VirginiaTech
Invent the Future

Emerging Applications of Reservoir Computing in Cyber Physical Systems Security

Kian Hamedani
PhD Student

Committee Members: Dr. Marius K. Orlowski(chair), Dr. Lingjia Liu, Dr. Yang (Cindy) Yi

Department of ECE, Virginia Tech
PhD Qualifying Exam : April 25th, 2018

Outline

- Biological Neural Networks
- Artificial Neural Networks
- Recurrent Neural Networks(RNNs)
- Reservoir Computing
- Attack Detection in Smart Grids
- Face Recognition
- Future Steps
- Conclusion

Biological Neuron

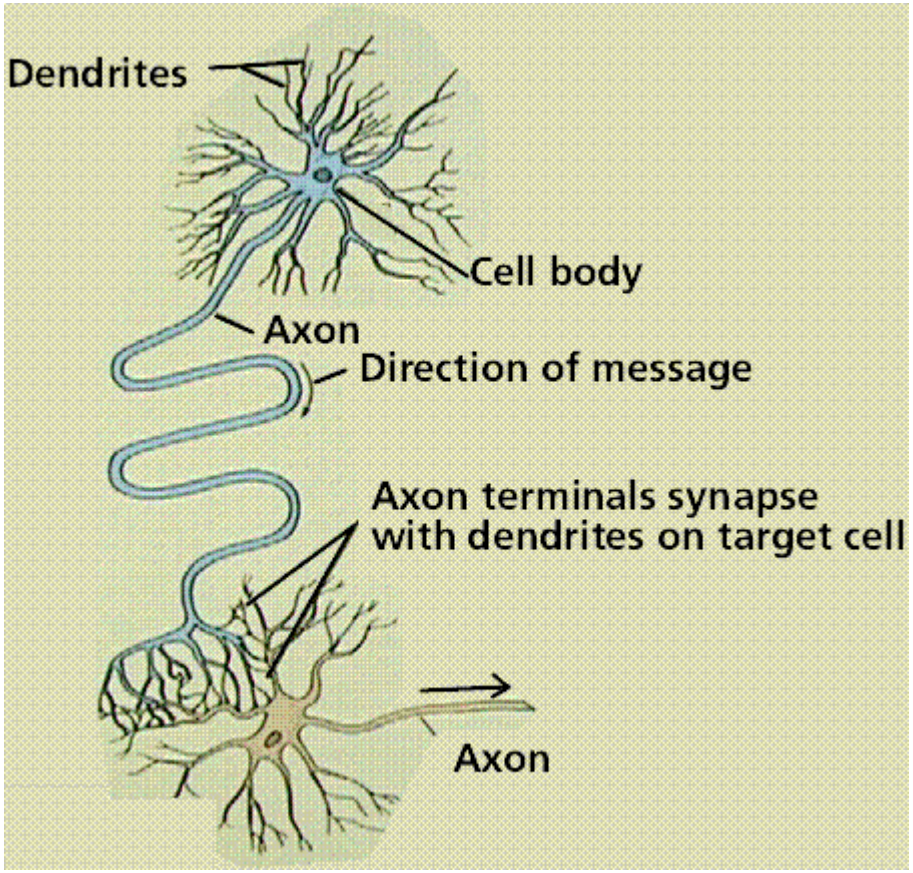
- A cell that specializes in communication
- A neuron:

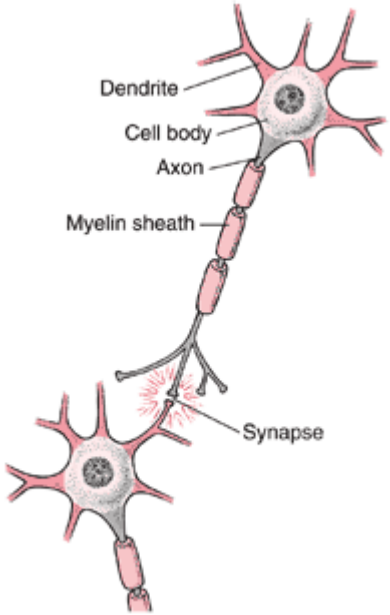
  a) receives information from other neurons, through its *dendrites*

  b) integrates those signals, and

  c) sends messages to other neurons through its *terminal buttons*

Biological Neuron





VirginiaTech
Invent the Future

Biological Neurons

- *dendrites* - the receivers
- *soma* - neuron cell body (sums input signals)
- *axon* - the transmitter
- *synapse* - point of transmission
- neuron activates after a certain *threshold* is met

Learning occurs via electro-chemical changes in effectiveness of *synaptic junction*.

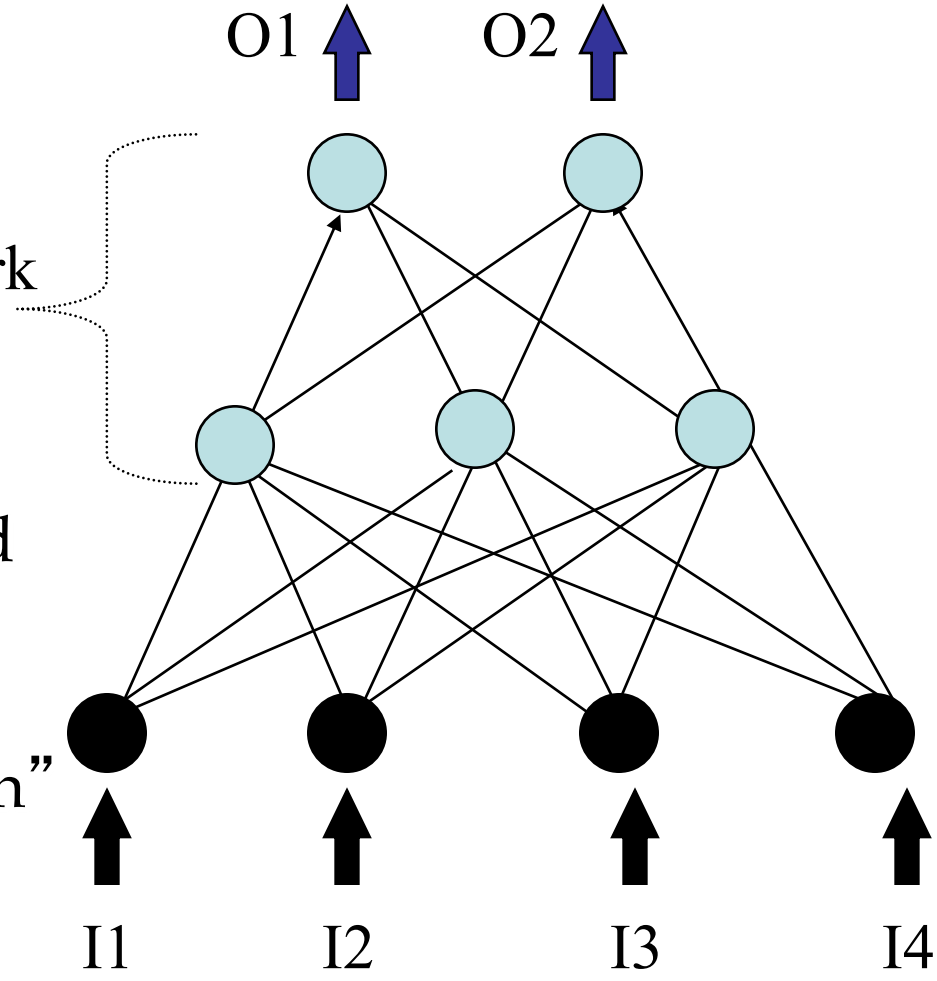
Artificial Neural Networks

Inherent Advantages of the Brain:

"distributed processing and representation"

- Parallel processing speeds
- Fault tolerance
- Graceful degradation
- Ability to generalize

Artificial Neural Networks



VirginiaTech
Invent the Future

Artificial Neural Networks

- Widrow-Hoff or Delta Rule for Weight Modification

$$w_i(t+1)=w_i(t)+\Delta w_i \quad \Delta w_i=\eta d x_i(t)$$

Where:

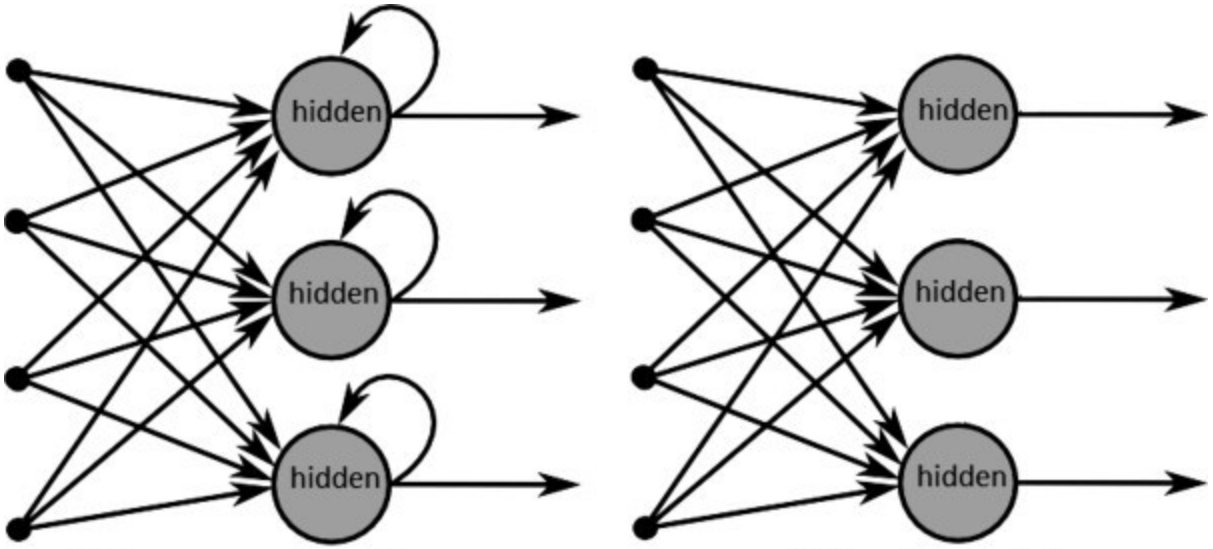
η = *learning rate* ($o < \eta <= 1$), typically set = *0.1*

d = *error signal* = desired output - network output

= $t - y$

VirginiaTech
Invent the Future

RNNs



(a) Recurrent neural network

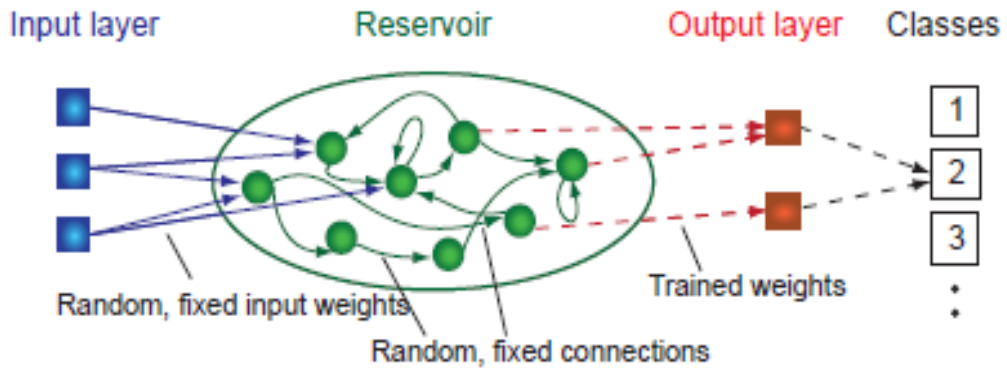
(b) Forward neural network

Recurrent neural networks (RNNs) are capable of exploiting the underlying correlation within the data.

Reservoir Computing

- In general, a typical RC system is composed of three different layers.
- The first layer is the input layer, the second one is the reservoir composing of randomly connected, and the final layer is called the readout layer.
- Output layer uses a linear combination of the reservoirs to produce the desired output.
- It has been shown in many cases that RC systems have shown better performance than the traditional RNNs .

Reservoir Computing



$$\widehat{y(k)} = \sum_{i=1}^{N} w_i . x\left[k\tau - \frac{\tau}{N}(N - i)\right]$$

Liquid state machine (LSM) and echo state networks (ESN) are two most popular RC systems.

