Design of Adaptive IDS with Regulated Retraining Approach

Anazida Zainal[1], Mohd Aizaini Maarof[1], Siti Mariyam Shamsuddin[2], and Ajith Abraham[3]

[1] Information Assurance and Security Research Group,
[2] Soft Computing Research Group,
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia
81310 Skudai, Johor
[3] IT for Innovations, EU Center of Excellence, Technical University of Ostrava,
Czech Republic
{anazida,aizaini,mariyam}@utm.my, ajith.abraham@ieee.org

Abstract. Computer networks are becoming more insecure and vulnerable to intrusions and attacks as they are increasingly accessible to users globally. To minimize possibility of intrusions and attacks, various intrusion detection models have been proposed. However, the existing procedures suffer high false alarm, not adequately adaptive, low accuracy and rigid. The detection performance deteriorates when behavior of traffic is changing and new attacks continually emerge. Therefore, the need to update the reference model for any given anomaly-based intrusion detection is necessary to keep up with these changes. Severe changes should be addressed immediately before the performance is compromised. Available updating approaches include dynamic, periodic and regulated. Unfortunately, none considers severity of changes to trigger the updating. This paper proposed an adaptive IDS model using regulated retraining approach based on severity of changes in network traffic. Therefore, retraining can be done as and when necessary. Changes are denoted by ambiguous decisions and assumed to reflect insufficient knowledge of classifiers to make decision. Results show that the proposed approach is able to improve detection accuracy and reduce false alarm.

Keywords: adaptive, intrusion detection, dynamic, regulated.

1 Introduction

Information is becoming ubiquitous with Internet infrastructure and sensitive information exposure is inevitable. Studies covering the prevention, detection and the forensic aspect of computer network attacks have long being researched on. The prevention techniques such as encryption, Virtual Private Network (VPN) and firewall alone seem to be inadequate. It reduces exposure rather than monitors or eliminates vulnerabilities in computer systems (Ghosh et al., 1998). Therefore, it is important to have

A. Ell Hassanien et al. (Eds.): AMLTA 2012, CCIS 322, pp. 590–600, 2012.

a detecting and monitoring system to protect important data. The outraging incident of Morris Worm in 1988, Code Red in 2001 and followed by SQL Slammer in 2003 (Langin and Rahimi, 2010) had handicapped many organizations including businesses, military, education and others. The importance to safeguard network against confidentiality, integrity and availability (CIA) breaches is an important issue and intrusion detection plays vital role in ensuring a secure network. This increasing importance of computer network security motivates various aspects of security related research that provide new solutions, which might not be achievable by conventional security approaches.

An Intrusion Detection System (IDS) is an automated system that can detect a computer system intrusion either by using the audit trail provided by an operating system or by using the network monitoring tools. The main goal of intrusion detection is to detect unauthorized use, misuse and abuse of computers by both system insiders and external intruders (Kim, 2002; Kim et al., 2007). IDS does not eliminate any preventive mechanism but provides the defense in safeguarding the computer system. In IDS, misuse and anomaly are the two types of detection approaches. Misuse detection can detect known attacks by constructing a set of signatures of attacks while anomaly detection recognizes novel attacks by modeling normal behaviors (Xu and Wang, 2005). The outcome of this modeling is called reference model. A significant deviation from the model of reference indicates a potential threat. Anomaly detection approach is popular because it is a possible approach to detecting unknown or new attacks (Denning, 1987; Forrest et al., 1996; Warrander et al., 1999). Unfortunately, anomaly detection approach suffers high false alarm especially when IDSs use pattern recognition algorithms in operational environments (Giacinto et al., 2003).

Two major problem characteristics of IDS are; trend in network traffic; and limitation of the existing IDS tools and techniques. Normal traffic patterns are changing due to changes in work practices and nature of intrusions usually polymorph and continuously evolve (Wu and Banzhaf, 2010). Therefore, intrusion detectors must undergo frequent retraining to incorporate new normal traffic samples into the training data for classifying novel attacks and changes from existing normal behavior (Zhang and Shen, 2004). The periodic reconstruction of reference model can provide adaptation to the new environment (Tapiador *et al.*, 2004) and this will ensure that the new learnt model is relevant. Modern IDS requires adaptability in order to respond to constantly changing threat environment (Shafi and Abbas, 2009). Unfortunately many of the existing intrusion detection methods (misuse detection and anomaly detection) are generally incapable of adapting detection systems to the change of circumstance, which causes a declination of detection precision and rise in false alarm rate and it remains a major problem in IDS (Hossain and Bridges, 2001; Giacinto *et al.,* 2003; Yu *et al*., 2005; Yang *et al.,* 2005; Xu and Wang, 2005). Traditional anomaly based methods commonly build a static (rigid) reference model based on training dataset during modeling and then utilize this model to predict on new network behavior data at detecting stage (Yang *et al.,* 2005). With time, this reference model becomes irrelevant and obsolete.

