Integrated ANN, EC, FL, and Algebraic Means for Cyber Security

Vahid Rahmati[1], Amir Ghorbani

I. Background

Machine learning (ML) and data mining (DM) are expanding concepts discussing human-like[2]—and therefore efficient data acquisition and procession—by computer systems, robots, and non-human actors labelling and deciding based on some rational procedure of selection [1]–[3]. So, likewise other computational tools and algorithms, ML and DM are tools that can be used in different fields from improving certain mathematical algorithms and models to applying them on social information for medical purposes [4]–[6]. This proposal mainly concerns with the use of smart methods for the cyber security (CS) [7], or generally security of inter-connected objects—such as internet of things (IoT) [8]. The problems that are generally being resolved are called cyber intrusion detection (ID) problems using ID systems (IDSs) [9].

In fact, all of the activities including unauthorized use, duplication, alteration, and damage of information systems—both from internal of the organizations and external sources of attack—must be relieved by IDSs. But, IDSs can't solve any problem unless the problem is detected using cyber analytics (SA) such as: misuse or signature based, anomaly-based, and hybrid. Indeed, Artificial Neural Networks (ANNs), together with EC or Fuzzy logic (FL), are employed for intrusion detection but these networks may suffer from some deficiencies. A known deficiency is low speed of convergence because of local minima compared with convex quadratic optimization [9].

As the author has worked on ANNs and specifically on their improvements [10]–[12], and has an enough insight over Fuzzy systems [13] with both Sugeno and Mamdani input types, therefore, proposes the classifier ANNs with improved convergence plus fast Fuzzy systems. Where the rules and relations of some attack scenarios are unknown, we must use Fuzzy systems because they're used to extract relations based on simple rule settings. However, this is done by expertise of the designer every time, on the other hand, ANNs learn by themselves using a set of teaching patterns injected to their inputs. These relations include parameters like protocol identifier (ID), source and destination ports, source address, destination address, ICMP type and code, raw data and its length, post and get contents and more [9], [14].

It's clear that use of EC/ANN and Fuzzy systems are not exactly the same. Fuzzy systems are better to be used when the number of parameters are few, for example in transmission intrusion attacks with port, IP, protocol parameters. On the other hand for advanced network misuses, and systematic keyword attacks, we must use ANNs as their mechanisms on learning automatically differs them from Fuzzy systems lacking automatic learning. The direct EC application becomes evident when the generated rules need to be evolved meaning the shape of attacks are being reformed, however the types not, and we need to update rule databases without the help of a human operator.

The work on network security itself needs good insight on the communications protocols, but improving machine learning methods is mainly a mathematical topic. It seems, with respect to literature, many attempts focus on direct use of ANNs, EC, and Fuzzy systems, but almost all of them rely on developments of these means in the field of artificial intelligence (AI) and they don't try to propose independent tools. The nature of network security and its importance needs independent observation and production of analysing tools even though based on AI.

II. More Details

This part suggests the artificial tools plus a mathematical model for possible use aimed at cyber security in the event of a salient attack.

1- **ANN based method:** An ANN is used to classify the network TCP connections, to stop insecure ones, by being trained using learning pattern based on basic, content, and traffic features. These features are almost contained in every data set to simulate attack scenario. The duration (D), protocol type (PT), flag (F), land (L), src_bytes (SBs), dst_bytes (DBs), wrong_fragment (WF), and urgent (U) are basic features. In the new method the service type is separated from basic features and therefore the datasets that train our ANN must be categorized by service types including 1- http 2- ftp 3- telnet and others. It means to date, there were not much distinction between SA for different service (S) types, but in the new method for every type an independent ANN is trained. The reason behind can be cleared by an example: in a DOS (Denial of Service) attack on a remote computer with S=http, src_bytes and dst_bytes surge and the number of connections also increase. In a distributed DOS (DDOS), the number of connections with various IPs will rise even more. Now, for S=ftp, and for big values of D, many systems use simultaneous connections (multi connections at the same time). In this case the D for every connection is decreased corresponding to the decreased vales of SBs and DBs. Many ANNs may consider this also as an attack based on high bandwidth consumption on the server. In the new method this is not considered as an attack and users can access data unceasingly. The benefits are accurate threat detection but the dark side is high run time and need for more processing powers [9].

[1] Correspondent: vahidrahmati9170@gmail.com, vahid.rahmati@icdst.org

[2] Generally, human-like means smart method such as evolutionary computation (EC), using evolutionary algorithms (EAs), which may also use the modelling of behaviour of living organs.

2- **Mathematical method (MM):** In [15], a new non-linear, algebraic method for system approximation was presented. The method uses smoothing and mapping functions to model a system based on different algebraic forms. When ANNs aren't suitable, it's possible to use these models instead. The benefits of a simple model is its easy implementation and low cost and run time.

3- **EC:** Based on GA [16], using a collection of threat logs to study the patterns of threat activity, it's possible to establish associations between the network services a host is running and the kinds of threats to which it's vulnerable. Therefore the GA gives the probabilistic values measurable directly by observations to develop an automatic CS strategy. As mentioned in [17], much of the design procedures for CS is based on human knowledge with slow decision makings leading to less efficiency as network systems are spreading globally and there's an urgent need for new security assessments measures. The method uses weighted averages (WAs) and ordered weighted averages (OWAs) with EAs. The benefit is less time to run compared to ANNs but still more expensive, however accurate, compared to MM.

