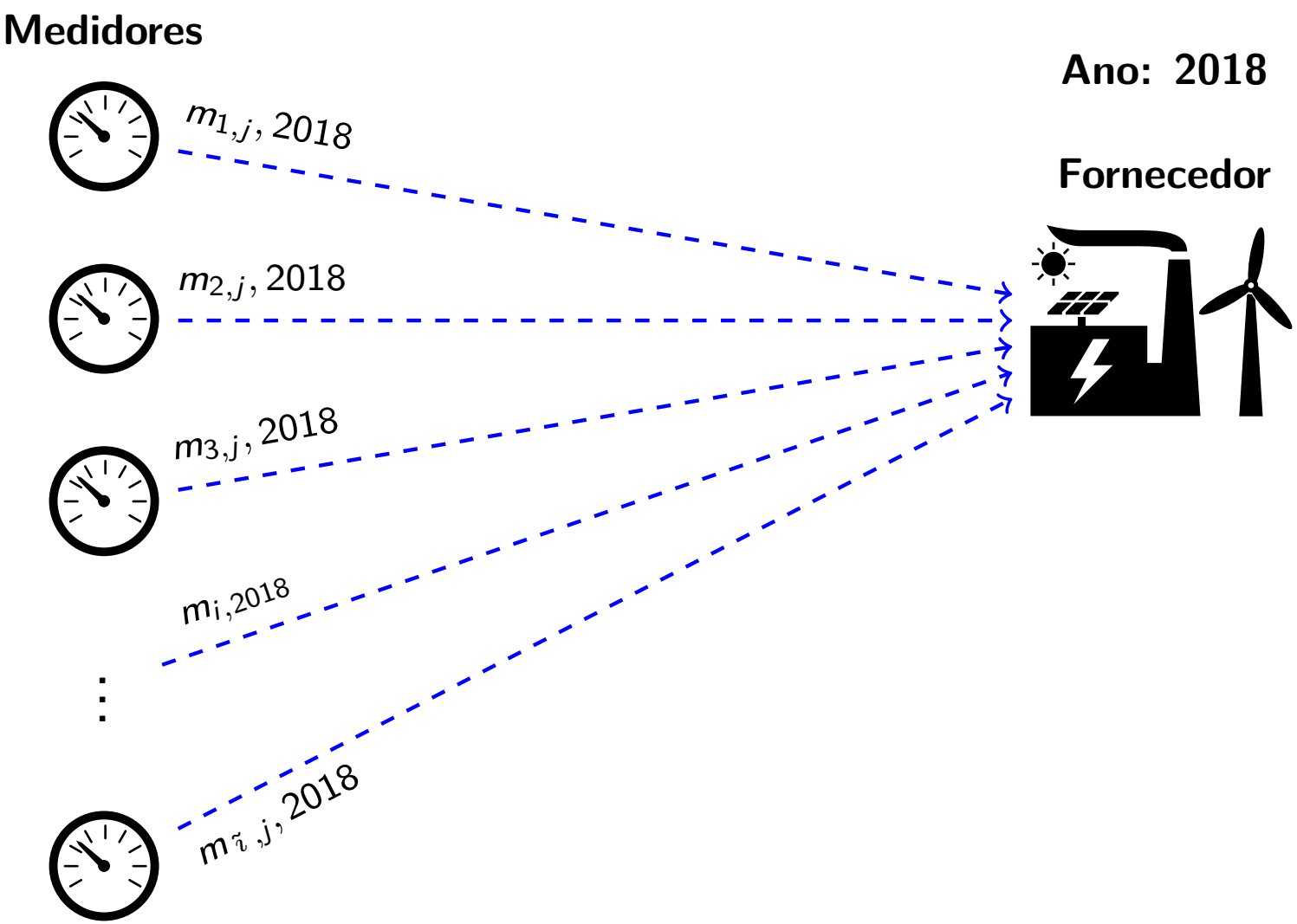
Getting Smart

Coletando por Ano



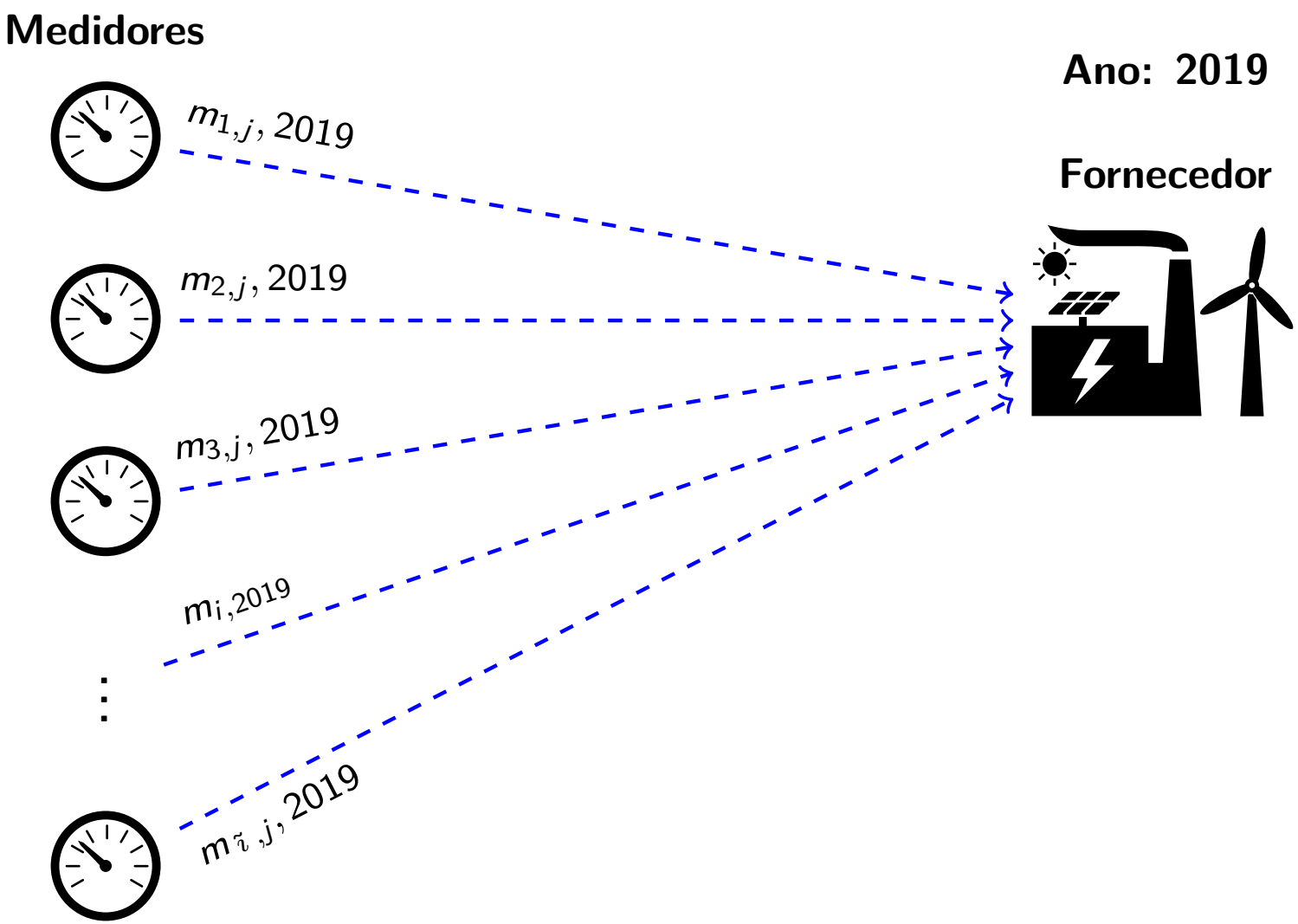
Getting Smart

Coletando por Ano



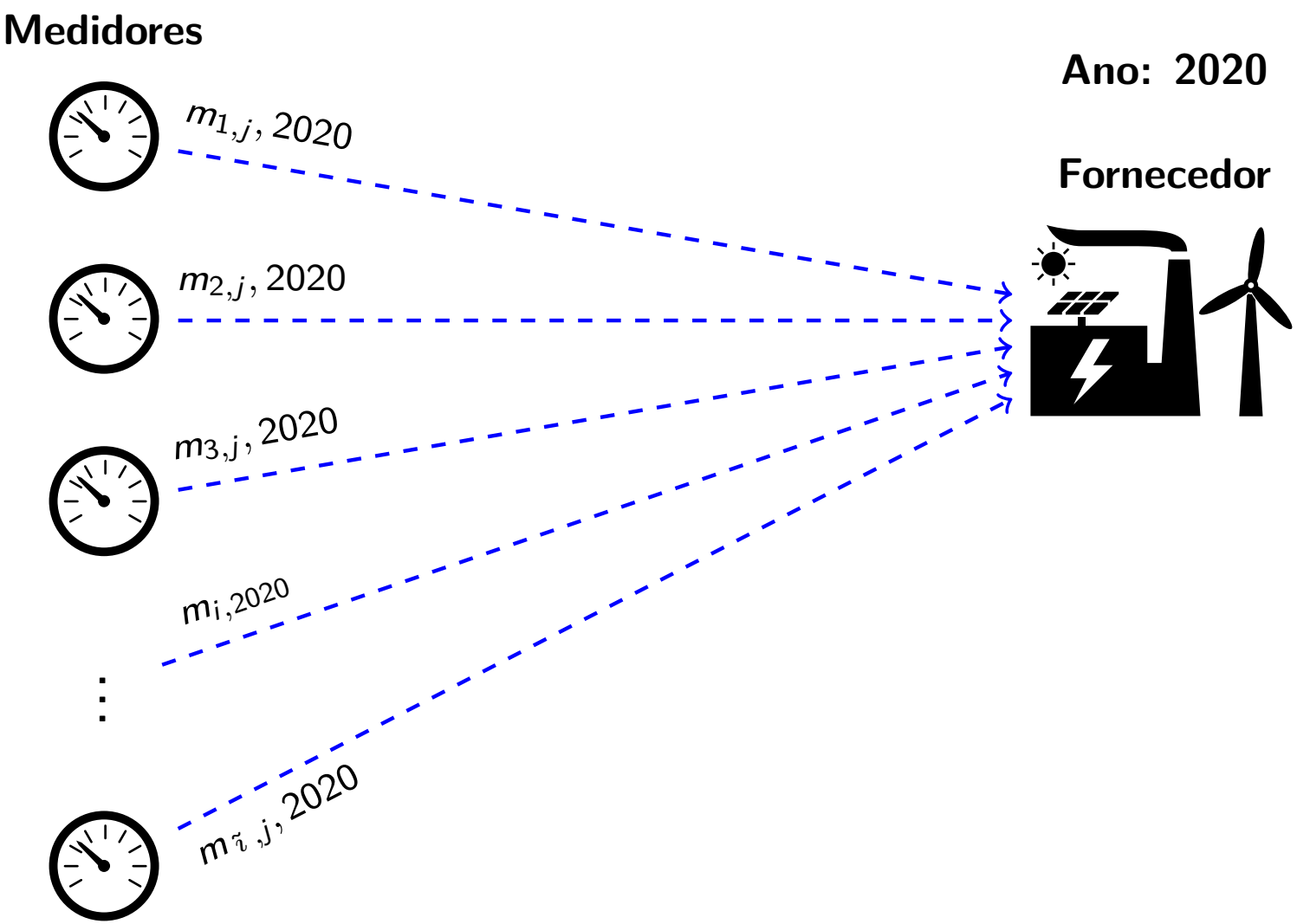
Getting Smart

Coletando por Ano



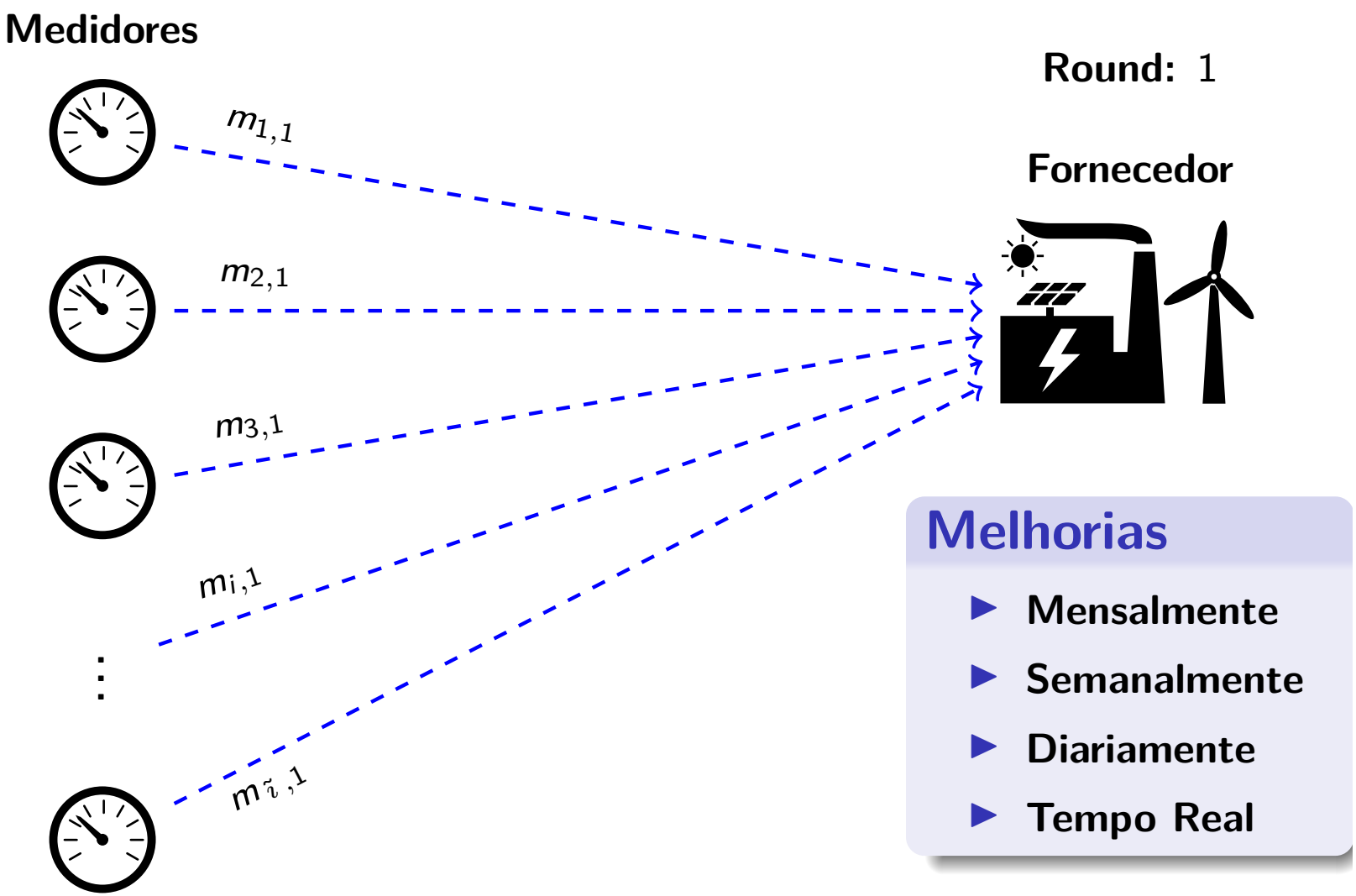
Getting Smart

Coletando por Ano



Getting Smart

Coletando por Rodada

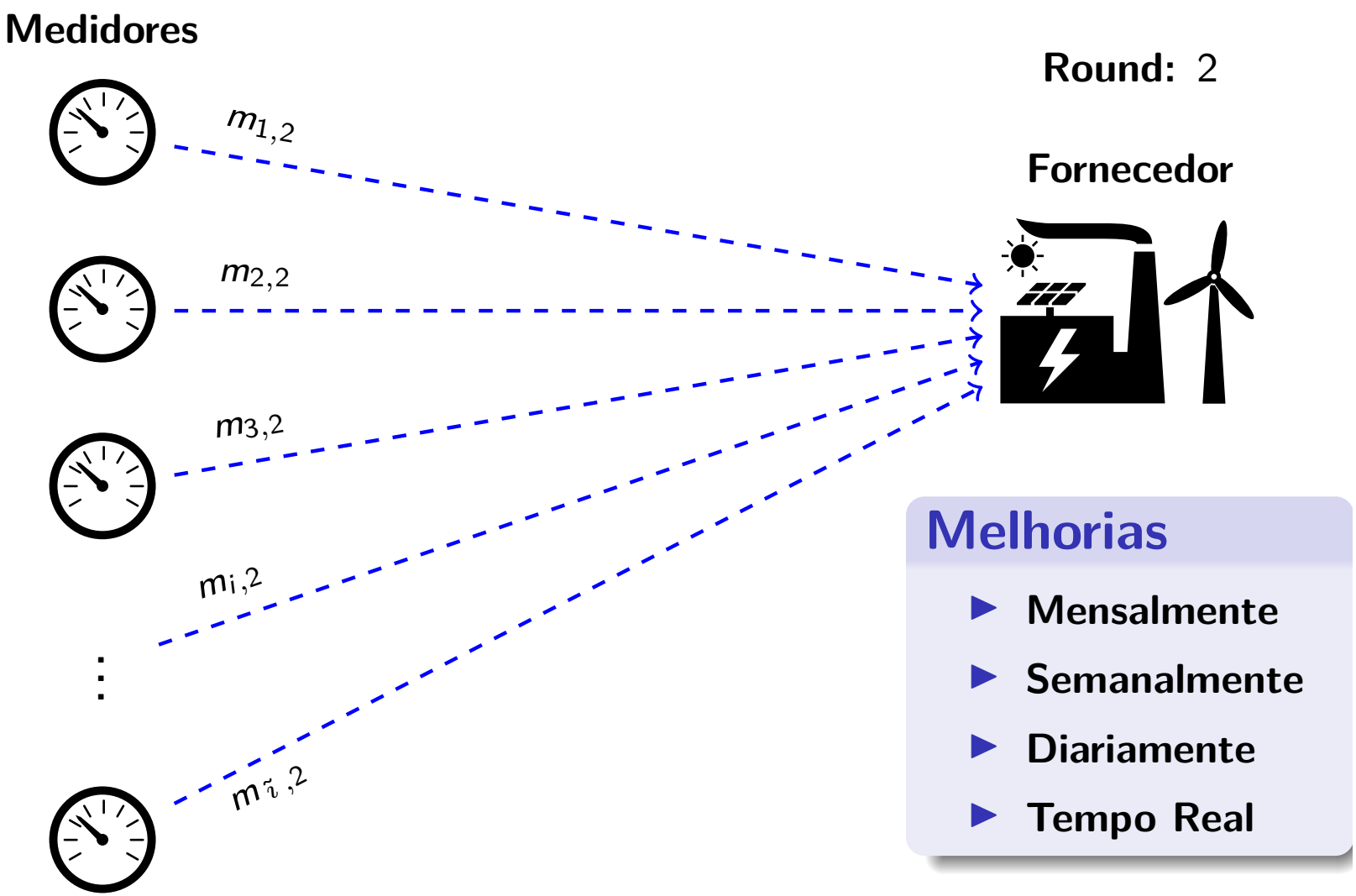