There are few major challenges in anomaly-based IDS and among the critical ones are high workload and inability to update reference model which has direct impact on

accuracy of detection. The scope of this paper will focus workload reduction and adaptability.

The chapter is organized into six sections. Section 2 gives an overview on adaptive IDS and some existing approaches toward building adaptability into IDS and Section 3 explains the design of the proposed Adaptive IDS. Section 4 describes experimental procedure follows by Section 5 describing results obtained and discussion. Finally Section 6 summarizes and concludes the paper.

2 Adaptive Intrusion Detection System

Since the Normal network traffic patterns are changing and new attacks are continually evolved, IDS needs to be updated. Failure to update these changes may degrade its detection performance. This is undesirable as the network of computers needs to be protected and firewall alone is not sufficient. Adaptive IDS in the context of this work refers to the ability of an IDS to dynamically change the model of reference through relearning or retraining in addressing the dynamic nature of network traffic pattern.

A typical stationary anomaly-based IDS system requires only one-time training which is done at the beginning of IDS system development in order to obtain reference model. This model was then utilized to predict network behavior during detection stage (Yang et al., 2005). However, it is important to note that intrusions usually polymorph and continuously evolve (Wu and Banzhaf, 2010). Therefore, it resulted in poor performance. Besides associated with low detection rate, its inability to adapt to the changes that occur in both normal and attack traffic patterns, would cause high false alarms (Eskin et al., 2000; Hossein et al., 2003; Xu and Wang, 2005; Liu et al., 2007; Shafi and Abbas, 2009). Therefore, an intrusion detection system must be able to adapt to the changing environment while still recognizing abnormal activities (Hossain and Bridges, 2001).

Table 1 summarizes related researches on adaptive IDS from year 2000 to 2009. The issue is how to make IDS adaptive. Adaptive in this context refers to an ability to update in order to cope with the changes happen in the network traffic. Generally, the models are either rule-based or model-based.

In rule-based approach, a new rule will be added to the existing rule set and retraining is required in model-based approach.

Although an update can be instantly done, this approach has some drawbacks and they are:

1. the detection time is affected as the list grows
2. initial rule-sets must be comprehensive to avoid excessive rules add-on
3. lacks of flexibility as slight variation to the sequence may affect activity to rule comparison

Shafi and Abbas (2009) managed to curtail the list of rules to a predefined size. This was achieved by pruning less significant or less generalized existing rules and replaced by new significant and generalized rules. Usually changes in the environment

were detected when sequence extracted from an instance does not match with any of the available rules as implemented in Fan and Stolfo (2002) and Shafi and Abbas (2009). Despite the automatic rule generation, human intervention is still required to confirm the label for sequence in the newly created rule before it can be updated. In contrast to the growing list of rules, model-based approach produces a model with consistent size. Therefore, detection time remains short and unchanged. However, it requires retraining using the whole training dataset together with the additional new training data in order to update the reference model.

The updating strategies as listed in first column of Table I can be classified as, periodic updating, regulated updating, dynamic updating and manual updating. The description of each strategy is given below.

