Detection of High-level Anomaly Events in Utility Networks

Michael Orlov, SCE/SE
noexec.org

CSCML 2018, BGU/CS
21.06.2018

Who am I?

- Head of Cyber OPs Program @ SCE
- Evolutionary Computation researcher
- *Liberté Linux* developer, as “Maxim Kammerer”

LENTA.RU четверг, 29.06.2017, 00:06:15
издание Rambler Media Group
Интернет, Технологии

Пресс-конференция

Максим Каммерер. Фото из личного архива

Максим Каммерер, создатель дистрибутива д настоящих "анонимусов" Liberté Linux

Как обеспечить безопасность общения в интернете?
Из-за утечки SMS, отправленных абонентам "Мегафона", достоянием общественности стали лич интимные сообщения, телефонные номера адресатов и в некоторых случаях даже связки логинов электронной почты и социальных сетей. Насколько стоит доверять операторам связи и актуальн выражение "это не телефонный разговор"? Как обеспечить конфиденциальность общения и мож гарантировать абсолютную анонимность в интернете? На эти и другие вопросы читателей "Лент Максим Каммерер, создатель дистрибутива для настоящих "анонимусов" Liberté Linux.

SCE
SHAMOON COLLEGE OF ENGINEERING
Cyber Operations Program

Detection of High-level Anomaly Events

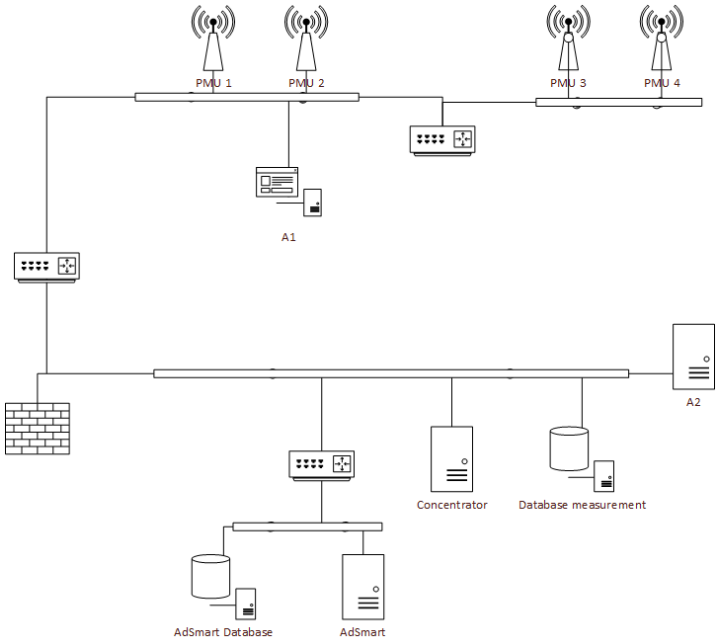
- Heterogeneous electricity grid as an Example
- Simple intrusions are fairly easy to detect
  - result in local spikes that are inconsistent with the global grid configuration
- Extensive intrusions are very hard to detect
  - local spikes exist, but stand out less, and are more coordinated

The Solution

- Differentiate between unreliable low-level events and detection of high-level intrusions
- Continuously learn a model of low-level events and detect change of behavior as an anomaly
- M.Sc. project performed by Mr. Yvgeniy Dranko

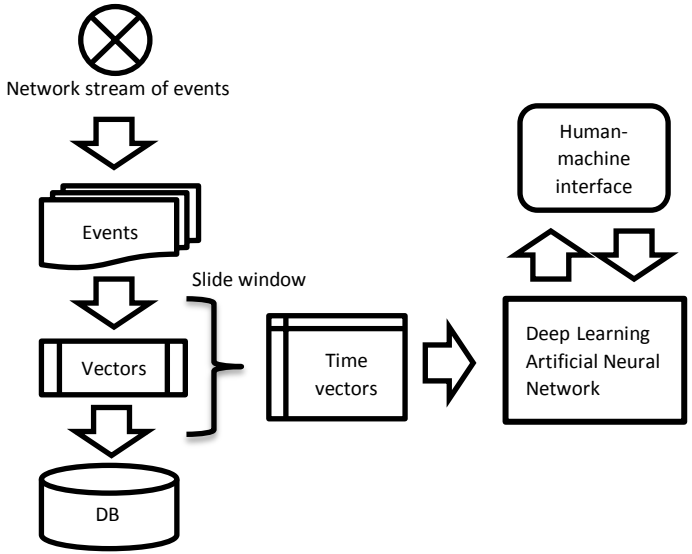
Implementation Details

- Low-level events detected from PMUs:

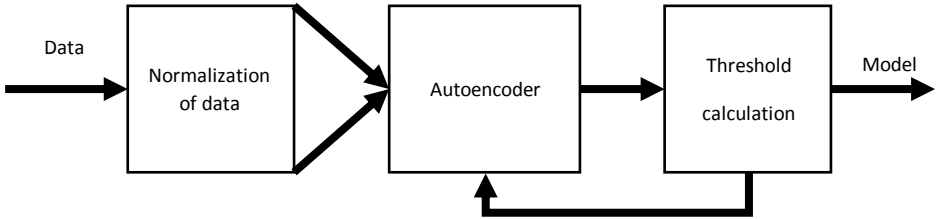


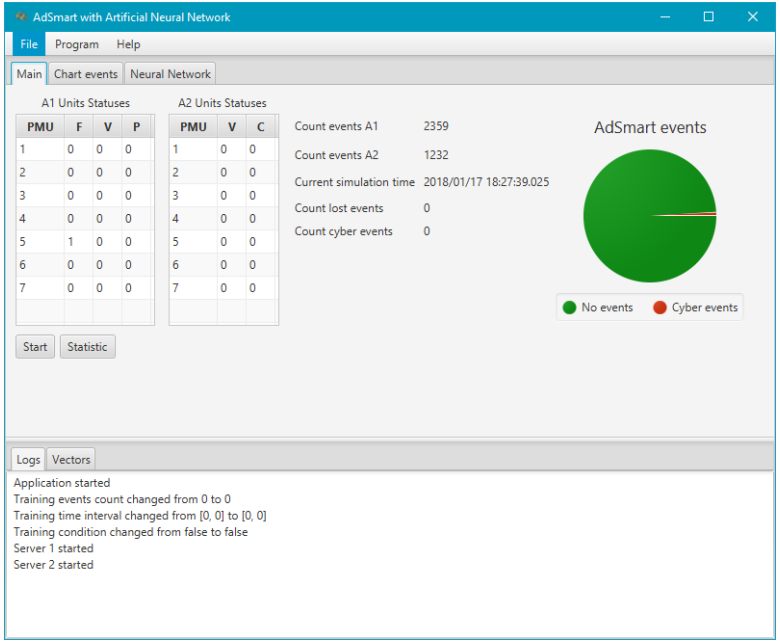
Implementation Details

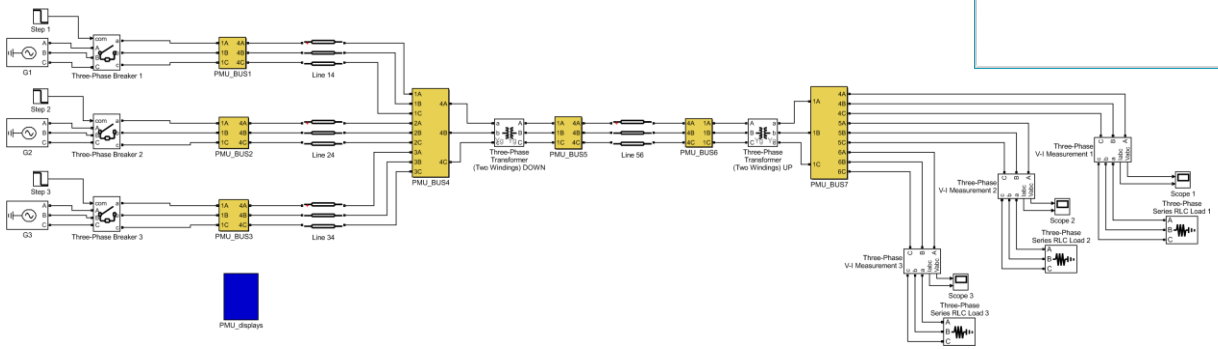
- Neural network learns a model of low-level events



POC


Data
Normalization of data
Autoencoder
Threshold calculation
Model


AdSmart with Artificial Neural Network
File
Program
Help
Main
Chart events
Neural Network
A1 Units Statuses
PMU F V P
1 0 0 0
2 0 0 0
3 0 0 0
4 0 0 0
5 1 0 0
6 0 0 0
7 0 0 0
A2 Units Statuses
PMU V C
1 0 0
2 0 0
3 0 0
4 0 0
5 0 0
6 0 0
7 0 0
Count events A1 2359
Count events A2 1232
Current simulation time 2018/01/17 18:27:39.025
Count lost events 0
Count cyber events 0
AdSmart events
No events
Cyber events
Start
Statistic
Logs
Vectors
Application started
Training events count changed from 0 to 0
Training time interval changed from [0, 0] to [0, 0]
Training condition changed from false to false
Server 1 started
Server 2 started


Step 1
G1
Three-Phase Breaker 1
PMU_BUS1
Line 14
Step 2
G2
Three-Phase Breaker 2
PMU_BUS2
Line 24
Step 3
G3
Three-Phase Breaker 3
PMU_BUS3
Line 34
PMU_BUS4
Three-Phase Transformer (Two Windings) DOWN
PMU_BUS5
Line 56
PMU_BUS6
Three-Phase Transformer (Two Windings) UP
PMU_BUS7
Three-Phase V-I Measurement 1
Three-Phase V-I Measurement 2
Three-Phase V-I Measurement 3
Scope 1
Scope 2
Scope 3
Three-Phase Series RLC Load 1
Three-Phase Series RLC Load 2
Three-Phase Series RLC Load 3
PMU_displays

Market

- Power plants SCADA cybersecurity
- OIL/Gas pipelines control
- Etc.