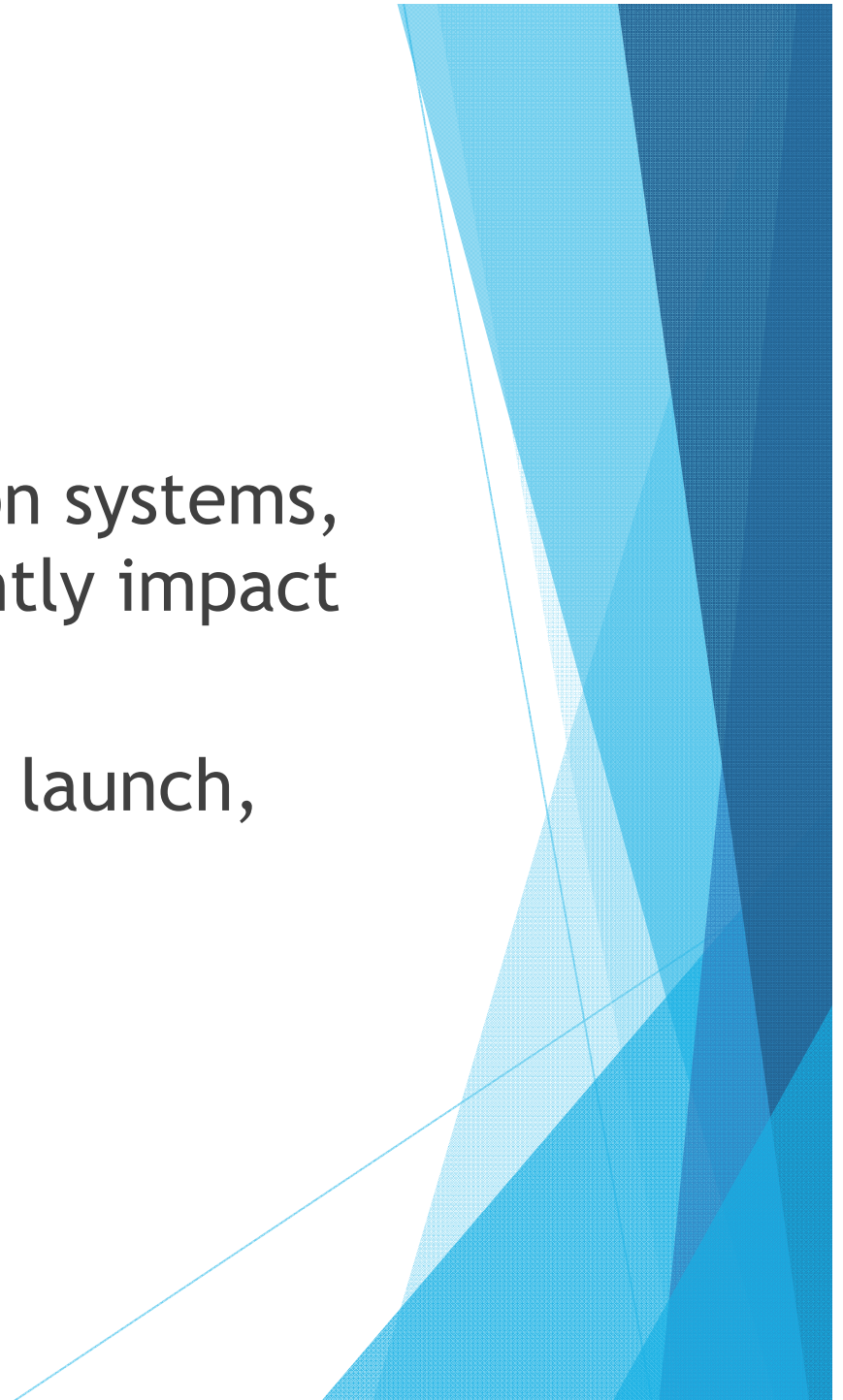
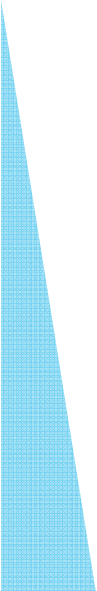


