INTRUSION DETECTION BASED ON THE ARTIFICIAL IMMUNE SYSTEM

Danijela D. Protić
Serbian Armed Forces, General Staff,
Department for Telecommunication and Informatics (J-6),
Center for Applied Mathematics and Electronics,
Belgrade, Republic of Serbia,
e-mail: adanijela@ptt.rs,
ORCID iD: http://orcid.org/0000-0003-0827-2863

DOI: 10.5937/vojtehg68-27954; https://doi.org/10.5937/vojtehg68-27954

FIELD: Computer sciences
ARTICLE TYPE: Original scientific paper

Abstract:

Introduction/purpose: The artificial immune system is a computational model inspired by the biological or human immune system. Of particular interest in artificial immune systems is the way the human body reacts to new pathogens and adapts to remain immune for a long period after a disease has been combated, which refers to the recognition of known malicious attacks and the way the immune system identifies self-cells not to be reacted to, which refers to the anomaly detection.

Methods: Negative selection, positive selection, clonal selection, immune networks, danger theory, and dendritic cell algorithm are presented.

Results: A variety of algorithms and models related to artificial immune systems and two classification principles are presented; one based on the detection of a particular attack and the other based on anomaly detection.

Conclusion: Artificial immune systems are often used in intrusion detection since they are accurate and fast. Experiments show that the models can be used in both known attack and anomaly detection. Eager machine learning classifiers show better results in the decision, which is an advantage if runtime is not a significant parameter. Dendritic cell and negative selection algorithms show better results for real-time detection.

Key words: artificial immune system, intrusion detection.

Introduction

Artificial immune systems (AISs) are computational models inspired by the human immune system (HIS). The HIS is a complex, adaptive system of cells and molecules that protects the body against a variety of pathogens and distinguishes self- from non-self- cells. It recognizes, responds to and remembers the pathogens from previous attacks in order to force quicker fight against intruders in the future. The HIS consists of two different inter-related subsystems which act together. The innate immune system provides a general protective mechanism present from birth and makes a quick response immediately after the exposure to the invader and its recognition (De Castro & Von Zuben, 1999, p.95). The adaptive response takes several weeks to become effective. Once activated, the components of the adaptive immune system proliferate and create mechanisms for the elimination of foreign substances called antigens (Timmis et al, 2008, pp.11-32). The cells responsible for adaptive immunity are B cells which originate in the bone marrow and T cells which originate in the thymus. AISs describe concepts of positive and negative selection, clonal selection, immune networks, and a variety of other concepts of immunology. In order to map the processes involved in the HIS to AISs, a few considerations have to be taken into account: how to represent antigens and antibodies, what are memory cells, how to calculate affinity, etc.

The goal of intrusion detection is to build a system which recognizes malicious attacks or unusual network behavior and generate alerts. There are two basic trends in intrusion detection: misuse detection, based on the knowledge accumulated from previous attacks and anomaly detection, based on search for deviation of usual computer network behavior. Of particular interest in AISs is the way the human body reacts to new pathogens and adapts to remain immune for a long period after a disease has been combated (misuse detection). Also of interest is the way the immune system identifies self-cells which are not to be reacted to (anomaly detection).

AIS concepts and algorithms

A distinction between what is self and what is not (non-self) is determined by an antibody that can be recognized by the antigen binding sites on other antibodies. If the HIS cannot perform this distinction, it may be triggered against self (Haag et al, 2007, pp.420-435).

Negative selection

In the HIS at birth, all new immature T-cells must undergo a process of negative selection in the thymus, where self-reactive T-cells binding with self-proteins are destroyed. Immature T cells, which react against self cells, are eliminated by the immune system through controlled cell death - apoptosis**.** Other T cells mature, leave the thymus and circulate throughout the body to perform protective functions against non-self antigens (Forrest et al 1994, pp.202-212). The negative selection algorithm (NSA) consists of two phases: generation of a detector set and monitoring with detection of new instances. The starting point of the NSA is to produce a set of self strings *S* that define the normal state of the system. The task is to generate a set of detectors *D* that only recognize the complement of *S*. The candidates that match are eliminated while the rest are kept as detectors. In the detection stage, the detectors are applied to new data in order to classify them as being self or non-self (Ji & Dasgupta, 2007, pp.223-251). The matching rule can be defined as a distance between the detector and the data instance within the threshold such as the Hamming distance, or the Euclidean distance.

