Low-Cost, High-Throughput Cyber-Physical Synthesis of Encrypted DNA

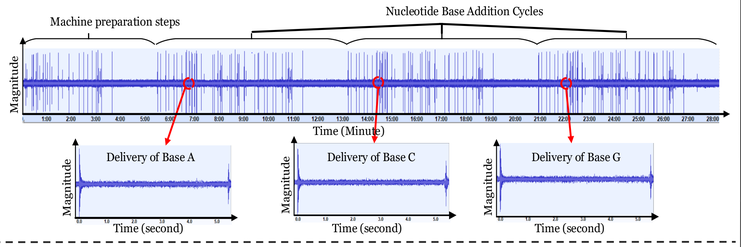
Sina Faezi*, Sujit Chhetri*, Arnav Malawade*, William Grover**, Philip Brisk**,
Deepan Muthirayan*, Pramod Khargonekar*, Mohammad Al Faruque*

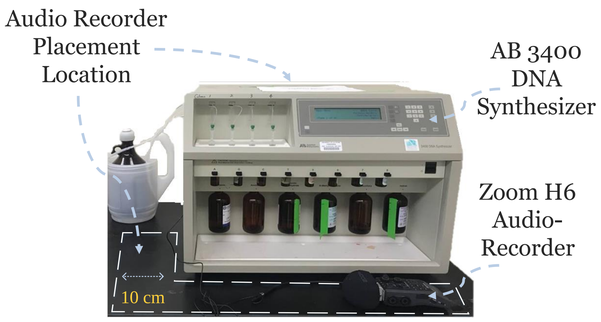
*University of California Irvine **University of California Riverside

Acoustic Side Channel Attacks on DNA Synthesizers

Overview

In this project we propose and implement a novel, acoustic side- channel attack methodology on DNA synthesizers to steal the type and order of the bases which are synthesized. This vulnerability can lead to the theft of intellectual property and financial loss.



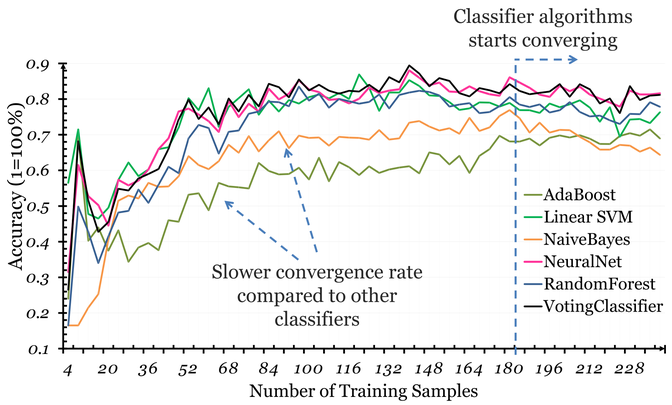


Our test bed

Methodology

DNA Synthesizer Use Cases: Crop optimization, drug discovery, medical treatment, data storage, etc.
Security Concerns: bioterrorism, confidentiality of synthesized DNA.
Key Observations: Solenoid valves and fluid pipes (which generate acoustic noise) are in asymmetric spatial locations inside the machine.

Results



- **88.07%** average random base classification accuracy.
- Robust to common noise in the environment.
- Postprocessing tools (e.g., **BLAST**) compensate for errors.

Broader Impact

- This work raises awareness among the bioengineering community to consider the possibility of a new set of attacks against the confidentiality of DNA synthesizers.
- Similar attack methods could potentially be used to breach the confidentiality of other information sensitive bioCPS tools.
- We show the potential for a government agency to non-intrusively monitor the synthesis of DNA by malicious parties to prevent large scale bioterrorist attacks.

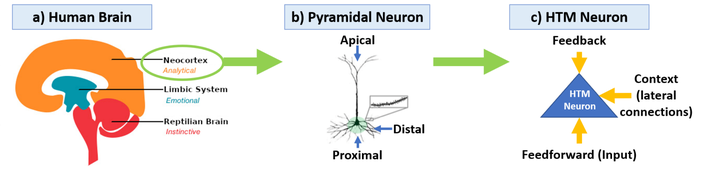
Related Publication

Faezi, S. , Chhetri, S. R., Malawade, A. V., Chaput, J., Grover, W. H., Brisk, P., and Al Faruque, M. A.. “Oligo-Snoop: A Non-Invasive Side Channel Attack Against DNA Synthesis Machines” accepted to be published in The Network and Distributed System Security Symposium (NDSS’ 2019)