A Novel Physical Layer Spoofing Detection Based on Sparse Signal Processing

Ning Wang (BUPT), Shichao Lv
(IOT), Ting Jiang (BUPT),
and Ge Zhou (BUPT)

Concerns

- ▶ In wireless communication systems, spoofing attack significantly impact the information security;
- ▶ This attack is not hard to launch, but the threat is high;



Current situation

- Traditional cryptographic authentication
- Physical layer authentication scheme: RSS
- Physical layer authentication scheme: CSI


Investigation



Detects spoofing attack during the communication process;



How to use the signal processing means to realize authentication;



How to exploit the original signal characteristic;

Contributions

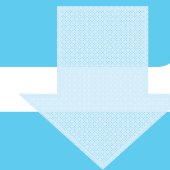
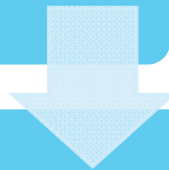
- ▶ We propose that utilizing the sparse signal processing to implement spoofing detection.
- ▶ For examining the correlation, we establish an Automatic Representative Selection Algorithm (ARSA) to search for the optimal target.

SYSTEM SETUP

The sparse representation
of the original signal.

Automatic representative
selection algorithm (ARSA)

Correlation detection



1 sparse representation

- ▶ Sparse decomposition

$$\mathbf{y} = \mathbf{D}\mathbf{x} = \sum_{k=1}^N d_k \mathbf{x}_k$$

- ▶ Principal component analysis (PCA)

$$\mathbf{p}_v = \mathbf{E}\mathbf{p}$$

2 Automatic representative selection algorithm (ARSA)

► Feature extraction

First feature is concentration ratio:

$$F^{(1)} = \frac{\sum_{k=2n-1-i}^{2n-1+i} d(i)}{\sum_{k=0}^{2n-1} d(i)}$$

Second feature as the middle section variance:

$$F^{(2)} = \sum_{k=2n-1-i}^{2n-1+i} \left(d(i) - \frac{1}{2i-1} \sum_{k=2n-1-i}^{2n-1+i} d(i) \right)^2$$

2 Automatic representative selection algorithm (ARSA)

The shape imbalance as the third feature:

$$F^{(3)} = \sum_{k=2n-1+i}^{2n-1} d(i) - \sum_{k=1}^{2n-1-i} d(i)$$

- ▶ Combination feature

$$F = \mu_1 F^{(1)} + \mu_2 F^{(2)} + \mu_3 F^{(3)}$$

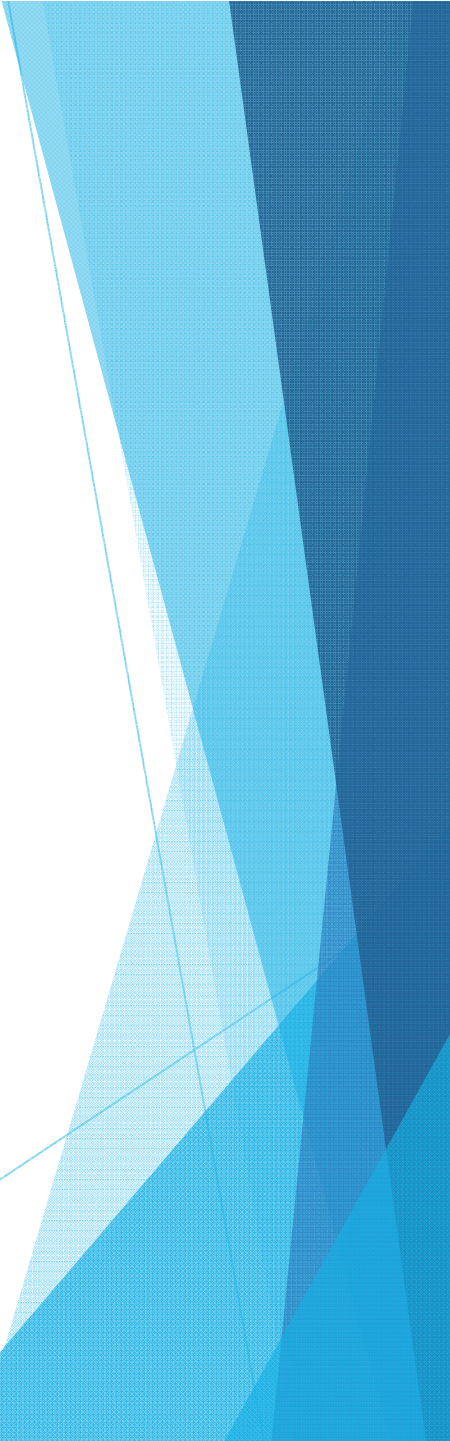
- ▶ These single feature are mapped into the feature vector, then the probability distribution of each value is