Positive selection

If the T cell recognizes self-molecules, it causes apoptosis and dies. If it does not react, it is tested with non-self molecules. If the T cell is not able to recognize them, it dies. T cells that can react with non-self molecules survive. This is positive selection (Sri Lakshmi, 2014, pp.367-372). T cells are selected because of their lack of recognition of self. Positive selection ensures removing lymphocytes with ineffective receptors allowing the effective antibodies the space to clone and survive, which maintains a controlled size of population (repertoire) (Haag et al, 2007, pp.420-435). T cells that can pass through the thymus react to non-self cells, but they are unable to react to self cells.

Clonal selection

Burnet (1959) proposed the clonal selection theory which describes the HIS basics. The immune response is made possible by the antigen-recognizing surface receptor molecules of both the B and T cells and is based on the complementarities between the antibody receptor and the antigen (De Castro & Timmis, 2002b). An antibody can potentially identify another antibody if their receptor arrangement matches. If the HIS cannot perform this distinction, it may be triggered against self (Haag et al, 2007, pp.420-435). As a response to an antigenic stimulus, the organism activates the cells that match a particular antigen which proliferate and secrete antibodies (De Castro & Timmis, 2002a, pp.669-674). Cells are stimulated to produce clones of themselves very quickly, thus producing more antibodies at high speed (Aickelin & Dasgupta, 2005). In 2002, De Castro & Von Zuben (De Castro & Von Zuben, 2002) presented the algorithm named CLONALG, developed to perform pattern recognition and optimization. The authors demonstrated the ability of the algorithm to learn a set of input patterns by "selecting, reproducing and mutating a set of artificial immune cells". They highlighted two important features of affinity maturation of B cells that can be applied in artificial immune systems: 1) proliferation of B cells is proportional to the affinity of the antigen that binds, and 2) mutations suffered by the antibody of a B cell are inversely proportional to the affinity of the antigen. When applied to pattern matching, a set of patterns *S* to be matched are considered to be antigens. The task of CLONALG is then to produce a set of memory antibodies *M* that match *S*.

Immune network theory

The immune network theory (INT) proposed by Jerne (1974, pp.373-389) suggested that the HIS is composed of a regulated network of cells and molecules that recognize one another even in the absence of antigens (De Castro & Von Zuben, 2001). Jerne concluded that the immune system must display a behavior or activity resulting from interactions with itself and from these interactions immunological behavior such as tolerance and memory emerge. The discrete immune network model (DINM) is proposed by Timmis & Neal (2001, pp.121-130).

Danger theory

In 1994, Matzinger (Matzinger, 1994) proposed a new immunological danger model. The immune system does not concentrate to distinguish between self and non-self, but to danger and safe. The main idea is that the immune system should not react to "non-self but harmless" but to "self but harmful". The theory claims that an immune system response is triggered by alarm signals sent out when danger is "detected". The activated antigen presenting cells are able to provide the necessary co-stimulatory signal to the T helper cells that subsequently control the adaptive immune response. The danger signals are emitted by ordinary cells of the body that have been injured due to an attack by a pathogen. The main objective of the danger theory based system (DTBS) is to reduce false positive and negative errors and maintain high detection accuracy of the model.

Dendritic cell algorithm

In the danger theory, danger is measured by damage to cells indicated by distress signals sent out when cells die from unnatural causes (Aickelin & Cayzer, 2002, pp.141-148). The signals are detected by dendritic cells (DCs) that have three modes of operation: immature, semi-mature, and mature. In the immature state, a DC collects an antigen along with safe and danger signals from its local environment. DCs are able to integrate these signals to decide whether the environment is safe or dangerous. If safe, a DC becomes semi-mature and, upon presenting an antigen to T-cells, the DC causes T cell tolerance. If dangerous, the DC becomes mature and causes the T cell to become reactive on antigen-presentation. The DC algorithm (DCA) introduces the notion of danger signals as well as safe and pathogen-associated signals which all contribute to the context of a data signal at any given time.

