Detection, Recognition, and Localization of Multiple Cyber/Physical Attacks through Event Unmixing

Wei Wang, Yang Song, Li He, Penn Markham, Hairong Qi, Yilu Liu
Electrical Engineering and Computer Science Department
University of Tennessee

Contact: Hairong Qi, hqi@utk.edu

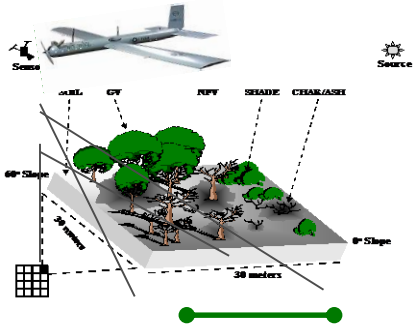
Motivation and Challenge

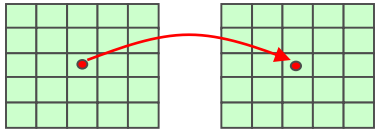
- Objective
  - To detect, recognize, and localize (both temporally and spatially) attacks from multiple sources using data collected from the ultra-wide-area monitoring network (e.g., FNET)
- Motivation
  - Conventional power systems are designed to be robust to accidental failures (e.g., N-1, N-2, or even N-3 contingencies). Nevertheless, under the post 9/11 environment, simultaneous coordinated strikes become a realistic threat, which will lead to N-X operations under emergency.
  - Researchers at the Trustworthy Cyber Infrastructure for the Power Grid (TCIP) Cyber Trust Center also reported [1] that through the usage of a commercially available Power simulator and publicly available power flow data, a small set of breakers was found whose tripping would lead to a blackout almost the scale of the August 2003 blackout. This will put the interconnected power network in a greater danger that the original power system planner had never envisioned.

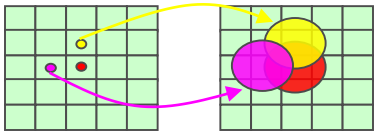
[1] W. H. Sanders, "Building cyber-physical resiliency into the grid," *IEEE-SA Computer Society Smart Grid Vision Workshop*, August 8, 2011.

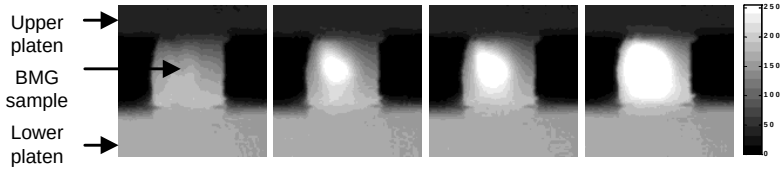
Background: Mixture and Unmixing

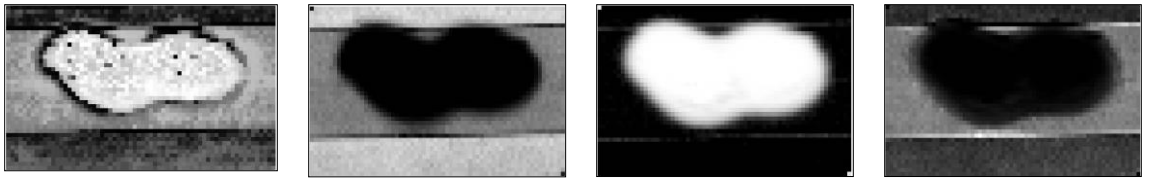
- Target detection at the subpixel level in remote sensing
- Speaker identification - The cocktail party problem
- Image restoration
- Heat source analysis from surface temperature evolution pattern in bulk metallic glass (BMG)
- Hidden weapon detection using terahertz images











Event Unmixing

Rationale – Event Unmixing

- Events seldom occur in an isolated fashion. Cascading events are more common and realistic which create multiple disturbances. The electromechanical waves generated from multiple disturbances will interfere with each other and the measurements taken at an FDR would more than likely be a mixture.
- Linear mixture analysis has been widely used due to its effectiveness and simplicity, where the sensor readout at a single location is given by

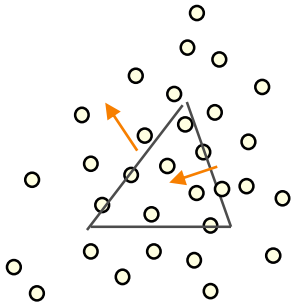
$$x=As+n$$

  - x: an *l*-element column vector, the measured mixture or **observation**
  - A: an *lxc* source matrix with each column indicating a **root event signature**
  - s: a *c*x1 column vector or **abundance vector**, indicating the mixing coefficients satisfying certain constraints
  - n: the noise vector
- If given A, i.e., the signature matrix, s is traditionally estimated using methods such as Unsupervised Fully Constrained Least Squares (UFCLS) or Nonnegatively Constrained Least Squares (NCLS). Event detection can be conducted by identifying the event signature with a non-zero (or comparatively larger) corresponding abundance. The problems in traditional abundance estimation methods include
  - The estimated abundance may have values on each signature – not suitable for rare event detection
  - Very computationally intensive

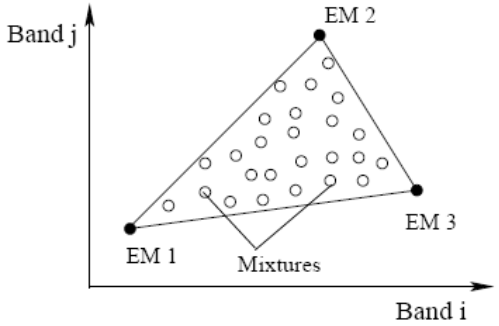
Initial Trial

- x=As+n
- Unsupervised unmixing using minimum volume constraints, J(A)

$$\text{minimize} \quad f(\mathbf{A},\mathbf{S}) = \frac{1}{2}\left\|\mathbf{X}-\mathbf{AS}\right\|_F^2 + \lambda J(\mathbf{A})$$
$$\text{subject to} \quad \mathbf{A} \geq 0,\ \mathbf{S} \geq 0,\ \mathbf{1}^T\mathbf{S} = \mathbf{1}^T$$

