Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 6 (2011) pp. 462–468

Fuzzy Clustering Based Anomaly Detection for Updating Intrusion Detection Signature Files

Anish Abraham Padath, Barbara Endicott-Popovsky

Campus Health Services Administration
University of Washington
Seattle, WA 98195 USA
anishap@uw.edu

Director for the Center of Information Assurance and Cybersecurity
University of Washington
Seattle, WA 98195
endicott@uw.edu

Abstract: **The majority of systems today categorize data either by misuse detection or anomaly detection: each approach has its relative merits and demerits. Perfect detection, like perfect security, is simply not an attainable goal given the complexity and rapid evolution of modern systems. An Intrusion Detection System (IDS) can, however, strive to raise the bar for attackers by reducing the efficacy of large classes of attacks and increasing the work factor required to achieve a system compromise. The coordinated deployment of multiple intrusion detection systems promises to allow greater confidence in the results of and to improve the coverage of intrusion detection, making this a critical component of any comprehensive security architecture. Traditional anomaly detection methods lack adaptive captivity in complex and heterogeneous network. Especially while facing high noise environments, or the situation of updating profiles not in time, intrusion detection systems will have high false alarm rate.**

In this research study, anomaly detection based on fuzzy clustering is proposed for updating signature files. Fuzzy clustering integrates the advantage of fuzzy set theory and conventional clustering algorithms so that the improved algorithm can identify zero day attacks (anomalies), which conventional misuse network intrusion detection would fail to detect. The approach allows recognizing not only known attacks but also to detect suspicious activity that may be the result of a new, unknown attack. Once new attacks are detected, then this information could be used to update the signature files of the misuse intrusion detection systems.

Keywords: *Intrusion detection system, misuse detection system, anomaly detection system, fuzzy clustering.*

I. Introduction

Attacks on computer infrastructures are becoming an increasingly serious problem. With the increase of Internet users and its application potential in every field, we rely on computers and the information they carry in almost every aspect of our lives. Whether it is banking, e-commerce businesses, health care, law enforcement, real estate, air transportation, or education, we are all becoming increasingly dependent upon networked computers. It is these interconnected networks that now make up the "cyber" infrastructure. Yet it is this infrastructure that, if not protected, is prone to information warfare attacks by cyber criminals and terrorists. The possibilities and opportunities are limitless; unfortunately, so too are the risks and chances of malicious intrusion. This has made computer security an essential concern for network administrators. Programming errors cannot be avoided as the complexity of system and application software is changing rapidly leaving behind exploitable weaknesses. Intrusion detection is therefore required as an additional wall for protecting systems.

Either misuse or anomaly intrusion detection is useful, not only in detecting successful intrusions, but also in providing important information for timely countermeasures. At present, network flow anomaly detection is described in the literature, but detection accuracy has been far from desirable. Nevertheless, anomaly detection plays a valuable role in discovering unknown anomaly network intrusion and in detecting network failure.

II. Literature Review

Intrusion detection has been an active field of research for the past two decades. As network computers and the Internet began playing a vital role in society, security has become a primary concern. In 1980, [1] first proposed that audit trails should be used to monitor threats. The importance of such data had not been comprehended at that time and all the available system security procedures were focused on denying access to sensitive data from an unauthorized source. Later in 1997 [2] proposed the concept of intrusion detection

as a solution to the problem of providing a sense of security in computer systems. Intrusion detection systems (IDS) were conceived of as tools designed to monitor and analyze computer or network events in order to detect suspect patterns that may indicate a network or system attack [3].

Many IDSs only handle one particular audit data source. Updating these systems is expensive and slow. Some recent research, as well as commercial IDSs, have begun to provide built-in mechanisms for customization and extension [4]. According to [5] and [6] Intrusion detection techniques can be categorized into signature detection and anomaly detection. Signature detection systems use patterns of well-known attacks or weak spots of the system to match and identify known intrusions. Anomaly detection systems flag as anomalies observed activities that deviate significantly from the established normal usage profiles. This intrusion detection model is independent of system, type of intrusion and application environment.

