Brief Industry Paper: HDAD: Hyperdimensional Computing-based Anomaly Detection for Automotive Sensor Attacks

Ruixuan Wang‡, Fanxin Kong§, Hasshi Sudler∗, Xun Jiao‡,
‡Villanova University, §Syracuse University, ∗Internet Think Tank

Hyperdimensional Computing

- **Hyperdimensional computing** (HDC) is an emerging computing scheme that leverages the abstract patterns and mathematical properties of vectors in high dimensional space, inspired by human brain functionality.
- HDC works with hypervectors (HV), which are high dimensional (e.g., 10000), holographic vectors with i.i.d.
- There're three **basic operations**, **Addition**, **Multiplication** and **Permutation** and three **core modules Encoding**, **Training** and **Inference** in HDC.

Basic operations:

Addition: perform element-wise add between two HVs

$$\vec{H}_p + \vec{H}_q = \langle h_{p1} + h_{q1}, h_{p2} + h_{q2}, \ldots, h_{pn} + h_{qn} \rangle$$

Multiplication: perform element-wise multiply between two HVs

$$\vec{H}_p * \vec{H}_q = \langle h_{p1} * h_{q1}, h_{p2} * h_{q2}, \ldots, h_{pn} * h_{qn} \rangle$$

Permutation: perform a circular shifting over a HV

$$\rho_1(\vec{H}) = \langle h_n, h_1, h_2, \ldots, h_{n-1} \rangle$$

Core Modules:

Encoding: Project feature data into hyperdimensional space

$$\vec{H} = E(\mathcal{R}, \vec{F}) = E(\mathcal{R}_1[f_1], \mathcal{R}_2[f_2], \ldots, \mathcal{R}_m[f_m])$$

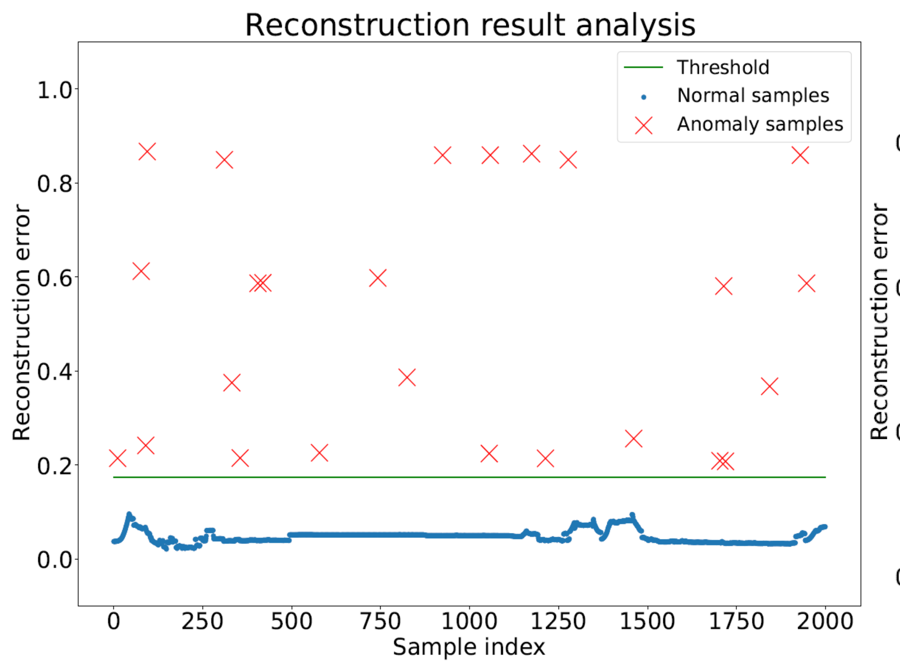
Training: Aggregating HVs with same label to build a classifier

$$\mathcal{A} = \{\vec{A}^1, \vec{A}^2, \ldots, \vec{A}^k\} = \{\sum \vec{H}^1, \sum \vec{H}^2, \ldots, \sum \vec{H}^k\}$$