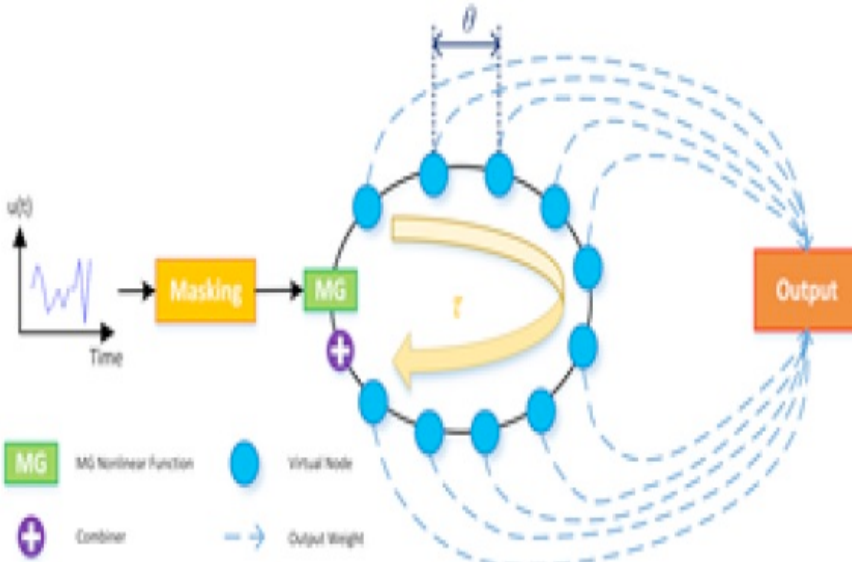
Reservoir Computing

- Create random weight matrices
- Rescale reservoir weights so that max absolute eigenvalue close to one (edge of stability)
- Excite reservoir with input and record all states
- Train readouts by minimizing $(Aw-b)^2$

Delayed Feedback Network

Delay exists in almost all the with dynamics.
Inevitably, delays may even occur in the brains when information is transmitted from one neuron to the other.

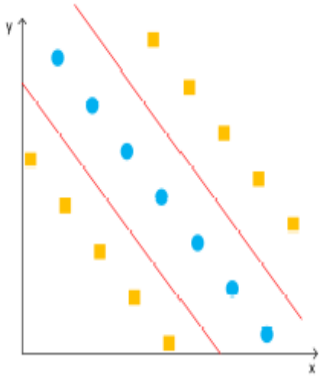
Delay differential equations are used to mathematically represent the delayed systems.

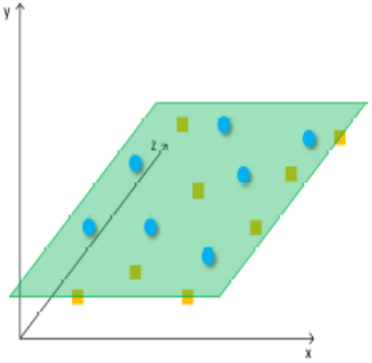


For any delayed systems, the dynamics of the system depends not only on the current states but also the previous states

Delayed Feedback Network

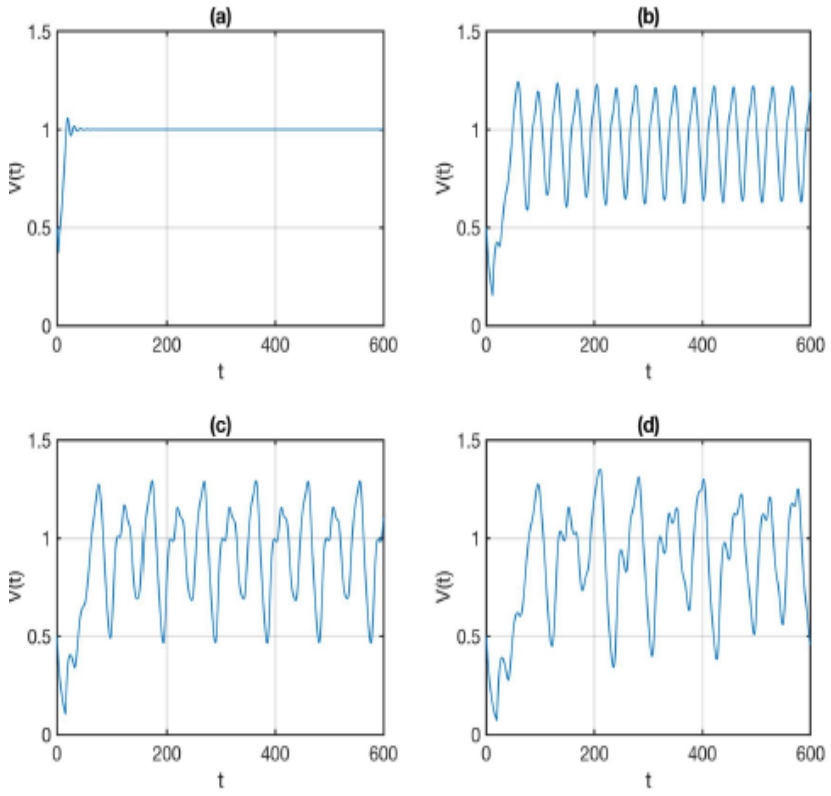
Applying DFR on the data will map it to a higher dimensional space that makes the data linearly separable



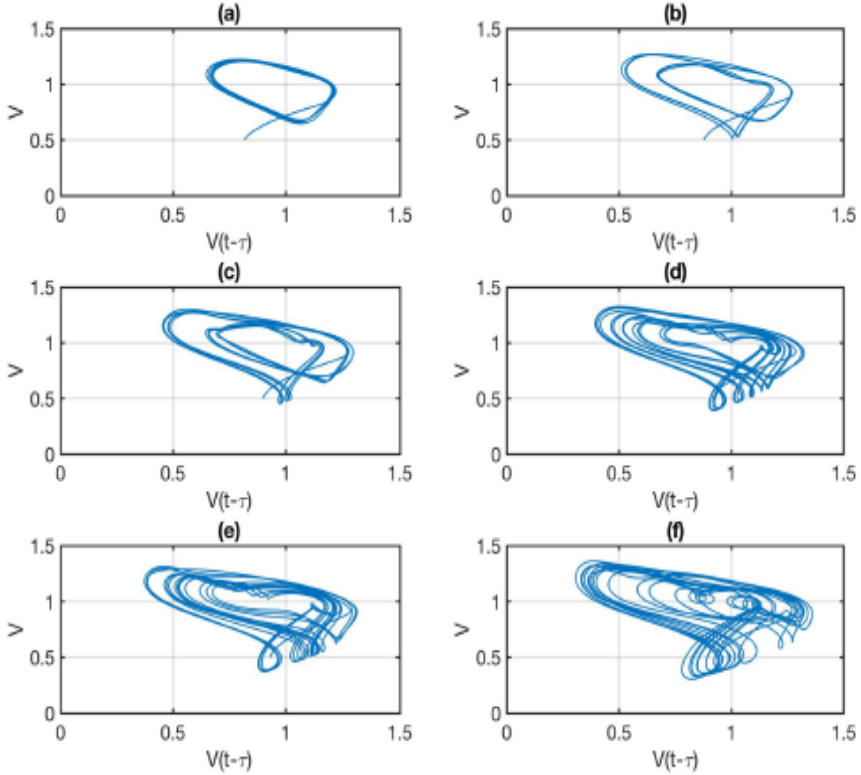


Several studies have shown that the Lyapunov dimension of a chaos system directly corresponds to the delay of the loop