Underlying IDS is the concept of rule-based pattern matching. Models of normal usage of the system are verified against actual usage and any significant deviation from normal is flagged. This model has served as an abstraction for further developments in this field. This generic intrusion detection model [7] is depicted in Figure 1. Different techniques and approaches have been used in later developments.

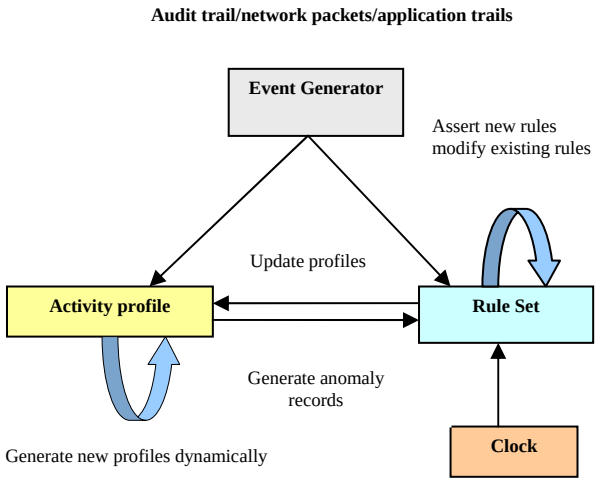

Figure 1: A Generic Intrusion Detection Model [7]

In 1998, [8] established an anomaly detection model that integrated association rules and frequency episodes with fuzzy logic to produce patterns for intrusion detection. Later in 2003, [9] developed an anomaly intrusion detection system combining neural networks and fuzzy logic. Also [10] applied genetic algorithms to optimize the membership function for mining fuzzy association rules.

The above researchers have made various contributions to using artificial intelligence techniques in anomaly intrusion detection. All use a static classifier or a static decision boundary to classify data, and then detect possible intrusions; however, security requirements may differ for various applications. This suggests the value of a dynamic decision boundary that could be set for different applications. This research proposes development of fuzzy clustering for anomaly detection for different levels of security requirements. It is expected that there will be some connection between detection accuracy of a decision boundary and the computational complexity of classification using this boundary.

Anomaly detection systems compute statistical models for normal network traffic and generate alarms when there is a large deviation from the normal model. Example systems have been developed, such as (Stealthy Portscan Anomaly Detection Engine) SPADE [11], (Packet Header Anomaly Detection) PHAD [12] and (Application Layer Anomaly detector) ALAD [13]. SPADE is an anomaly detector that acts as a plug-in preprocessor to SNORT. While PHAD is designed to detect anomalous behavior of network traffic packets and ALAD computes (statistical) models for normal network traffic and generates alarms when there is a large deviation from the normal model. Other techniques have been proposed as detection engines, for example using clustering and classification [14], autonomous agents and distributed intrusion detection [15], and a hidden Markov model [16]. [17] and [18] provide a useful survey of these applications.

III. Significance of the study

Detecting computer break-ins and other malicious activities is a signal detection problem. The aim is to distinguish malicious use from legitimate use. There are currently several different approaches to this problem and several different Intrusion Detection System (IDS) implementations available. Different detection methodologies can be employed to search for evidence of attack. While anomaly detection typically uses threshold monitoring to indicate when a certain established metric has been reached, misuse detection techniques frequently use rule-based expert systems. Further, misuse detection systems rely on definitions of misuse patterns, i.e., the descriptions of attacks or unauthorized actions [19]. The purpose of this research is to investigate and evaluate intelligent systems as a possible tool to model efficient Intrusion Detection Systems. Our specific objectives are to investigate and test whether anomaly detection systems can be used to generate attack rules for misuse detection systems. We examine issues concerning testing and operational use of IDS.