Table 1. Related Works on Adaptive IDS

Updating Strategy	Researchers	Detection Techniques	Training & Testing Data
Periodic	Hofmeyr, 1999	Model-based (AIS)	subnet at CS Dept, Univ.of New Mexico
	Kim, 2003	Model-based (AIS)	Trouble shootout data
Regulated	Hossain *et al*., 2003	Similarity measure & rule-based	mail & web servers, MSU
	Liu *et al*., 2007	Model-based	KDDCup 1999 datasets
	Burbeck and Tehrani, 2007	Clustering	KDDCup 1999 datasets
Dynamic	Lee *et al*., 2000	Rule-based	LBL and IWSS16 datasets
	Fan and Stolfo, 2002	Rule-based (RIPPER)	1998 DARPA IDS Evaluation dataset
	Lee *et al*., 2002	Rule-based	LBB-CONN-7 (TCP/IP network traffic)
	Chavan *et al*., 2004	Rule-based	KDDCup 1999 datasets
	Yang *et al*., 2005	Rule-based	KDDCup 1999 datasets
	Lee *et al*., 2006	Incremental Clustering (+Kernel Method)	KDDCup 1999 datasets
	Jemili *et al*., 2007	Statistical (Bayesian Network)	KDDCup 1999 datasets
	Shafi and Abbas, 2009	Rule-based (UCSm)	KDDCup 1999 datasets
Manual	Eskin *et al*., 2000	Model-based (*manually set the period for model generation, based on weekly data collected*)	System calls
	Yu *et al*., 2005	Clustering & rule-based (*manually applied the rule mining algorithm to extract rules from cluster*)	KDDCup 1999 datasets
	[1]Xu and Wang, 2005	Model-based (*Notion of adaptive refers to dynamic composition of several classifiers*)	KDDCup 1999 datasets
	[2]Tang *et al*., 2008	Rule-based (*reordering the sequence of rules based on specified metric performance*)	KDDCup 1999 datasets

(a) Periodic Updating

Update is done in certain interval or time frame. A lifespan is imposed to a classifier and after it has expired, the same classifier will undergo retraining (with some additionally new data) as such the new model will reflect the new patterns of normal and attacks.

(b) Dynamic Updating

The changes are incorporated as and when they are detected. In rule-based, usually a newly created rule will be appended to the existing rule set.

(c) Regulated Updating

The update is triggered when a preset threshold is met and usually associated with changes. Usually the regulated updating can be divided into two type which are quantity-based and quality-based threshold. An example of quantity-based is the work of Liu *et al*. (2007).

(d) Manual Updating

Feedback by the system administrator is required especially when the IDS starts to produce false alarms such as in Burbeck and Tehrani (2007). Since manual update heavily relies on human intervention, it is not the interest of this study to cover this particular updating strategy.

Hofmeyr (1999) and Kim (2003) implemented periodic updating strategy mimicking human antibodies replenishment concept in Artificial Immune System (AIS). Both works imposed lifespan on the validity of the detectors (classifiers), where a new set of detectors were created when the previous detectors age expired. Periodic updating strategy is not suitable especially when the occurrence of changes to normal network traffic patterns and emergence of new attacks are unpredictable. Worst case scenarios of this approach are described in Section 2.6.4. Periodic updating approach does not require any triggering event because the updating is scheduled. Therefore, changes in the network traffic patterns are irrelevant. Meanwhile, dynamic updating requires continuous update if changes are rapid. One of the seminal works on adaptive IDS was done by Lee et al. (2000) started with rule-based adaptive IDS. The traditional association rule mining proposed by Lee et al. (2000) was replaced by recent rule-mining techniques such as Fuzzy Inference and Artificial Neural Network as done by Chavan et al. (2004) and Liao et al. (2007) and Genetic Algorithm and Learning Classifier System by Shafi and Abbas (2009). Dynamic updating strategy is pursued until now. Table 2.2 reveals that it is common to adopt dynamic updating approach when the proposed models are rule-based. Dynamic updating adds new rule when there is no rule match the tested instance. Another updating approach is regulated. This approach commonly requires threshold to trigger the update such as in Hossain et al. (2003), Liao et al. (2007) and Burbeck and Tehrani (2007). Hossain et al. (2003) used sliding window and changes are measured relative to the traffic captured in one window size. Assumption on gradual change denotes changes in Normal behavior have led to poor performance. Meanwhile, Liu et al. (2007) used amount of uncertain

instances and Burbeck and Tehrani (2007) used amount of false alarms as a threshold to trigger updating. Usually model-based together with clustering are used in this regulated updating approach as in Liu et al. (2007) and Burbeck and Tehrani (2007).

3 The Proposed Adaptive Intrusion Detection Model

Most of the existing intrusion detection system suffers from several problems and among them are high resource consumption and high overhead, high false alarm, poor detection accuracy. The proposed model is designed to address the following issues:

(i) High overhead due to voluminous data. Some are unnecessary recognition.
(ii) Low detection accuracy and high false alarm due to obsolete model of reference.
(iii) Poor detection due to; vague boundary between normal and abnormal and imbalanced data problem.
(iv) Note: The issue of severe class imbalanced is not considered in this study.