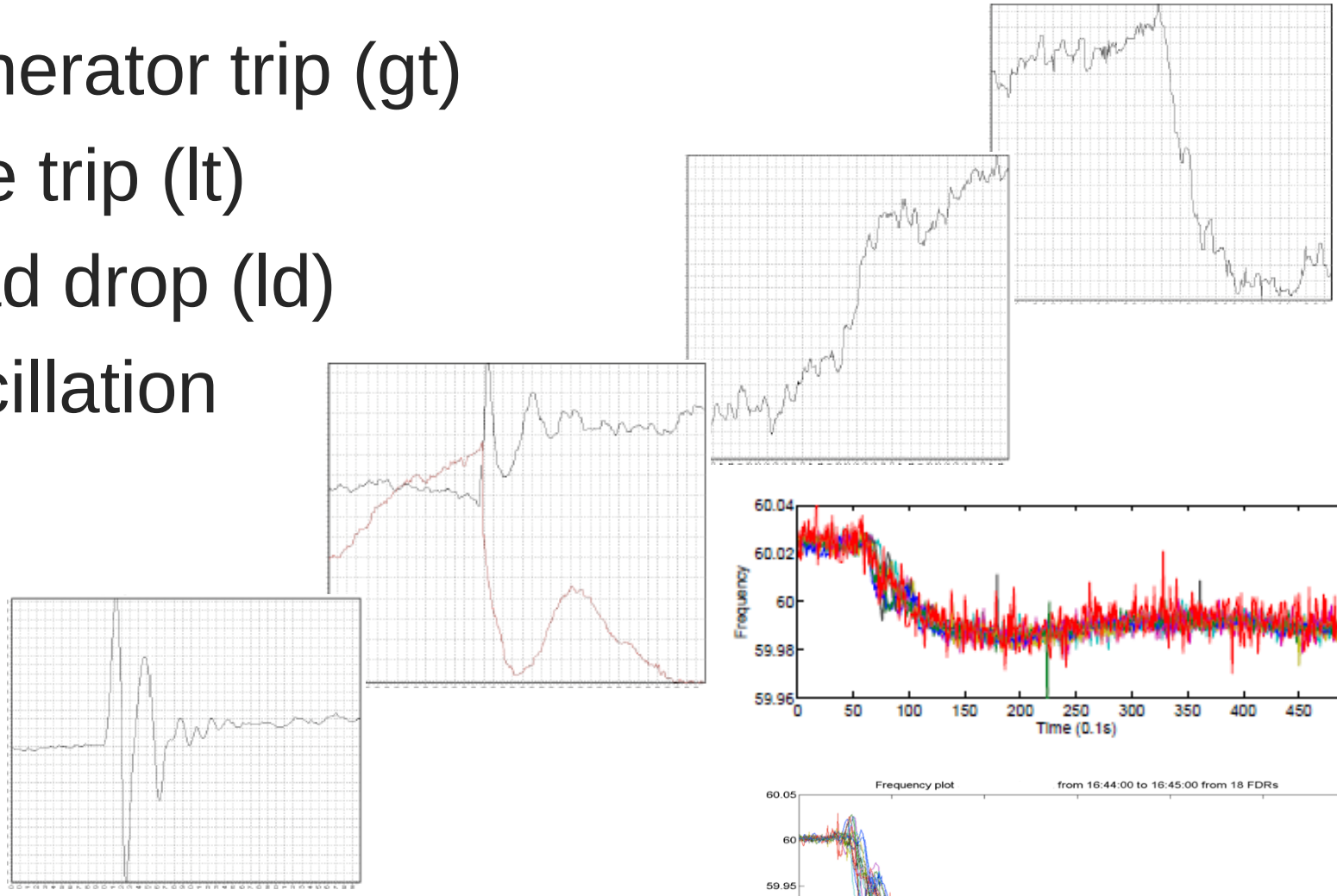


- Failed!
- What are the challenges?
  - The construction of signature matrix, A
  - The dynamics of cascading events
- What is a good constraint?
  - The sparsity constraint
  - Signature training and learning



Root Event Signatures

- Generator trip (gt)
- Line trip (lt)
- Load drop (ld)
- Oscillation



Algorithm - Sparsity-constrained Unmixing

- x=As+n
- Abundance estimation via sparse coding
  - The sparse coding formulation (an NP-hard problem): minimize the number of non-zero elements in s while s is subject to the least-square constraint

$$\min \|s\|_0 \quad \text{s.t.} \quad \|As - X\|_2^2 \leq \epsilon$$

  - If s is sufficiently sparse, we can solve for s by instead minimizing the l_1-norm

$$\min \|s\|_1 \quad \text{s.t.} \quad \|As - X\|_2^2 \leq \epsilon$$

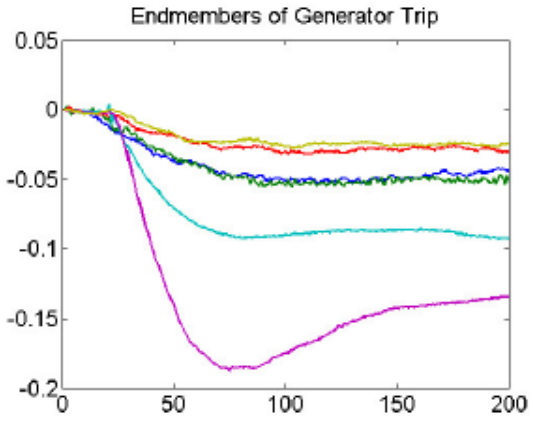
  - "Feature sign search" is used to solve the optimization problem

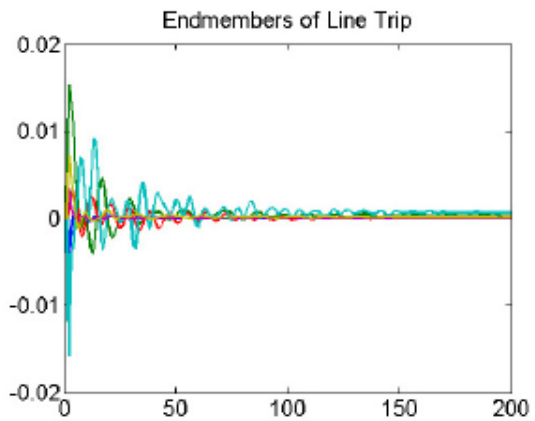
$$s = \underset{s}{\operatorname{argmin}} \|X - As\|_2^2 + \lambda \|s\|_1$$

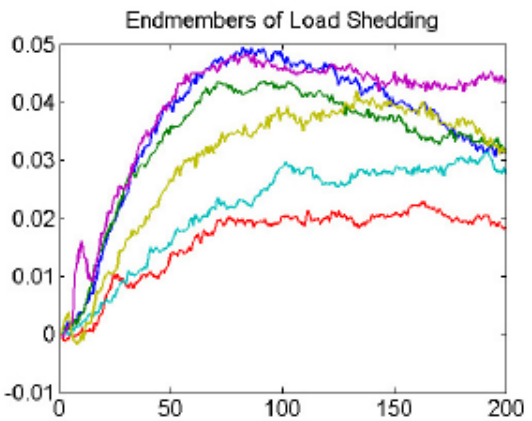
Sparsity-constrained Unmixing – Dictionary Construction

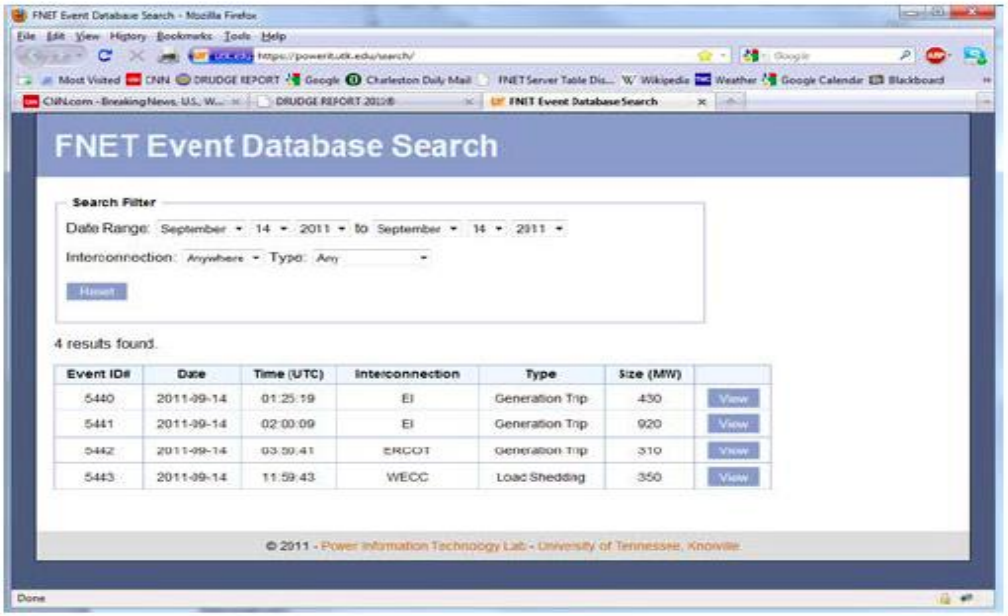
- Signature dictionary learning – Design an overcomplete dictionary that incorporates temporal information
  - Training root event signature (done offline)
    - **Generator trip** (547 from EI, 415 from WECC, 189 from ERCOT) and **load shedding** (160 from EI, 346 from WECC) data are retrieved from the FNET database
    - Since FNET doesn't detect **line trips** yet, we use PSS/E to generate signatures for line trips. A 16,000-bus model of the EI was used for simulation. Approximately 75 buses corresponding to actual FDRs were selected as the measurement points, and lines adjacent to these buses were tripped one at a time (257 training cases)
    - K-mean clustering is used to extract 6 (i.e., k=6) representing root event signatures for each event from all the above training cases

