

Evolving Neural Network Intrusion Detection System for MCPS

Nishat Mowla*, Inshil Doh*, KiJoon Chae*

Department of Computer Science and Engineering, Ewha Womans University, Seoul, Korea

nishat.i.mowla@gmail.com, isdoh1@ewha.ac.kr, kjchae@ewha.ac.kr

Abstract— Medical Cyber Physical Systems (MCPS) are some of the most promising next generation technologies so far. Like many other systems connected to a wider network such as internet, MCPS are also vulnerable to various forms of network attacks. For detecting such diverse forms of attack, we need smart and efficient mechanisms. Human intelligence is good enough to track such attacks but when it is a huge number of traffic it is no more a feasible process to detect them manually as it is time consuming and computationally intensive. Machine learning techniques embracing artificial intelligence are emerging as powerful tools to detect abnormalities in the network data. Supervised Neural Networks are some of the most efficient techniques to perform such classification. In this paper, we propose neural network technique that evolves based on classification, elimination and prioritization while considering time, space, and accuracy to efficiently classify the four major types of network attack traffic found in an effectively pruned KDD dataset.

Keywords— MCPS, Machine Learning, Neural Networks, Intrusion Detection System

I. INTRODUCTION

We are moving towards an era where various forms of body worn devices that can record multiple physiological signals, such as ECG and heart rate or even more sophisticated devices that measure physiological markers such as body temperature, skin resistance, gait, posture, and EMG. Medical Cyber Physical Systems are the much-promised technologies which aim at providing remote healthcare to patients using the sensor information collected from such body worn devices [14]. With great prospect come great responsibilities. The data collected from these devices can be stored in a public or private cloud to be later analysed by the hospital authorities. Therefore, assuring the accessibility of the personal health information during the transmission from the sensory networks to the cloud and from the cloud to doctors' mobile devices will necessitate the design of an intelligent malicious traffic detection system which would prevent normal traffic from getting the proper connection [15].

Machine learning classification techniques are popular when it comes to the issue of classifying normal from abnormal. Among them recently deep learning techniques such as Neural Network are shown to act as powerful tools in order to classify various forms of network attack exploits.

In this paper, we propose an evolving neural network based intrusion detection system for detecting the four key major forms of network attack types by evolving the multi-class data to a 2-class problem following classification based data pruning and class prioritization.

We discuss some of the related works in sections II. In section III we discuss our proposed mechanism and evaluation results followed by the conclusion in section IV.

II. RELATED WORKS

Intrusion Detection Expert System was first proposed by Dorothy E. Denning [1]. It had a rule-based expert system to detect known types of intrusions with a statistical anomaly detection component based on profiles of users, host systems and the target systems. Later, a new version called Next-Generation Intrusion Detection Expert System was developed [2].

A. Anomaly Detection

The idea of using anomaly detection came into mainstream with DARPA Intrusion Detection Evaluation in information security released in 1998 and 1999 in conjunction with the MIT [3]. However, it was shown that the DARPA datasets are not appropriate to simulate real network systems [4] initiating the need for development of new datasets for developing IDS.

B. Machine Learning Techniques

Various forms of existing machine learning techniques are used for developing IDS. [5] and [6] discusses a survey of these techniques. Among them one of the most promising techniques called the neural network consists of a collection of actions to transform a set of inputs to a set of searched outputs through a set of simple processing units, or nodes and connections between them. There are schemes for both supervised and unsupervised learning techniques such as multi-layer perceptron [7] and self-organizing maps [8] respectively. Neural networks are ideal when we consider all the various forms of network attack traffic that we can experience based on the misuse detection model and the anomaly detection model [9]. Different existing dataset are used to evaluate the performance of IDS using neural networks in many research works [10].