In order to solve the above problem situations, two solution concepts are formulated and they are; improve data representation through feature selection and update the model of reference through regulated retraining.

The model comprises of three components; (i) Pre-detection, (ii) Detection and (iii) Training and Retraining as shown in Figure 1. The modular design focuses on solving two respective problems. **Predetection** focuses on reducing the workload of an IDS by performing feature selection which will reduce the dimension of the data itself. Currently, there are 41 attributes (based on Intrusion Detection KDDCup dataset) and reduction can speed up the detection time. Furthermore, using only significant features may also improve the detection accuracy. (Chebrolu *et al*., 2005). Next stage of the model is called **Detection**. A supervised approach is used to classify the incoming instance. Weak decision which falls in the range of $L \leq \theta \leq U$ (where θ indicates the decision value) is also called ambiguous decision. This ambiguous decision will be assigned a weight corresponds to the degree of ambiguity (where decision 0 and 1 represent absolute *Yes* and *No* and decision value of 0.5 carries the highest degree of ambiguity). This is called Weight Mapping. Assumption made in the study is that ambiguity denotes changes. Weight Mapping is a component in **Training and Retraining** stage. The weight will be accumulated until it reaches a predefined threshold. Once the threshold is reached, a clustering technique will cluster the instances (traffic connections) with weak decisions ($L \leq \theta \leq U$) into the respective traffic classes (Normal, Probe, DoS, U2R and R2L). These instances later will be appended to the train datasets for each respected classes (Normal, Probe, DoS, U2R and R2L).

In the study, Linear Genetic Programming was used to do detection and Fuzzy c-Means was used to cluster the instances with ambiguous decision values. Normal, Probe and Dos were represented by 8 features, each with different feature subset. Meanwhile U2R and R2L were represented by 7 features. Similarly, they are different feature subset.

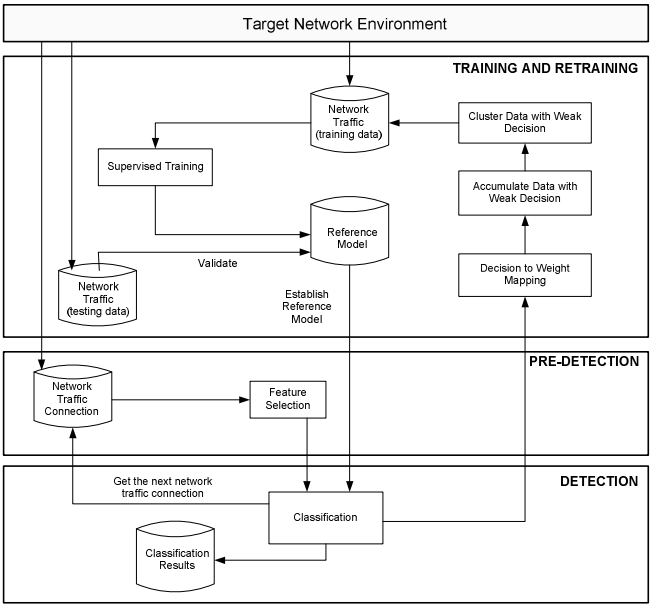

Fig. 1. Design of Adaptive IDS

4 Experiments

The dataset used in the experiments was obtained from 1998 DARPA Intrusion Detection Evaluation Program prepared by MIT Lincoln Labs also known as KDDCup 1999 datasets. These datasets were used in many of IDS works such as in Liu et al. (2007), Shafi and Abbas (2009) and Li et al., (2009). Tsai et al. (2009) reported there have been 30 major IDS studies used KDDCup 1999 datasets in their research. According to Wu and Banzhaf (2010), KDDCup 1999 dataset is the largest publicly available and sophisticated benchmarks for researchers to evaluate intrusion detection algorithms or machine learning algorithms. Figure 2 shows data used in the experiment.