Signatures Learned



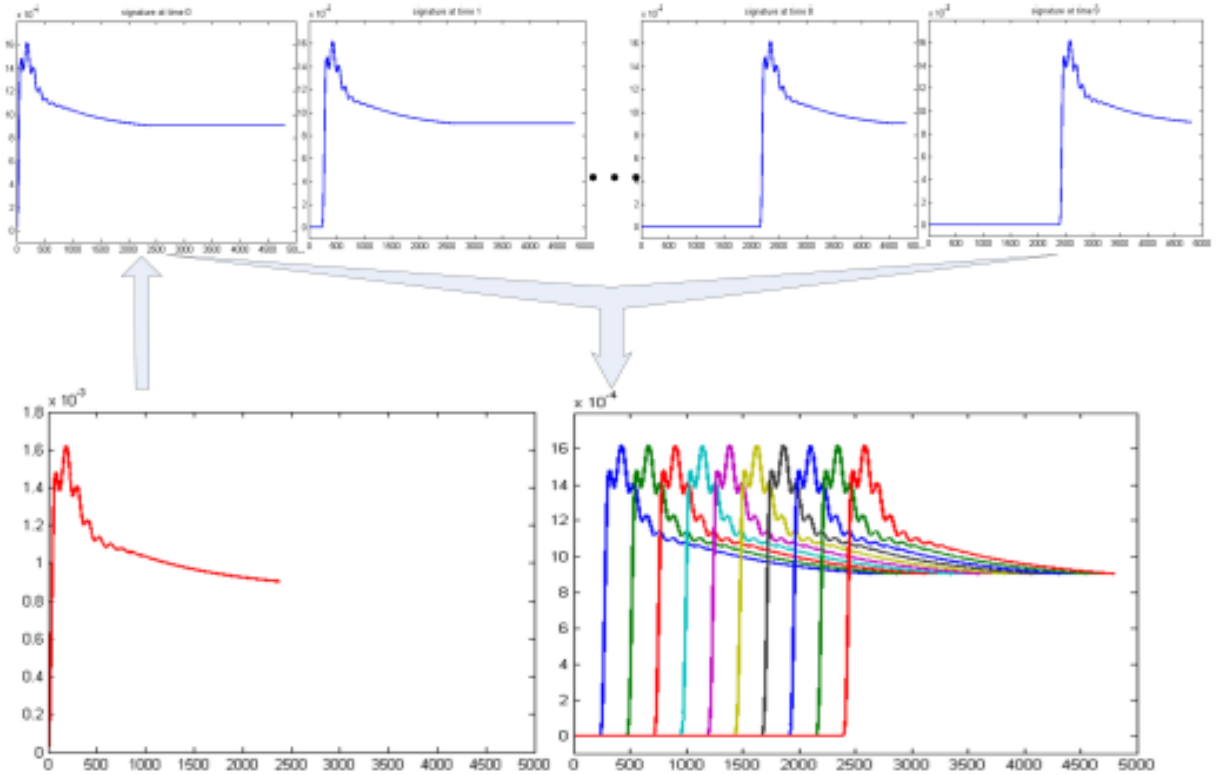






Dictionary Construction – Cont'

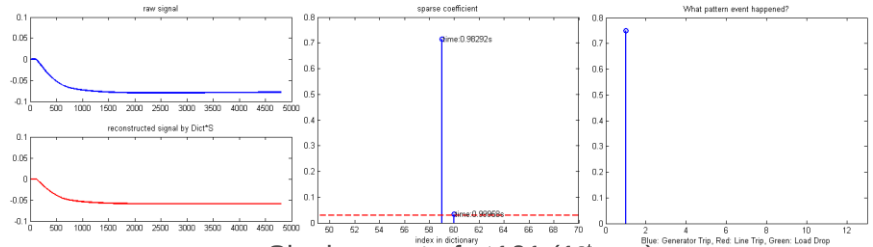
- Construction of overcomplete dictionary - Temporal span of root event signature (done online)
  - For each root event signature learned above (6 for each of the three events), time-shift the signature by 0.1t seconds, t =1,...,200, to the right to generate all possible occurrence time of that event. Note that the interval 0.1 second can be changed with higher resolution, e.g., 0.01 second, which means the algorithm can resolve multiple events occurred at a finer scale.



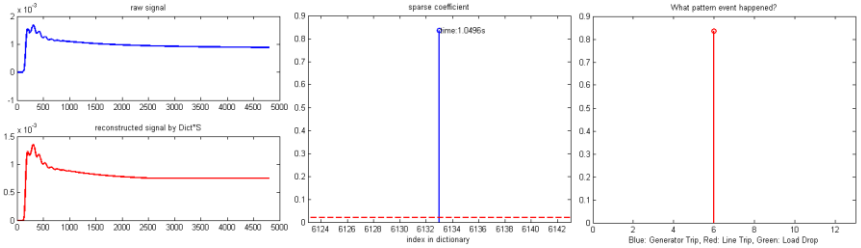
Results – Simulated Events

- The model: A 23-bus model supplied from PSS/E is used. The model represents a small power system with 3,200 MW of load. The system contains several different voltage levels ranging from 13.8 kV at the generator buses to 500 kV at the transmission buses. It represents a variety of generation sources including nuclear, thermal, and hydro.
- Root event signatures: since this is a small power grid, we simply extracted 5 generator trip signatures (gt), 3 line trip generators (lt), and 5 load drop signatures (ld) to form the root event signature matrix
- Both single event and multiple event detections are accurate in terms of both detection and temporal localization

Single event detection

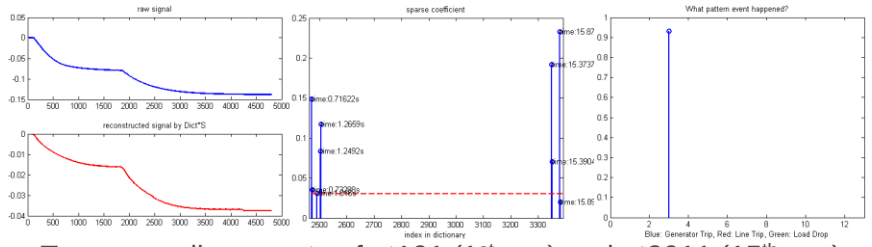


Single event of gt101 (1st sec)

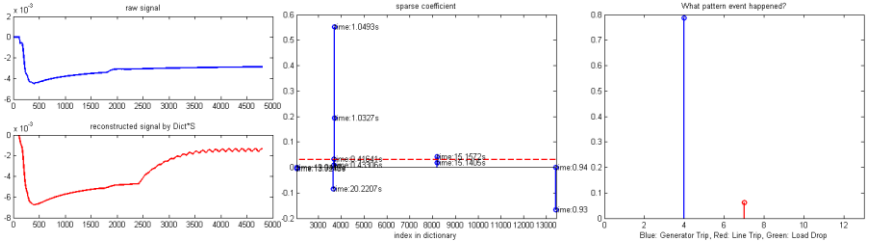


Single event of lt152-153 (1st sec)

Multiple event detection



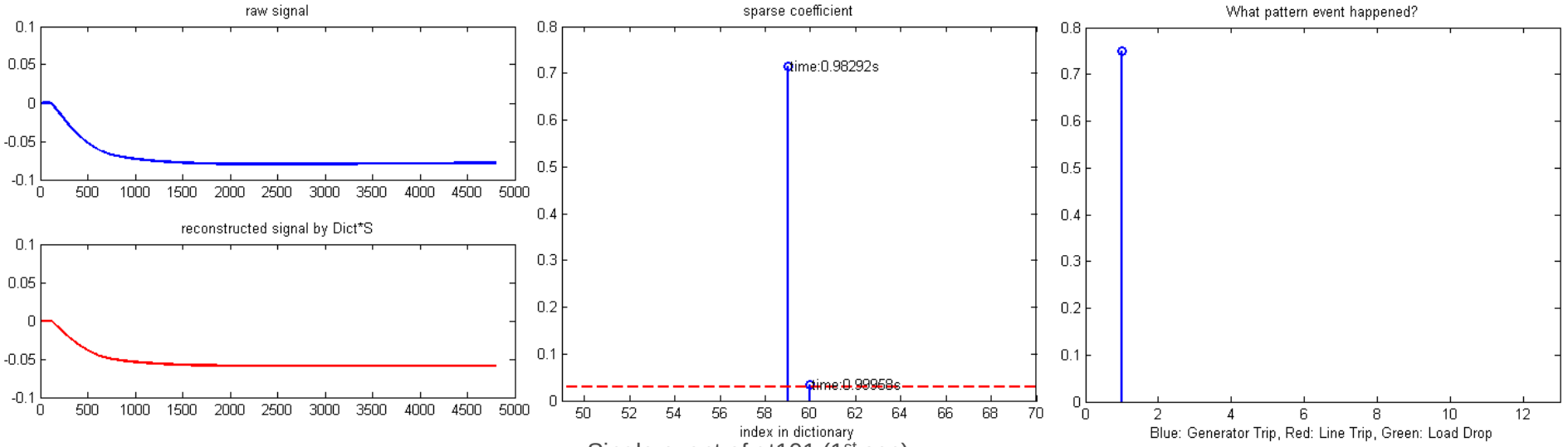
Two cascading events of gt101 (1st sec) and gt3011 (15th sec)



