# Detection of High-level Anomaly Events in Utility Networks

Michael Orlov

Shamoon College of Engineering, Beer Sheva, Israel
orlovm@noexec.org

**Abstract.** This entrepreneurship pitch submission describes a POC for detecting high-level anomaly events in utility networks such as power grids, water plants, pressurized pipelines, etc.

**Keywords:** Cyber anomalies · Machine learning · Power grids.

## 1 Introduction and Project Description

Utility networks with complex topologies, such as heterogeneous electricity grids, wide-area water pipelines, and so forth, are vulnerable to cybersecurity intrusions [3]. A defining feature of such intrusions is that while simple intrusions are fairly easy to detect, since they result in local spikes that are inconsistent with the global grid configuration, extensive intrusions are much harder to detect. Local spikes exist in such attacks, but stand out less, and are coordinated in order to prevent automatic detection.

The proposed solution is to differentiate between detection of unreliable low-level events, and detection of high-level intrusions at a higher abstraction level that is created by automatically learning the behavioral model of low-level events.

## 2 Proof-of-Concept Implementation

Figure 1 shows detection of low-level events such as power and current surges, as detected by the power-management units (PMUs) that are positioned in key locations over the heterogeneous power grid. While such events may point to a low-level intrusion, the false-positives rate is high. In addition, a sophisticated attacker may coordinate intrusions at different points in the network in such a way that an attempt to filter-out the false-positives will also filter the actual intrusion.

In order to create a higher level of abstraction that represents unexpected changes in behavior of low-level events, a deep learning neural network is used in order to learn a model of low-level events, as illustrated in Figure 2 and Figure 3. Use of a neural network for this purpose is different from using one to detect anomalies as-is, which is an established research area as well [1, 2].

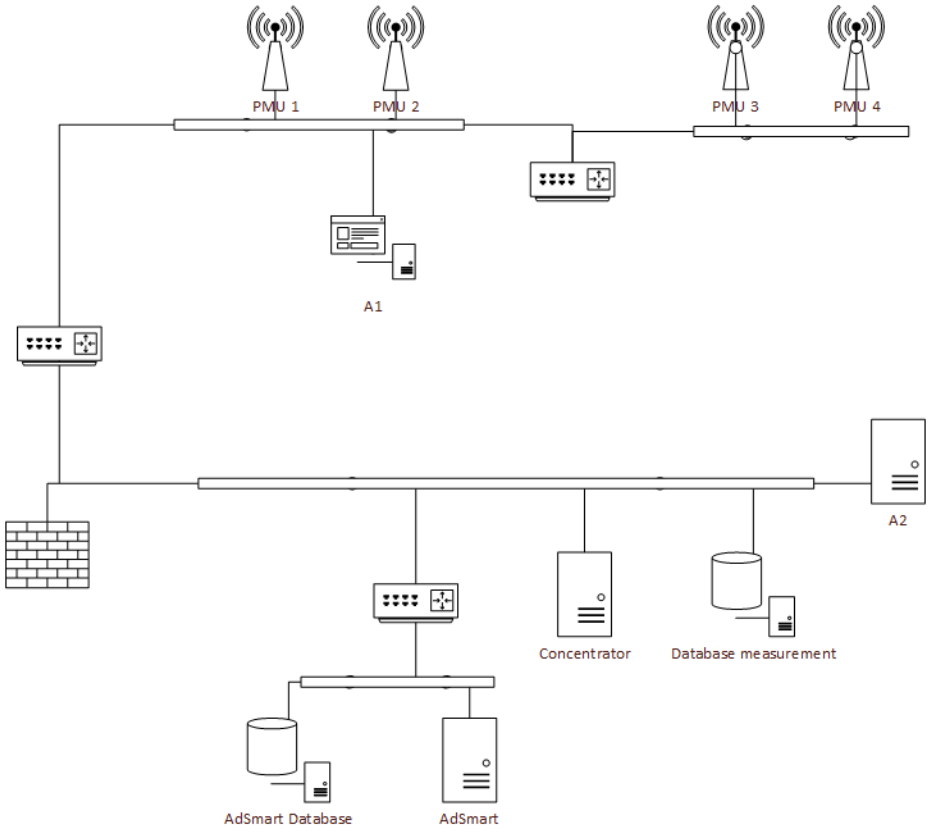


**Fig. 1.** Low-level events are detected from power management units (PMUs). AdSmart is the high-level events modeler described in this paper, whereas A1 and A2 are algorithms that detect low-level events.