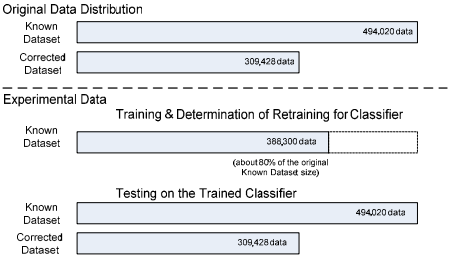

Fig. 2. Data Distribution

Table 2. Distribution of Known dataset in windows unit

	Normal	Probe	DoS	U2R	R2L	Total
w-1	31,315	111	3,817	4	53	35,300
w-2	7,983	719	26,582	1	15	35,300
w-3	19,191	978	15,093	4	34	35,299
w-4	6,088	616	28,406	0	190	35,300
w-5	6,649	895	26,903	20	833	35,300
w-6	0	0	35,300	0	0	35,300
w-7	0	0	35,300	0	0	35,300
w-8	0	0	35,300	0	0	35,300
w-9	0	0	35,300	0	0	35,300
w-10	5,894	359	29,043	4	0	35,299
w-11	892	117	34,289	2	0	35,300
w-12	406	1	34,891	2	0	35,300
w-13	8,824	181	26,288	6	1	35,300
w-14	10,037	129	24,945	9	0	35,120

5 Results and Discussion

Figure 3(a) to 3(c) graphically shows the number of retraining activated for different threshold values. When retraining is activated, it gains additional knowledge about the data since the previous instances with ambiguous decisions were part of the training data (after recommendation from clustering exercise).

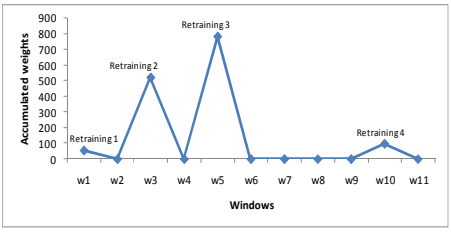

Fig. 3(a). Number of retraining when threshold is small

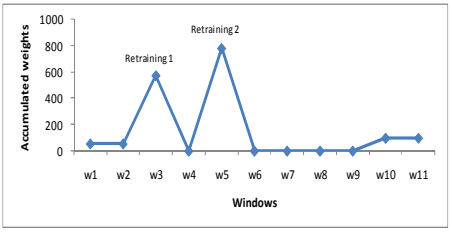

Fig. 3(b). Number of retraining when threshold is medium

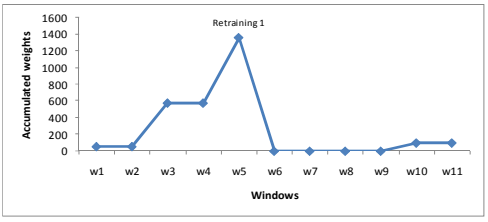

Fig. 3(c). Number of retraining when threshold is medium

Table 3(a). Confusion matrix for Adaptive IDS (A-IDS) Model on Known dataset

		Detection					Total	Accuracy (%)
		Normal	Probe	DoS	U2R	R2L		
A-IDS Model								
Actual	Normal	91,838 (**94.41**)	2672 (2.75)	1713 (1.76)	783 (0.80)	271 (0.28)	97,277	94.409
	Probe	53 (1.29)	4,036 (**98.30**)	4 (0.10)	0 (0.00)	13 (0.32)	4,106	98.295
	DoS	74 (0.02)	7 (0.002)	391,374 (**99.98**)	1 (0.00)	1 (0.00)	391,457	99.979
	U2R	17 (32.69)	5 (9.62)	0 (0.00)	27 (**51.92**)	3 (5.77)	52	51.923
	R2L	63 (5.60)	6 (0.53)	0 (0.00)	20 (1.78)	1,037 (**92.10**)	1,126	92.096

In bracket is % ; Overall Accuracy = 98.85%; False Alarm Rate = 5.60% and Hit Rate = 99.95%

Table 3(b). Validation results for Adaptive IDS (A-IDS) Model on Corrected dataset

		Detection					Total	Accuracy (%)
		Normal	Probe	DoS	U2R	R2L		
A-IDS Model								
Actual	Normal	56,635 (**93.47**)	249 (0.41)	3,553 (5.86)	1 (0.00)	156 (0.26)	60,594	93.466
	Probe	675 (16.20)	3,484 (**83.63**)	0 (0.00)	0 (0.00)	7 (0.17)	4,166	83.629
	DoS	6 (0.003)	0 (0.00)	229,847 (**99.997**)	0 (0.00)	0 (0.00)	229,853	99.997
	U2R	32 (45.71)	2 (2.86)	0 (0.00)	19 (**27.14**)	17 (24.29)	70	27.143
	R2L	7,137 (43.66)	46 (0.28)	0 (0.00)	5 (0.03)	9,159 (**56.03**)	16,347	56.029

In bracket is % ; Overall Accuracy = 96.179%; False Alarm Rate = 6.534% and Hit Rate = 96.865%

Small threshold for A-IDS requires frequent retraining and a large threshold makes the system suffers from low detection accuracy due to inadequate knowledge to predict but it requires less retraining. In summary, the regulated retraining approach with threshold set to medium value has triggered retraining twice. First retraining was done at the end of third window (w-3). The second retraining was performed at the end of

fifth window (w-5). Adaptive IDS Model was tested on Known and validated on Corrected datasets. Its performance on Known dataset is summarized in Table 3(a) and validation performance on Corrected dataset is shown in Table 3(b).