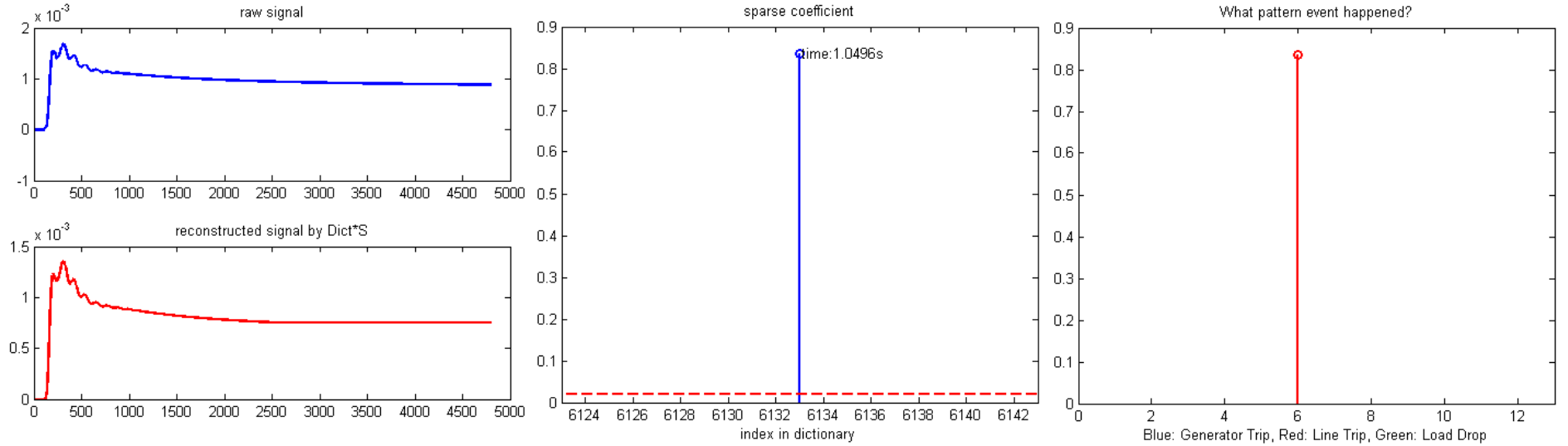
Two cascading events of gt101 (1st sec) and lt3004-3005 (15th sec)

Left: original signal vs. reconstructed signal. Mid: sparse coefficient or abundance. Right: event type detection

Simulation – Single Event

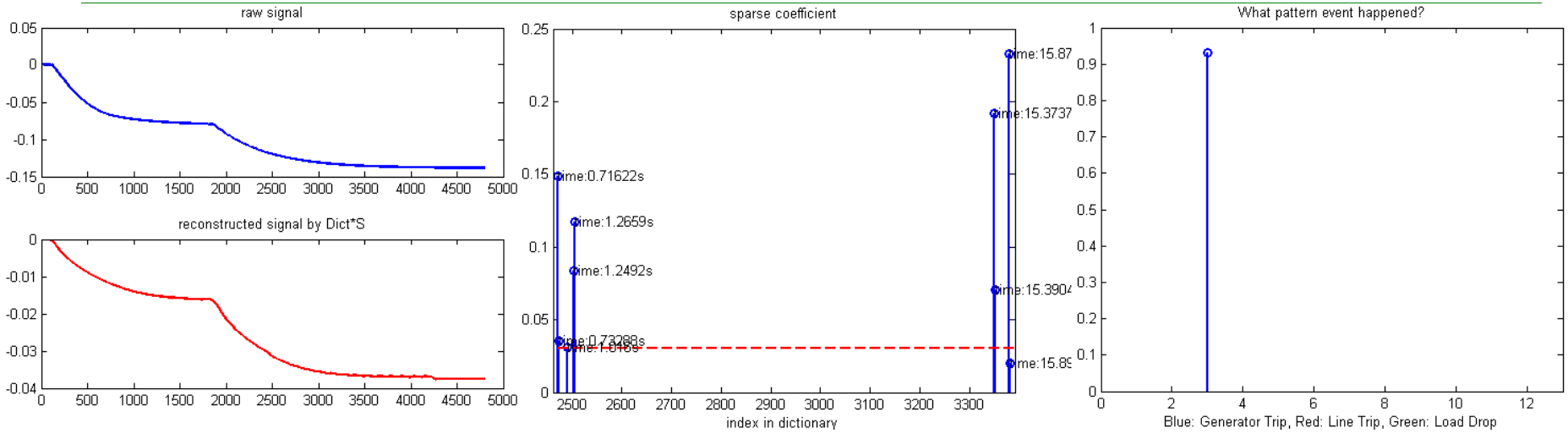


Single event of gt101 (1st sec)

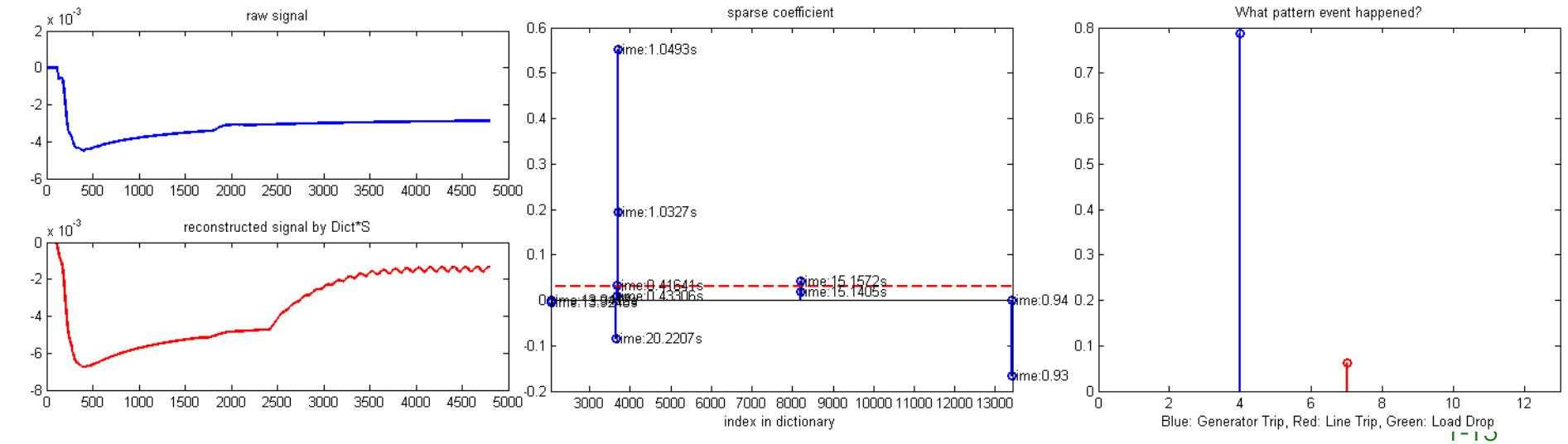


Single event of lt152-153 (1st sec)

Simulation – Multiple Events



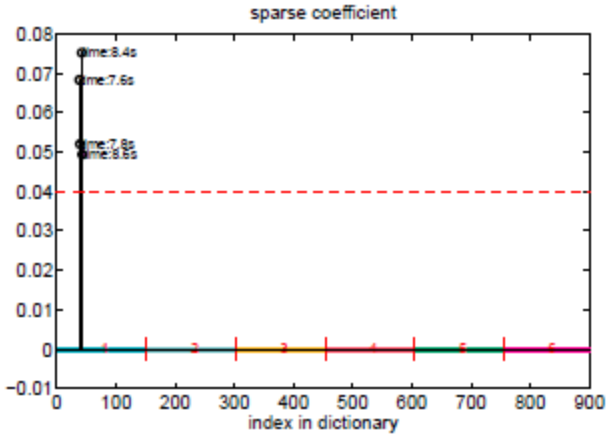
Two cascading events of gt101 (1st sec) and gt3011 (15th sec)