C. Modern IDS

Modern IDS have difficulty in dealing with high speed network traffic while attackers can utilize that to hide their exploits by IDS overloading with irrelevant information while executing an attack [11]. A memory efficient multiple character-approaching architecture suited for ASIC implementations was proposed in [12]. The focus mainly went into memory management which could reduce the accuracy. Therefore, to manage higher traffic throughput and increasing link speed hardware accelerators were used to create various forms of NIDS. [13] depicts that while working with a huge number of data, a two-class problem is always more accurate than multi-class problem. In our approach, we try to combine lessons from all the related works and develop a time and space efficient but relatively more accurate mechanism as will be discussed in the next section.

III. PROPOSED MECHANISM

There is always a trade-off between time, space and accuracy while designing an efficient Intrusion Detection System. When we increase the number of classes to be distinguished, the accuracy of the machine learning model decreases while the IDS becomes slow. Again, when we decrease the number of attributes, the accuracy of the system goes down while the IDS work faster. Reducing the number of attributes is not a good idea since various forms of attacks can only be classified when we have an abundant number of attributes to distinguish them from others. Therefore, we try to create a mechanism which is both time and space efficient and also relatively more accurate. However, to overcome the various penalties to the techniques due to huge data handling, we utilize the benefit of a two-class problem since it is time efficient and relatively more accurate. As we go down the process we also try to make it space efficient by a logical elimination process. However, we also make sure all the classes come in the process of classification step by step while we try to maintain a 2-class problem. The following subsection describes our scheme in more detail.

A. Proposed scheme

The approach is to start with the two basic classes namely normal and attack classes. Once the data are identified not to belong to the normal class we eliminate the normal class instances and re-construct a two-class problem by taking one class of attack as our most prioritized attack and the other class as other attack type class. If the data are not identified to be our most prioritized attack type, then the instances for this attack class are removed and a new two class problem is constructed by following the same prioritization procedure. Fig 1 shows the basic workflow of our ANN (Artificial Neural Network) based 2-class IDS mechanism in general.

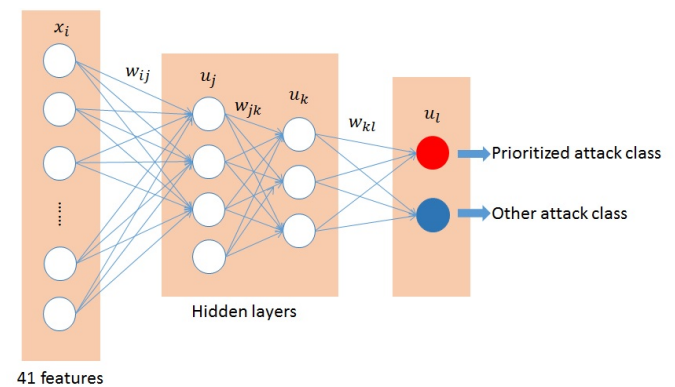


Figure 1. ANN based 2-class IDS mechanism

In the above figure x_i are the feature vectors input to the ANN system. In our case, we used 41 features provided by the KDD dataset [17]. u_j and u_k are the hidden layers which are also called the intermediary output layers. u_l is the final output layer which helps us to identify the classes. w_{ij} , w_{jk} and w_{kl} are the weight from x_i to u_j , u_j to u_k and u_k to u_l respectively.

Currently there are 4 major types of network attack traffic namely DoS, Probe, R2L and U2R. Among them DoS refers to all the network traffic flooding attack types. Relevant features include source bytes, packet rates etc. Probe attacks are attacks conducted by sending meaningless packets in order to gain knowledge about the network. They are often detected by features such as duration of connection or source bytes. R2L refers to remote access attacks where the attacker tries to gain access to a remote system. Relevant features include duration of connections, service requested or failed log-in attempts. U2R is the type of attack in which the attacker tries to log-in to a normal account and then gain root administrator access. They are often identified by features such as number of files created or number of shell prompts invoked [16]. On these 4 major types of network attack traffic we apply our evolving mechanism which, as discussed before, can be summarized to follow three major steps discussed below.