Applications of AISs

Malicious attacks, hardware failure, or human errors can be considered anomalies. Detection of anomalies is based on irregularities in the pattern with respect to the normal pattern. Anomaly detection creates a model of normal behavior of the system and then looks for activities that differ from the created model. The main idea is to learn from examples of one class and generate the detectors of deviations. The HIS, by its nature, does not perform optimization. There are various optimization algorithms such as CLONALG, opt-aiNet, and B-cell algorithm, which are all based on the clonal selection principles. All the approaches use cloning, mutation, and selection to build a population of solutions. The earliest AIS algorithm for unsupervised clustering was aiNet, proposed by De Castro and van Zuben (2001).

AIS-based intrusion detection systems

Intrusion detection systems (IDSs) monitor computer network traffic in order to detect malice or anomalies. IDSs can be either network-based or host-based. The network-based IDS (NIDS) scans network packets at audits packet information and logs suspicious packets into the log file. The host-based IDS (HIDS) monitors information collected from individual computer systems. There are two basic advantages of an AIS over an IDS: 1) it provides passively proactive protection via negative detection, and 2) it is capable of adapting to dynamically changing environment.

Performances of the models

Performances of the models are often measured based on: true positive (*TP*), true negative (*TN*), false positive (*FP*), and false negative (*FN*), where *TP* represents the number of positive samples correctly classified as positive, *TN* represents correctly classified negatives as negative, *FN* represents the number of positive samples wrongly classified as negative, and *FP* represents the number of negative samples wrongly classified as positive. The key criterion which differentiates classifiers is prediction accuracy (*ACC*), which represents the ratio of the number of instances correctly classified to the total number of instances (Eq. 1).

$$ACC = \frac{TP + TN}{TP + TN + FP + FN}, \qquad (1)$$

Researchers often use other measures such as the false positive rate (*FPR*) that is defined as the probability that a false alarm will be raised (Eq. 2),

$$FPR = \frac{FP}{TN + FP}. \quad (2)$$

or the false negative rate (*FNR*) which is the probability that a TP will be missed by the classifier (Protic, 2020, pp.603-605) (Eq. 3).

$$FNR = \frac{FN}{TP + FN} \quad (3)$$

Detection of a specific attack

Once an attack has been discovered, the signature of the attack is stored in the black-list used to check against the normal network traffic and to detect if an attack has happened. Newly discovered attacks are added to the dataset of known attacks. The disadvantages of misuse detection are dependence on the size and the efficiency of the black-list, and vulnerability to a zero-day attack. Publicly available datasets often used for the known attack detection are the KDD Cup '99 and the NSL-KDD dataset. The KDD Cup ‘99 dataset is collected by simulation of the operation of a typical US Air Force Local Area Network with attacks classified into four categories: 1) probe, 2) denial of service (DoS), 3) user to root (U2R), and 4) remote to local (R2L). The dataset contains 41 features which fall into the following categories: 1) basic, 2) traffic, 3) content, 4) host-related attack, and 5) normal behavior (Aggarwal & Sharma, 2015, pp.842-851). On the other hand, the KDD Cup ‘99 dataset contains redundant and duplicate records which prevent classifying the other records. To fix these issues, Tavallaee et al (2009) proposed the NSL-KDD dataset that consists of selected features from the KDD Cup‘99 dataset excluding redundant records in the training set and duplicates in the test set (Protic, 2018, pp.585-586).

Many authors presented various results on the specific attack recognition. Al-Dabagh & Ali (2011, pp.381-390) presented the dendritic cell algorithm for the detection of DoS in the real time. Flow-based DoS detection schemes for high speed networks have been proposed by Wang et al (2012, pp.646-650) as an effective supplement to payload-based solutions. The existing flow-based solutions had serious limitations in detecting unknown attacks and efficiently identifying real attack flows buried into the background traffic, and had difficulty to adapt to attack dynamics. To address these issues, the authors proposed a flow-based DoS detection scheme based on Neighborhood Negative Selection (NNS) as the detection algorithm for unknown DoS attacks, and identified attack flows from massive traffic.