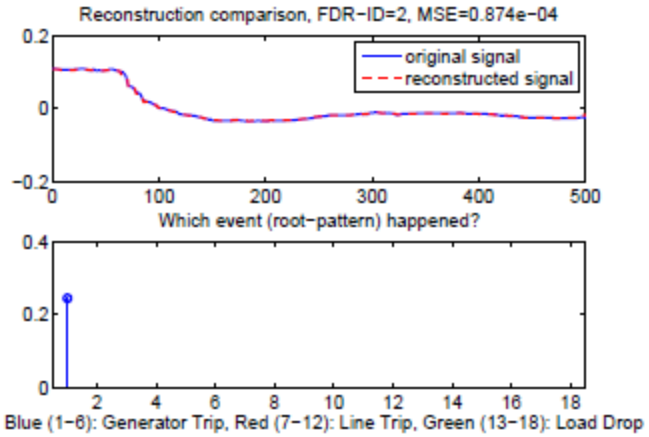


Two cascading events of gt101 (1st sec) and lt3004-3005 (15th sec)

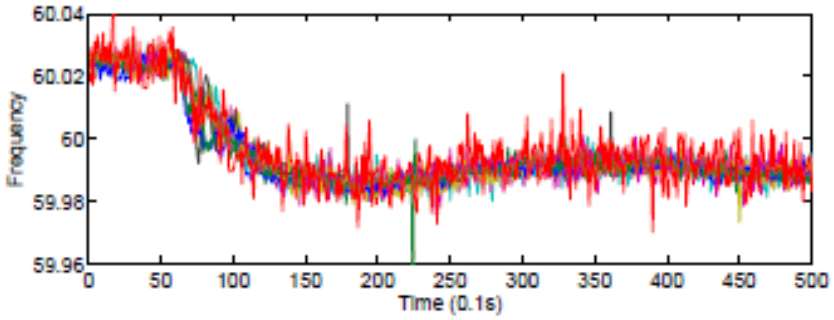
Results – Real Case (Single Event)

- **Single Event Detection and Temporal Localization**
  - One single generator trips were successfully detected from 10 out of 10 FDRs.
  - Each FDR detected the events with different time delay which can be further utilized for event localization purpose.





Event detection on FDR 2: one event is detected and temporally localized as the occurring time of the largest coefficient.



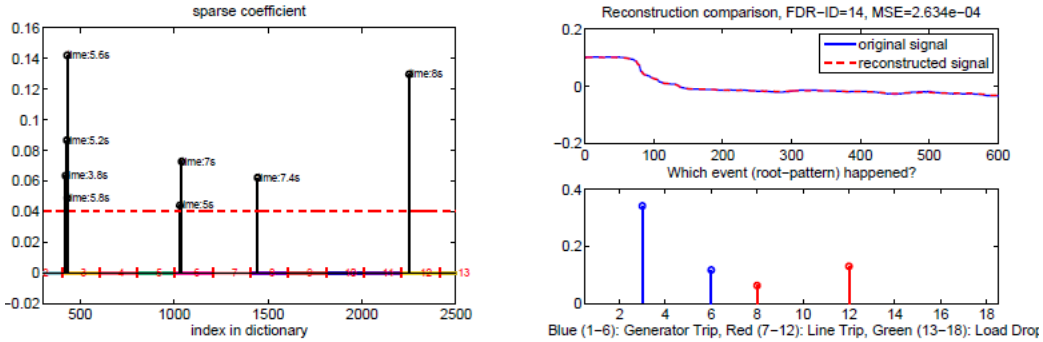
Plots of 10 raw FDR signals without denoising.

FDR	1	2	3	4	5
GenTrip1	8.4s	8.4s	8.8s	8.4s	8.6s
FDR	6	7	8	9	10
GenTrip1	9.0s	7.8s	7.2s	8.4s	7.8s

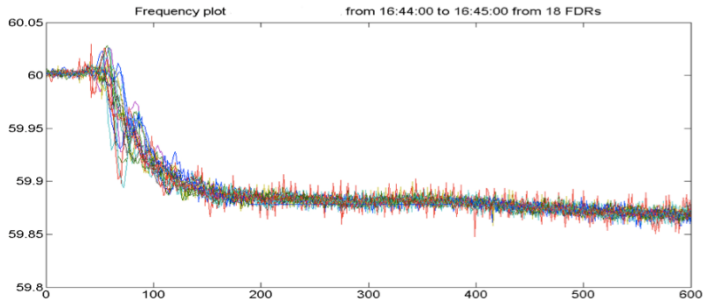
Temporally localized on different FDRs!
Why different occurring time?
The FDRs will receive event wave at different time.
The delays are very important for spatial localization!

Results – Real Case (Multiple Events)

- **Multiple Event Detection and Temporal Localization**
  - Two generator trips (event3 and event4) were successfully detected from 16 out of 18 FDRs and two line trips were successfully detected from 17 out of 18 FDRs.
  - Each FDR detected the events with different time delay which can be further utilized for event spatial localization purpose.



Event detection on FDR 14



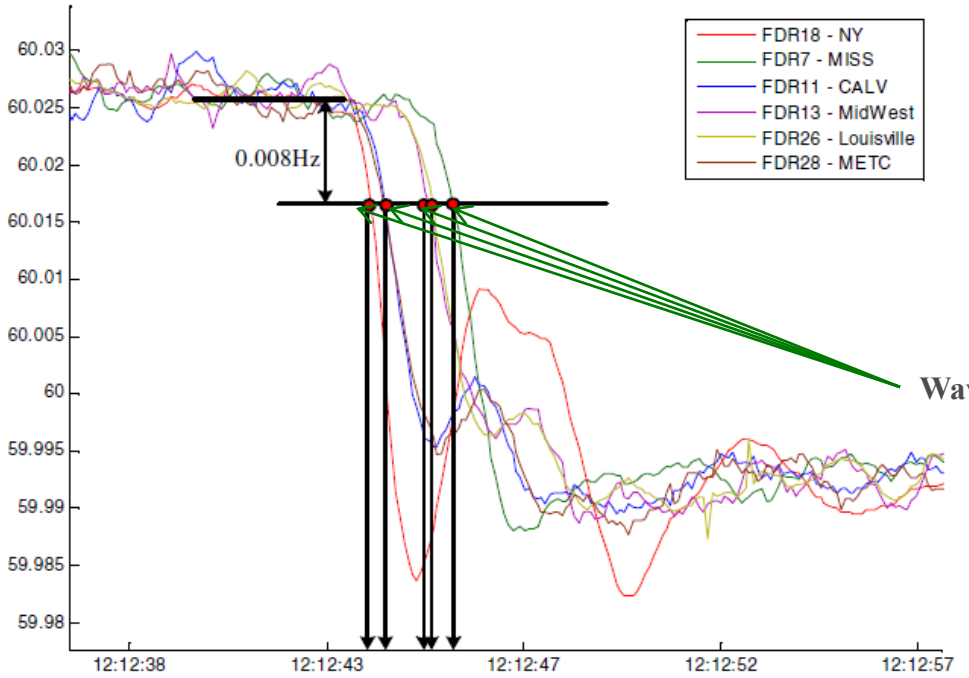
Plots of 18 raw FDR signals without denoising. (Denoising is necessary before performing event detection algorithm!)

FDR	1	2	3	4	5	6
GenTrip3	5.4s		4.0s	7.0s	5.2s	4.6s
GenTrip6	6.2s	4.2s	3.2s	7.6s	4.6s	4.2s
LineTrip8	9.2s	7.2s	7.8s	7.6s	9.0s	6.2s
LineTrip12	7.2s	6.2s		5.6s	6.4s	7.4s
FDR	7	8	9	10	11	12
GenTrip3	4.4s	4.0s	4.6s	4.2s	4.0s	4.2s
GenTrip6	6.4s	3.8s	6.8s	4.0s	6.0s	5.4s
LineTrip8	6.8s	5.6s	8.6s	6.0s	6.6s	8.6s
LineTrip12	7.2s	5.8s	7.2s	6.0s	6.6s	7.2s
FDR	13	14	15	16	17	18
GenTrip3	5.0s	5.6s	4.2s		3.6s	4.4s
GenTrip6	4.2s	7.0s	3.8s	4.4s	3.2s	7.8s
LineTrip8	9.0s	7.4s	6.8s	7.6s	7.8s	6.2s
LineTrip12	7.0s	8.0s	7.2s	7.4s	5.8s	6.4s

Each individual event is temporally localized on different FDRs!