1) Classification: Our classification follows the ANN model of Multi-Layer Perceptron (MLP) working on a 2-class problem. Initially a normal class and an attack class are taken as the 2-classes.

2) Elimination: After a successful classification the class with the lowest possibility is eliminated to effectively prune the analysed network traffic and a new 2-class problem is constructed from the later class.

3) Prioritization: In this step, a class with higher priority to be analysed is taken as the first form of class while making the other class as other attack type class.

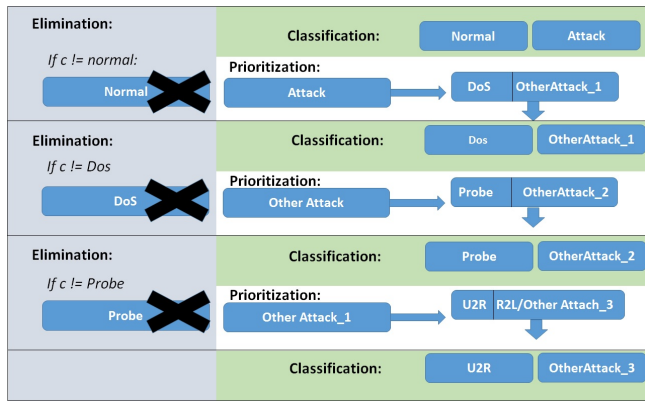


Figure 2. Evolving ANN based 2-class IDS mechanism

Fig. 2 shows our evolved ANN mechanism working with these three major steps for efficient classification. We prioritize the attacks as DoS, Probe, U2R and R2L respectively. Our mechanism in the form of an algorithm for the four major types of network attack traffic is shown in Fig. 3.

Algorithm 1 Evolving ANN Intrusion Detection System

```

class = sum of 2 or more classes;
normal = 1;
attack = 0;
i = 1;
c = classification result;
run classification test;
if c == 0 && class == TRUE then
  remove normal instances;
  dos = 1;
  other_attacki = 0;
  if c == 0 && class == TRUE then
    remove dos instances;
    probe = 1;
    other_attacki+1 = 0;
    if c == 0 && class == TRUE then
      remove probe instances;
      U2R = 1;
      R2L/other_attacki+2 = 0;
      if c == 0 && class == TRUE then
        traffic is R2L;
      else
        traffic is U2R;
    else
      traffic is probe;
  else
    traffic is dos;
else
  traffic is normal;

```

Figure 3. Evolving ANN Intrusion Detection System Algorithm for current four major network attack types

B. Performance Evaluation

We used all 41 features of KDD99 dataset [17] and evaluated the training time and detection accuracy of the ANN for different attack types. We use a total of 1200 data instances from all the four different kinds of network attack traffic along with normal network traffic. We also take samples from all the subclasses of the 4 major types of

network attack traffic. Table 1 shows all the sub-types of the 4-major network attack traffic that we used in our simulation [16].

TABLE 1. NETWORK ATTACK TRAFFIC

Attack class	Attack Types
DoS	Back, Land, Neptune, Pod, Smurf, Teardrop
Probe	Satan, Ipsweep, Nmap, Portsweep
R2L	Guess_Password, Ftp_write, Imap, Phf, Warezmaster
U2R	Loadmodule

In our first experiment, we show how the training time decreases as we decrease the number of classes from n to 2. Fig. 4 illustrates that as we decrease the number of classes, the number of training time also decreases significantly. This also depicts that if we have a huge number of classes reducing the sub-types to higher level types can effectively make the system faster.