$$p(F_l) = M_l/N$$

- ▶ Formulate this searching optimal threshold problem as an optimization problem, given by

$$\varepsilon = \arg \max_l \sigma_B^2(l), \quad l \in [1, \dots, L]$$

$$\text{Subject to } \begin{cases} \omega(l)(1 - \omega(l)) > 0 \\ \text{or } 0 < \omega(l) < 1 \end{cases}$$

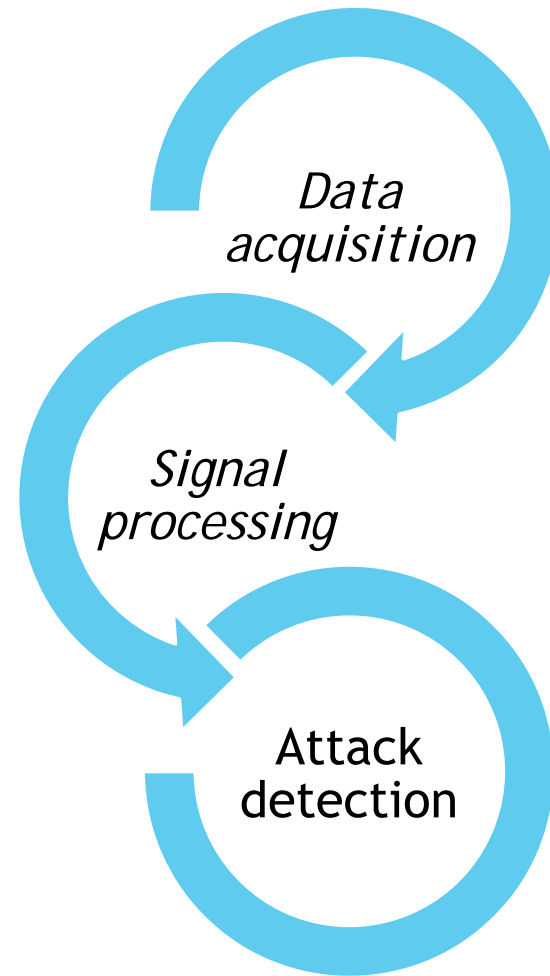
- 
- ▶ Solves this optimization problem, the optimal threshold ε can be obtained. Thus, the feature vector is dichotomized into two classes.
 - ▶ As a result, the target sparse coefficients, which corresponding to the dichotomized feature can be selected.

3 Correlation detection

- ▶ In this study, Pearson correlation coefficient is used to depict the degree of correlation.

$$r = \frac{\sum_{i=1}^n (o_i^{(a)} - \overline{o^{(a)}}) (o_i^{(b)} - \overline{o^{(b)}})}{\sqrt{\sum_{i=1}^n (o_i^{(a)} - \overline{o^{(a)}})^2} \sqrt{\sum_{i=1}^n (o_i^{(b)} - \overline{o^{(b)}})^2}}$$