A. Misuse Intrusion Detection System

A misuse pattern should summarize the distinctive features of an attack, called the signature of the attack. In the case of signature-based IDS, when a signature is identified, the IDS records relevant information about the incident in a log file. Signature-based systems are the most common examples of misuse detection systems. In terms of advantages, signature-based systems, by definition, are very accurate at detecting known attacks, where these are detailed in a signature database. Moreover, since signatures are associated with specific misuse behavior, it is easy to determine the attack type. On the other hand, their detection capabilities are limited to those within the signature database. As new attacks are discovered, a signature database requires continuous updating to include new attack signatures, resulting in potential scalability problems. Misuse detection is harder to automate since it requires applying many rules (as in [20]) or searching for many patterns (as in [21] and

[22]). Moreover, it is almost impossible to perform a proper testing of such systems due to an insufficient amount of information about real intrusion cases. When a new form of attack is identified, the signature must be manually encoded as a rule in the expert system in order for it to be identified in the network stream. Updates may be ignored or performed infrequently by the administrator, affecting the usefulness of the system. Rule-based systems also suffer from a lack of flexibility in the rule-to-audit record representation. Slight variations in an attack sequence can affect the activity-rule comparison to a degree that the attack is not detected by the intrusion detection mechanism. Figure 2 [23] depicts a simple misuse intrusion detection model.

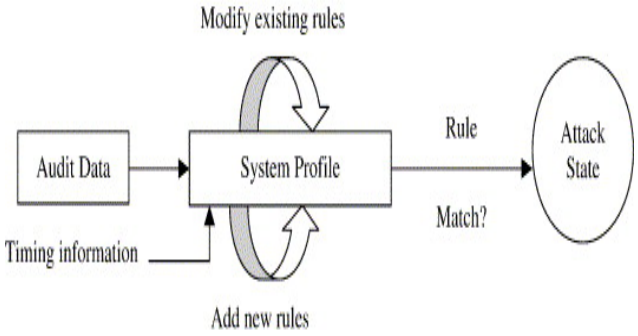

Figure 2: Misuse Intrusion Detection System [23]

B. Anomaly Intrusion Detection System

Anomaly detection systems use models of the acceptable behavior of users, referred to as normal behavior models. The basic principles of detecting intrusions by identifying "abnormal" behavior are outlined by Anderson [24]. Recently, this approach has been expansively developed and many implementations have been suggested [25, 26, 27, 28]. Anomaly-based IDSs search for any deviation from the (characterized) normal behavior, which are considered as anomalies or attacks.

As an advantage over signature based systems, anomaly-based systems can detect known and unknown (i.e., new) attacks as long as the attack behavior deviates sufficiently from normal behavior; however, if the attack is similar to normal behavior, it may not be detected. Moreover, it is difficult to associate deviations with specific attacks since anomaly-based IDSs only use models of normal behavior. As users change their behavior as a result of additional service or hardware, even normal activities of a user may raise alarms. In that case, models of normal behavior require redefinition in order to maintain the effectiveness. Figure 3 depicts an anomaly detection model as per [23].

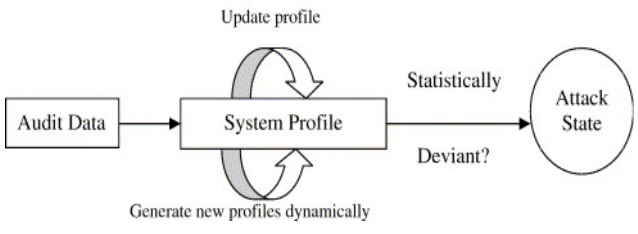

Figure 3: Anomaly Intrusion Detection System [23]

IV. Experimental Results

In this study, we focused on detecting insider attacks, which constitute a significant threat to computer systems. It has become a practice that many organizations only focus on protecting the network from external attacks, without deploying a proper detecting and prevention mechanism against internal intruders and, as a result, insider attacks may not be discovered. Insiders have a substantial amount of knowledge about the network architecture, files, systems etc. They potentially can plant trojan horses, browse through the network file system, overload the system, cause a system to crash, etc. While browsing unauthorized files violates confidentiality, trojan horses can threaten both the integrity and confidentiality of data on the system, overloading or crashing directly affects the availability of a network/system. Unfortunately, these types of attacks can be extremely difficult to detect.