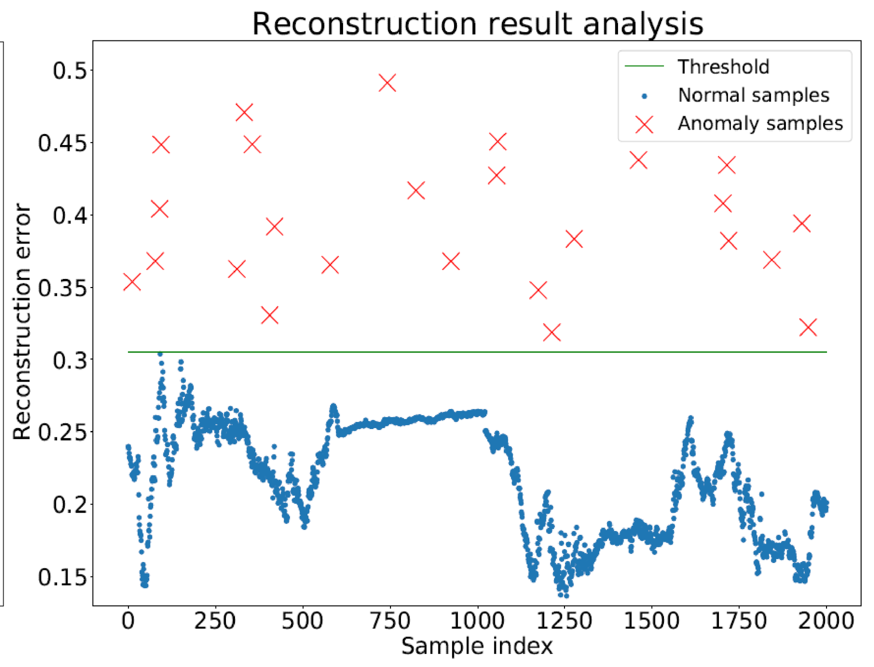
Inference: Deploy similarity check to determine the prediction result

$$l = argmax(\{\delta(\vec{H}_q, \vec{A}^1), \delta(\vec{H}_q, \vec{A}^2), \ldots, \delta(\vec{H}_q, \vec{A}^k)\})$$

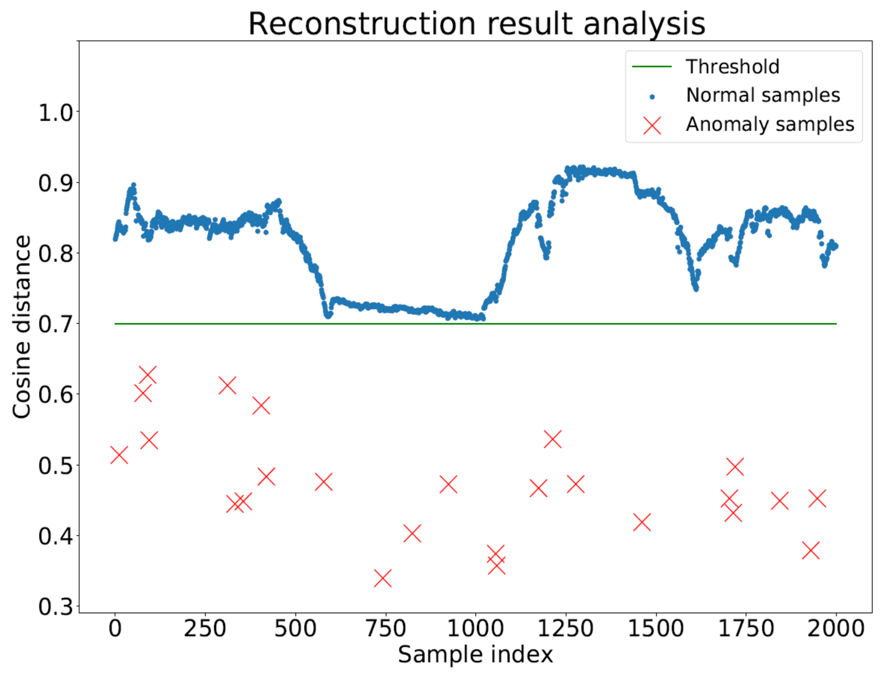
Experiment Results & Analysis



Reconstruction result (MSE distance)



Reconstruction result (MAE distance)