6 Conclusion

The lack of adaptability leads to obsolete reference model which resulted in poor detection accuracy and high false alarm rate. This paper has described the investigation on issues related to design and development of an adaptive intrusion detection model. The proposed A-IDS Model used the concept to adaptively learn the dynamic circumstances in network traffic and regularly update the reference model. The notion of adaptability was achieved by synergistically combining the supervised Linear Genetic Programming, Fuzzy c-Means clustering and weight mapping on ambiguous decisions. The reference pattern in A-IDS Model will undergo retraining when a specified degree of changes has been accumulated. The accumulated weight will trigger the A-IDS Model for retraining either when a sudden significant change has happened or when accumulated small changes have hit the threshold limit. The proposed Adaptive IDS promotes retraining based on the severity of changes in the network traffic. The experimental results provide evidence that a significant improvement was achieved for the detection accuracy especially for Normal class, overall accuracy and false alarm. Findings from this study also confirm the difficulty to recognize U2R and R2L classes. Besides the dynamic nature of network traffic, other challenges in IDS are the imbalance dataset and the vague decision boundary between normal and abnormal traffic. This will be the focus of our future work.

Acknowledgment. The authors would like to thank The Ministry of Higher Education of Malaysia (MOHE) and Universiti Teknologi Malaysia (UTM) for funding this study.

References

Burbeck, K., Tehrani, S.N.: Adaptive real-time anomaly detection with incremental clustering. Information Security Technical Report 12, 56–67 (2007)

Chavan, S., Shah, K., Dave, N., Mukherjee, S., Abraham, A., Sanyal, S.: Adaptive neuro-fuzzy intrusion detection systems. In: IEEE Proceedings of International Conference on Information Technology: Coding and Computing (ITCC 2004), vol. 1, pp. 70–74 (2004)

Chebrolu, S., Abraham, A., Thomas, J.P.: Feature deduction and ensemble design of intrusion detection systems. Journal of Computers and Security 24(4), 295–307 (2005)

Denning, D.E.: An Intrusion-Detection Model. IEEE Transactions on Software Engineering SE 13(2), 222–232 (1987)

Eskin, E., Miller, M., Zhong, Z.D., Yi, G., Lee, W.A., Stolfo, S.: Adaptive Model Generation for Intrusion Detection System. In: Proceedings of the ACMCCS Workshop on Intrusion Detection and Prevention, Athens, Greece (2000)

Fan, W., Stolfo, S.: Ensemble-based Adaptive Intrusion Detection. In: Proceedings of 2nd SIAM International Conference on Data Mining (SDM 2002), Arlington, VA, April 11-13 (2002)

Forrest, S., Hofmeyr, S.A., Somayaji, A., Longstaff, T.A.: A sense of self for Unix Processes. In: IEEE Proceedings of Symposium on Security and Privacy, pp. 120–128 (1996)

Ghosh, A.K., Wanken, J., Charron, F.: Detecting Anomalous and Unknown Intrusions Against Programs. In: Proceedings of the 14th Annual Computer Security Applications Conference, AC-SAC (1998)

Giacinto, G., Roli, F., Didaci, L.: Fusion of multiple classifiers for intrusion detection in computer network. Pattern Recognition Letters 24(12), 1795–1803 (2003)

Hofmeyr, S.A.: An Immunological Model of Distributed Detection and Its Application to Computer Security. Ph.D. Thesis. Computer Science Dept of University of New Mexico, United States (1999)

Hossein, M., Bridges, S.M.: A Framework for an Adaptive Intrusion Detection System With Data Mining. In: Proceedings of the 13th Annual Canadia Information Technology Security Symposium, Ottawa, Canada (2001)