A. Feature Reduction

Since the amount of audit data that an IDS needs to examine is very large, even for a small network, classification manually is impossible. Analysis is difficult, even with computer assistance because extraneous features can make it harder to detect suspicious behavior patterns. Complex relationships exist between features, which are practically impossible for humans to discover. IDS must therefore reduce the amount of data to be processed. This is extremely important if real-time detection is desired. Reduction can occur in one of several ways: 1) data that is not considered useful can be filtered, leaving only potentially interesting data, 2) data can be grouped or clustered to reveal hidden patterns. By storing the characteristics of the clusters instead of individual data, overhead can be significantly reduced, 3) finally, data sources can be eliminated using feature selection.

The data for our experiments was prepared by the 1998 DARPA intrusion detection evaluation program by MIT Lincoln Labs. The original data contains 744 MB of data with 4,940,000 records. The data set has 41 attributes for each connection record plus one class label. Some features are derived features, which are useful in distinguishing normal connection from attacks. These features are either nominal or numeric. Some features examine only the connections in the past two seconds that have the same destination host as the current connection, and calculate statistics related to protocol behavior, service, etc. These are called same host features. Some features examine only the connections in the past two seconds that have the same service as the current connection and are called same service features. Some other connection records were also sorted by destination host, and features were constructed using a window of 100 connections to the same host instead of a time window. Our experiments have three phases namely data reduction, a training phase and a testing phase. In the data reduction phase, important variables for real-time intrusion detection are selected by feature selection. We selected the same features for insider attack detection as given by [30]. The data set for our experiments contains 11982 randomly generated records, having 41 features and 2 features. The labels of the 41 features and their corresponding network data features are shown in table 1:

Table 1. Network Data Feature Labels

Label	**Network Data Feature**	**Label**	**Network Data Feature**	**Label**	**Network Data Feature**	**Label**	**Network Data Feature**
A	*duration*	*L*	*logged_in*	*W*	*count*	*AH*	*dst_host_ same_srv_rate*
B	*protocol-type*	*M*	*num_compromised*	*X*	*srv_count*	*AI*	*dst_host_diff_srv_rate*
C	*service*	*N*	*root_shell*	*Y*	*serror_rate*	*AJ*	*dst_host_same_ src_port_rate*
D	*flag*	*O*	*su_attempted*	*Z*	*srv_serror_rate*	*AK*	*dst_host_srv_ diff_host_rate*
E	*src_bytes*	*P*	*num_root*	*AA*	*rerror_rate*	*AL*	*dst_host_serror_rate*
F	*dst_bytes*	*Q*	*num_file_creations*	*AB*	*srv_rerror_rate*	*AM*	*dst_host_srv_ serror_rate*
G	*land*	*R*	*num_shells*	*AC*	*same_srv_rate*	*AN*	*dst_host_rerror_rate*
H	*wrong _fragment*	*S*	*num_access_files*	*AD*	*diff_srv_rate*	AO	*dst_host_srv_rerror_ rate*
I	*urgent*	*T*	*num_outbound_cmds*	*AE*	*srv_diff_host_rate*		
J	*hot*	*U*	*is_host_login*	*AF*	*dst_host_count*		
K	*num_falied_logins*	*V*	*is_guest_login*	*AG*	*dst_host_srv_count*		