Melhorias

- Mensalmente
- Semanalmente
- Diariamente
- Tempo Real

Getting Smart

Coletando por Rodada

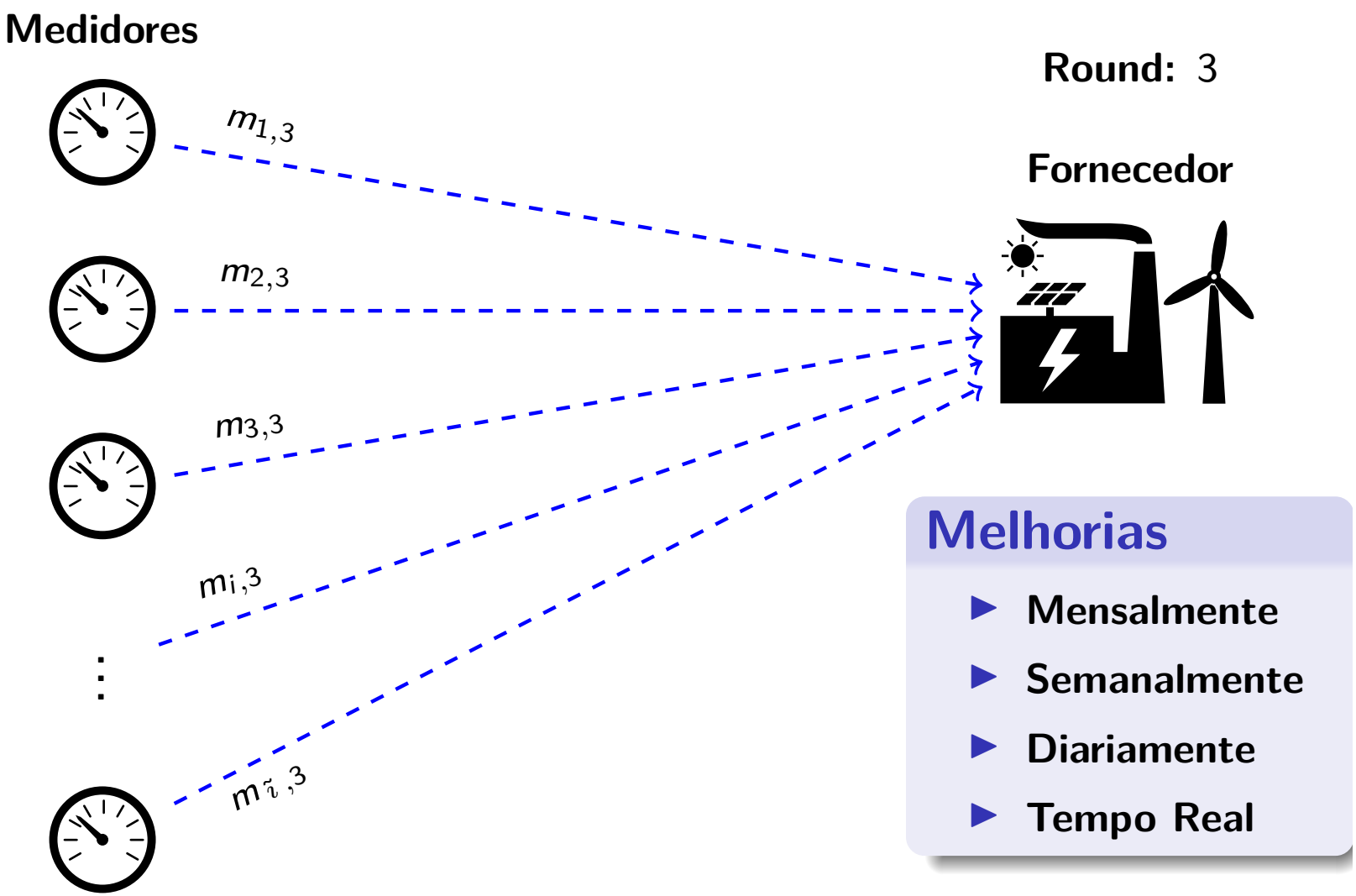


Melhorias

- Mensalmente
- Semanalmente
- Diariamente
- Tempo Real

Getting Smart

Coletando por Rodada

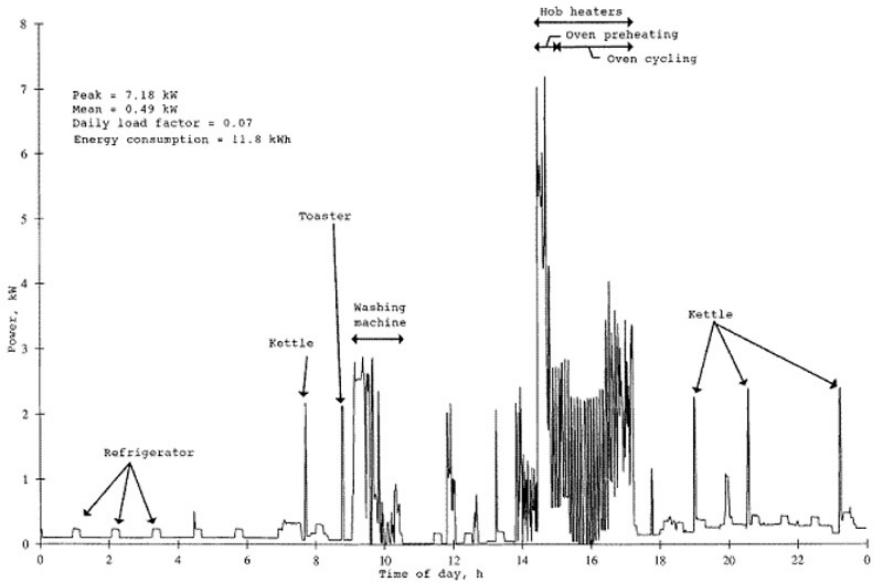


Melhorias

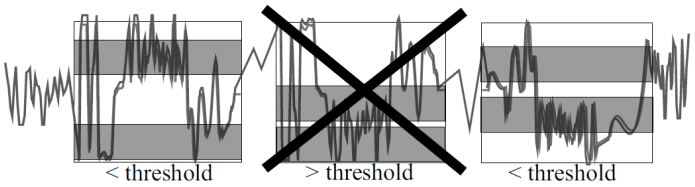