Event Spatial Localization

- **Traditional Localization Method**
  - **Wave-front Arrival Time** (detected based on an empirical threshold!)



  - **Geographic and Geometrical Triangulation** [3].
    Assumption: the time delay is linearly related to the distance between the FDR location and the event location.

[3] T. Xia, H. Zhang, R. Gardner, J. Bank, J. Dong, J. Zuo, Y. Liu, L. Beard, P. Hirsch, G. Zhang, and R. Dong, "Wide-area frequency based event location estimation," in Power Engineering Society General Meeting, IEEE, 2007, pp. 1–7.

Event Spatial Localization

- **Limitations of Traditional Localization Method**
  * Only can handle single event, cannot discriminate multiple events involved cascading event!
  * The wave-front arrival time is not accurate enough for spatial localization!

- **Advantages of the Proposed Event Unmixing Algorithm**
  * Can unmix each individual single event from a mixture signal that multiple events cascadingly involved!
  * The detected occurring time of each individual event should be more stable! (More robust to noise and more accurate)

- **Triangulation**
  * Use the same triangulation algorithm but with good spatial localization performance.

Event Spatial Localization – Single Event

CURENT

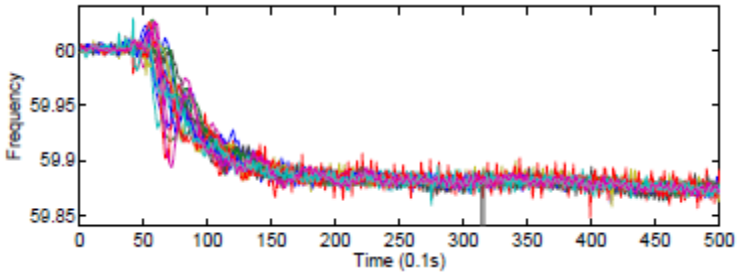
Localization error: 60 miles

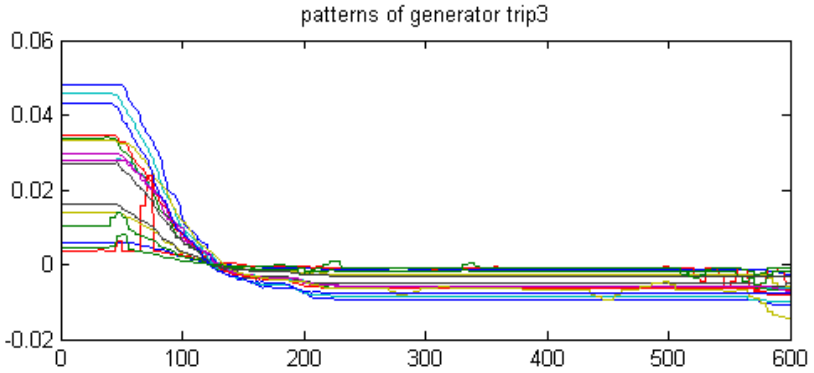
Event Spatial Localization

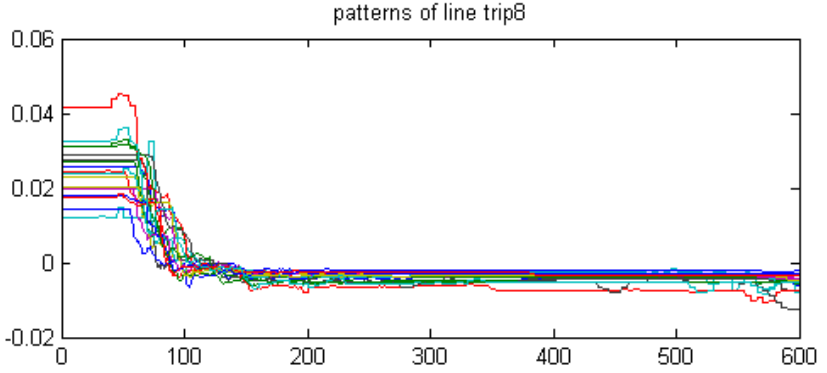
- **Example of a Multiple-Event**

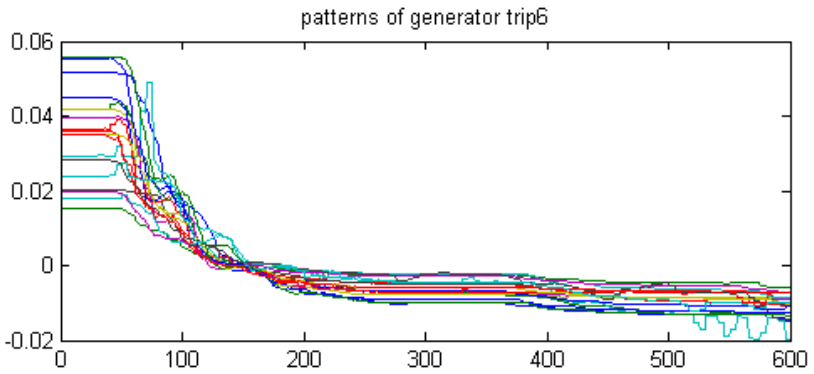
Individual Event Separation

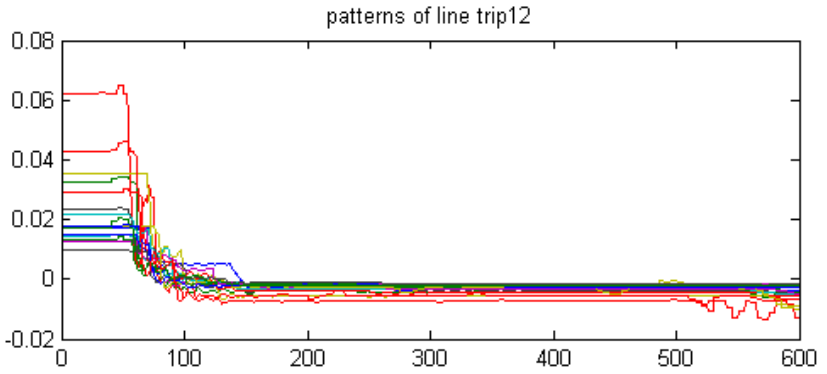
Apply Wave-front arrival detection on each individual event











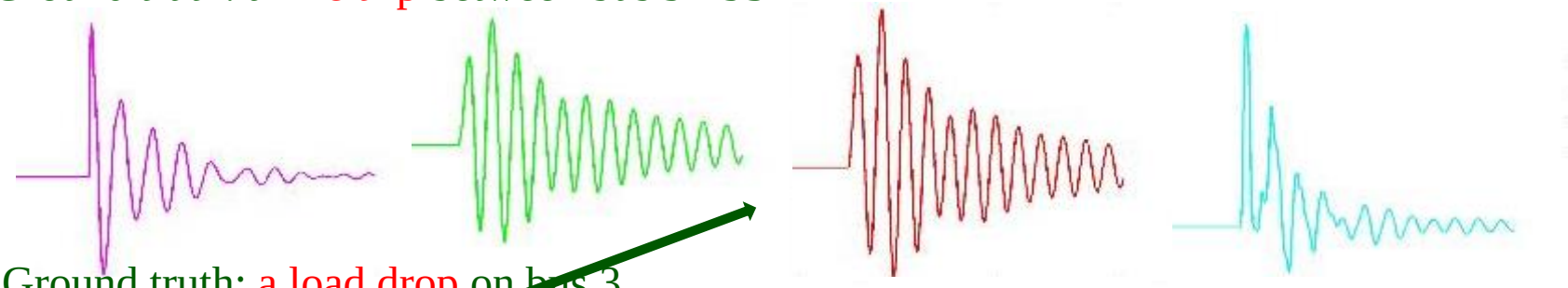
Event Spatial Localization – Multiple Event

Localization error: GT (105 mi), LT (122 mi)