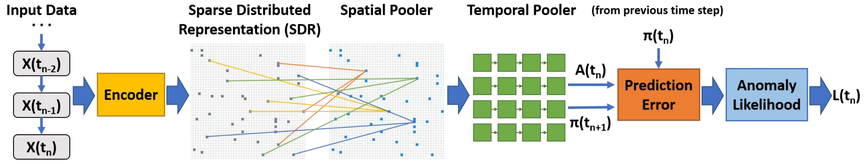
Neuroscience-Inspired Algorithms for Predictive Maintenance

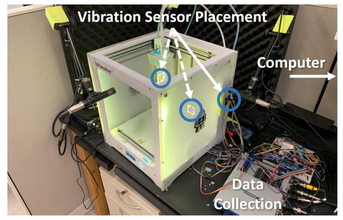
Overview

In this project we propose a method of performing online, real-time anomaly detection algorithm for the predictive maintenance of manufacturing systems using Hierarchical Temporal Memory (HTM), inspired by the human neocortex.



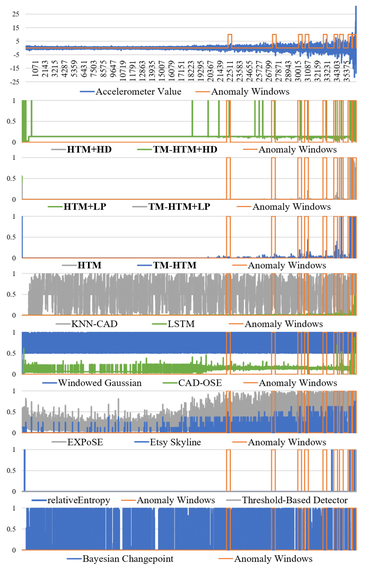
Methodology





Experiments: We evaluate our methodology at preemptively detecting real-world bearing failures and synthesized 3D printer failures from vibration data.
Anomaly Detection: anomalies manifest in sensor data before component failures occur.
Challenges: bearing vibration signals are non-stationary, making statistical methods ineffective. Noise is also significant in manufacturing environments. Typical solutions are also domain-specific and not generalizable.
Benefits of HTM: efficient online learning, robust to noise, generalizes across applications without fine tuning

Results



- On the Numenta Anomaly Benchmark, HTM scores **64.71**, beating the state-of-the-art deep-learning (49.38) and statistical (61.06) methods.
- HTM is more robust to noise than other methods
- HTM can learn and perform well from a single pass while LSTM requires 1000 epochs.

Anomaly Detector	Scoring Profile			Runtime (s)
	Standard	Low FN	Low FP	
TM-HTM+HD (Ours)	**67.05**	**73.33**	56.57	4728
HTM+HD (Ours)	66.38	71.93	55.33	5792
Windowed Gaussian	64.75	70.50	57.35	336
HTM+LP (Ours)	64.03	69.12	**57.47**	21084
HTM (Ours)	59.75	66.24	47.63	4277
TM-HTM+LP (Ours)	54.12	61.53	43.03	18508
TM-HTM (Ours)	54.39	63.33	32.47	3156
Etsy Skyline [35]	47.53	51.51	43.75	742632
CAD-OSE [33]	46.88	52.81	40.96	3589
EXPoSE [32]	41.75	44.80	36.96	5575
Threshold-Based	37.75	43.75	25.21	125
Relative Entropy [34]	34.97	37.05	32.94	806
LSTM [31]	33.99	38.13	28.38	43698
KNN-CAD [36]	32.31	43.06	4.69	4393
Random	3.06	9.16	0.00	233
BC [37]	0.00	0.00	0.00	10270
Null	0.00	0.00	0.00	235

TABLE I
NORMALIZED NAB SCORES FOR ANOMALY DETECTION ON THE BEARING FAILURE DATASET.

Broader Impact

- HTM is a practical solution for real-world predictive maintenance as it is domain agnostic, robust to noise, and can learn efficiently and continuously on consumer hardware.
- HTM is able to effectively model non-stationary signals from complex multi-axis systems such as the 3D printer, which are conventionally difficult to model.

Related Publication

Malawade, A. V., Costa, N. D., Muthirayan, D., Khargonekar, P. P., & Al Faruque, M. A.. “Neuroscience-Inspired Algorithms for the Predictive Maintenance of Manufacturing Systems,” published in *IEEE Transactions on Industrial Informatics* (TII’ 2021).

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: CMMI 1739503