- Mensalmente
- Semanalmente
- Diariamente
- Tempo Real

Tópicos

O Problema da Privacidade



[NIST]



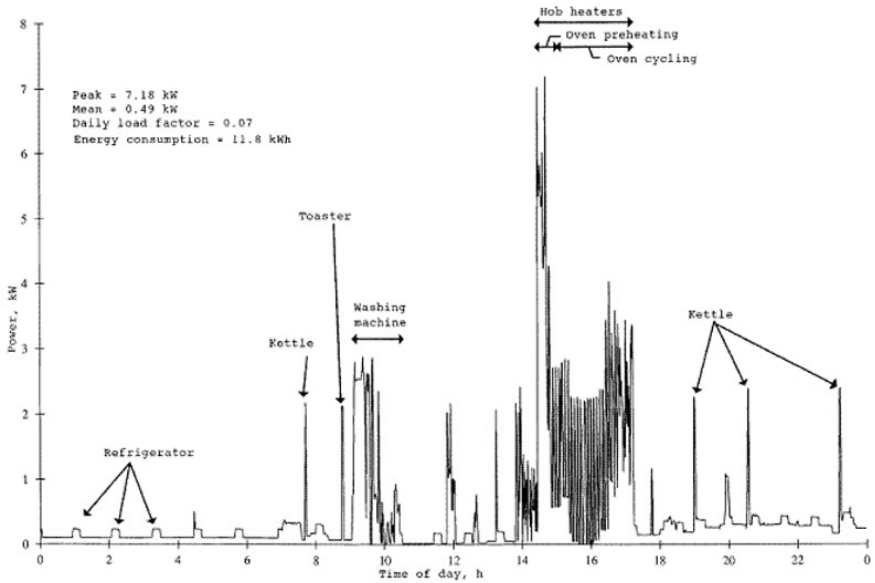
output matches to logfile

movie tng1
chunk 1 at 2103h

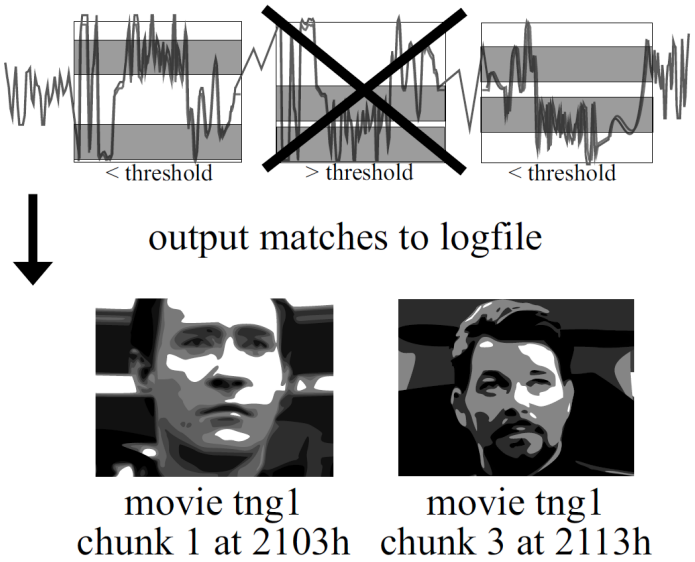
movie tng1
chunk 3 at 2113h

[GJL12]

O Problema da Privacidade



[NIST]



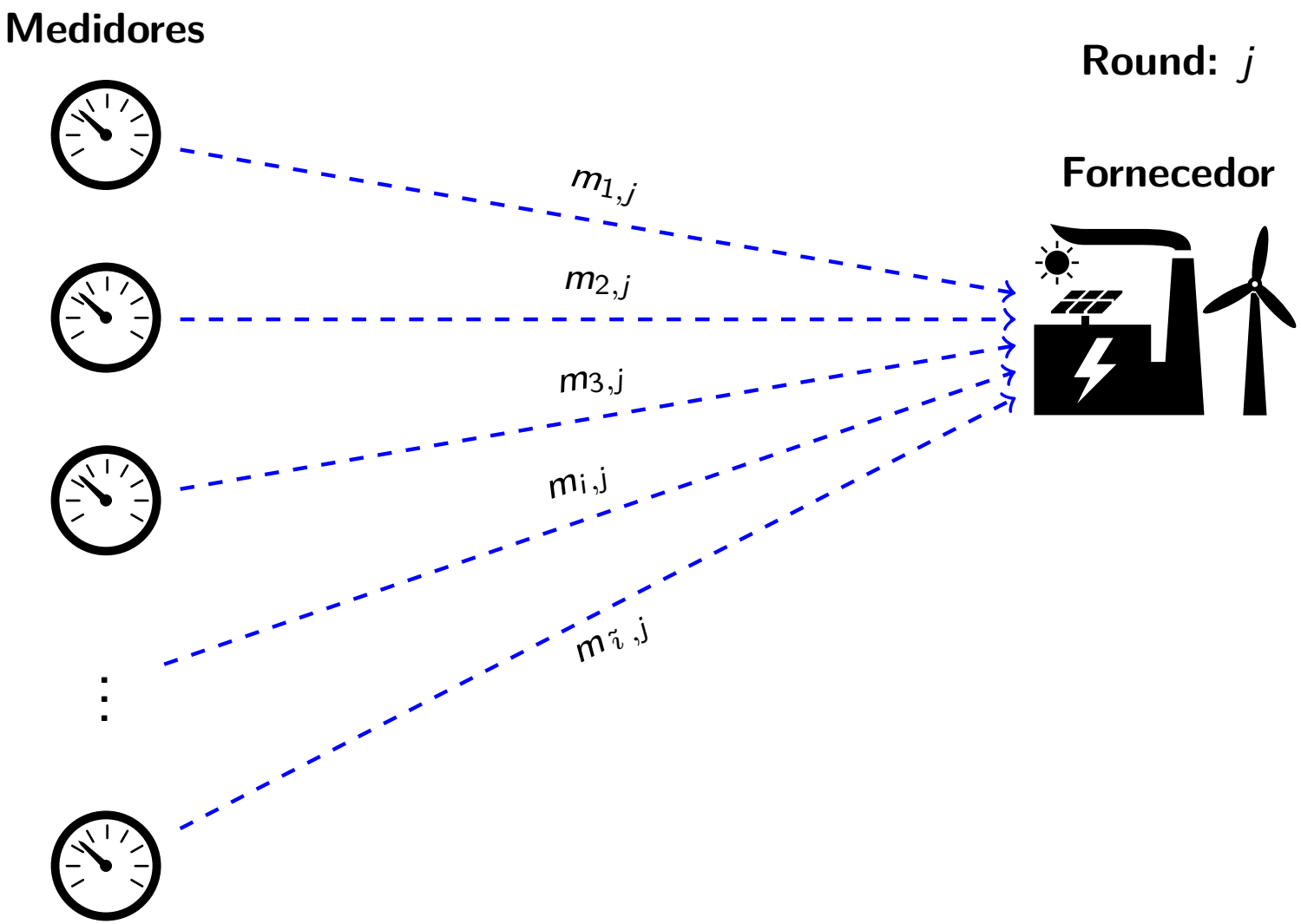
[GJL12]