Delayed Feedback Network



Dynamic Behavior of nonlinear

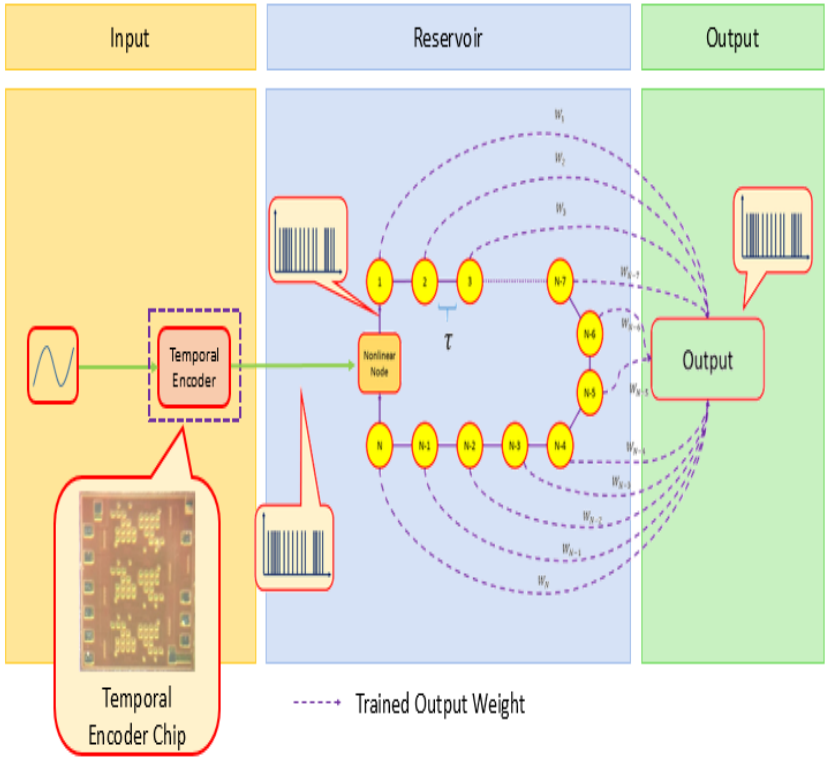


Phase Portrait of Dynamic System

VirginiaTech
Invent the Future

Delayed Feedback Network

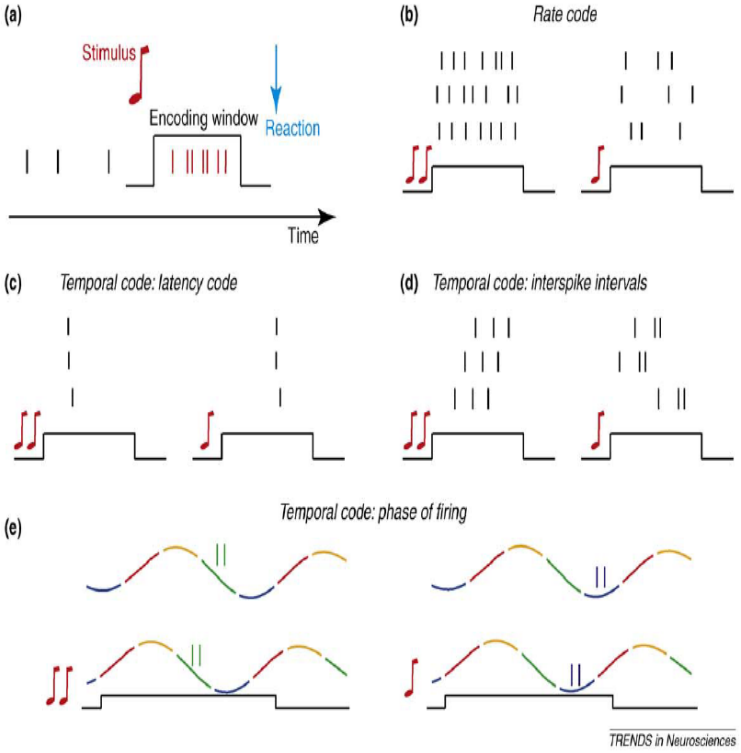
- The input will be injected directly to the nonlinear node. In order to compensate the loss of parallelism.
- There are several choices for the nonlinear node, but, since we have to deal with spikes, due to their energy efficiency, the input node of the reservoir layer will be a leaky-integrate and fire (LIF) neuron .



VirginiaTech
Invent the Future

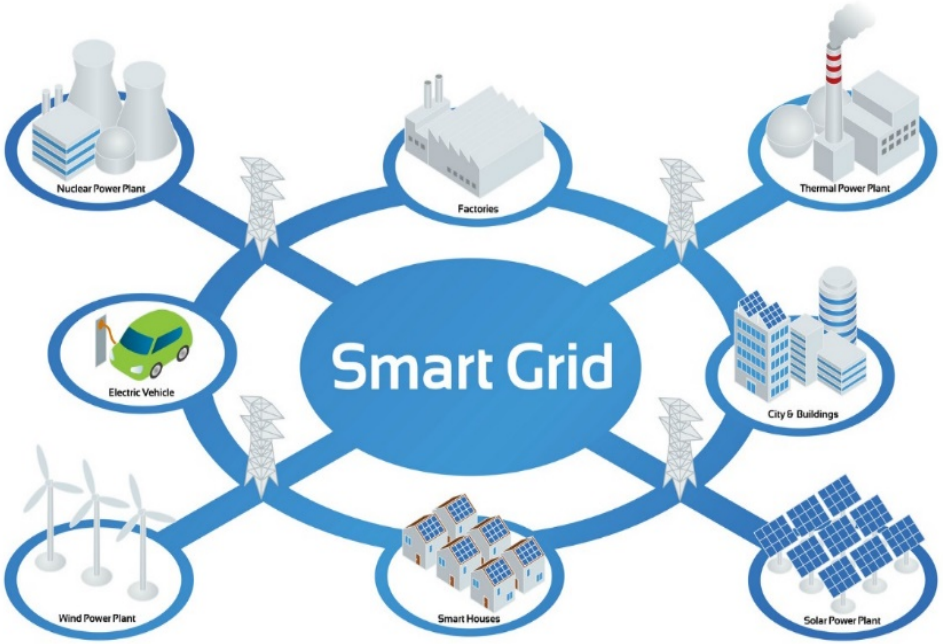
Neural Encoding

- There have been several schemes proposed to encode the neural information.
- Rate encoding and temporal encoding are the two mostly schemes .
- Temporal encoding is subdivided into three main groups including: latency code, interspike intervals and phase of firing .
- In rate encoding a code consists of a number of spikes occurring in a time frame after the stimulus appears .
- In temporal encoding based on latency code, the time in which the first spike occurs is used for encoding.
- Interspike interval coding is another scheme that uses the intervals between different spikes for encoding



Smart Grids

- Smart grids are to make a reliable power transmission network and connection between consumers and generators.
- They are really vulnerable to cyber-attacks, and thus it is a very important and challenging task to provide a secure network of the smart grids.
- MATPOWER 5.1 has been used to produce the smart grids measurement matrix.
- MATPOWER allows the users to run the toolbox with different numbers of buses.