Anomaly detection

NIDSs are deployed at the computer network level and work by tracking network traffic. The aim of such systems is to detect if there was an attack or not. If an attack is detected, NIDSs rise an alert and create/respond to the log of attack (depending on the NIDS configuration). The anomaly-based NIDSs are deployed in the most critical parts of the computer network and learn from the network behavior. The longer the IDS is in the network, the more effective it will be. Any deviation from the normal traffic is considered an anomaly. The threshold level configured in the anomaly-based IDS will dictate the detection of anomalies. The main issue of such IDSs is a high level of FP. For that reason, the system has to be configured not to become insensitive to such alarms.

For the purpose of anomaly detection, the Kyoto 2006+ dataset is often used in experiments. It is built on real network traffic collected from 2006 to 2015 on five different computer networks inside and outside the Kyoto University. The records consist of 14 statistical features derived from the KDD Cup ‘99 dataset and 10 additional features which can be used for further analyses of systems. During the observation period, ~50 million sessions of normal traffic and ~43 million sessions of attacks and ~425 thousands sessions of unknown attacks were recorded.

One of the results on anomaly detection presented in this paper is based on NSA and the NSL-KDD dataset. The IDS proposed by Kumarvel (2016) that is based on the algorithm Elberfeld and Textor (2011, pp.534-542) shows lesser FP, lesser computational overhead and higher detection rates if compared with the literature. A Java application has four modules: 1) input (captures traffic from the input); two types of files are to be fed into the input module – the self file is used for training and generation of the detector set while the test file uses a packet of normal traffic that is to be monitored, 2) the network converter converts the data into binary strings, 3) the negative selection module generates detectors, and 4) classification. The Hamming distance, r-contiguous matching, and r-chunk matching are used to compute affinity (Kumarvel, 2016, pp.23-31). The testing of the IDS was based on the false alarm rates, the Receiver Operating Characteristics (ROC) analysis and the testing environment. Another example of anomaly detection based on NSA is proposed by Shen (2012, pp.18-48). The scheme consists of two weighted feature selection algorithms based on the Rough Set Algorithm (RSA) and Linear Genetic Programming (LGP). Weighting the contribution of the parameters in the IDS improved the performance of the algorithms. The results indicate that the proposed scheme outperforms most of the existing IDS on the same testing data set.

The aim of the research conducted by Murad & Mohd. Aizani, (2012, pp.147-154) was to address the impact of the feature reduction in designing an anomaly detection system based on the immune network theory to detect novel attacks. The results on anomaly detection show that the detection rate ranges from 80.25% to 82.25%, while the FPR ranges from 0.1975 to 0.1775.

AIS vs. machine learning

AIS and machine learning (ML) - based IDSs have advantages and disadvantages one over the other. AIS algorithms are easy to be used in classification (supervised learning) or clustering (unsupervised learning). The methods used in the AIS design include: 1) generation of antibodies, 2) diversity, 3) distributed systems, 4) dynamic systems, 5) self-organizing memory, and 6) noise/error tolerance. However, there are several issues that can occur during the evaluation of models, so several questions have to be answered: *How to determine antigens, antibodies and B cells?, How to define memory cells?, How to determine the similarity between an antigen and an antibody?, and What are the basic calculations in the AIS models?* It is obvious that both supervised and unsupervised learning can be used to develop AIS-based IDSs. The CLONALG and Hypermutation are instance-based models. Negative and positive selection algorithms are algorithms with regularization (positive selection) and clustering algorithms (negative selection). Immune networks are algorithms with regression or with associated rules. The danger theory is based on the decision tree, or the associated rules algorithms. Dendritic cell algorithms work in the similar way to the danger theory algorithms but the tolerance to the signal indicating danger has to be properly set.

