CERIAS

The Center for Education and Research in Information Assurance and Security

Directed Infusion of Data (DIOD) for Secure Data Transfer

Tyler Lewis, Arvind Sundaram, Hany S. Abdel-Khalik, Purdue University
Ahmad Y. Al Rashdan, Idaho National Laboratory

Introduction

- Data informatics has revolutionized critical infrastructure using **artificial intelligence** and **machine learning**
- AI/ML is a **double-edged sword** – the information they rely on can be used against them
- System owners are **reluctant** to share data due to concerns of **reverse-engineering** and **data leaks**.
- Need for a data masking methodology that prevents AI and data analysts from being **overly inquisitive**, i.e., must only extract relevant info.
- Existing data masking methodologies are **unsuitable** for industrial data – significant computational overhead and do not preserve physical properties.

Directed Infusion of Data

- Novel data masking paradigm that preserves AI-relevant information and discards proprietary details
- Masked data possesses the same inferential properties as the original, but cannot be tied to the proprietary system – transformation is **utility-preserving**
- Methodology can be **fine-tuned** to the needs of a variety of AI/ML applications
- Suitable to several data types and scenarios including timeseries, image data, audio data, and many more
- Similar techniques are broken by high-dimensional techniques – DIOD allows neural networks, complex classifiers, and non-linear techniques

Masking Nuclear Data

- Extracts information using a reduced order modelling techniques identifying two subsets of data
  - $\psi(x)$, the fundamental metadata – **identity of the system**
  - $\phi(\alpha)$, the inferential metadata – **inferentially-relevant** characteristics (e.g., variable dependencies, class labels, etc.)
- Masked data constructed by convoluting the subsets from the proprietary data and an unrelated, generic dataset

$$y_P(x,\alpha) \approx \sum_{i=1}^{r} \psi_i^P(x)\phi_i^P(\alpha)$$

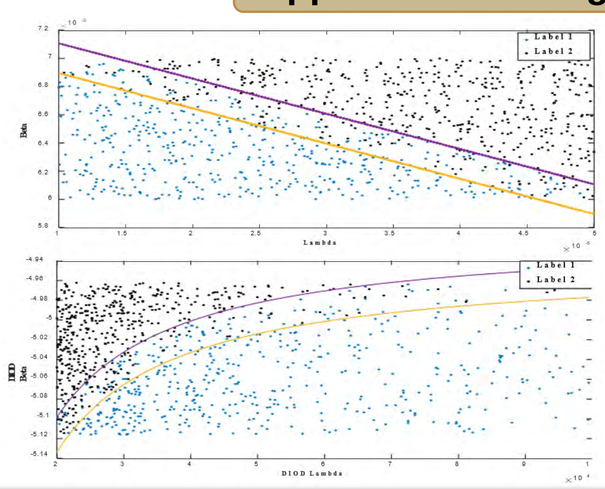
$$y_G(x',\alpha') \approx \sum_{i=1}^{r} \psi_i^G(x')\phi_i^G(\alpha')$$

$$y_D(x',\alpha) = \sum_{i=1}^{r} \psi_i^G(x')\phi_i^P(\alpha)$$

- **One-way transformation**: The original nuclear data cannot be recovered from the modified data
- Requires a **one-time computational cost** for data decomposition and can be **efficiently scaled** to large number of datasets for subsequent transformations.
- Generic data can be any unrelated set of data – from images of animals, to pop songs, to similar timeseries.
- Utilizes **mutual information** to assess results;

Applications & Ongoing Work

- Masked Data gives **equivalent inference** to original data
- Returns the same solution for problems like condition monitoring and regression
- Extensions of DIOD to condition monitoring problems, linear dynamics and securely generate synthetic data
- Current work investigates control problems with DIOD



This work was supported by the Idaho National Laboratory and the Light Water Sustainability Program

Related Work:

1. Arvind Sundaram, Hany S. Abdel-Khalik, and Ahmad Al Rashdan, “Deceptive Infusion of Data (DIOD): A Novel Data Masking Paradigm for High-Valued Systems,” *Nuclear Science and Engineering*, 2022.
2. Arvind Sundaram, Hany S. Abdel-Khalik, and Mohammad Abdo “Preventing Reverse-Engineering of Critical Industrial Data with DIOD,” *Nuclear Technology*, 2022.
3. Ahmad Al Rashdan, Arvind Sundaram, Tyler Lewis, and Hany S. Abdel-Khalik, “A Novel Data Obfuscation Method to Share Nuclear Data for Machine Learning Application”, *Light Water Reactor Sustainability Program*, INL/RPT-22-69871, 2022.

PURDUE UNIVERSITY

CERIAS