Fuzzy Logic Model for Digital Forensics: A Trade-off between Accuracy, Complexity and Interpretability

Andrii Shalaginov
Center for Cyber- and Information Security, Norwegian University of Science and Technology
andrii.shalaginov@ccis.no

Abstract

The Cyber Crime Investigation is challenged by large and complex data as a key factor of emerging Information and Communication Technologies. The size, the velocity, the variety and the complexity of the data have become so high that data mining approaches are no more efficient since they cannot deal with Big Data. As a result, it can be infeasible to represent specific evidences found in such data in a Court of Law in a human-perceivable manner. Moreover, majority of computational methods result in complex and hardly explainable models. However, Soft Computing, a computing with words, can be beneficial in such case. In particular, hybrid Neuro-Fuzzy is capable of learning understandable and precise fuzzy rule-based model. This paper presents novel improvements of NF architecture and corresponding results.

1 Introduction

Neuro-Fuzzy (NF) is an obvious choice for computational method that is able to combine computational intelligence and human-understandable linguistic inference model in Digital Forensics (DF) applications. DF science is mainly concerned with data-driven methods, so investigators have to decide what methodology should be used and how. Since manual analysis is limited and in many cases cannot compete with an automated done by Machine Learning (ML), an expert might not be able to find any useful traces of evidences. Our preliminary results show that NF method has a poor accuracy and a high complexity model. On the other hand, it complies with the Daubert Standards/Criteria for models testing and interpreting them according to the requirements [Feldman and O'Connor, 2001] from USA case in 1993. As law is established in a set of commonly accepted and discussed rules, Cyber Crime Investigations are based on these rules and corresponding investigation methods are developed. Daubert Standards define whether testimony and derived evidences can be accepted in a Court of Law as valid. The *first criterion* defines whether a method is based on a testable hypothesis. It can be said that ML classification methods are based on hypothesis and can automatically make a decision whether to accept or reject corresponding null-hypothesis. The *second criterion* states that the error rates should be known for used scientific method. The *third criterion* requires ML method to be well-known and peer-reviewed. As ML society is actively developing and testing new methods and applications, there are plenty of academic and industrial publications on ML methods with results in different areas. Finally, the *fourth criterion* states that the scientific methods have to be accepted in the community. The main problem of NF lays in the need to represent fuzzy rules from Self-Organizing Map (SOM) clustering in a "forensically-sound manner" as mentioned by [McKemmish, 2008] without changing the original data properties (traces of evidences). Existing NF with SOM clustering generates a large number of rules that do not comply with Daubert Standards and do not provide a reliable human-understandable model. This paper gives an insight into our work on revised and improved NF that is suitable for DF applications.

2 Theoretical Background

NF is a Hybrid Intelligence method that assembles Fuzzy Logic (FL) and Artificial Neural Network (ANN) into a classification model as shown in the Figure 1. The NF data flow is divided into two logical stages [Kosko, 1996]:

1^{st} **NF stage** is an unsupervised procedure that groups samples based to their similarity. The input data sample is a real-valued vector $X = \{x_i \in R, 0 \leq i \leq M-1\}$ that is characterized as a point in M-dimensional space. SOM is trained, resulting in groups of samples later to be used for fuzzy patch construction. The main challenge is the determination of the number of SOM nodes, e.g. width and height of the map. The outcome of this stage is a set of clusters that each form a fuzzy patch based on the statistical parameters inheritance in each group. Originally, Vesanto [Vesanto *et al.*, 2000] proposed to use number of SOM nodes equal to $S = 5 \cdot \sqrt{N}$, where N is a number of data samples.

2^{nd} **NF stage** is a supervised procedure. On this stage, a set of fuzzy rules (based on fuzzy patches) are converted as neurons into ANN with corresponding weights assigned. The iterative training procedure results in more accurate model.

3 Contributions & Results

Preliminary studies showed that original NF has a poor performance and a high complexity of the model. Our contribution in this field is two-folded. (i) Revised NF method capable

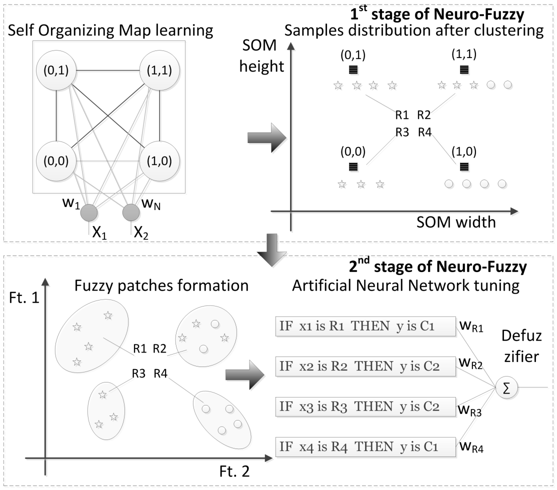

Figure 1: Neuro-Fuzzy architecture

of handling complex and non-trivial data:

1. The trade-off between the accuracy of NF model and its interpretability can be achieved using exploratory data analysis. Extraction of optimal SOM parameters can be done using such analysis instead of Vesanto method [Shalaginov and Franke, 2015b].
2. An empirical pseudo-radius α of hyper-ellipsoid suggested by Kosko is automatically calculated by χ^2 goodness of fit estimation [Shalaginov and Franke, 2015c].
3. Triangular and Kosko projection-based Membership Functions (MF) cannot incorporate all data. In contrary, a new Gaussian MF allows to provide robust estimation of membership degree with respect to data stretchiness and angle [Shalaginov and Franke, 2015a].
4. Multinomial classification problems have not been sufficiently explored before in DF. New defuzzification function in NF and better SOM nodes configuration give more reliable performance [Shalaginov *et al.*, 2016].

Further, (ii) we created a novel dataset consisting of 328,337 binaries categorized (10,362 families and 35 categories) Windows PE32 viruses [Shalaginov *et al.*, 2016]. Samples from this dataset were examined using static and dynamic behavioural analysis. Also we performed a number of experiments with community-accepted large-scale datasets (KDD Cup 1999, SUSY, HIGGS, etc) that proved reliability of the proposed improvements. For KDD Cup 1999 dataset original NF results in 15,081 fuzzy rules with 94.8% accuracy vs 12 rules with 98.9% by revised NF. Also some ML methods failed to be trained with such data.

4 Discussions & Conclusions

This paper addresses application of Fuzzy Logic for Digital Forensics, in particular automated Neuro-Fuzzy method capable of deriving human-like models of data in Cyber Crime Investigations. Due to increase in volume and complexity of data, classical computational approaches are no longer reliable neither can handle high precision over incomplete data. Therefore, we believe that data-driven approach based on Fuzzy Logic may be beneficial for data representation in a Court of Law. In particular, a trade-off between the accuracy of the model and the interpretability can be optimized using Neuro-Fuzzy in Digital Forensics applications. The improved model includes exploratory data analysis for optimal SOM configuration, new fuzzy patches and membership function. Wide range of experiments proved the ability to extract lower amount of fuzzy logic rules and achieve higher classification performance on malware detection and network traffic analysis problems. Our future works includes synergy of Deep Learning and Neuro-Fuzzy.

Acknowledgments

I would like to acknowledge valuable discussions with supervisor Katrin Franke. Also grateful for support from COINS Research School of Computer and Information Security.

References

[Feldman and O'Connor, 2001] Elliott R Feldman and Esquire Cozen O'Connor. Criteria for admissibility of expert opinion testimony under daubert and its progeny. Technical report, Tech. rep, Cozen O'Connor, 2001.

[Kosko, 1996] Bart Kosko. *Fuzzy engineering*. Prentice-Hall, Inc., 1996.

[McKemmish, 2008] Rodney McKemmish. When is digital evidence forensically sound? In *IFIP — The International Federation for Information Processing*, pages 3–15. Springer Science+Business Media, 2008.

[Shalaginov and Franke, 2015a] Andrii Shalaginov and Katrin Franke. Automated generation of fuzzy rules from large-scale network traffic analysis in digital forensics investigations. In *7th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2015)*. IEEE, 2015.

[Shalaginov and Franke, 2015b] Andrii Shalaginov and Katrin Franke. A new method for an optimal som size determination in neuro-fuzzy for the digital forensics applications. In *International Work-Conference on Artificial Neural Networks*, pages 549–563. Springer International Publishing, 2015.

[Shalaginov and Franke, 2015c] Andrii Shalaginov and Katrin Franke. A new method of fuzzy patches construction in neuro-fuzzy for malware detection. In *IFSA-EUSFLAT*. Atlantis Press, 2015.

[Shalaginov *et al.*, 2016] Andrii Shalaginov, Lars Strande Grini, and Katrin Franke. Understanding neuro-fuzzy on a class of multinomial malware detection problems. In *International Joint Conference on Neural Networks (IJCNN) 2016*, pages 684–691. Research Publishing Services, 2016.

[Vesanto *et al.*, 2000] Juha Vesanto, Johan Himberg, Esa Alhoniemi, and Juha Parhankangas. Self-organizing map in matlab: the som toolbox. In *In Proceedings of the Matlab DSP Conference*, pages 35–40, 2000.