EU - Official Journal L No.315

80% of households equipped with smart meters by 2020 in EU

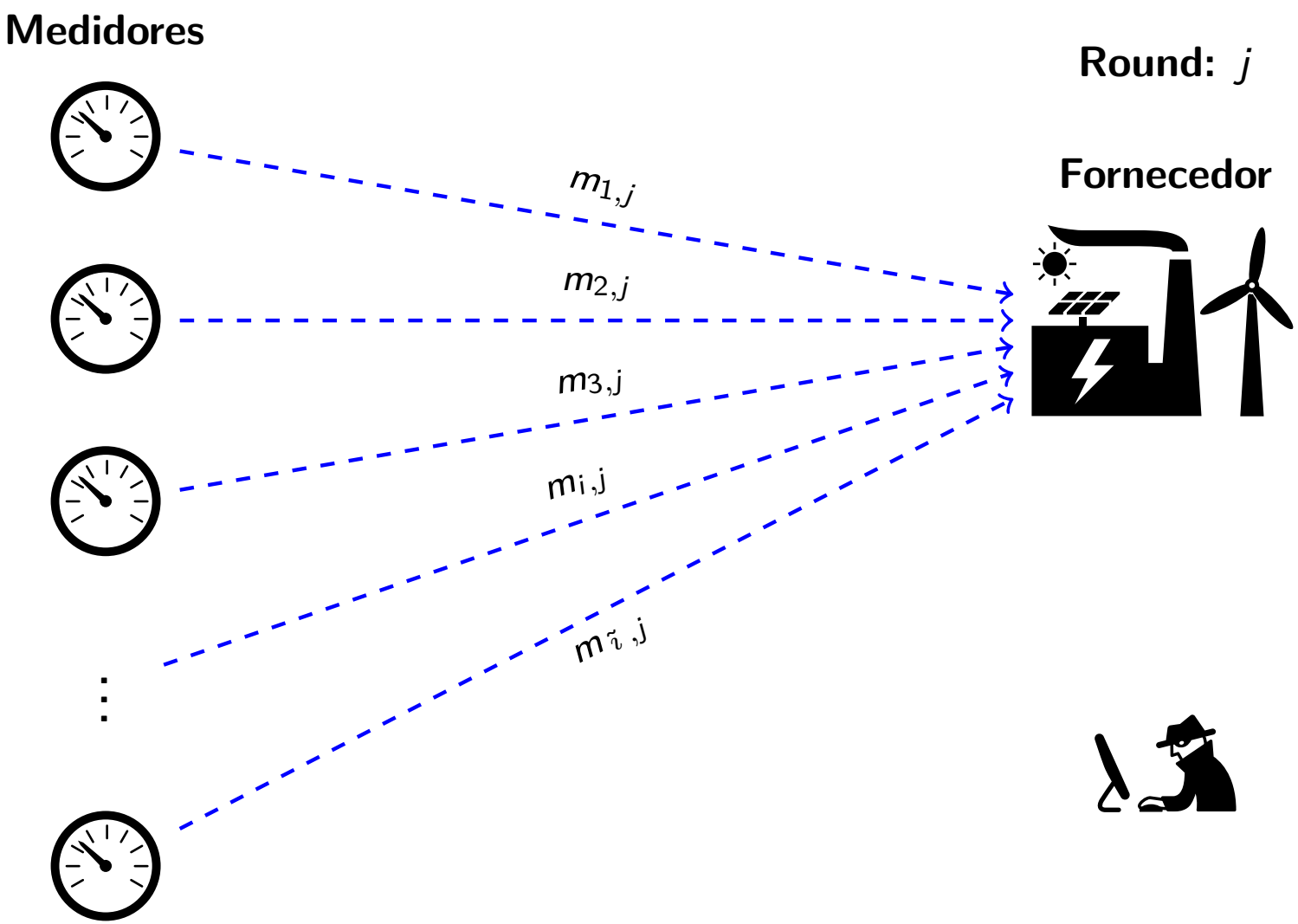
Necessidade de Criptografia

Interceptando Todas as Mensagens



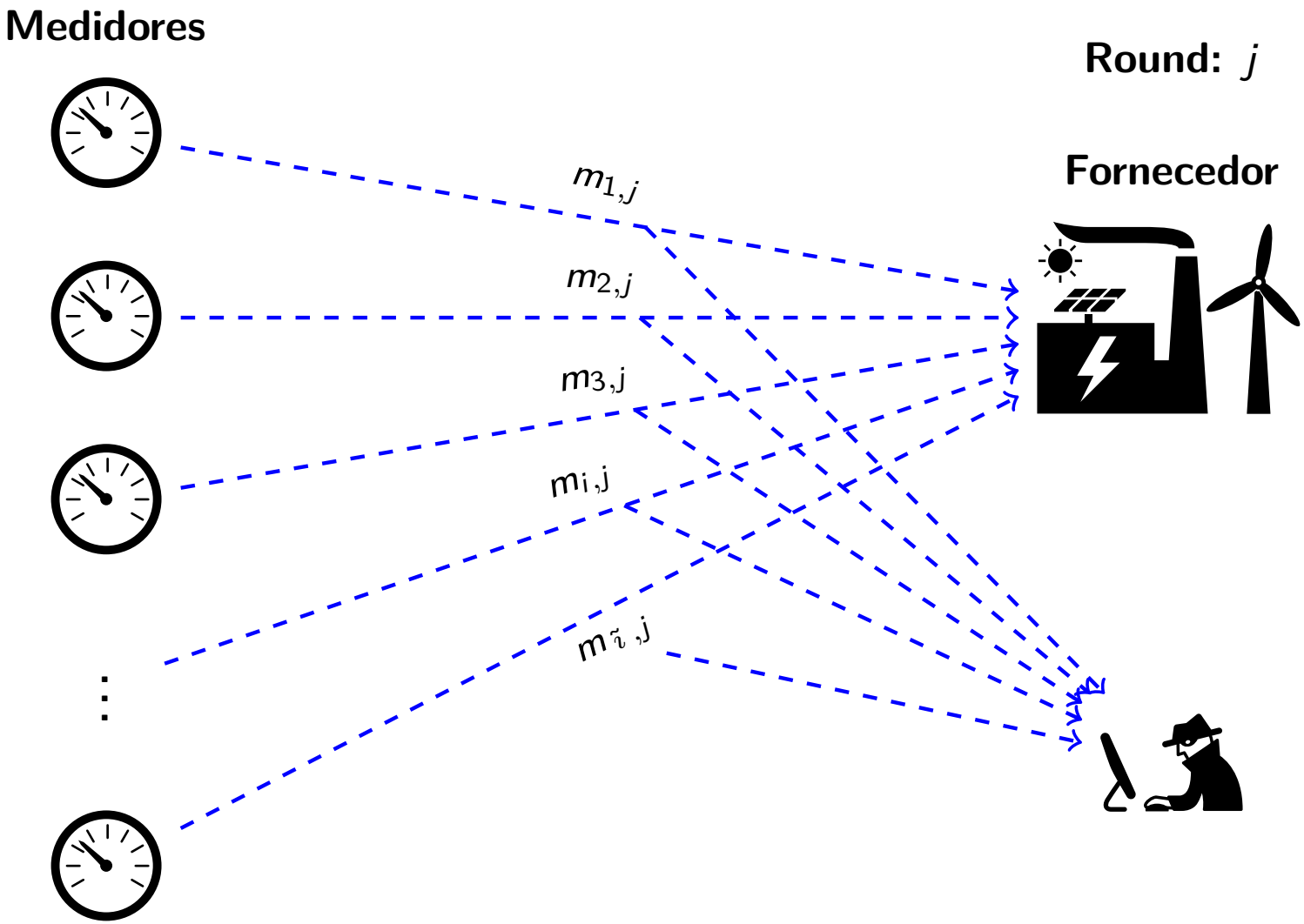
Necessidade de Criptografia

Interceptando Todas as Mensagens

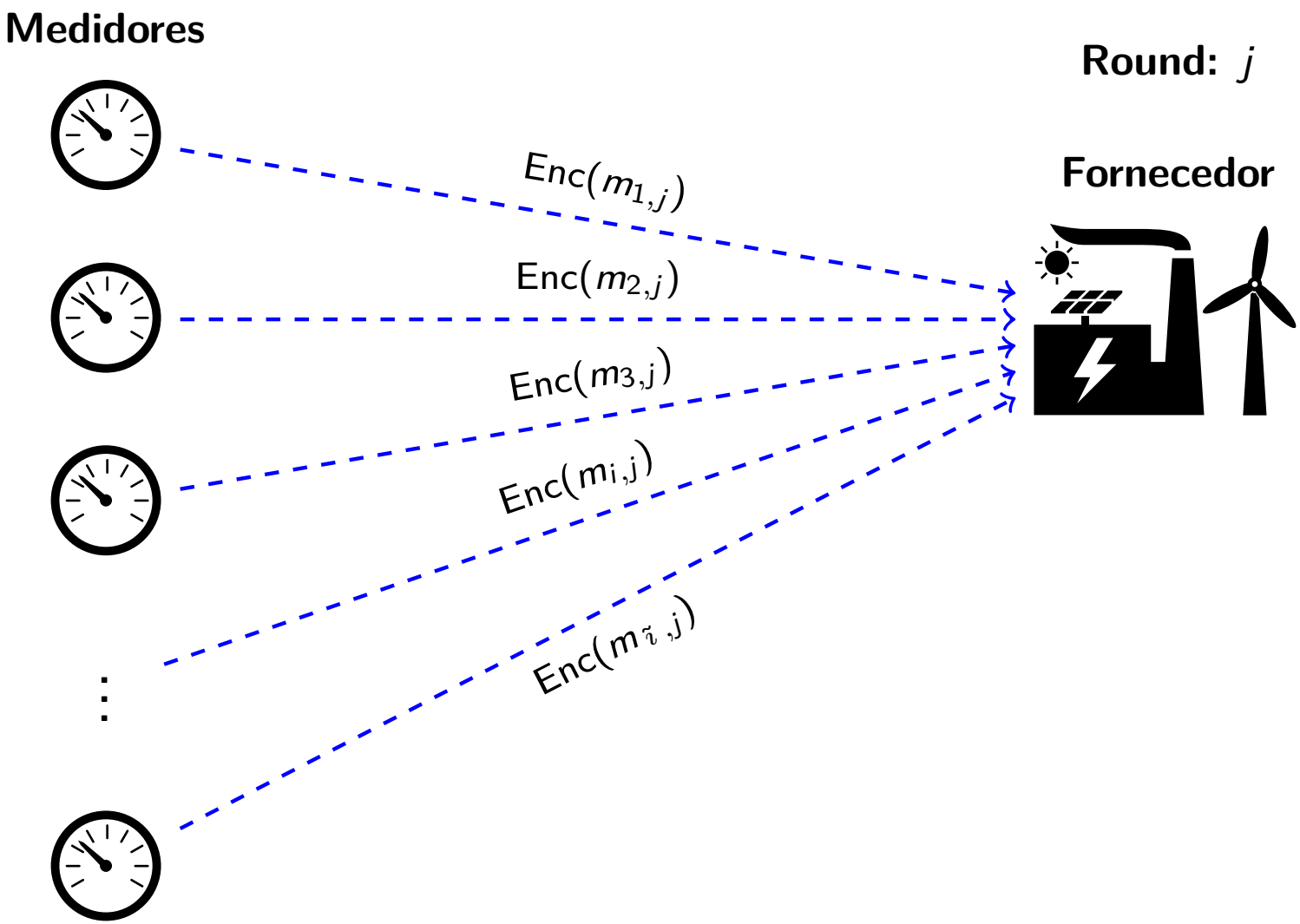


Necessidade de Criptografia

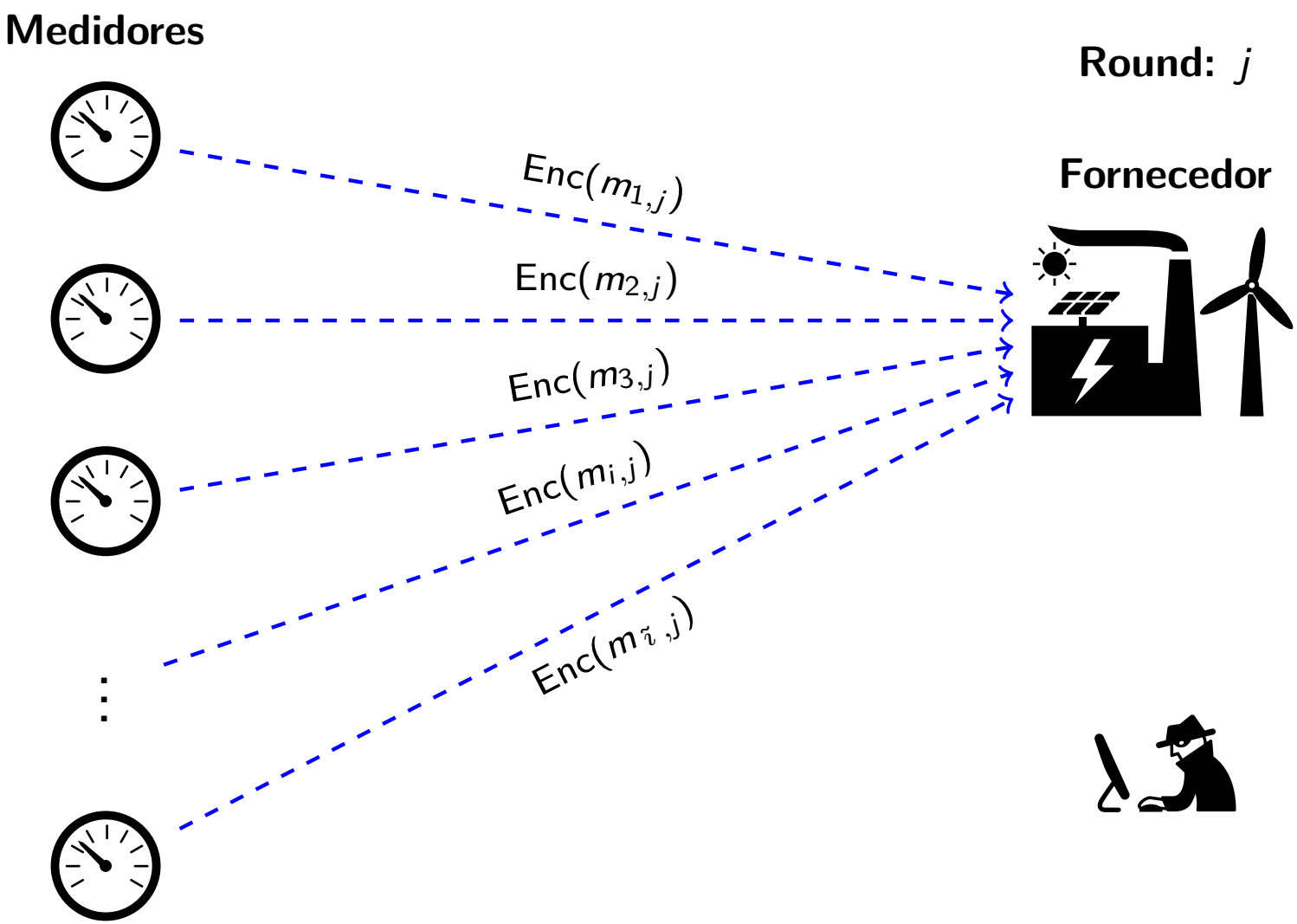
Interceptando Todas as Mensagens



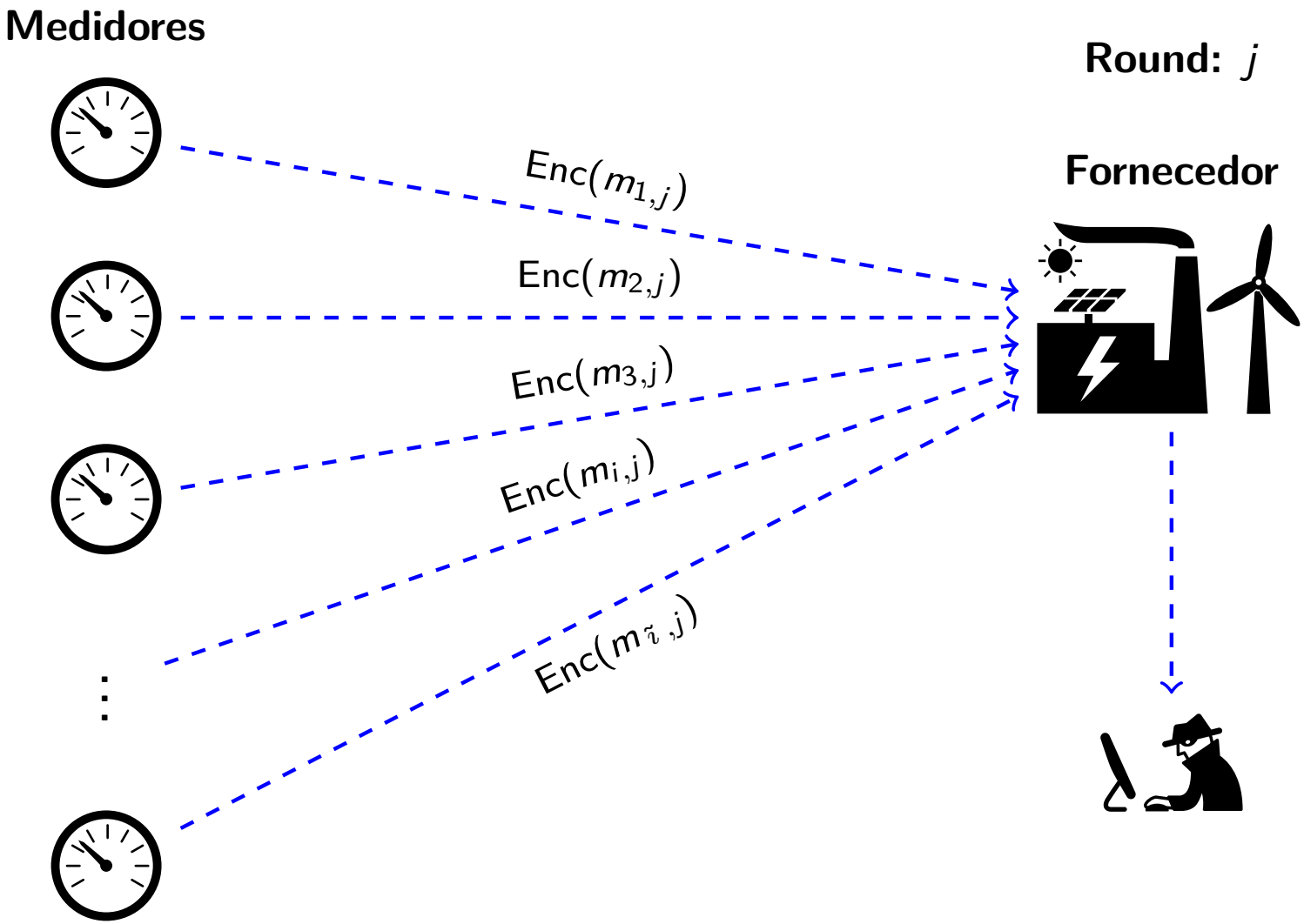
Necessidade de Agregação



Necessidade de Agregação



Necessidade de Agregação



O que o fornecedor precisa?

Consumo Consolidado versus Faturamento

Laboratório Nacional de Computação Científica

Rodada	1	2	$\cdots$	$\tilde{j}$	**Fatura**
Meter 1	$m_{1,1}$	$m_{1,2}$	$\cdots$	$m_{1,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{1,j}$
Meter 2	$m_{2,1}$	$m_{2,2}$	$\cdots$	$m_{2,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{2,j}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
Meter $\tilde{i}$	$m_{\tilde{i},1}$	$m_{\tilde{i},2}$	$\cdots$	$m_{\tilde{i},\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{\tilde{i},j}$
Consolidado	$\sum_{i=1}^{\tilde{i}} m_{i,1}$	$\sum_{i=1}^{\tilde{i}} m_{i,2}$	$\cdots$	$\sum_{i=1}^{\tilde{i}} m_{i,\tilde{j}}$	$=$

O que o fornecedor precisa?