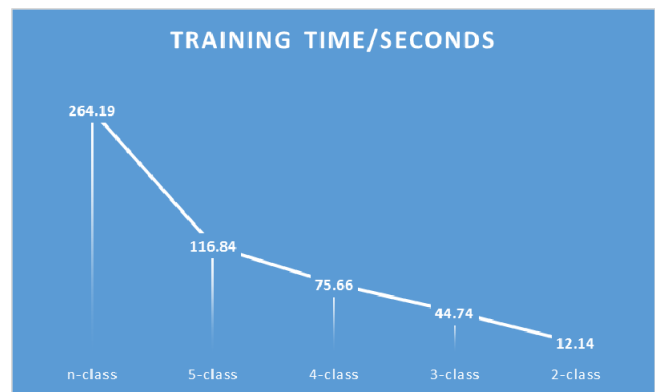


Figure 4. Change in training time as the number of classes are decreased

Fig. 5 shows the comparison between the linear class reduction in neural network and our evolved class reduction performance. Here case 1 is all the 5 classes included (normal, dos, probe, R2L, U2R), case 2 is all the 4 classes included (dos, probe, R2L, U2R), case 3 is all the 3 classes included (probe, R2L, U2R) and class 4 is the 2 classes included (R2L and U2R). In case of our evolved 2-class mechanism case 1 means normal and attack class, case 2 means dos and other attack class, case 3 means probe and other attack class, case 4 means R2L and U2R class. As can be seen from the following figure our evolved 2-class mechanism is more time efficient than the normal n -class mechanisms and, as can be seen, the difference of time efficiency tends to be higher as we increase the initial total number of classes in case 1.

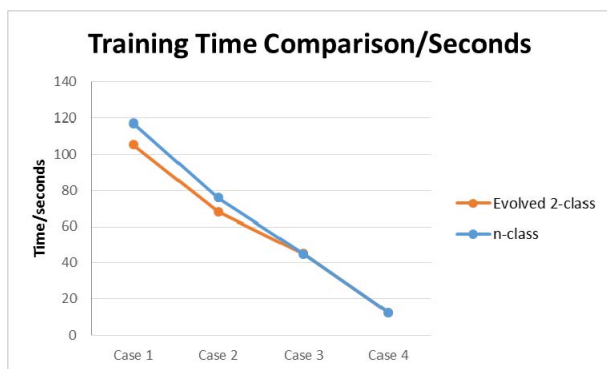


Figure 5. Training time comparison between n-class and evolved 2-class

In terms of accuracy also our evolved 2-class model is more efficient as well as it also reduces the space taken by need-based pruning after each case. Fig. 6 shows the correct classification results of our evolved 2-class model versus the normal n-class neural network classification.



Figure 6. Correctly classified instances

As can be seen from the above figure our evolved 2-class model has higher correct classification in all the 4 cases of network attack traffic analysis. Since we have four major network attack traffic categories our model has only 4 cases. We believe our proposed mechanism can scale in other types of attacks with a higher number of classifications.

IV. CONCLUSIONS

In this paper, we have proposed an Intrusion Detection System inspired by evolving neural network classification technique in order to detect the key 4 different types of network attack traffic that can occur in a Medical Cyber Physical System Network. We have shown that our proposed mechanism enhances the performance of the traditional supervised multilayer perceptron neural network technique. Our mechanism, however, doesn't have a standardized mechanism for attack prioritization yet. Therefore, in future work we hope to identify and develop techniques to prioritize the attack traffic class based on attack prediction mechanisms.

ACKNOWLEDGMENT

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A2011788). Kijoon Chae is the corresponding author.