The experiments presented in this paper are conducted to four data sets from the Kyoto 2006+ dataset. Each dataset consists of different number of instances (158572, 129651, 128740 and 136625). Of all instances, 70% were used for training and 30% were used for testing the models. Of 24 features from the Kyoto 2006+ dataset, nine features are used for classifiers': Flag, IDS_detection, Count, Same_srv_rate, Serror_rate, Srv_serror_rate, Dst_host_count, Dst_host_srv_count, Dst_host_same_src_port_rate, and Dst_host_serror_rate. The Label feature indicated whether the session was an attack or not. Features are chosen based on expert knowledge and the pre-processing algorithm which cuts all categorical features, removes statistical features, cuts all features which can be used for further analyses, cuts all features that cannot be normalized into the range [-1,1] and normalizes the remaining instances into the range [-1,1] by applying the tangent hyperbolic function (Protić & Stanković, 2018, p.43).

Four ML models are used for the binary classifications: the Decision tree (DT) (Sebastiani, 2012, p.13), the support vector machine (SVM) (Burges, 1998, p.291), the k-Nearest Neighbor (k-NN), and the weighted k-NN (wk-NN) (Hechenbichler & Schilep, 2004). The results show high accuracy for the k-NN and the wk-NN, followed by the DT and the SVM. The fastest model is the DT. The processing time (sum of training and testing time) is more than 100 times shorter than the processing time for all the other models (Table 1).

Table 1 – Accuracy and processing time
Таблица 1 – Точность и время обработки
Табела 1 – Тачност и време обраде

No	Size	Model	Accuracy	Processing time
1	158572	k-NN	98.3%	275.72s
		wk-NN	98.4%	277.32s
		SVM	98.1%	449.35s
		DT	97.2%	3.8452s
2	129651	k-NN	91.8%	175.84s
		wk-NN	91.8%	173.32s
		SVM	98.3%	254.32s
		DT	97.3%	3.3104s
3	128740	k-NN	98.2%	193.82s
		wk-NN	98.1%	194.81s
		SVM	97.8%	280.82s
		DT	97.2%	3.3033s
4	136625	k-NN	99.3%	194.83s
		wk-NN	99.4%	194.23s
		SVM	99.1%	217.32s
		DT	98.3%	8.3169s

As it can be seen, the wk-NN has the highest accuracy (up to 99.5%), while the accuracies of both k-NN and DT classifiers are much higher than the accuracy of the SVM. A significantly shorter processing time of the DT model is due to the Iterative Dichotomy 3 algorithm. The results point to the given pros and cons of the models. Eager ML models are very accurate but the training and testing time can be very long. This is not the characteristic that suits the real-time for detection of the attack such as DoS or Distributed DoS (DDoS). On the other hand, DT models are very fast but their accuracy is significantly low and corresponds to the accuracy of the IDS based on the immune network theory. NSAs are highly accurate but the processing time of these algorithms can be significantly slow if the number of the detectors is high and the threshold is not set well. Also, NSAs are mostly used in anomaly detection. ML models based on the SVM showed better results in the detection of U2R and R2L attacks. The results also showed that the accuracy of the models trained and tested on the real data flow is higher than the accuracies of the model trained on the simulated data.

Conclusions

Artificial immune systems are accurate and fast computational models inspired by the human immune system. They are often used in intrusion detection. There are two trends in intrusion detection: signature and anomaly detection. The basic concepts of AIS are negative selection, positive selection, clonal selection, immune networks, danger theory, and dendritic cell algorithm. IDSs based on the AIS are often compared to IDSs based on ML. Experiments on different datasets show that the models can be used in both known attack and anomaly detection. Eager ML classifiers show better results in the decision, which is an advantage if processing time is not significant. Dendritic cell algorithms and negative selection algorithms show better results for real-time detection.

References

Aggarwal, P. & Sharma, S.K. 2015. Analysis of KDD Dataset Attributes –Class Wise for Intrusions Detection. *Procedia Computer Science*, 57, pp.842-851. Available at: https://doi.org/10.1016/j.procs.2015.07.490.