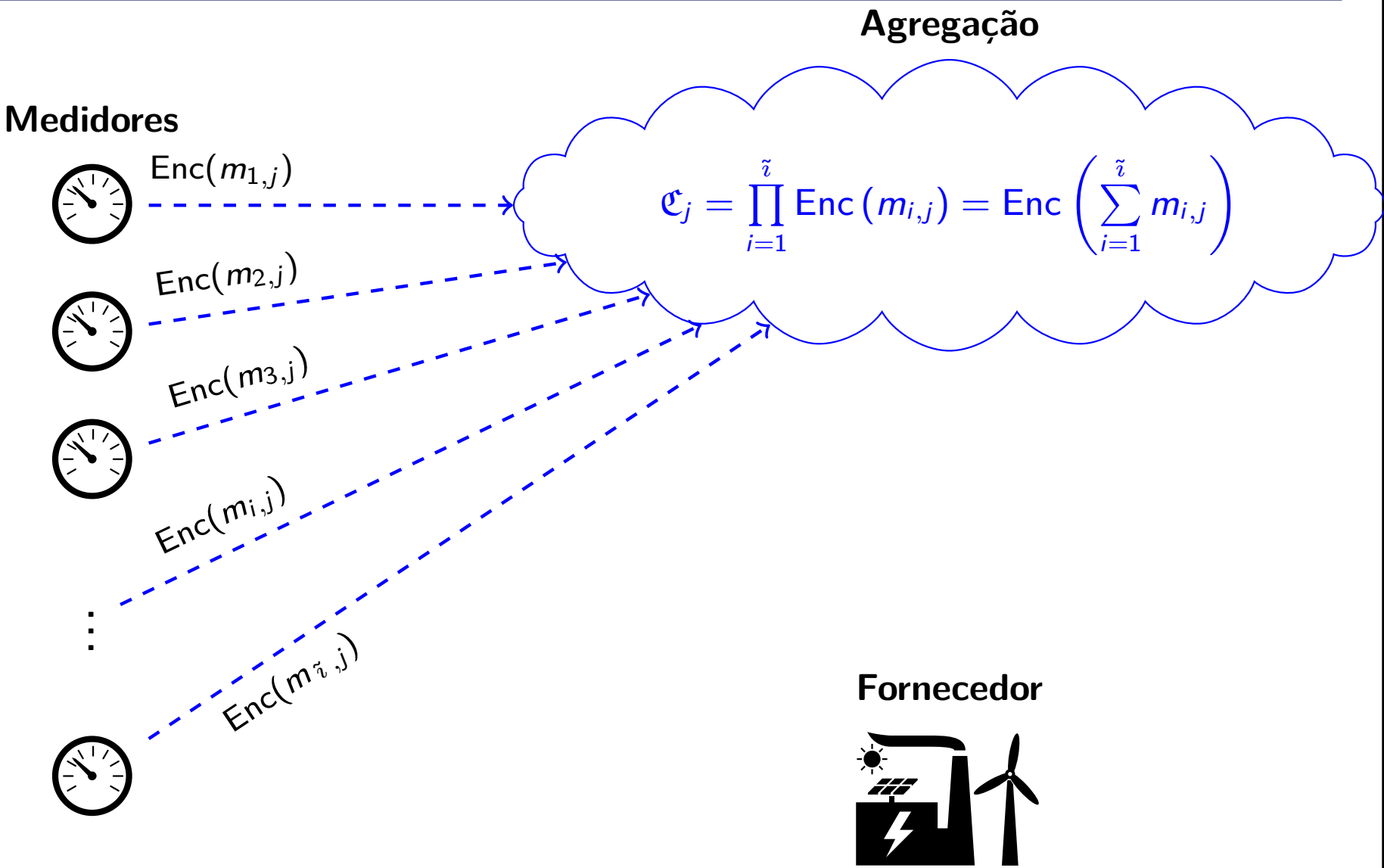
Consumo Consolidado versus Faturamento

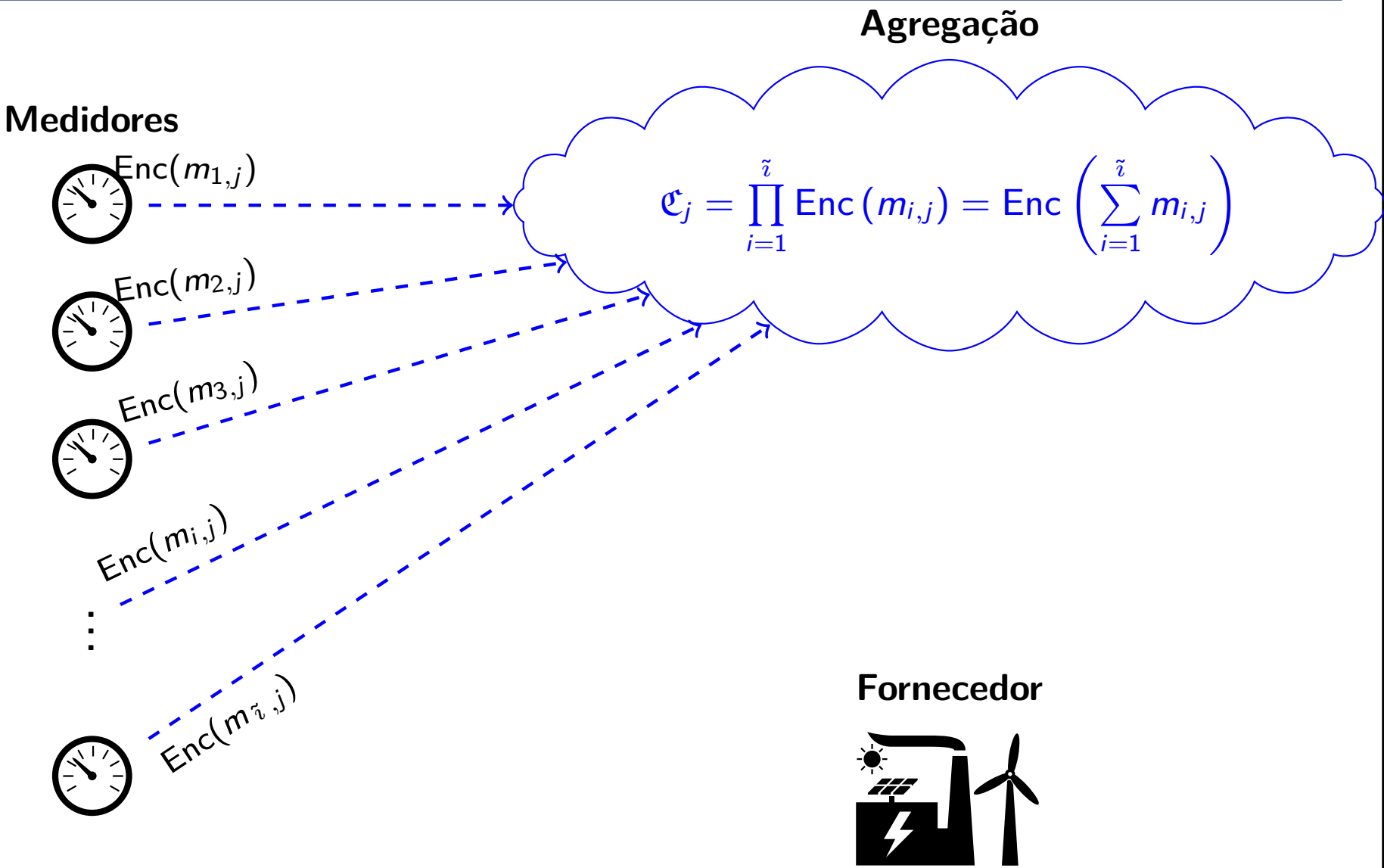
Laboratório Nacional de Computação Científica

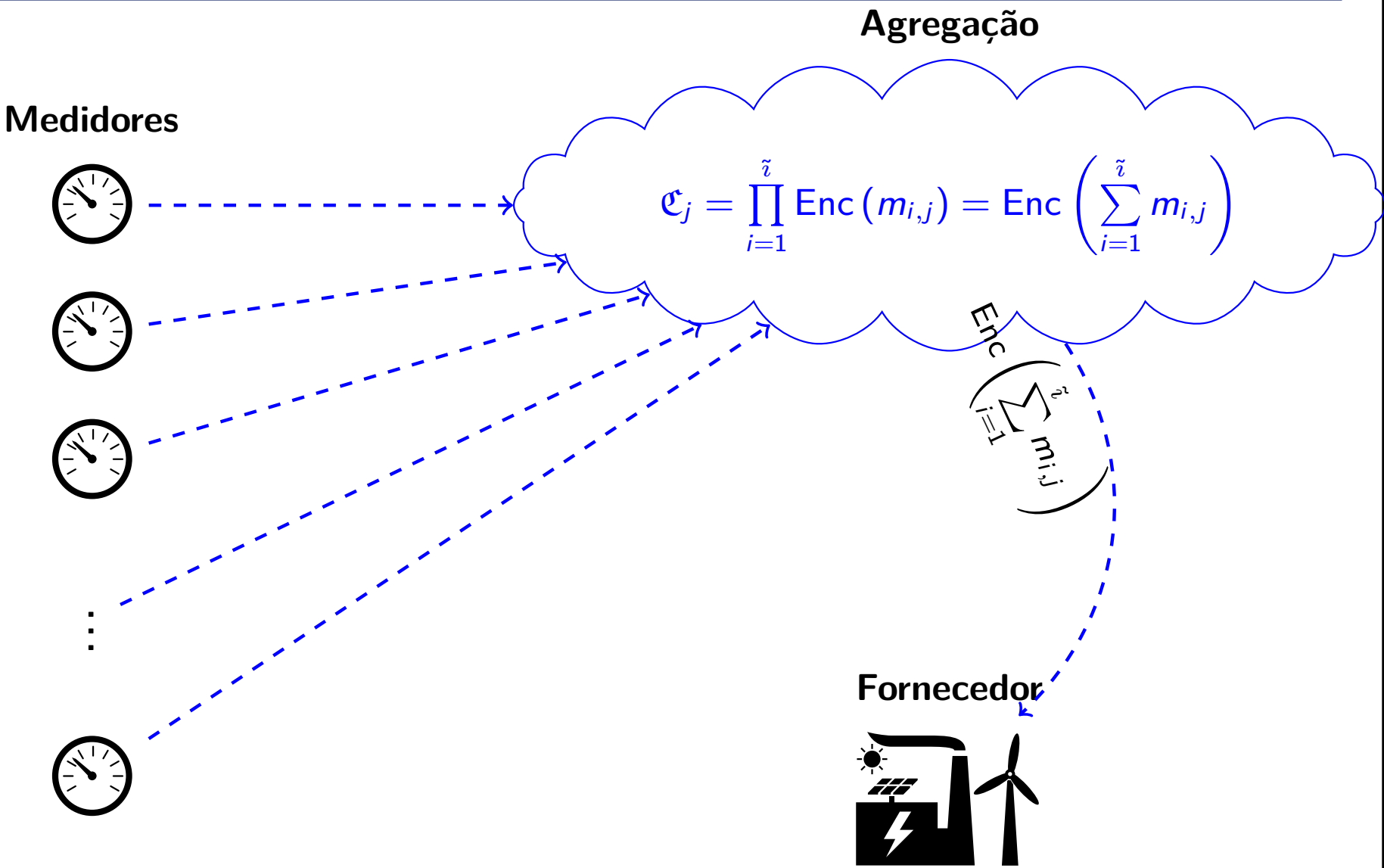
Rodada	1	2	$\cdots$	$\tilde{j}$	**Fatura**
Meter 1	$m_{1,1}$	$m_{1,2}$	$\cdots$	$m_{1,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{1,j}$
Meter 2	$m_{2,1}$	$m_{2,2}$	$\cdots$	$m_{2,\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{2,j}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
Meter $\tilde{i}$	$m_{\tilde{i},1}$	$m_{\tilde{i},2}$	$\cdots$	$m_{\tilde{i},\tilde{j}}$	$\sum_{j=1}^{\tilde{j}} m_{\tilde{i},j}$
Consolidado	$\sum_{i=1}^{\tilde{i}} m_{i,1}$	$\sum_{i=1}^{\tilde{i}} m_{i,2}$	$\cdots$	$\sum_{i=1}^{\tilde{i}} m_{i,\tilde{j}}$	$=$

✗ ✓

PPPs apenas funcionam com grandes agregações.