VirginiaTech
Invent the Future

Smart Grid Attack Formulation

- $z = Hx + n$
- The measurement vector which is the output of different net meters on the buses is stated as z.
- H corresponds to the state vector,
- $x$is the voltage phase of the buses
- and n is the environment noise

Smart Grid Attack Formulation

- $\check{z} = Hx + a + n$
- One of the first algorithms which was introduced to deal with FDI problem is called State Vector Estimation (SVE).
- What is done in that method is that a residual stated as ρ is calculated.
- If the value of ρ exceeds a threshold value, it is said that the z vector has been attacked .
- $\rho = \|\check{z} - H\hat{x}\|_2^2$

Smart Grid Attack Formulation

- $\hat{x} = (H^T \Lambda H)^{-1} H^T \Lambda z$
- In case $a = HC$, the attack would be hidden.
- $\rho = \|\check{z} - H\hat{x}\|$
- $= \|z + a - H(x + (H^T \Lambda H)^{-1} H^T \Lambda a)\|$
- $= \|z - Hx + (HC - H(H^T \Lambda H)^{-1} H^T \Lambda HC)\|$
- $= \|z - Hx + (HC - HC)\|$
- $= \|z - Hx\| \leq \tau$

Smart Grid Attack Detection using DFN and MLP

- FDI problem can also be formulated as a classification problem.
- In this experiment, two different sets of data were used.
- The data which has been attacked by hidden attack and the data which its measurements have been attacked by direct or not-hidden attack vectors.
- The experiments were performed on 1000 samples for every experiments and the experiments were repeated 10 times, which runs totally 10000 times

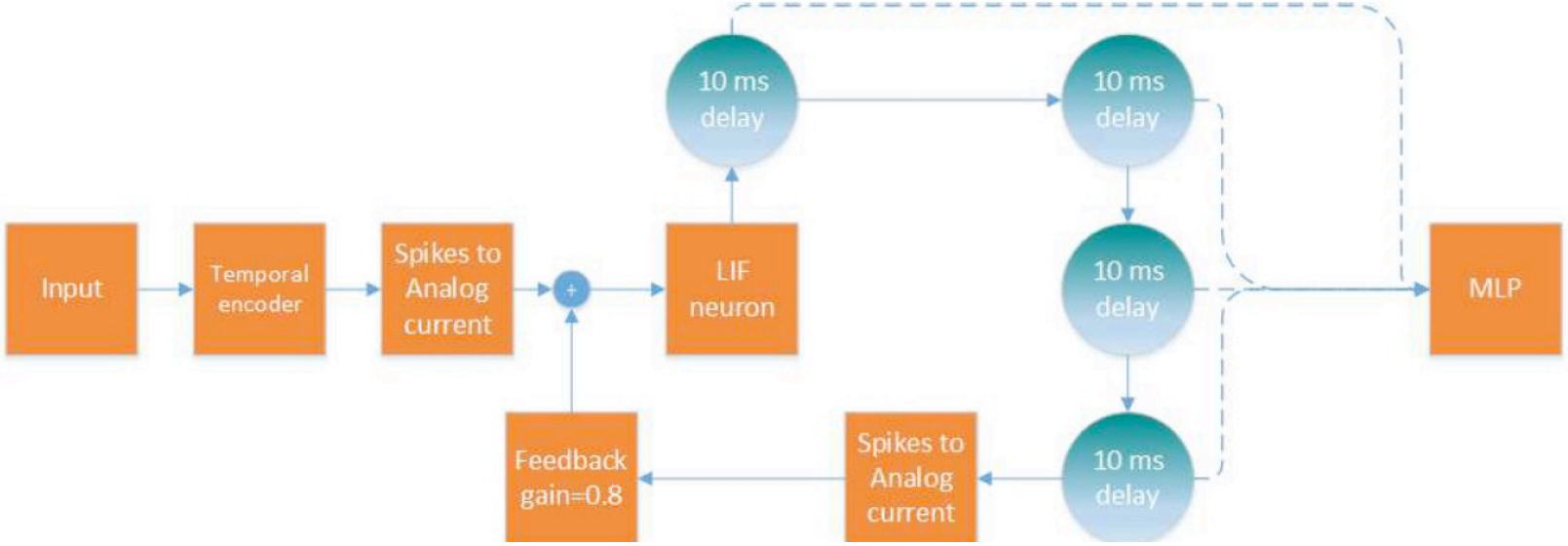
Smart Grid Attack Detection using DFN and MLP

- The first step is to encode the z using temporal encoder.
- After that every spike train extracted from the temporal encoder has to be converted to an analog current.
- $I^i = \sum_{tj} K\left(t - t^j\right) H\left(t - t^j\right)$,
- where H is the Heaviside function
- I^i is the analog current of the, *i-th* sample in the z
- t^j is the time of occurrence of the *j-th* spike in the corresponding spike train of the *i-th* sample achieved from the temporal encoder

Smart Grid Attack Detection using DFN and MLP

- $K(t - t^j) = V_0 \cdot \left(exp - \left(\frac{t-t^j}{\tau_s}\right) - exp - \left(\frac{t-t^j}{\tau_f}\right)\right)$
- As it was mentioned before, the nonlinear node of the DFN is chosen as an LIF neuron.
- The analog current signals for the attacked samples and samples from the non-attacked sample were applied on the DFN.
- Then the output of the LIF neuron was shifted 10ms in time to produce the state of the first virtual node.