Aickelin, U. & Cayzer, S. 2002. The Danger Theory and Its Application to Artificial Immune Systems. In: *CARIS 2002: 1st International Conference on Artificial Immune Systems,* University of Kent at Canterbury, UK, pp.141-148, September 9-11. Available at: http://dx.doi.org/10.2139/ssrn.2832054.

Aickelin, U. & Dasgupta, D. 2005. Artificial Immune Systems. In: Burke, E. & Kendal, G. (Eds.) *Introductory Tutorials in Optimization, Decision Support and Search Methodology* [e-book section] Alphen aan den Rijn: Kluwer. Available at: http://eprints.nottingham.ac.uk/336/1/05intros_ais_tutorial.pdf [Accessed: 10 August 2020].

Al-Dabagh, N.B.I & Ali, I.A. 2011. Design and implementation of artificial immune system for detecting flooding attacks. In: *International Conference on High Performance Computing & Simulation (HPCS)*, Istanbul, pp.381-390, July 4-8. Available at: https://doi.org/10.1109/HPCSim.2011.5999850.

Burges, M. 1998. Computer Immunology. In: *Proceedings of the 12th Systems Administration Conference (LISA '98)*. Boston, MA, USA, pp.283-298, December 6-11 [online]. Avialble at: https://www.usenix.org/legacy/event/lisa98/full_papers/burgess/burgess_html/burgess.html [Accessed: 10 August 2020].

Burnet, F.M. 1959. *The clonal selection theory of acquired immunity.* Nashville, Tennessee, USA: Vanderbilt University Press. Available at: https://doi.org/10.5962/bhl.title.8281.

De Castro, L.N. & Timmis, J. 2002a. An artificial immune network for multimodal function optimization. In: *Proceedings of the 2002 Congress on Evolutionary Computation. CEC'02 (Cat. No.02TH8600),* Honolulu, HI, USA, pp.669-674, May 12-17. Available at: https://doi.org/10.1109/CEC.2002.1007011.

De Castro, L.N. & Timmis, J. 2002b. *Artificial Immune Systems: A New Computational Intelligence Approach.* London: Springer-Verlag Publishing. ISBN: 978-1-85233-594-6.

De Castro, L.N. & Von Zuben, F.J. 1999. Artificial Immune Systems: Part I – Basic Theory and Applications. *Technical Report TR - DCA 01/99,* pp.1-95.

De Castro, L.N. & Von Zuben, F.J. 2001. aiNet: An Artificial Immune Network for Data Analysis. In: Abbas, H.A., Sarker, R.A. & Newton, C. (Eds.) *Data Mining: A Heuristic Approach.* USA: Idea Group Publishing [online]. Available at: http://www.dca.fee.unicamp.br/~vonzuben/research/lnunes_dout/artigos/DMHA.PDF [Accessed: 10 August 2020].

De Castro, L.N. & Von Zuben, F.J. 2002. Learning and optimization using the clonal selection principle. *IEEE Transactions on Evolutionary Computation,* 6(3), pp.239-251. Available at: https://doi.org/10.1109/TEVC.2002.1011539.

Elberfeld, M. & Textor, J. 2011. Negative selection algorithms on strings with efficient training and linear-time classification. *Theoretical Computer Science*, 412(6), pp.534-542. Available at: https://doi.org/10.1016/j.tcs.2010.09.022.

Forrest, S., Perelson, A.S., Allen, L. & Cherukuri, R. 1994. Self-nonself discrimination in a computer. In: *Proceedings of 1994 IEEE Computer Society Symposium on Research in Security and Privacy,* Oakland, CA, pp.202-212, May 16-18. Available at: https://doi.org/10.1109/RISP.1994.296580.

Haag, C.R., Lamont, G.B., Williams, P.D. & Peterson, G.L. 2007. An artificial immune system-inspired multiobjective evolutionary algorithm with application to the detection of distributed computer network intrusions. In: *GECCO '07: Proceedings of the 9th annual conference companion on Genetic and evolutionary computation,* London, UK, pp.2717-2724, July. Available at: https://doi.org/10.1145/1274000.1274035.

