



Energy Fraud Detection

VITALY FORD

Smart Meter Data

- Source: Irish Social Science Data Archive Center [1]

Meter ID	Encoded date/time	Energy consumption value kWh
1392	19503	0.140
1392	19504	0.138
...
1187	22028	1.367
1187	22029	1.425
1392	19940	0.234

Energy Fraud

- Identify energy fraud
- Types of fraud
 - Unauthorized connection is established to a power line for stealing energy from another consumer
 - Consumer reports less energy consumed than actually used

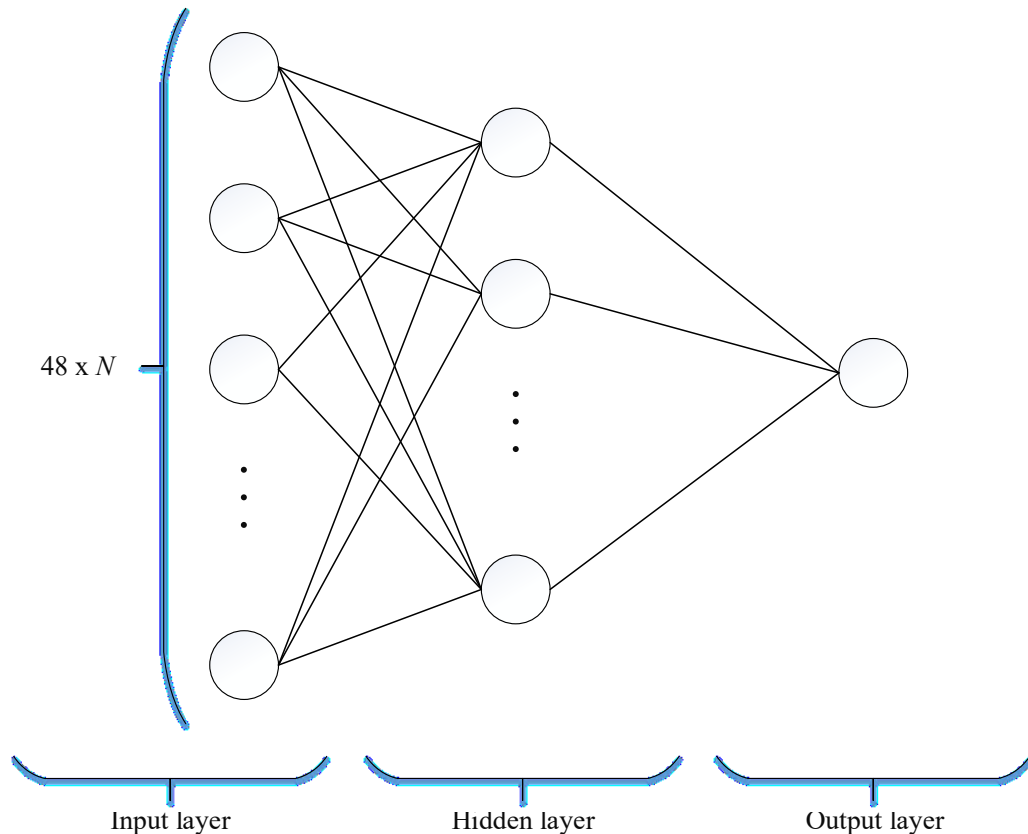
Fraud Simulation

- Random noise deviating from 0 to 0.5 kW/h (imitating the first type of the energy fraud)
- Random noise deviating from -0.5 to 0 kW/h (imitating the second type of the energy fraud)

Approach

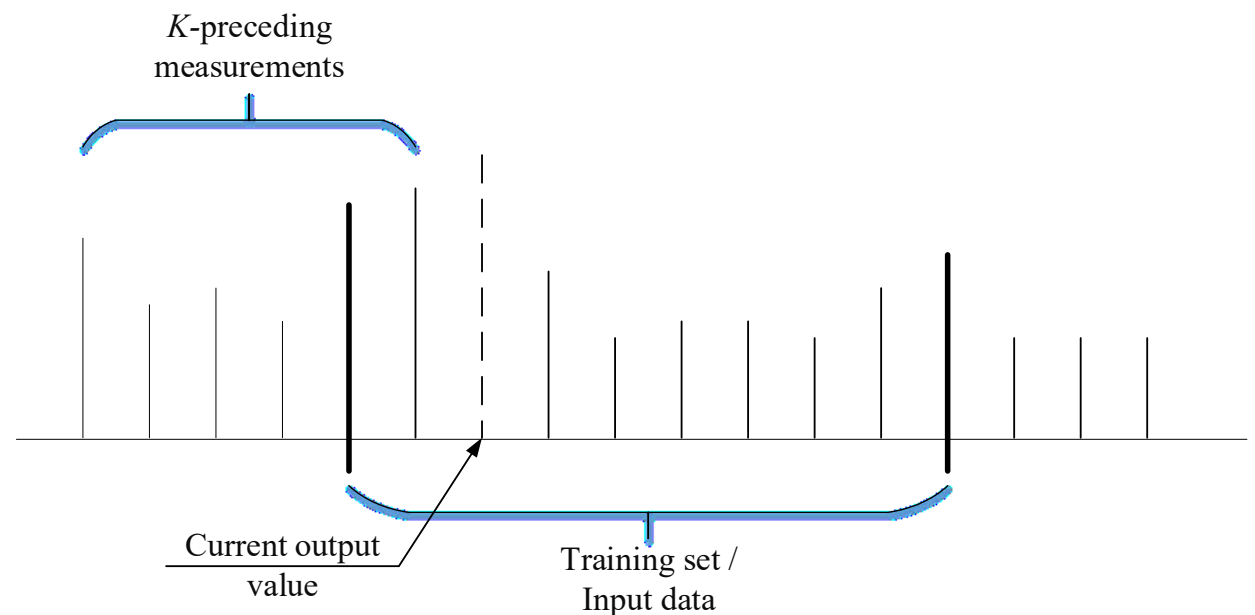
- Use of Decision Trees [2] and Artificial Neural Networks [3]
- Input: historical data representing three-day energy consumption
- Output: predicted energy consumption for the subsequent time frame

Approach (cont.)



Goal: build a model to predict energy consumption values, based on historical data.

Training set generation: for a known current output node value, the input layer nodes are generated by selecting K -consecutive preceding energy consumption measurements.



Confusion Matrix

Metric	Percentage
True Positives	93.75%
True Negatives	75.00%
False Positives	25.00%
False Negatives	6.25%

References

1. Commission for Energy Regulation, Irish Social Science Data Archive, *ucd.ie*. [Online]. [Accessed: October 1, 2015]. Available: <http://www.ucd.ie/issda/data/>
2. C. Cody, V. Ford, and A. Siraj, “Decision Tree Learning for Fraud Detection in Consumer Energy Consumption”, accepted at the *14th IEEE International Conference on Machine Learning and Applications*, December 9-11, 2015.
3. V. Ford, A. Siraj, and W. Eberle, “Smart Grid Energy Fraud Detection Using Artificial Neural Networks”, in *Proceedings of the 2014 IEEE Symposium Series on Computational Intelligence*, December 9-12, 2014.