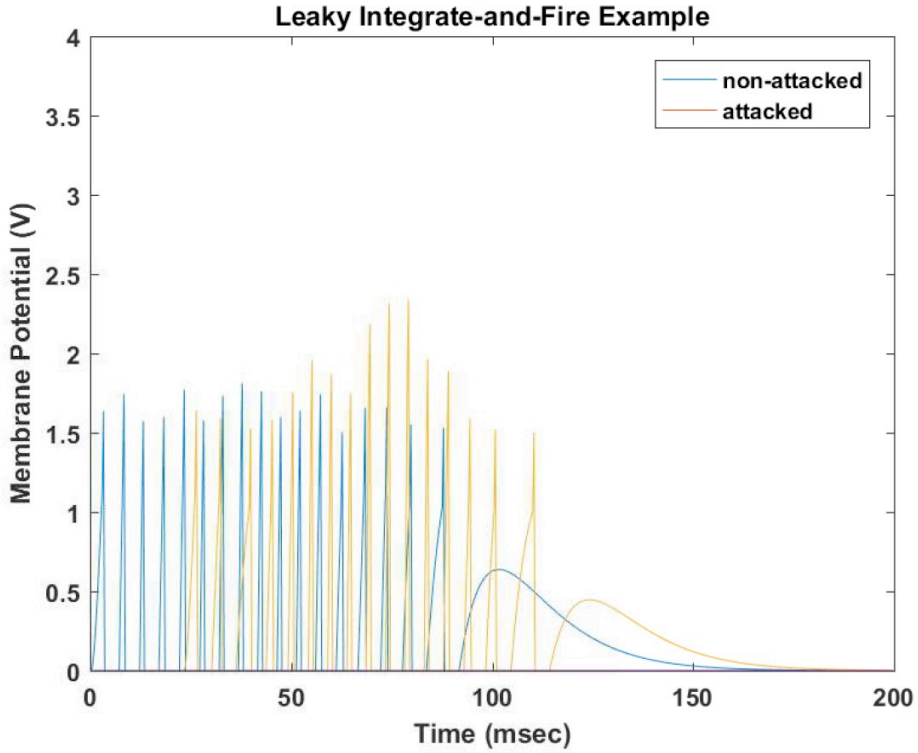
System Model



Hamedani, Kian, et al. "Reservoir Computing Meets Smart Grids: Attack Detection using Delayed Feedback Networks." *IEEE Transactions on Industrial Informatics* (2017).

VirginiaTech
Invent the Future

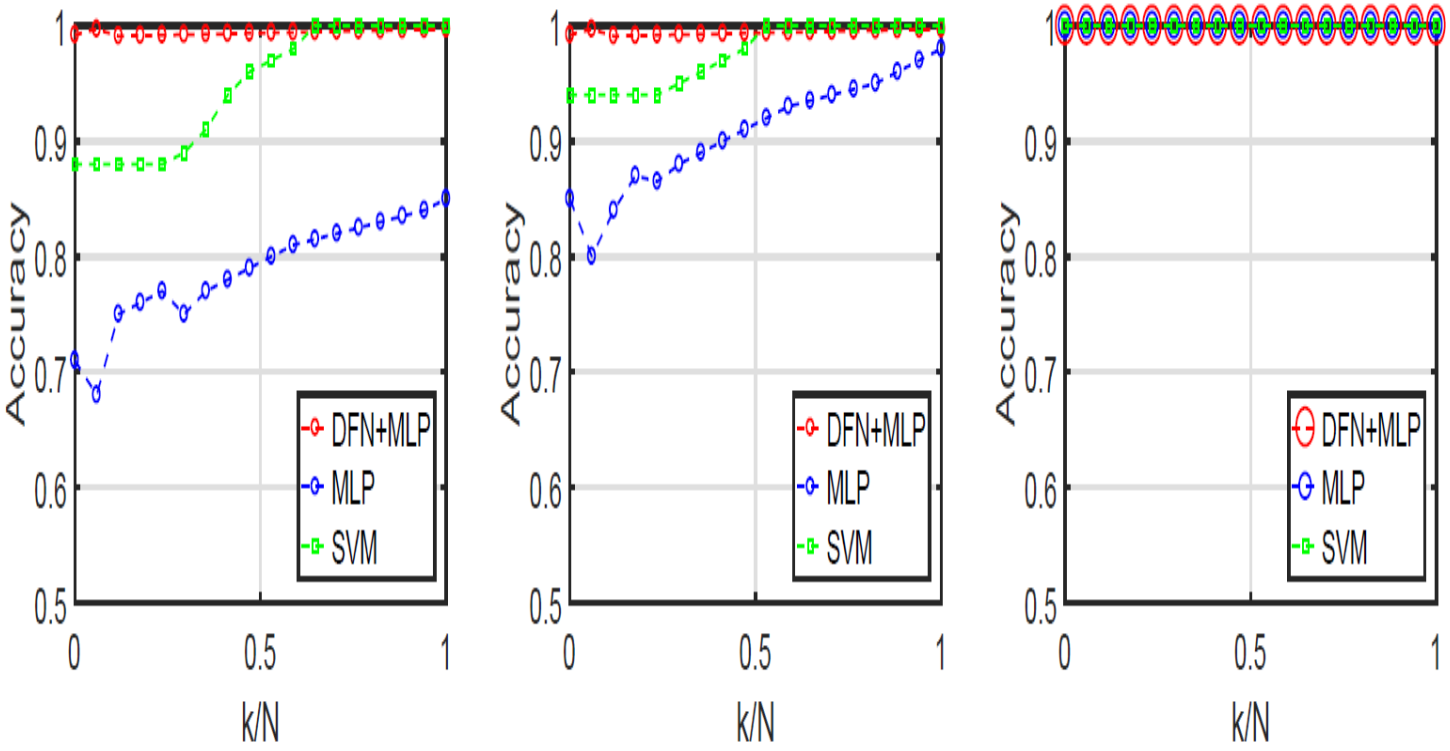
Simulation Results



$$\text{Accuracy} = (TP + TN) / (TP + TN + FP + FN)$$

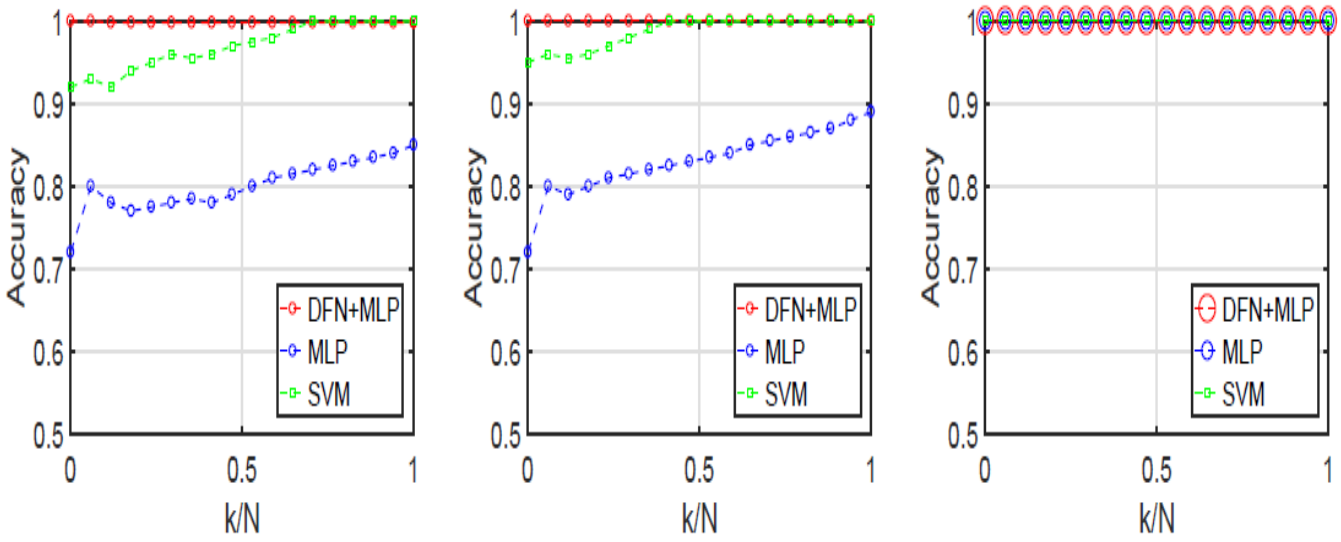
VirginiaTech
Invent the Future

Simulation Results



Accuracy of direct attack detection for three different methods, a=0.1,1,10.