REFERENCES

- [1] D. E. Denning, "An Intrusion-Detection Model," in IEEE Symposium on Security and Privacy, 1986, pp. 118–131.
- [2] D. Anderson, T. Frivold, and A. Valdes, "Next generation Intrusion Detection Expert System (NIDES): A summary," SRI Int., no. May 1995, p. 47, 1995.
- [3] M. Lincoln Laboratory, "DARPA Intrusion Detection Data Sets." [Online]. Available: <https://www.ll.mit.edu/ideval/data/>. [Accessed: 07-Apr-2016].
- [4] J. McHugh, "Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory," ACM Trans. Inf. Syst. Security., vol. 3, no. 4, pp. 262–294, 2000.
- [5] J. Singh and M. J. Nene, "A Survey on Machine Learning Techniques for Intrusion Detection Systems," Int. J. Adv. Res. Computer Communication Eng., vol. 2, no. 11, pp. 4349–4355, 2013.
- [6] S. K. Wagh, "Survey on Intrusion Detection System using Machine Learning Techniques," Int. J. Computer Appl., vol. 78, no. 16, pp. 30–37, 2013.
- [7] C. Qiu, J. Shan, B. Polytechnic, and B. Shandong, "Research on Intrusion Detection Algorithm Based on BP Neural Network," vol. 9, no. 4, pp. 247–258, 2015.
- [8] L. Vokorokos, A. Baláz, and M. Chovanec, "Intrusion detection system using self-organizing map," Informatica, vol. 6, no. 1, pp. 1–6, 2006.
- [9] J.-P. Planquart, "Application of Neural Networks to Intrusion Detection," 2001.
- [10] S. K. Sahu, S. Sarangi, and S. K. Jena, "A detail analysis on intrusion detection datasets," Souvenir 2014 IEEE Int. Adv. Computer Conf. IACC 2014, pp. 1348–1353, 2014.
- [11] V. Paxson, "Bro: a system for detecting network intruders in real-time," Computer Networks, vol. 31, no. 23–24, pp. 2435–2463, 1999.
- [12] H. Lu, K. Zheng, B. Liu, X. Zhang, and Y. Liu, "A memory-efficient parallel string matching architecture for high-speed intrusion detection," IEEE J. Sel. Areas Communication, vol. 24, no. 10, pp. 1793–1803, 2006.
- [13] L. Dhanabal and S. P. Shantharajah, "A Study on NSLKDD Dataset for Intrusion Detection System Based on Classification Algorithms," vol. 4, no. 6, pp. 446–452, 2015.
- [14] M. Alam, S. Abedin, M. Ameen and C. Hong, "Web of Objects Based Ambient Assisted Living Framework for Emergency Psychiatric State Prediction," Sensors, Vol. 16, No. 9, September 2016
- [15] Ovunc Kocabas, Tolga Soyata, and Mehmet K. Aktas, "Emerging Security Mechanisms for Medical Cyber Physical Systems", IEEE/ACM Transactions on Computational Biology and Bioinformatics, Vo. 13, No. 3, June 2016
- [16] S. Potluri, C. Diedrich, "Accelerated deep neural networks for enhanced Intrusion Detection System", 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1-8, September 2016
- [17] KDD 99 dataset, http://tunedit.org/repo/KDD_Cup/KDDCup99.arff



Nishat Mowla received the B.S degree in Computer Science from Asian University for Women, Chittagong, Bangladesh in 2013, an M.S. degree in Computer Science and Engineering from Ewha Womans University, Seoul, Korea in 2016. She is currently a PhD student at Ewha Womans University, Seoul, Korea. Her research interests include next generation network security, IoT network security and network traffic analysis.



Inshil Doh received the B.S. and M.S. degrees in Computer Science at Ewha Womans University, Korea, in 1993 and 1995, respectively, and received the Ph.D. degree in Computer Science and Engineering from Ewha Womans University in 2007. From 1995-1998, she worked in Samsung SDS of Korea to develop a marketing system. She was a research professor of Ewha Womans University in 2009~2010 and of Sungkyunkwan University in 2011.

She is currently an assistant professor of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. Her research interests include wireless network, sensor network security, and M2M network security.



Prof. Chae received the B.S. degree in mathematics from Yonsei University in 1982, an M.S. degree in computer science from Syracuse University in 1984, and a Ph.D. degree in electrical and computer engineering from North Carolina State University in 1990. He is currently a professor in Department of Computer Science and Engineering at Ewha Womans University, Seoul, Korea. His research interests include sensor network, smart grid, CDN, SDN and IoT, network protocol design and performance evaluation.