Ensemble Learning Methods for Power System Cyber-Attack Detection

Abstract

- Power system is one of the most important industrial control systems in today's society. In recent years, power systems have been well researched and developed extensively with a high rate.
- In order to optimally integrate systems and reduce costs, lots of advanced information technologies are involved into power systems. Traditional power system is changing to the smart power grid rapidly.
- Therefore, modern power systems are now exposing to the public network and information security is becoming a new threat to resilience.
- In this work, we explore the suitability of ensemble learning methods as a means of detecting power system cyber-attack.
- We evaluate various ensemble learning methods as cyber-attack detectors and discuss the practical implications for deploying ensemble learning methods as an enhancement to existing power system architectures.

Existing

- The main task of power system is transmitting of electricity to the customers.
- Power systems have been designed with the fault tolerance mechanisms and redundancy to perform this task, but information security was not a consideration at the time.
- As formerly physically isolated power systems were joined to the Internet for integrated control and management, it bring about a greater potential for unauthorized access and uncovered these systems to the same vulnerabilities that trouble traditional computer systems and networks.

Proposed

- we explore the suitability of ensemble learning methods as a means of detecting power system cyber-attack.
- We evaluate various ensemble learning methods as cyber-attack detectors and discuss the practical implications for deploying ensemble learning methods as an enhancement to existing power system architectures

HARDWARE REQUIREMENTS

- Processor – Pentium –III
- Speed – 1.1 Ghz
- RAM – 256 MB(min)
- Hard Disk – 20 GB
- Floppy Drive – 1.44 MB
- Key Board – Standard Windows Keyboard
- Mouse – Two or Three Button Mouse
- Monitor – SVGA

SOFTWARE REQUIREMENTS

- Operating System : Windows 8
- Front End : Java /DOTNET
- Database : Mysql/HEIDISQL

Conclusion

- The classification approaches to machine learning are still not widely used in ICS as an intrusion detection system.
- Especially, using ensemble learning methods in an ICS environment is a relatively new topic.
- According to the results of applying ensemble learning methods to these power system datasets, it can be concluded that ensemble learning is available approach to providing reliable decision support to power system operators on whether the system is under attack.

Reference

[1] Thomas H. Morris and Wei Gao. Industrial control system cyber attacks. In International Symposium on ICS and Scada Cyber Security Research, pages 22–29, 2013.

[2] Bayu Adhi Tama and Kyung Hyune Rhee. A combination of pso-based feature selection and tree-based classifiers ensemble for intrusion detection systems. Advances in Computer Science and Ubiquitous Computing, pages 489–495, 2015.

[3] Srinivas Mukkamala, Andrew H. Sung, and Ajith Abraham. Intrusion detection using an ensemble of intelligent paradigms. Journal of Network and Computer Applications, 28(2):167–182, 2005.

[4] Sandhya Peddabachigari, Ajith Abraham, Crina Grosan, and Johnson Thomas. Modeling intrusion detection system using hybrid intelligent systems. Journal of Jiangxi University of Science and Technology, 30(1):114–132, 2007.