Hechenbichler, K. & Schilep, K. 2004. Weighted k-Nearest Neighbor Techniques and Ordinal Classification. S*onderforschungsbereich 386*, Paper 399, pp.1-16 [online]. Available at: https://epub.ub.uni-muenchen.de/1769/1/paper_399.pdf [Accessed: 10 August 2020].

Jerne, N.K. 1974. Towards a Network Theory of Immune System. *Ann Immunol (Paris),* 125C(1-2), pp.373-389. PMID: 4142565.

Ji, Z. & Dasgupta, D. 2007. Revisiting Negative Selection Algorithms. *Evolutionary Computation,* 15(2), pp.223-251. Available at: https://doi.org/10.1162/evco.2007.15.2.223.

Matzinger, P. 1994. Tolerance, danger, and the extended family. *Annual Review of Immunology,* 12, pp.991-1045. Available at: https://doi.org/10.1146/annurev.iy.12.040194.005015.

Murad, A.R. & Mohd. Aizani, M. 2012. Artificial Immune network Clustering Approach for Anomaly Intrusion Detection. *Journal of Advances in Information Technology,* 3(3), pp.147-154. Available at: https://doi.org/10.4304/jait.3.3.147-154.

Protić, D.D. 2018. Review of KDD CUP ’99, NSL-KDD and KYOTO 2006+ Datasets. *Vojnotehnički glasnik/Military Technical Courier*, 66(3), pp.580-596. Available at: https://doi.org/10.5937/vojtehg66-16670.

Protić, D.D. 2020. Influence of preprocessing on anomaly-based intrusion detection. *Vojnotehnički glasnik/Military Technical Courier,* 68(3), pp.598-611. Available at: https://doi.org/10.5937/vojtehg68-27319.

Protić, D. & Stanković, M. 2018. Anomaly-Based Intrusion Detection: Feature Selection and Normalization Influence to the Machine Learning Models Accuracy. *European Journal of Formal Sciences and Engineering*, 2(3), pp.101-106. Available at: http://dx.doi.org/10.26417/ejef.v2i3.p101-106.

Sebastiani, F. 2002. Machine learning in automated text categorization. *ACM Computing Surveys,* 34(1), pp.1-47. Available at: https://doi.org/10.1145/505282.505283.

Shen, J. 2012. *Network intrusion detection by artificial immune system.* MA thesis. Melbourne, Australia: RMIT University - School of Engineering [online]. Available at: https://researchrepository.rmit.edu.au/discovery/fulldisplay?docid=alma9921863885901341&context=L&vid=61RMIT_INST:ResearchRepository&lang=en&search_scope=Research&adaptor=Local%20Search%20Engine&tab=Research&query=any,contains,Shen,%20J.%202012.%20Network%20Intrusion%20Detection%20By%20Artificial%20Immune%20System.&offset=0 [Accessed: 10 August 2020].

Sri Lakshmi, K. 2014. Implementation of Artificial Immune System Algorithms. *International Journal of Application or Innovation in Engineering and Management (IJAIEM),* 3(6), pp.367-372. Available at: https://www.ijaiem.org/Volume3Issue6/IJAIEM-2014-07-01-90.pdf.

Tavallaee, M., Bagheri, E., Lu, W. & Ghorbani, A.A. 2009. A detailed analysis of the KDD CUP 99 data set. In: *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications,* Ottawa, ON, Canada, July 8-10. Available at: https://doi.org/10.1109/CISDA.2009.5356528.

Timmis, J., Hone A., Stibor, T. & Clark, E. 2008. Theoretical advances in artificial immune systems. *Theoretical Computer Science,* 403(1), pp.11-32. Available at: https://doi.org/10.1016/j.tcs.2008.02.011.

Timmis, J. & Neal, M. 2001. A resource limited artificial immune system for data analysis. *Knowledge-Based Systems*, 14(3-4), pp.121-130. Available at: https://doi.org/10.1016/S0950-7051(01)00088-0.