Simulation Results



Accuracy of hidden attack detection for three different methods, a=0.1,1,10.

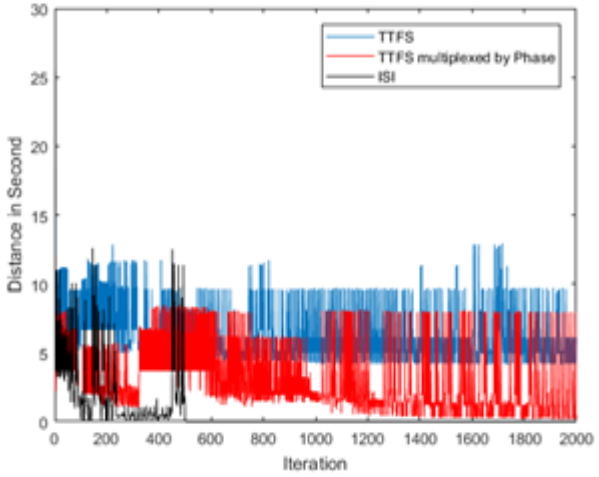
Smart Grid Attack Detection using DFN and Spiking Neural Networks

To make the system model more energy efficient, the read out layer will be a spiking neural networks layer.

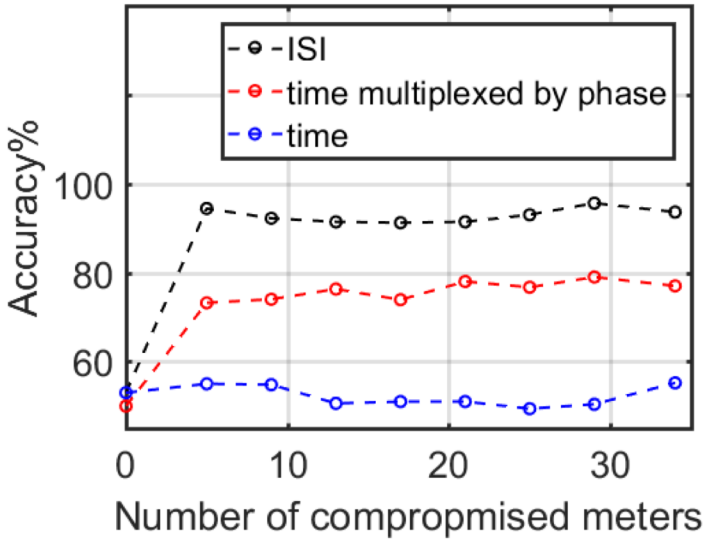
The attack model is dynamic, i.e.,

$$z(t) = H(x + 10cos(2\pi f_c t) \times N(0,1)) + n$$

Smart Grid Attack Detection using DFN and Spiking Neural Networks



Error(Distance) of training error



Attack Detection Accuracy

K. Hamedani, Lingjia Liu, Jialing Li, Shiyan HU and Yang Yi, "*Detecting Dynamic Attacks in Smart Grids: A Spiking Neural Network-Based Approach*", in Preparation.