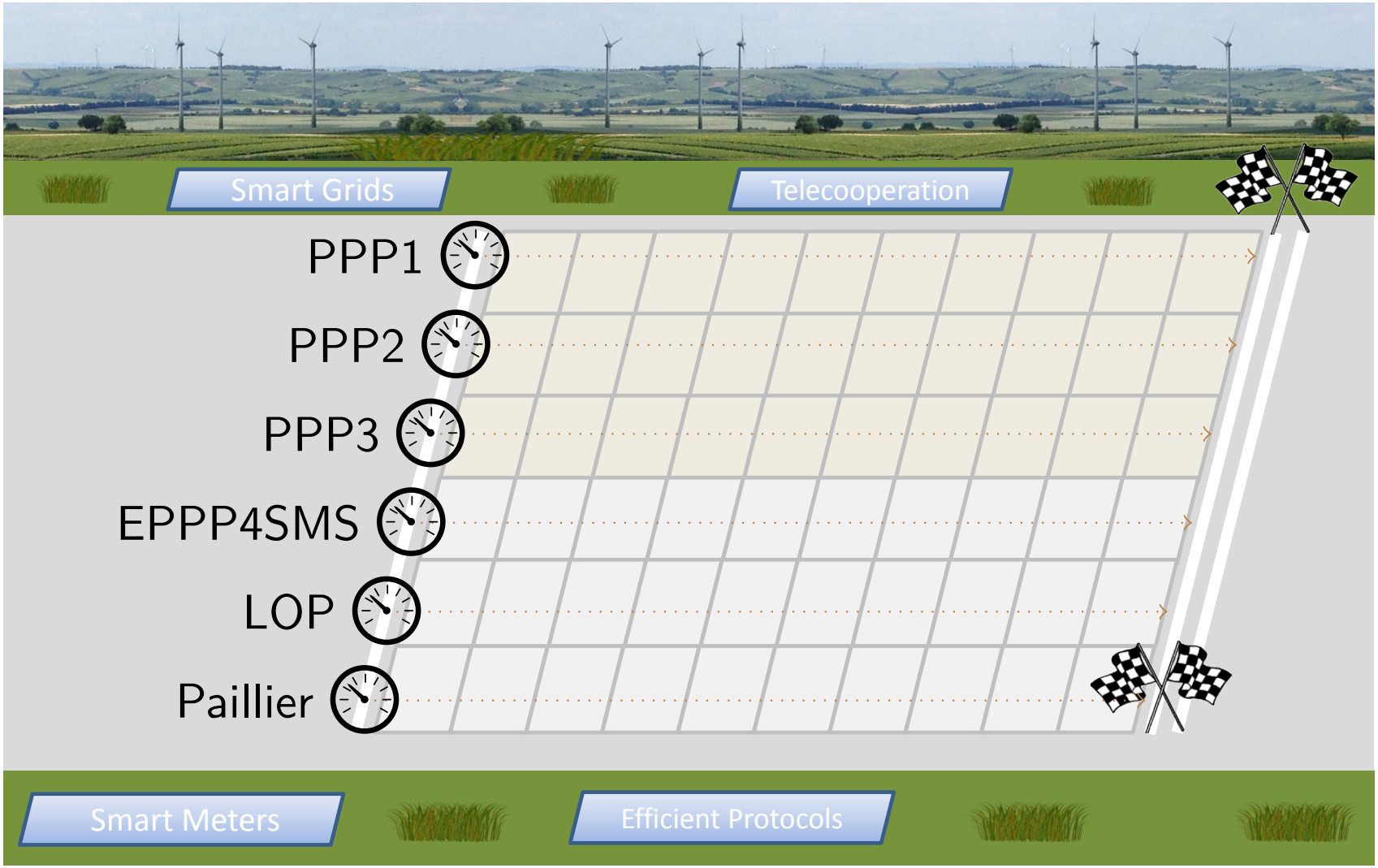

Agregação
Medidores
$\mathrm{Enc}(m_{1,j})$
$\mathrm{Enc}(m_{2,j})$
$\mathrm{Enc}(m_{3,j})$
$\mathrm{Enc}(m_{i,j})$
$\mathrm{Enc}(m_{\tilde{i},j})$
$\mathfrak{C}_j = \prod_{i=1}^{\tilde{i}} \mathrm{Enc}(m_{i,j}) = \mathrm{Enc}\left(\sum_{i=1}^{\tilde{i}} m_{i,j}\right)$
Fornecedor


Agregação
Medidores
Enc($m_{1,j}$)
Enc($m_{2,j}$)
Enc($m_{3,j}$)
Enc($m_{i,j}$)
Enc($m_{\tilde{i},j}$)
$\mathfrak{C}_j = \prod_{i=1}^{\tilde{i}} \mathrm{Enc}\,(m_{i,j}) = \mathrm{Enc}\left(\sum_{i=1}^{\tilde{i}} m_{i,j}\right)$
Fornecedor


Agregação
Medidores
$\mathfrak{C}_j = \prod_{i=1}^{\tilde{i}} \mathrm{Enc}(m_{i,j}) = \mathrm{Enc}\left(\sum_{i=1}^{\tilde{i}} m_{i,j}\right)$
Enc
$\sum_{i=1}^{\tilde{i}} m_{i,j}$
Fornecedor