EVALUATION

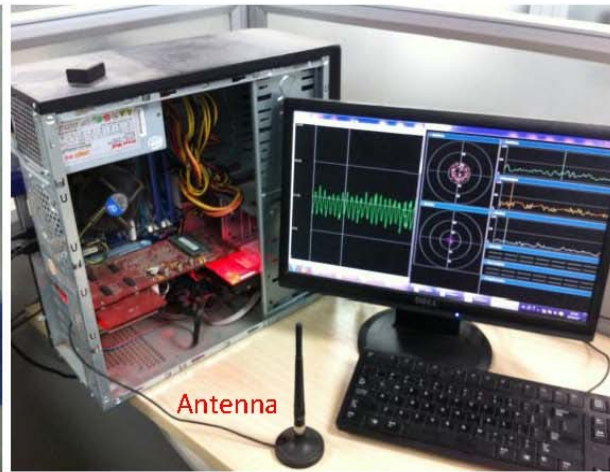
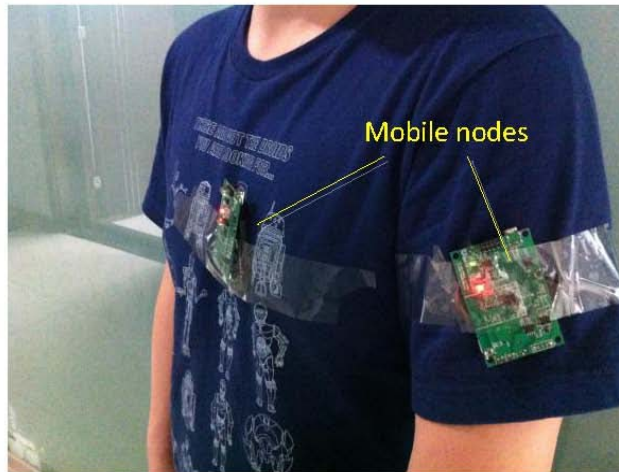


1 Data acquisition

- ▶ We configure two mobile nodes (homemade hardware based on IEEE 802.15.4) worn on the chest and the arms as signal transmitters.
- ▶ Software defined radio platform (SDR) is used to emulate the controller. (The utilized SDR is Microsoft Research Software Radio, also known as Sora)

1 Data acquisition

Mobile node and Software defined radio platform (Sora) in experiment.



Testing phase	Spoofing scenario	Normal scenario
Transmitting	Two mobile node	One mobile node
Received	One MAC address	One MAC address

2 Signal processing

- ▶ We select two signals (signal (a) and signal(b)) from the normal case, meanwhile, the other two signals (signal (c) and signal (d)) are extracted in the spoofing case;