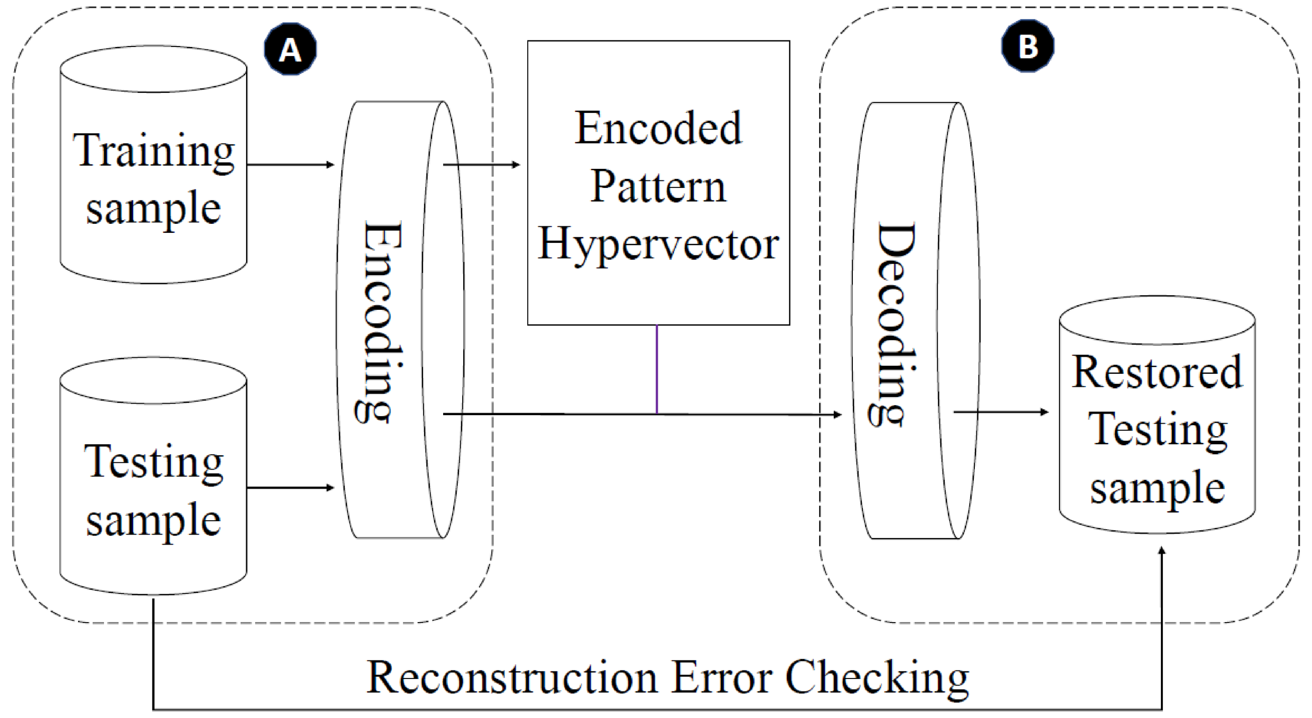


Reconstruction result (SIM distance)

Motivation

- Potential security vulnerabilities have been exposed since the growing connectivity and autonomy of modern vehicles.
- Multiple sensors on a vehicle can simultaneously respond to the same physical feature in a correlated manner. Meanwhile, the inherent correlation neither depends on the background knowledge nor has the cost increased by redundant sensors.
- Based on the observation, we propose to identify the consistency embedded in correlated data and use it for anomaly detection.
- **HDAD:** hyperdimensional computing (HDC)-based anomaly detection method

HDAD Structure Overview



HDAD anomaly detection with two key phases:

- **Pattern encoding**, where we encode training samples into hypervectors (HVs) for the pattern learning purpose.
- **Pattern decoding**, where we decode the HVs and reconstruct them to the original samples.
- After we finishing decoding, we do a reconstruction error check, where we check the reconstruction error between original and reconstructed sample.

The anomaly detection result are shown as above. For the First observation, we find all three distance models can achieve 100% anomaly detection accuracy, as all the anomaly samples and normal samples can be clearly separated by the calculated threshold.

For MSE-based and MAE-based models, the reconstruction errors of all anomalous samples, are higher than the calculated threshold. And for the cosine similarity-based detection, with a predefined threshold of 0.7, all the reconstructed anomaly samples have smaller similarity to their original patterns, but all the normal samples have higher similarity to their original patterns.

Conclusion & Future Works

- This paper presents HDAD, an anomaly detection approach based on the emerging HDC
- **This paper presents the first effort in using HDC for anomaly detection** and the promising result opens the door for this potential research direction. In our approach, **HDAD can achieve 100% detection accuracy** on a real-world vehicle sensors reading dataset.
- Our future work will consider using HDC for sample clustering or feature extraction and even use it for anomaly detection under more complected scenarios.