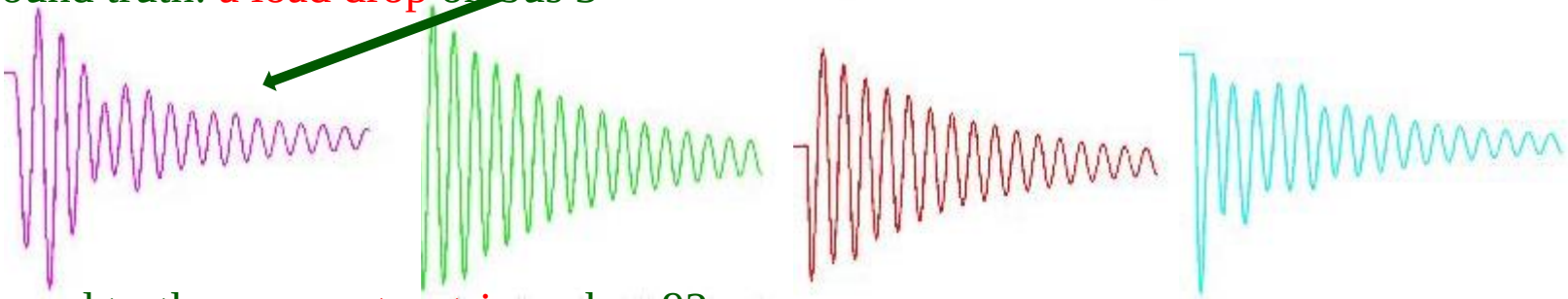
Challenge of LTB

Similarity: Different disturbances may cause the similar reaction on certain buses

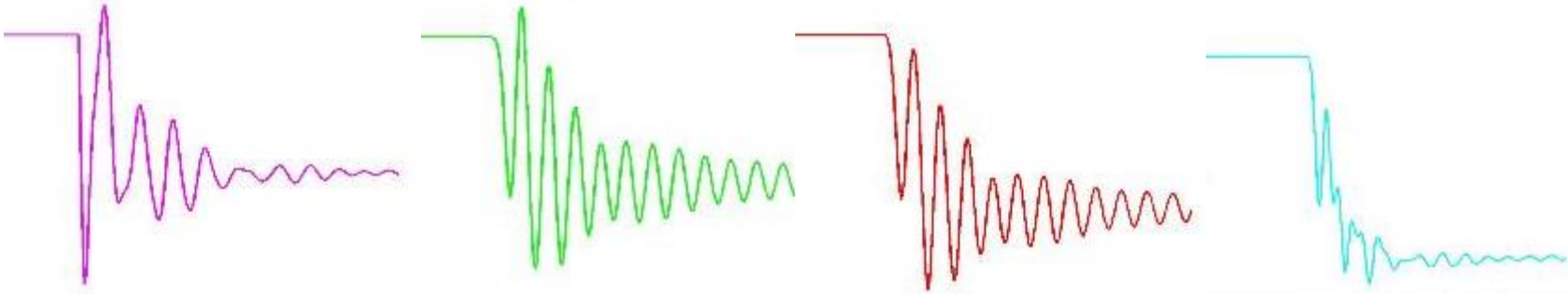
Ground truth: a line trip between bus 91-93



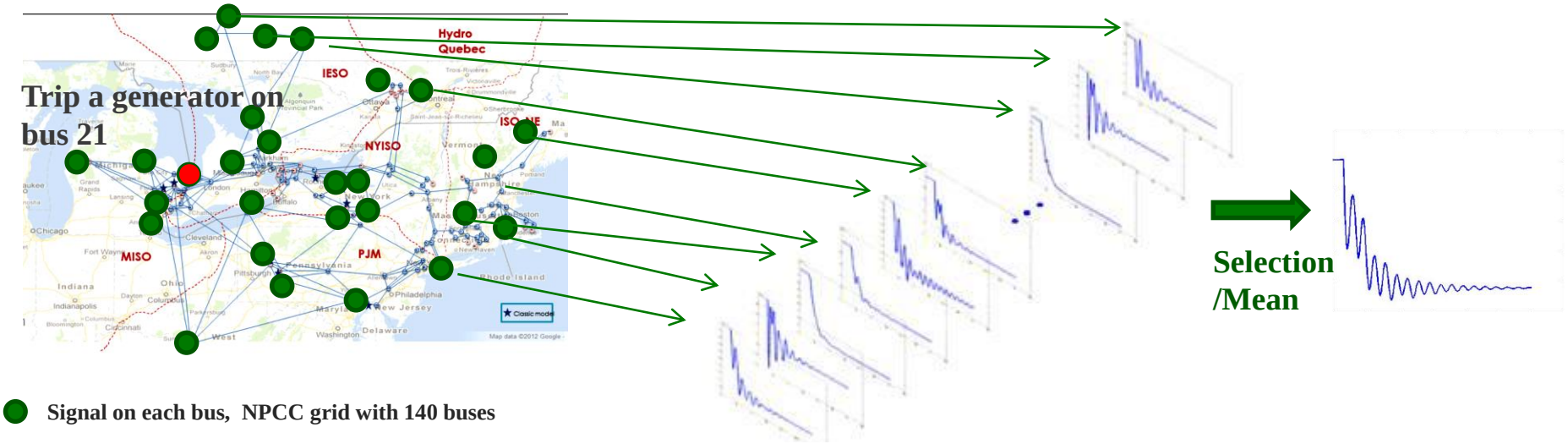
Ground truth: a load drop on bus 3



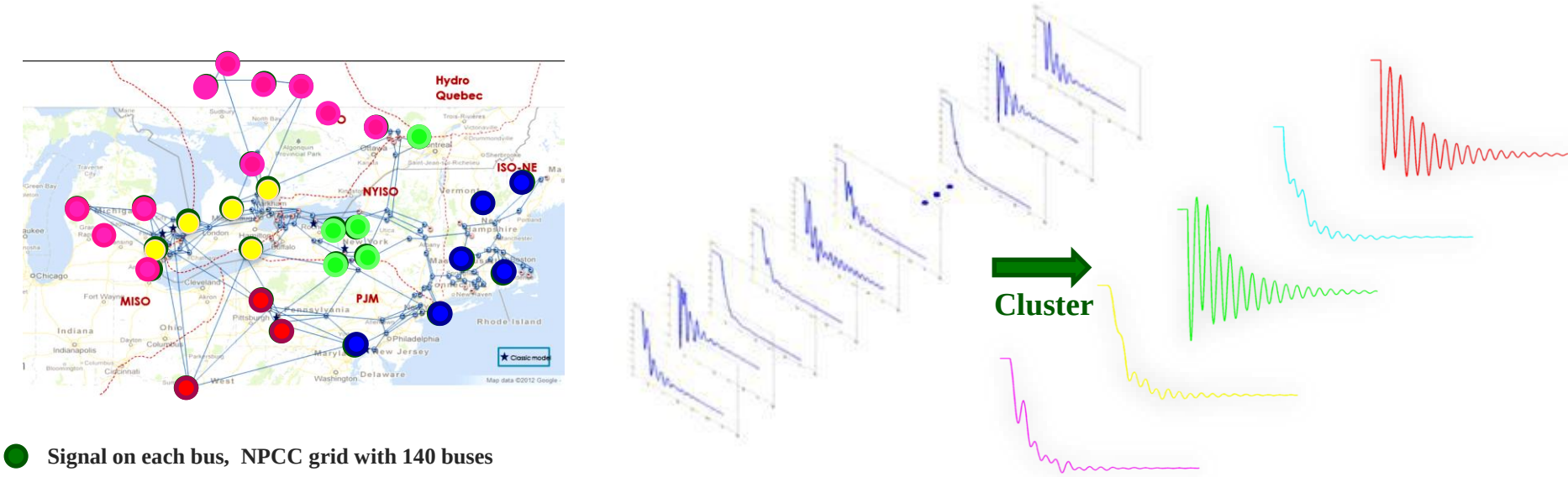
Ground truth: a generator trip on bus 92