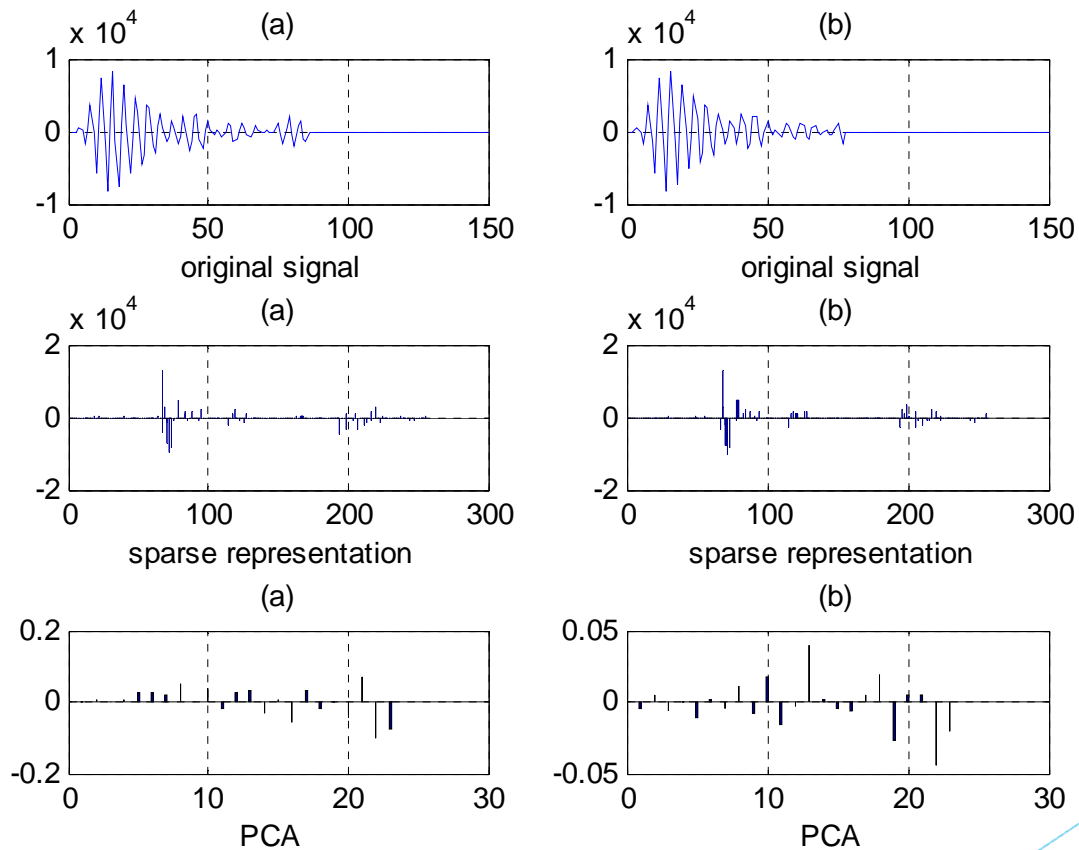
Sparse
representation

PCA

ARSA

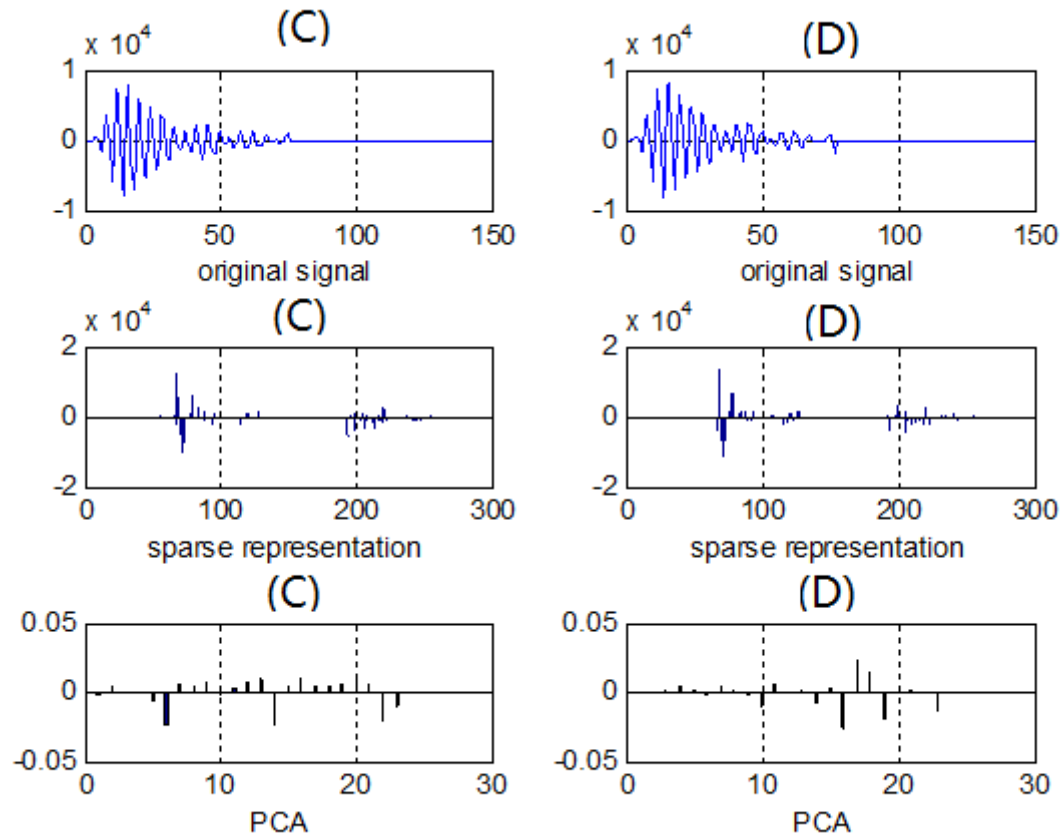
2 Signal processing

Signal processing under normal situations



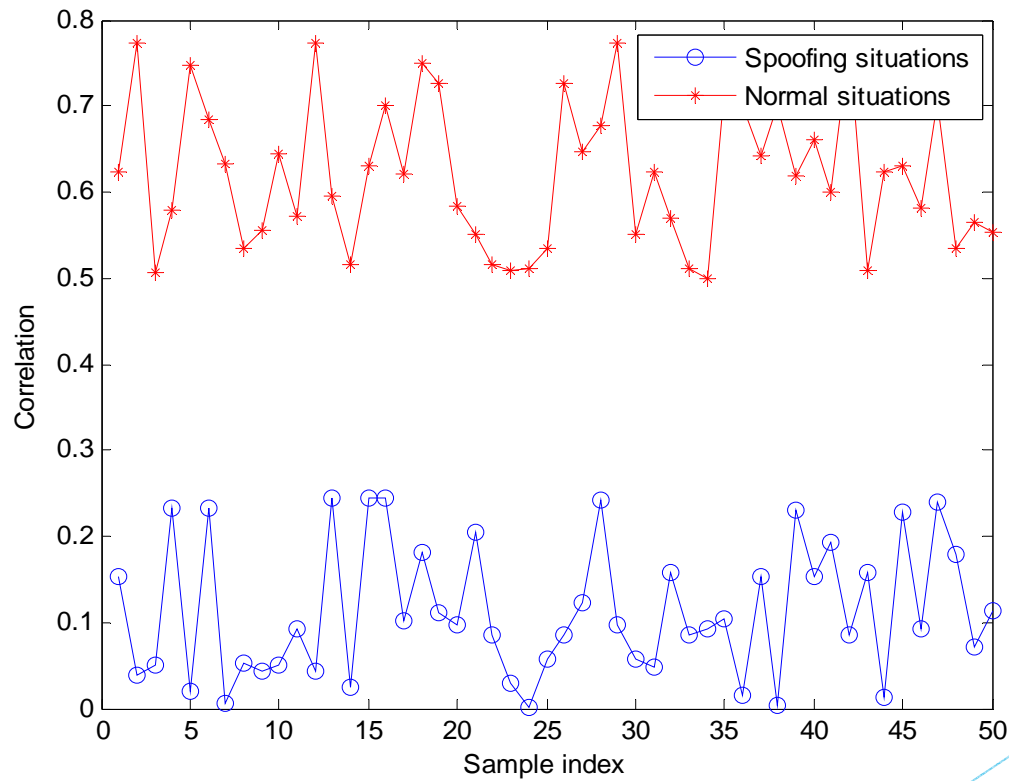
2 Signal processing

Signal processing under spoofing attack situation



3 Attack detection

The correlation analysis of the experiment



3 Attack detection

- ▶ Under the normal situation, transmitter has the similar channel, their sparse representation is more relevant;
- ▶ On the contrary, in spoofing attack situation, their channels are hard to parallel, so the correlation rate is very low;
- ▶ To address this problem, the traditional obvious method is threshold scheme;

CONCLUSION

- ▶ In this paper, we have formulated spoofing detection as a sparse signal processing;
- ▶ Based on the SDR platform, we performed indoor experiments to verify this proposed spoofing detection scheme;
- ▶ The experimental results on real measured data show that our sparse signal processing can easily distinguish the attack from normal situation.

Thank You! & Questions?