Table I. A brief comparison of techniques mentioned based on info from [1]–[3], [9], [18]–[26]

	ANNs	MM	EC	FL (non-adaptive)	FL (Adaptive)
Adv.	1- Accurate threat detection based on DB (with learning) 2- Automatic threat detection	1- Low run time 2- low cost	1- Good threat detection based on DB (with learning) 2- Acceptable run time	1- Low run time for few input parameters but many output patterns 2- Semi-automatic threat relief	1- Accurate threat detection 2- Reasonable run time
Disadv.	1- High run time 2- Local minima 3- High cost	1- Threat detection based on DB (no learning) 2- Edge resonation for big DBs	1- Slow on big DBs 2- Inaccurate for non-salient threats 3- Not fully automatic	1- Slow on big DBs (rule explosion) 2- Inaccurate for non-salient threats 3- Slow for many inputs and even few outputs	1- Threat detection based on DB (slow learning)—some FL systems learn based on ANNs

According to Table I, ANNs are good choices for high income companies preferring accurate threat detection as they can offer expensive infrastructures, but for medium to low income companies, it's better to use a combination of EC, MM, and FL. However, here, we suggest not to use ANNs in combination with other means—except for specific services— as the run time may suffer highly.

References

[1] C. C. Aggarwal, *Data Mining: The Textbook*. 2015.

[2] P. Louridas and C. Ebert, "Machine Learning," *IEEE Softw.*, vol. 33, no. 5, pp. 110–115, 2016.

[3] R. Mikut and M. Reischl, "Data mining tools," *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.*, vol. 1, no. 5, pp. 431–443, 2011.

[4] E. Alpaydın, *Introduction to machine learning*, vol. 1107. 2014.

[5] V. Dunjko, J. M. Taylor, and H. J. Briegel, "Quantum-Enhanced Machine Learning," *Phys. Rev. Lett.*, vol. 117, no. 13, 2016.

[6] A. Criminisi, "Machine learning for medical images analysis," *Medical Image Analysis*, vol. 33, pp. 91–93, 2016.

[7] J. J. P. Tsai and P. S. Yu, *Machine learning in cyber trust: Security, privacy, and reliability*. 2009.

[8] S. Li, T. Tryfonas, and H. Li, "The Internet of Things: a security point of view," *Internet Res.*, vol. 26, no. 2, pp. 337–359, 2016.

[9] A. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surv. Tutorials*, vol. PP, no. 99, p. 1, 2015.

[10] V. Rahmati, M. H. Yar, and A. R. Malekijavan, "Neural Networks New Capacity Factor Measurement for Improvement of SOM," *Int. J. Innov. Technol. Explor. Eng.*, vol. 3, no. 12, pp. 7–10, 2014.

[11] M. H. Yar, V. Rahmati, H. Reza, and D. Oskouei, "A Survey on Evolutionary Computation : Methods and Their Applications in Engineering," *Mod. Appl. Sci.*, vol. 10, no. 11, pp. 131–139, 2016.

[12] V. Rahmati, M. H. Yar, J. Khalilpour, and A. R. Malekijavan, "Back Propagation Artificial Neural Network Structure Error Reduction by Defined Factor of Capacity and Algorithm Reinforcement Method," *Int. J. Soft Comput. Eng.*, vol. 4, no. 4, pp. 34–39, 2014.

[13] V. Rahmati, "A Novel Low Complexity Fast Response Time PID Controller Based on Fuzzy Logic for DC Motors," in *C4I Conference at Shahid Sattari University, Tehran, Iran*, 2014, pp. 36–45.

[14] R. S. De Carvalho, "Impact of Communication System on Smart Grid Reliability , Security and Operation," pp. 0–5, 2016.

[15] V. Rahmati, "Improved Interpolation and Approximation through Order Manipulation," *Int. J. Emerg. Comput. Methods Eng.*, vol. 1, no. 1, pp. 1–10, 2016.

[16] S. Gil, A. Kott, and A.-L. Barabási, "A genetic epidemiology approach to cyber-security.," *Sci. Rep.*, vol. 4, p. 5659, 2014.

[17] S. Miller, C. Wagner, U. Aickelin, and J. M. Garibaldi, "Modelling cyber-security experts' decision making processes using aggregation operators," *Comput. Secur.*, vol. 62, pp. 229–245, 2016.

[18] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4. pp. 998–1010, 2012.

[19] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[20] O. Linda, M. Manic, T. Vollmer, and J. Wright, "Fuzzy logic based anomaly detection for embedded network security cyber sensor," in *IEEE SSCI 2011: Symposium Series on Computational Intelligence - CICS 2011: 2011 IEEE Symposium on Computational Intelligence in Cyber Security*, 2011, pp. 202–209.

[21] K. Göztepe, "Designing Fuzzy Rule Based Expert System for Cyber Security," *Int. J. Inf. Secur. Sci.*, vol. 1, no. 1, pp. 13–19, 2012.

[22] R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, no. October 2013, pp. 97–102, 2013.

[23] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," *Comput. Secur.*, vol. 49, pp. 70–94, 2015.

[24] M. Pratama, S. G. Anavatti, and E. Lughofer, "Evolving fuzzy rule-based classifier based on GENEFIS," in *IEEE International Conference on Fuzzy Systems*, 2013.

[25] J. J. Weinschenk, W. E. Combs, and R. J. Marks II, "Avoidance of rule explosion by mapping fuzzy systems to a union rule configuration," in *IEEE International Conference on Fuzzy Systems*, 2003, vol. 1, pp. 43–48.

[26] S. Zhao, M. Chandrashekar, Y. Lee, and D. Medhi, "Real-time network anomaly detection system using machine learning," *2015 11th Int. Conf. Des. Reliab. Commun. Networks*, pp. 267–270, 2015.