New idea



- Signal on each bus, NPCC grid with 140 buses

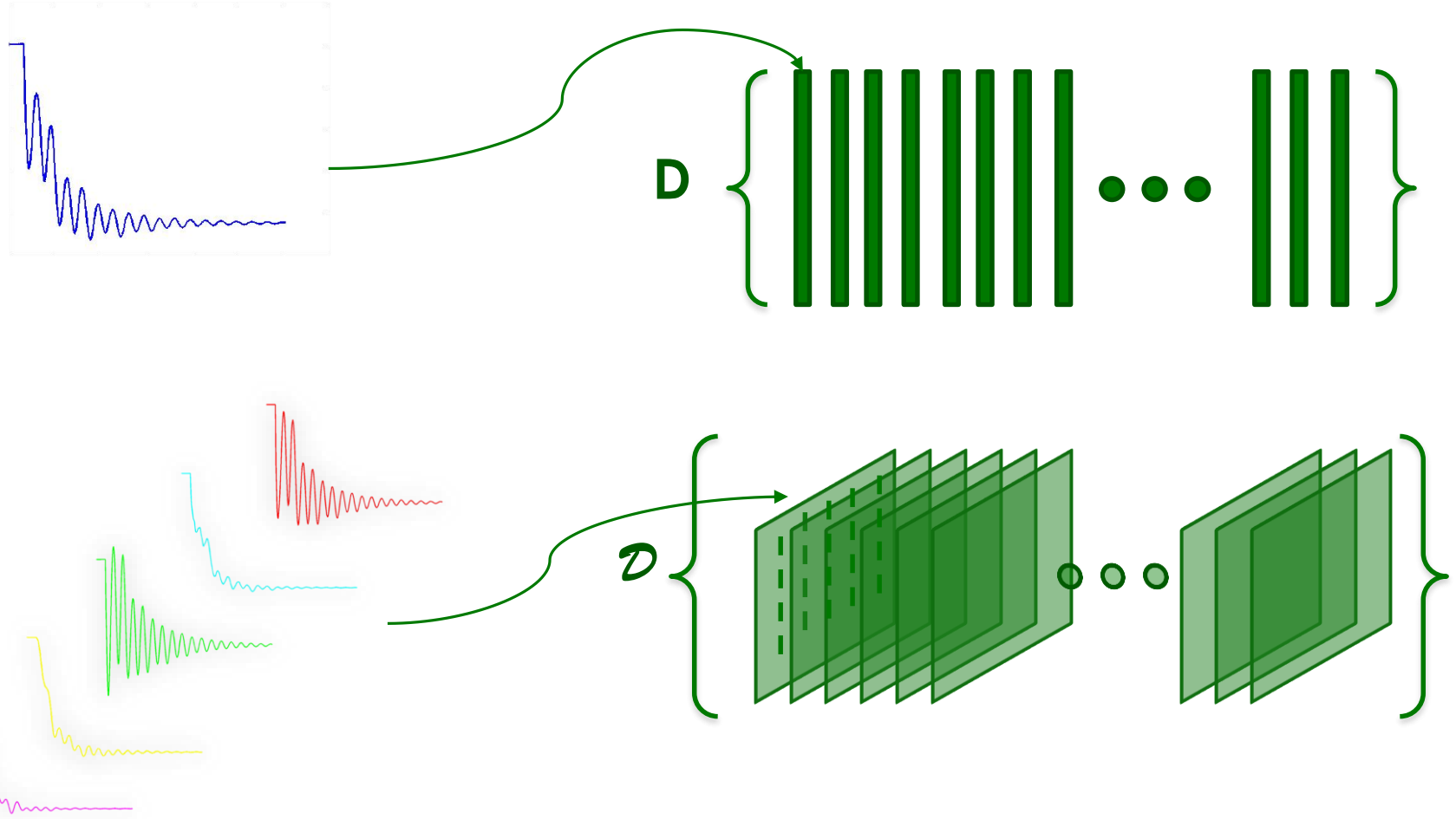


- Signal on each bus, NPCC grid with 140 buses

CURENT

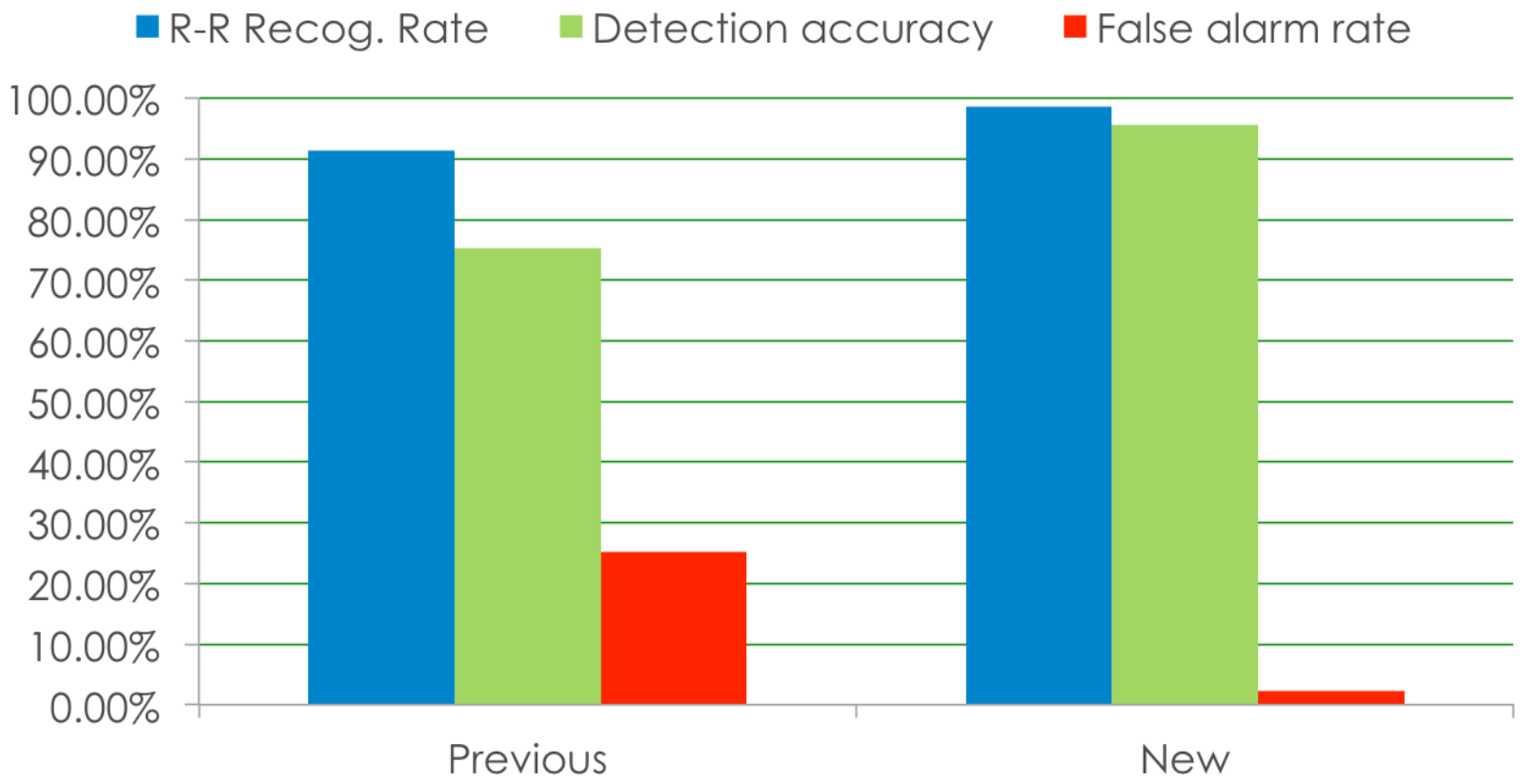
New idea

Basic idea: Unmixing/sparse coding is based on a group signals instead of a single signal.



Experiment results

Comparison: previous strategy and new strategy (different signal extraction methods and different spares coefficient analysis method)



Next Step …

- Further improve signal quality or frequency estimation accuracy
- Signature dictionary learning
  - Traditional parametric models using a fixed and finite number of parameters, e.g., k-means, can suffer from over- or under-fitting of data when there is a misfit between the complexity of the model.
  - The Bayesian nonparametric approach is an alternative to parametric modeling and selection. By using a model with an unbounded complexity, underfitting is mitigated, while the Bayesian approach of computing or approximating the full posterior over parameters mitigates overfitting.
  - The Dirichlet Process (DP), one of the most popular Bayesian nonparametric models, will be used for the learning of representative root event signatures
  - Not much improvement