The proof-of-concept is evaluated on a simulated power grid, as illustrated in Figure 4. Figure 5 shows a GUI that was implemented for testing the high-level events detection.

## 3 Conclusions

I have presented a POC for detecting high-level anomaly events in utility networks. The market for such a system could be power plants SCADA cybersecurity solutions, oil/gas pipelines control, and others. However, a test on real data is necessary. Moreover, deep learning has limited applicability for the approach, and advanced automatic learning methods like genetic programming are expected to yield more promising results.

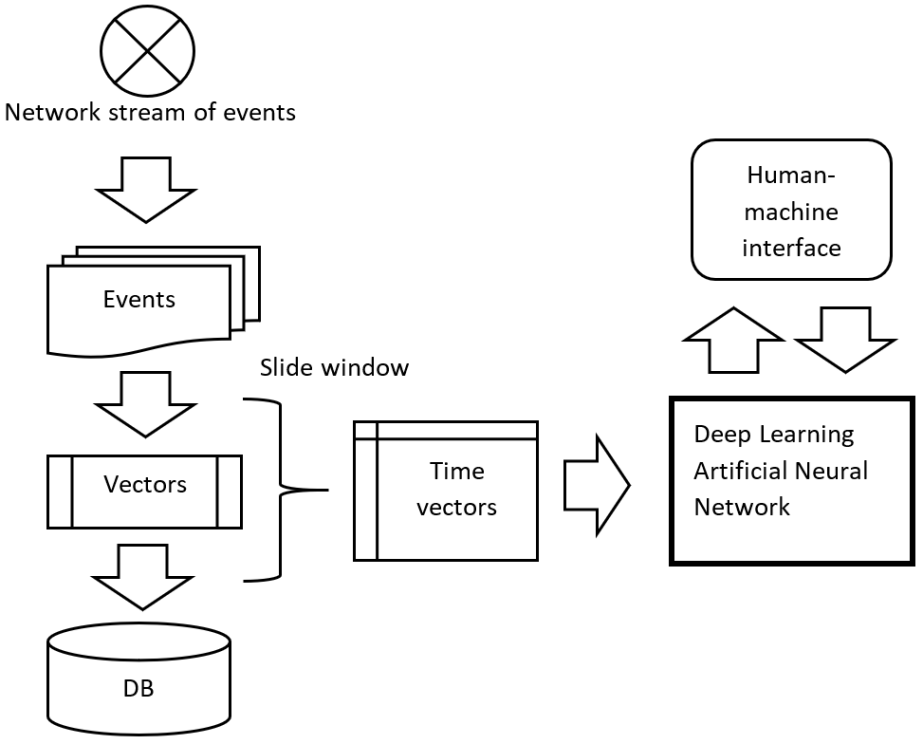


**Fig. 2.** Neural network learns a model of low-level events.

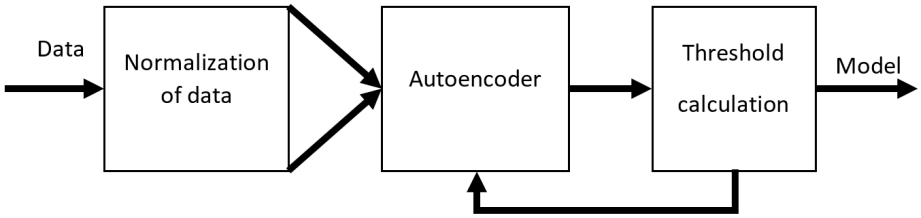


**Fig. 3.** Data flow for creating a model of low-level events.

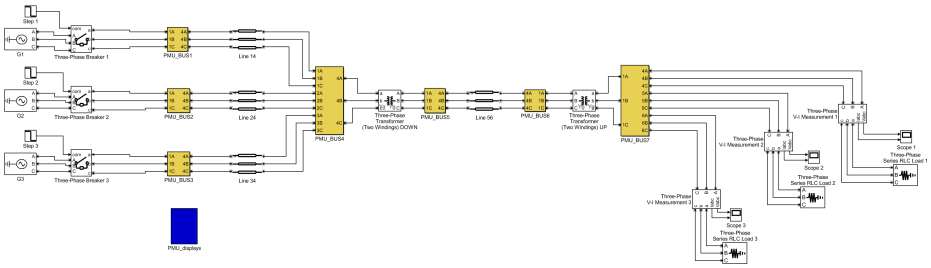

**Fig. 4.** A simulated power grid.

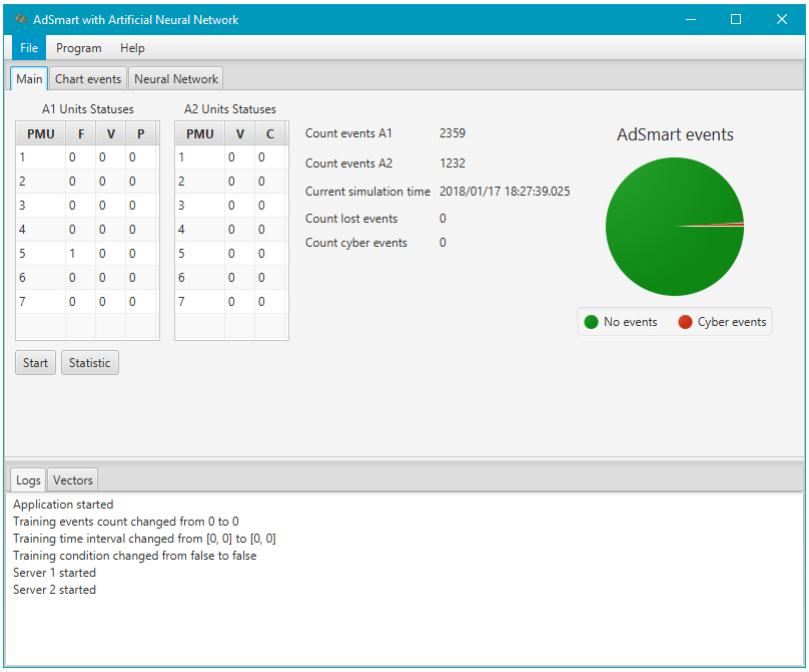


**Fig. 5.** A graphical user interface for the POC.

## Acknowledgments

The project described herein was implemented by M.Sc. student Mr. Yvgeniy Dranko.

## References

1. Kosek, A.M.: Contextual anomaly detection for cyber-physical security in smart grids based on an artificial neural network model. In: 2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG). vol. 00, pp. 1–6 (April 2016). https://doi.org/10.1109/CPSRSG.2016.7684103
2. Martinelli, M., Tronci, E., Dipoppa, G., Balducelli, C.: Electric power system anomaly detection using neural networks. In: Negoita, M.G., Howlett, R.J., Jain, L.C. (eds.) Knowledge-Based Intelligent Information and Engineering Systems. pp. 1242–1248. Springer Berlin Heidelberg, Berlin, Heidelberg (2004)
3. Mitchell, R., Chen, I.R.: A survey of intrusion detection techniques for cyber-physical systems. ACM Comput. Surv. **46**(4), 55:1–55:29 (Mar 2014). https://doi.org/10.1145/2542049