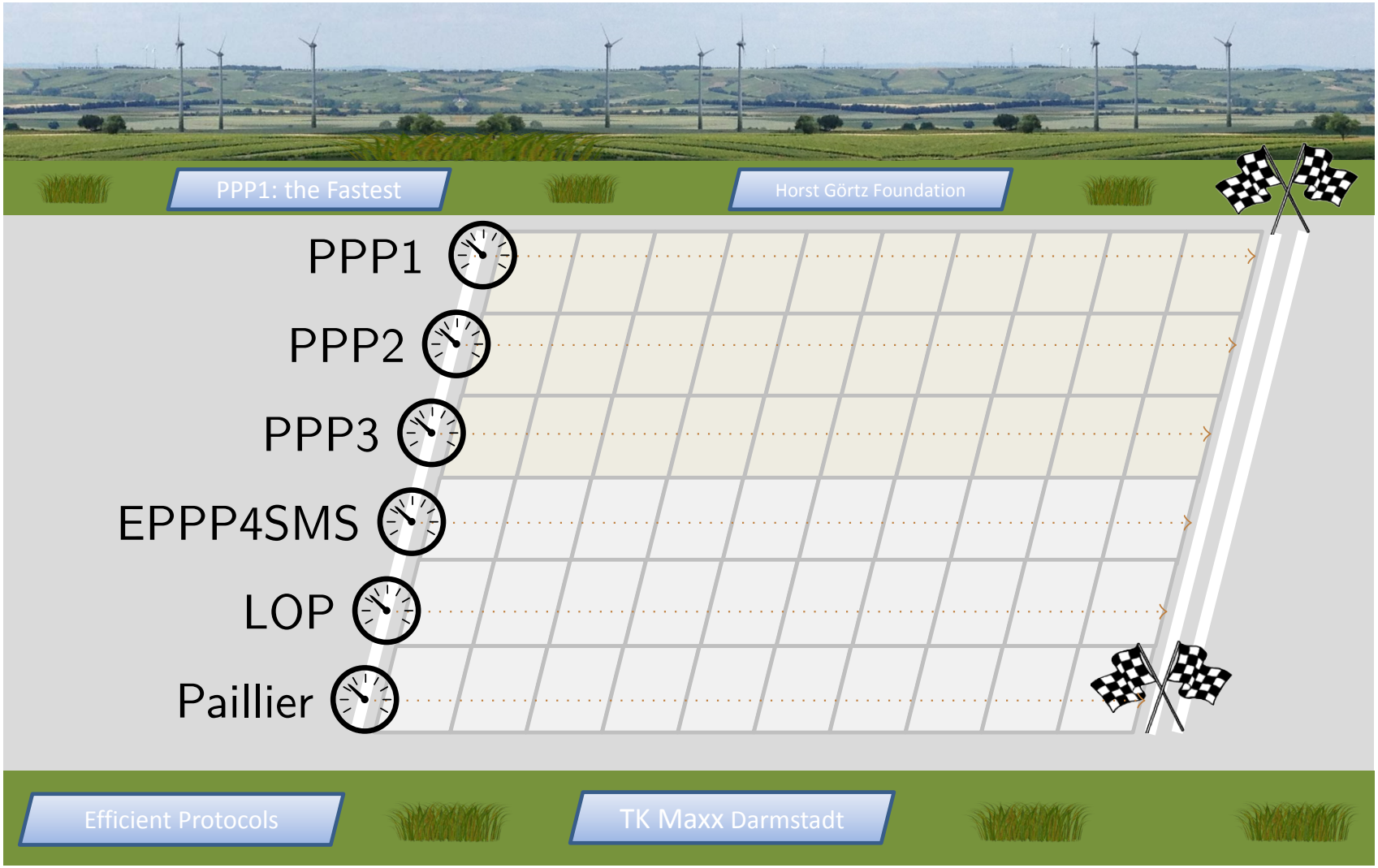
Performance

Corrida de Protocolos



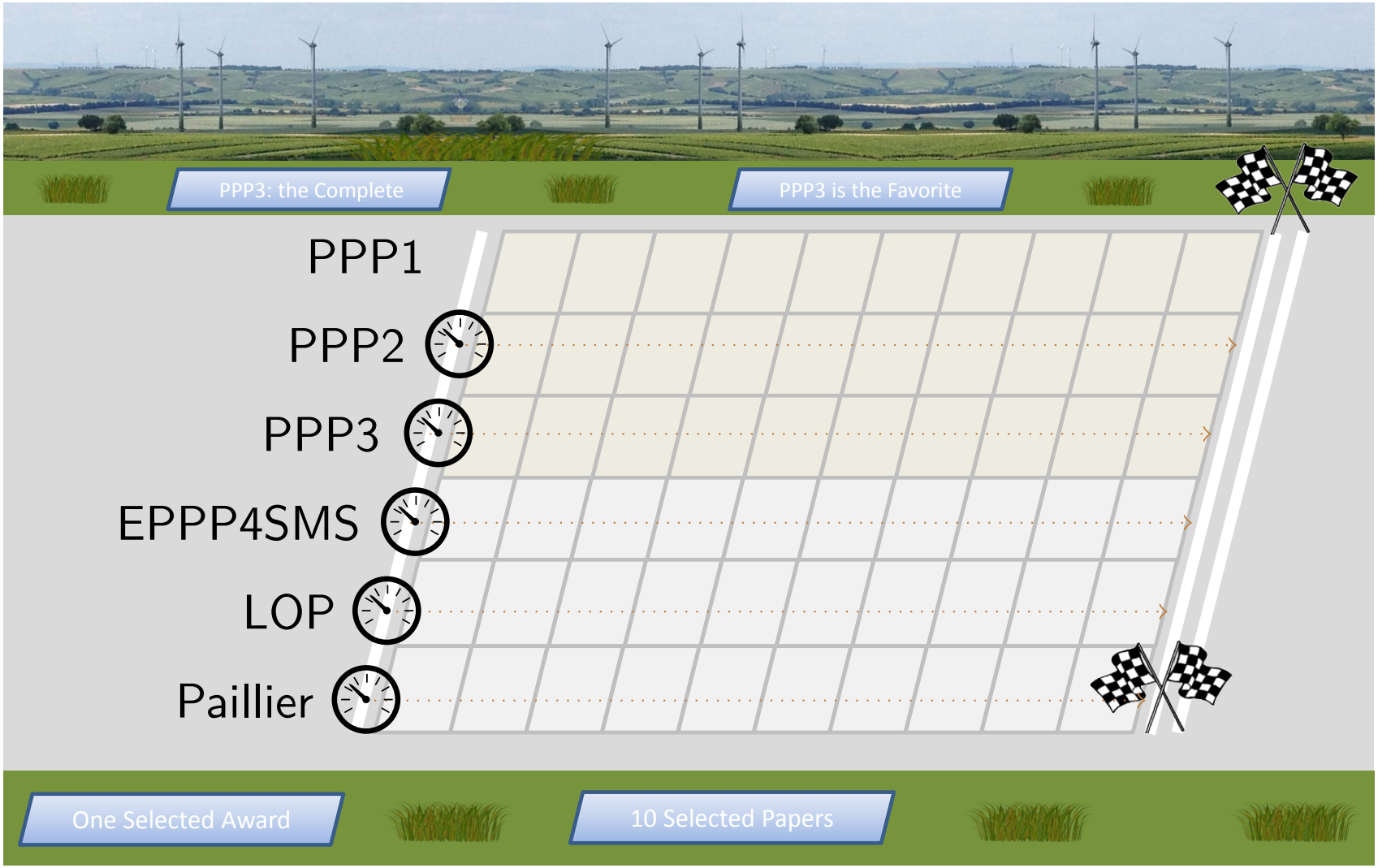
Performance

Corrida de Protocolos



Performance

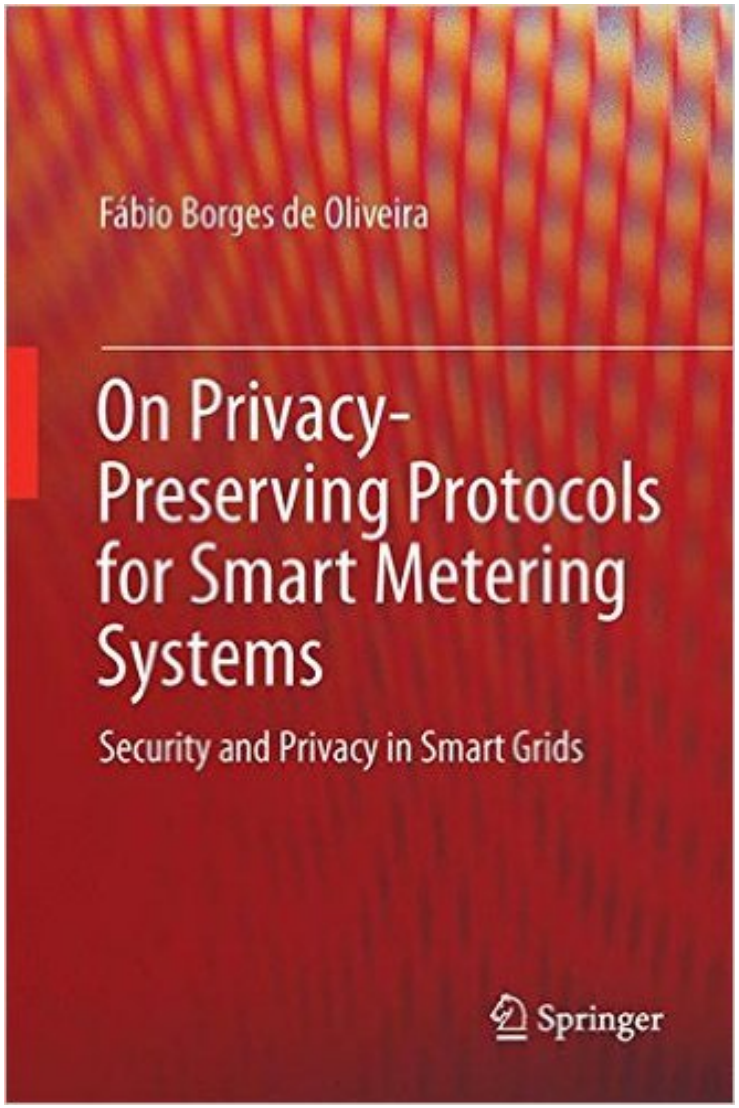
Corrida de Protocolos



Tópicos

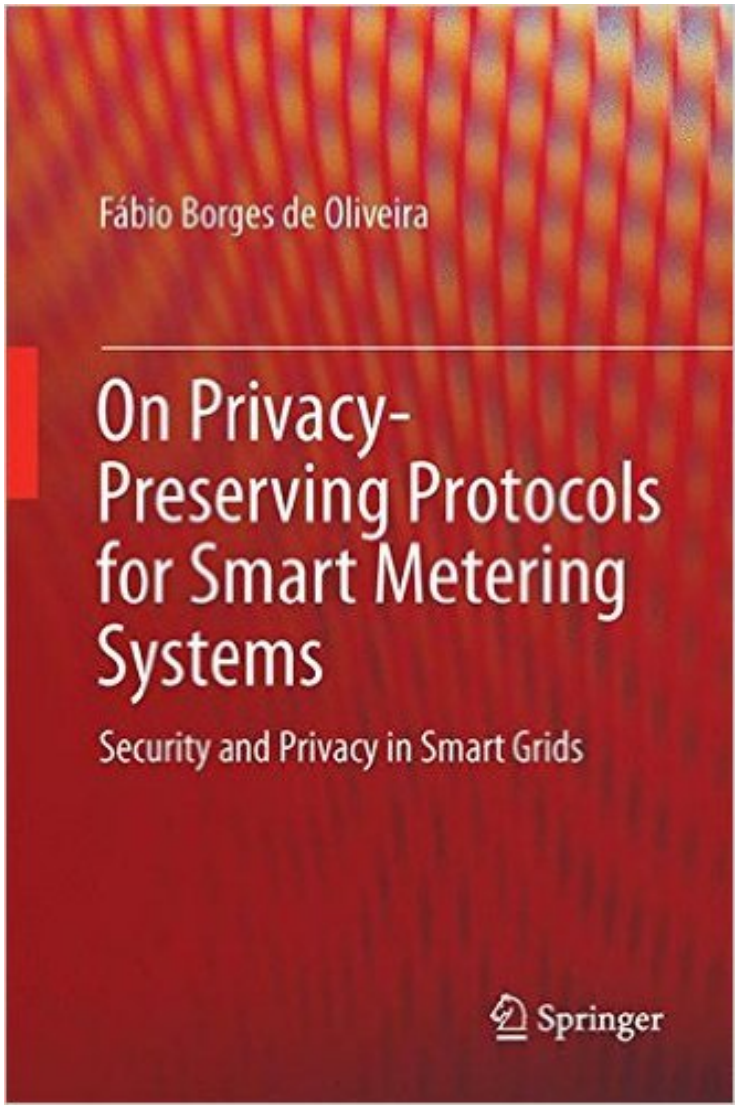
Conclusões

- Sustentabilidade



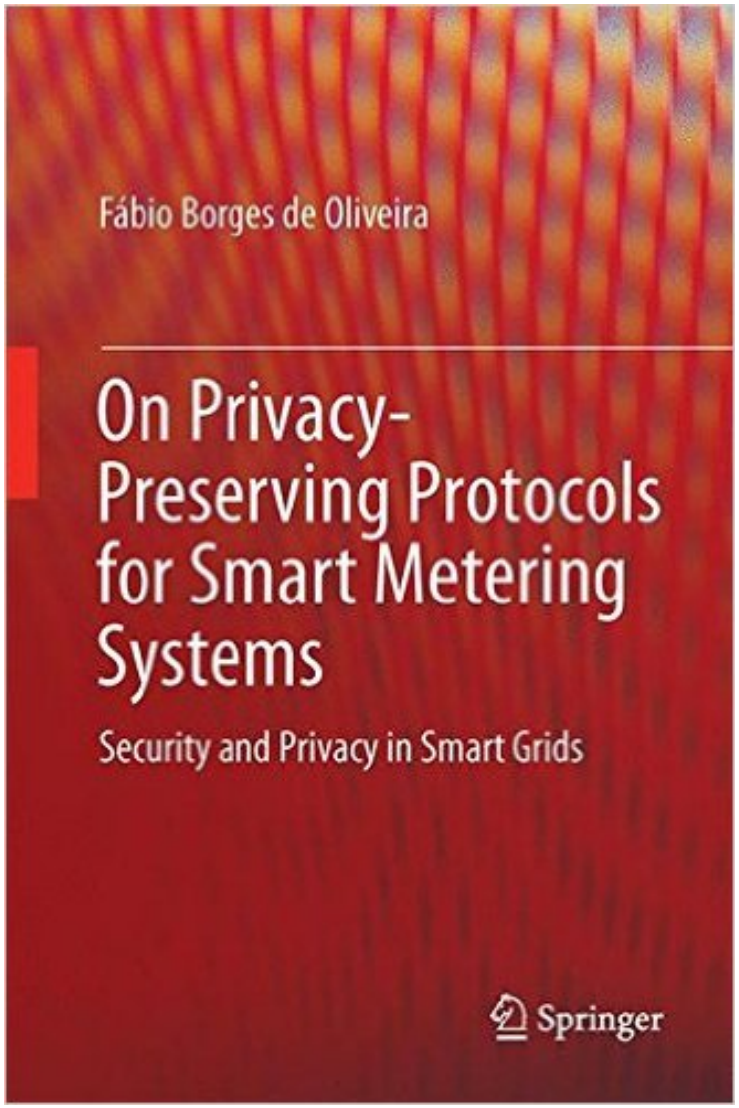
Conclusões

- Sustentabilidade
- Segurança



Conclusões

- Sustentabilidade
- Segurança
- Privacidade



Obrigado!

Laboratório Nacional de Computação Científica

Todas as sugestões são bem-vindas!

Contato: borges@lncc.br

Bibliography I

Ulrich Greveler, Benjamin Justus e Dennis Löhr. Identifikation von videoinhalten über granulare stromverbrauchsdaten. Em Neeraj Suri e Michael Waidner, editores, *Sicherheit*, volume 195 de *LNI*, páginas 35–45. GI, 2012.