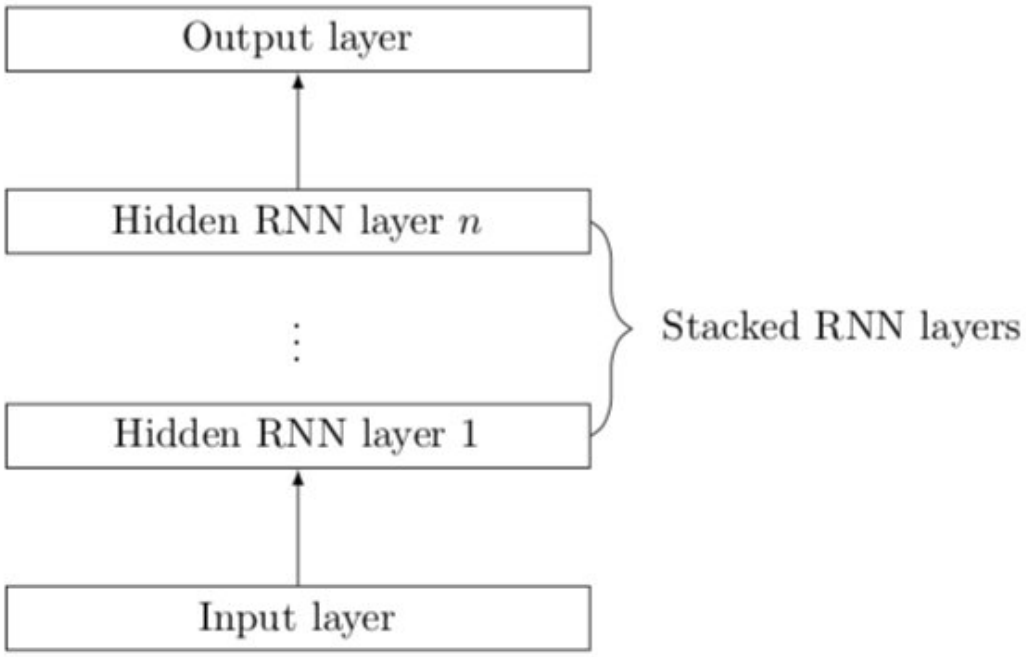
A new method to detect false data injection (FDI) attacks

January 22 2019, by Ingrid Fadelli



The architecture of the stacked RNN. Credit: Deng & Sun.

Researchers at Beijing Institute of Technology (BIT) have recently developed a new method to detect false data injection (FDI) attacks on critical infrastructure such as power grids. Their solution, outlined in a paper presented at the 44th Annual Conference of the IEEE Industrial

Electronics Society, uses a recurrent neural network (RNN) with several hidden layers, which is harder for FDI attacks to fool.

Cyber attacks on cyber physical systems (CPSs), particularly on infrastructure such as power grids, can cause significant chaos and disturbance for the people living in affected areas. For instance, in December 2015, the hack of a power grid in Ukraine affected over 230,000 people, leaving them without electricity for several hours.

While there are several existing methods to prevent cyber attacks, one particular type of attack, called false data injection (FDI), can bypass all conventional surveillance and security techniques. When successful, FDI attacks allow the attacker to compromise measurements from grid sensors, hindering a power grid's normal functioning and sometimes even damaging devices connected to it.

In recent years, researchers have been trying to develop effective tools to detect FDI attacks, to prevent them from causing serious infrastructural disruptions. Many of these recently developed methods employ machine learning techniques, such as supervised and semi-supervised learning algorithms.

Despite the promising results achieved by some of these approaches, most of them have a variety of flaws and limitations. For instance, some of these algorithms are prone to vulnerabilities exploited by variants of FDI attacks, while others cannot be effectively trained due to the limited amount of data related to real-world compromised measurements.

To address the limitations of existing tools for FDI detection, Qingyu Deng and Jian Sun, two researchers at BIT, developed a new method that uses a recurrent neural network (RNN) with several hidden layers. At the top of these hidden layers, the RNN has a fully-connected layer with a linear activation function.

Recent studies have found that RNNs can be particularly effective for time-series forecasting and anomaly detection, thus they could help to detect cyber-attacks. These prior findings are what encouraged Deng and Sun to develop an RNN that can detect FDI attacks.

"In this paper, we exploited the strong ability of recurrent neural networks (RNNs) on time-series prediction to recognize the potential compromised measurements," Deng and Sun wrote in their paper.

The RNN proposed by the researchers does not require labelled data to function and this makes it easier to apply in real-world scenarios. In an evaluation on the IEEE-14 bus test system, it attained remarkable results, effectively identifying compromised measurements with a small false alarm rate (FAR).

In the future, the RNN developed by Deng and Sun could help to detect FDI attacks on power grids and other critical infrastructure, preventing resulting issues, commotion and inconvenience. Further research could help to further develop the system, so it can achieve higher precision rates and a lower FAR.

More information: False data injection attack detection in a power grid using RNN. DOI: 10.1109/IECON.2018.8591079. ieeexplore.ieee.org/abstract/document/8591079