Wang, D., He, L., Xue, Y. & Dong, Y. 2012. Exploiting Artificial Immune systems to detect unknown DoS attacks in real-time. In: *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, Hangzhou, China, pp.646-650, October 30 - November 1. Available at: https://doi.org/10.1109/CCIS.2012.6664254.

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ, ОСНОВАННОЕ НА ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЕ

Даниела Д. Протич

Вооруженные силы Республики Сербия, Генеральный штаб,
Управление информатики и телекоммуникаций (J-6),
Центр прикладной математики и электроники,
г. Белград, Республика Сербия

РУБРИКА ГРНТИ: 20.00.00 ИНФОРМАТИКА:
20.15.05 Информационные службы, сети, системы в целом
ВИД СТАТЬИ: оригинальная научная статья

Резюме:

Введение/цель: Искусственная иммунная система − это вычислительная модель, вдохновленная биологической или человеческой иммунной системой, которая защищает организм от патогенов и различает собственные клетки от инородных. Особо интересным в искусственной иммунной системе является то, как человеческий организм реагирует на новые патогены и как он адаптируется, становясь невосприимчивым в течение длительного периода после борьбы с заболеванием, что относится к распознаванию уже известной атаки, и способу, которым иммунная система идентифицирует собственные клетки, на которые не реагирует и как обнаруживает аномалии.

Методы: В исследовании применялись следующие методы: отрицательный отбор, положительный отбор, клональный отбор, иммунные сети, теория опасности и алгоритм дендритных клеток.

Результаты: Представлены различные алгоритмы и модели, относящиеся к искусственным иммунным системам, и два принципа классификации: один основан на обнаружении конкретной атаки, а другой − на обнаружении аномалии.

Выводы: Искусственные иммунные системы часто используются для обнаружения вторжений в компьютерные сети, потому что они точные и быстрые. Эксперименты с различными наборами данных показывают, что модели можно использовать как для обнаружения атак, так и для обнаружения аномалий. Классификаторы на основе машинного обучения показывают лучшие результаты при принятии решений, что является большим преимуществом, если время обработки не является значимым параметром. Алгоритмы дендритных клеток и алгоритмы отрицательного отбора показывают лучшие результаты для обнаружения в реальном времени.

Ключевые слова: искусственная иммунная система, обнаружение вторжений.

ДЕТЕКЦИЈА НАПАДА ЗАСНОВАНА НА ВЕШТАЧКОМ ИМУНОМ СИСТЕМУ

Данијела Д. Протић

Војска Србије, Генералштаб, Управа за телекомуникације и информатику (J-6), Центар за примењену математику и електронику,
Београд, Република Србија

ОБЛАСТ: рачунарске науке, информационе технологије
ВРСТА ЧЛАНКА: оригинални научни рад

Сажетак:

Увод/циљ: Вештачки имуни систем (ВИС) инспирисан је биолошким имунолошким системом који разликује сопствене ћелије од оних које то нису. За ВИС је занимљив начин на који тело реагује на патогене и прилагођава се да остане имуно дужи период. То се односи на препознавање познатог напада и начин на који имуни систем идентификује сопствене ћелије на које не треба да реагује, и на откривање аномалије.

Методе: Приказане су методе негативне и позитивне селекције, затим клонирање, имуне мреже, теорија опасности и алгоритам дендритичних ћелија.

Резултати: Представљени су модели који се односе на ВИС и два принципа класификације – један заснован на детекцији одређеног напада, а други на детекцији аномалије.

Закључак: Вештачки имуни системи користе се у откривању упада у рачунарске мреже јер су тачни и брзи. Експерименти на различитим скуповима података показују да се модели могу користити у откривању напада или аномалија. Класификатори засновани на машинском учењу показују боље резултате у одлуци, што је велика предност ако време обраде није значајан параметар. Алгоритми дендритичких ћелија и алгоритми негативног одабира показују боље резултате за детекцију у реалном времену.

Кључне речи: вештачки имуни систем, детекција упада.

Paper received on / Дата получения работы / Датум пријема чланка: 10.08.2020.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 10.10.2020.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 12.10.2020.