Hossein, M., Bridges, S.M., Vaughn, R.B.: Adaptive Intrusion Detection wit Data Mining. In: Proceedings of IEEE Conference on Systems, Man & Cybernetics, pp. 3097–3103 (2003)

Jemili, F., Zaghdoud, M., Ahmed, M.: A Framework for an Adaptive Intrusion Detection System using Bayesian Network. In: IEEE Proceedings of Intelligence and Security Informatics, New Brunswick, New Jersey, pp. 66–70 (2007)

Kim, J.: Integrating Artificial Immune Algorithms for Intrusion Detection. PhD Thesis, Department of Computer Science, University College of London (2003)

Kim, J., Bentley, P.J., Aickelin, U., Greensmith, J., Tedesco, G., Twycross, J.: Immune System Approaches to Intrusion Detection – A Review. Natural Computing 6(4), 413–466 (2007)

Langin, C., Rahimi, S.: Soft computing in intrusion detection: the state of the art. Ambient Intelligent and Humanized Computing 1, 133–145 (2010)

Lee, H., Chung, Y., Park, D.: An Adaptive Intrusion Detection Algorithm Based on Clustering and Kernel-Method. In: Ng, W.-K., Kitsuregawa, M., Li, J., Chang, K. (eds.) PAKDD 2006. LNCS (LNAI), vol. 3918, pp. 603–610. Springer, Heidelberg (2006)

Lee, W., Stolfo, S.S., Mok, K.W.: Adaptive Intrusion Detection: A Data Mining Approach. Artificial Intelligence Review. Issues on the Application of Data Mining 14, 533–567 (2000)

Li, Y., Jun, L.W., Zhi, H.T., Tian, B.L., Chen, Y.: Building lightweight intrusion detection system using wrapper-based feature selection mechanisms. Computers and Security 28(6), 466–475 (2009)

Liao, Y., Vemuri, V.R., Pasos, A.: Adaptive anomaly detection with evolving connectionist systems. Network and Applications 30(1), 60–80 (2007)

Liu, G., Yi, Z., Yang, S.: A hierarchical intrusion detection model based on the PCA neural networks. Neurocomputing 70, 1561–1568 (2007)

Shafi, K., Abbass, H.A.: An Adaptive Genetic-based Signature Learning System for Intrusion Detection. Expert Systems with Applications 36(10), 12036–12043 (2009)

Tang, W., Cao, Y., Xi, M.Y., Won, H.S.: Study on Adaptive Intrusion Detection Engine Based on Gene Expression Programming Rules. In: Proceedings of International Conference on Computer Science and Software Engineering, pp. 959–963 (2008)

Tapiador, J.M.E., Teodoro, P.G., Verdejo, J.E.D.: Anomaly Detection Methods in Wired Networks: A Survey and Taxonomy. Computer Communications 27(16), 1569–1584 (2004)

Tsai, C.F., Hsu, Y.F., Lin, C.Y., Lin, W.Y.: Intrusion Detection by Machine Learning: A Review. Expert Systems with Applications 36(10), 11994–12000 (2009)

Warrander, C., Forrest, S., Pearlmutter, B.: Detecting intrusions using system calls: alternative data models. In: IEEE Proceedings of Symposium on Security and Privacy, pp. 133–145 (1999)

Wu, X.S., Banzhaf, W.: The Use of Computational Intelligence in Intrusion Detection Systems: A Review. Applied Soft Computing 10(1), 1–35 (2010)

Xu, X., Wang, X.: An Adaptive Network Intrusion Detection Method Based on PCA and Support Vector Machines. In: Li, X., Wang, S., Dong, Z.Y. (eds.) ADMA 2005. LNCS (LNAI), vol. 3584, pp. 696–703. Springer, Heidelberg (2005)

Yang, W., Yun, X.C., Zhang, L.J.: Using Incremental Learning Method for Adaptive Network Intrusion Detection. In: Proceedings of the 4th International Conference on Machine Learning and Cybernetics, Guangzhou, August 18-21, pp. 3932–3936 (2005)

Yu, Z.X., Chen, J.R., Zhu, T.Q.: A Novel Adaptive Intrusion detection system Based on Data Mining. In: Proceedings of the Fourth International Conference on Machine Learning and Cybernatics, Guangzhou, August 18-21, pp. 2390–2395 (2005)

Zhang, Z., Shen, H.: Application of online-training SVMs for real-time intrusion detection with different considerations. Computer Communications 28(12), 1428–1442 (2005)