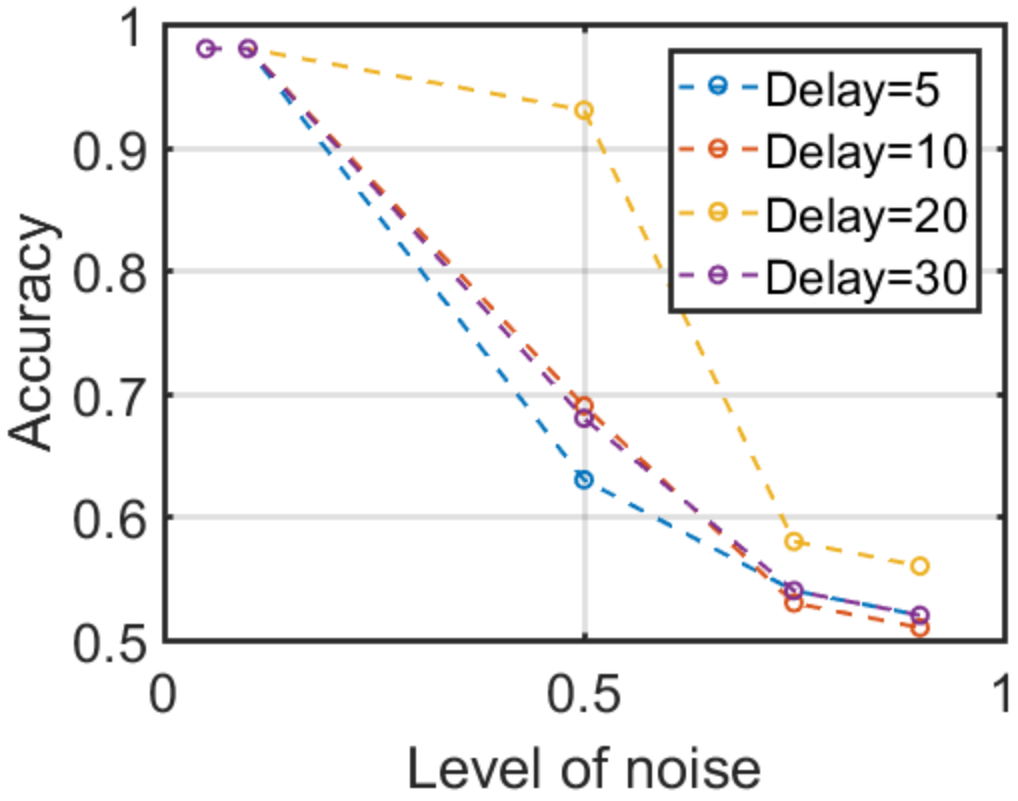
VirginiaTech
Invent the Future

Face Recognition using DFN and MLP

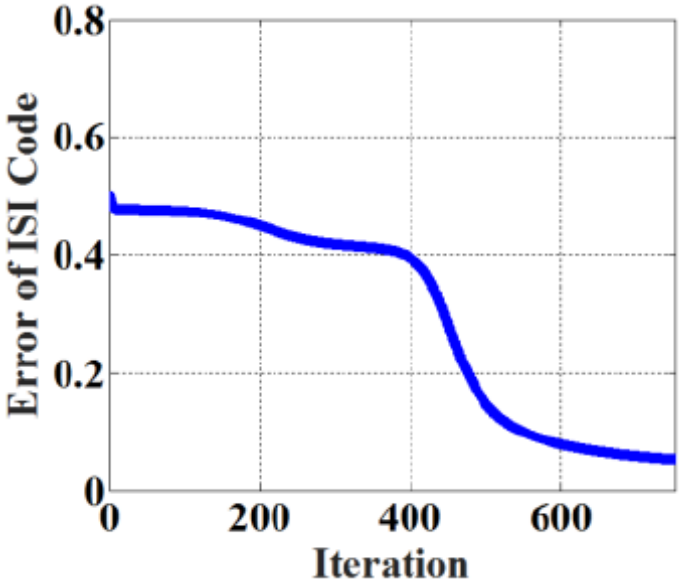
Zhao, Chenyuan, Kian Hamedani, Jialing Li, and Yang Yi. "Analog Spike-timing-dependent Resistive Crossbar Design for Brain Inspired Computing." *IEEE Journal on Emerging and Selected Topics in Circuits and Systems* (2017).

VirginiaTech
Invent the Future

Face Recognition using DFN and MLP



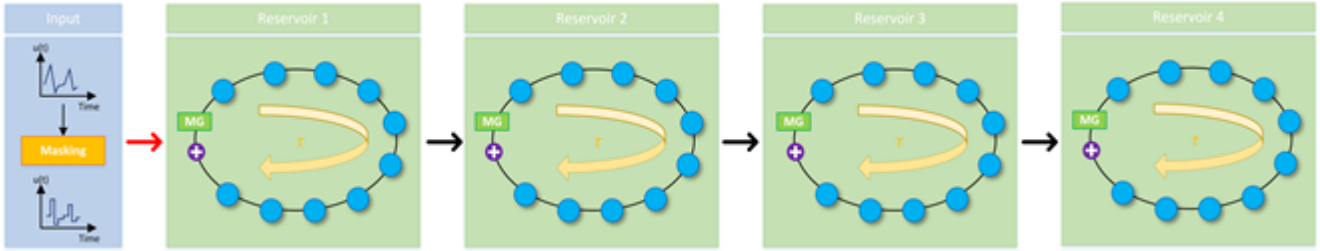
$$Test\ Accuracy = 1 - MSE,$$



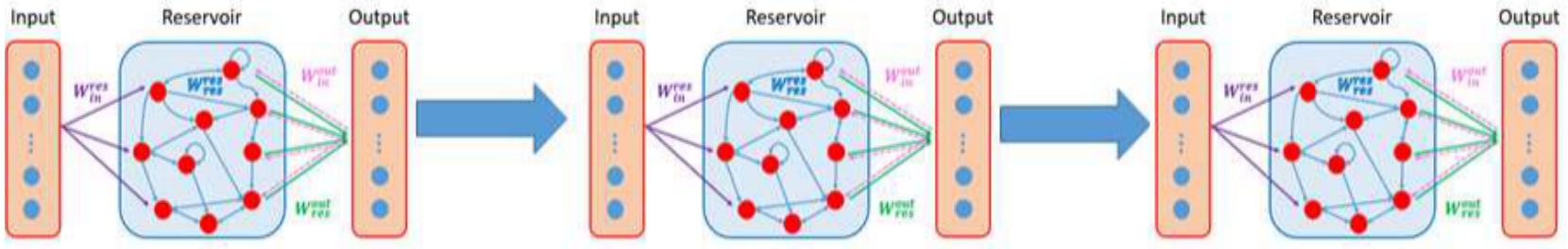
VirginiaTech
Invent the Future

Future Steps

- Applying Deep Structures of DFNs on more sophisticated attacks and in larger smarter grids.



- Implementing and applying Deep Structure of ESN



Future Steps

- Studying other domains of CPS cybersecurity like high performance computing (HPS) and internet of things (IoT)
- Applying the proposed networks on these domains.

Conclusion

- RC-based (DFN+MLP) attack detection strategy for smart grids is introduced.
- The introduced method constitutes of three main steps.
- Simulation results have shown that this algorithm can robustly detect attacks under different attack variations such as magnitudes and the number of compromised meters.
- In our next work we will show that we have been able to apply this model successfully on face recognition task from video frames
- Since there are spatio-temporal correlations among the meters in smart grids, RC-based attack detection can take full advantage of this spatio-temporal correlation yielding a better performance compared to existing solutions

Conclusion

- In the future steps, more complex attack models like dynamic attacks will be used.
- Deep structures of RC systems, like deep DFN or Deep ESN will be applied on more complex attack models in order to extract the spatio-temporal correlation among smart grid meters better.
- After that, other aspects of the CPS security, such as HPC systems security and IoT will also be studied and we will see if the proposed models for smart grids security are able to be applied on other security domains or not

Publications

- Hamedani, K., Liu, L., Atat, R., Wu, J., & Yi, Y. (2018). Reservoir computing meets smart grids: attack detection using delayed feedback networks. *IEEE Transactions on Industrial Informatics*, *14*(2), 734-743.
- Zhao, C., Hamedani, K., Li, J., & Yi, Y. (2018). Analog Spike-Timing-Dependent Resistive Crossbar Design for Brain Inspired Computing. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, *8*(1), 38-50.
- Li, J., Liu, L., Zhao, C., Hamedani, K., Atat, R., & Yi, Y. (2017). Enabling Sustainable Cyber Physical Security Systems Through Neuromorphic Computing. *IEEE Transactions on Sustainable Computing*.

Publications

- Li, J., Zhao, C., Hamedani, K., & Yi, Y. (2017, May). Analog hardware implementation of spike-based delayed feedback reservoir computing system. In *Neural Networks (IJCNN), 2017 International Joint Conference on* (pp. 3439-3446). IEEE.
- Bai, K., Li, J., Hamedani, K., & Yi, Yang (Cindy). (2017, June). Enabling a New Era of Brain-inspired Computing: Energy Efficient Analog Delayed Feedback Reservoir Computing System Design. Accepted , in *Design Automation Conference (DAC), 2018 55th ACM/EDAC/IEEE* . IEEE.

- K. Hamedani, Lingjia Liu, Jialing Li, Shiyan HU and Yang Yi, "*Detecting Dynamic Attacks in Smart Grids: A Spiking Neural Network-Based Approach*", in Preparation.

VirginiaTech
Invent the Future


Questions?