B.. Anomaly Detection Using Fuzzy Clustering

Clustering is the process of assigning data objects into a set of disjoint groups called clusters so that objects in each cluster are more similar to each other than objects from different clusters. Clustering techniques are applied in many application areas such as pattern recognition, data mining, machine learning, etc. In [31] authors have used hierarchical clustering methods for intrusion detection. In the hierarchical clustering method, creation of the clusters starts from either top to bottom or bottom to top. The author has used the bottom-to-top approach .In this approach, aggregation of data points start from a single data point, then clusters data point according to their distance. In [32] authors used the K-Mean evolution clustering method for intrusion detection. This method decreases the overhead of performing detection over whole datasets. Clustering algorithms for anomaly IDS that have been reported in the literature can be classified as hard clustering [33], [34] and fuzzy clustering [35], [36], [37], [38] methods.

After fuzzy theory was introduced by Lotfi Zadeh, researchers put fuzzy theory into clustering. Fuzzy algorithms can assign a data object partially to multiple clusters. The degree of membership in the fuzzy cluster depends on the closeness of the data object to the cluster centers. The most popular fuzzy clustering algorithm is fuzzy c-means (FCM) [39].

FCM partitions a collection of n vectors xi, i= 1,2…,n into c fuzzy groups and finds a cluster center in each group such that the cost function of dissimilarity measure is minimized. To accommodate the introduction of fuzzy partitioning, the membership matrix U is allowed to have elements with values between 0 and 1.The FCM objective function takes the form:

$$J(U,c_1,\ldots c_c) = \sum_{i=1}^{c} J_i = \sum_{i=1}^{c}\sum_{j=1}^{n} u_{ij}^{m} d_{ij}^{2} \qquad (1)$$

Where u_{ij}, is a numerical value between [0,1]; c_i is the cluster center of fuzzy group i; $d_{ij} = \|c_i - x_j\|$ is the Euclidian distance between i^{th} cluster center and j^{th} data point; and m *is* called the exponential weight which influences the degree of fuzziness of the membership (partition) matrix. Usually a number of cluster centers are randomly initialized and the FCM algorithm provides an iterative approach to approximate the minimum of the objective function, starting from a given position, and leads to any of its local minima.

C. Anomaly Detection Results

FCM finds 'n' number of clusters in the provided data set. In our experiments, we used 10 clusters. The membership function matrix U contains the grade of membership of each DATA point in each cluster. The values 0 and 1 indicate no membership and full membership, respectively. Grades between 0 and 1 indicate that the data point has partial membership in a cluster. At each iteration, an objective function (1) is minimized to find the best location for the cluster and its values are returned. Minimum amount of improvement is set as .00001.

Figures 4 and 5 illustrate the FCM clustering results showing anomalies for detecting insider attacks. The black dots illustrate cluster centers and the data points (red) on the right side depict outliers (anomalies).

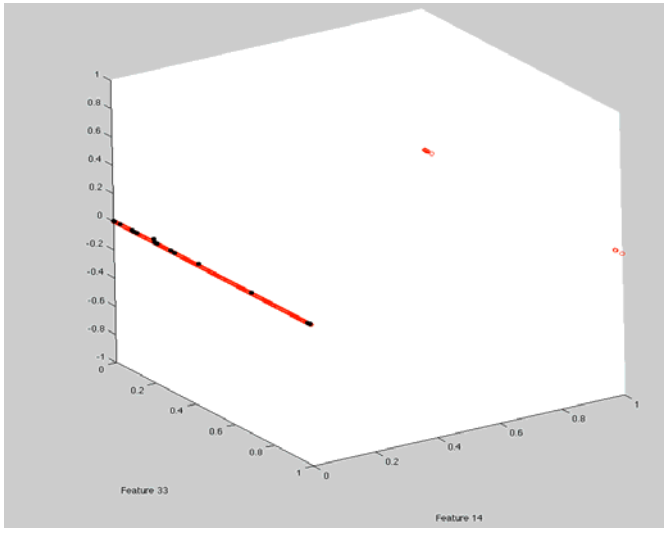

Figure 4: FCM clustering results using 41 features

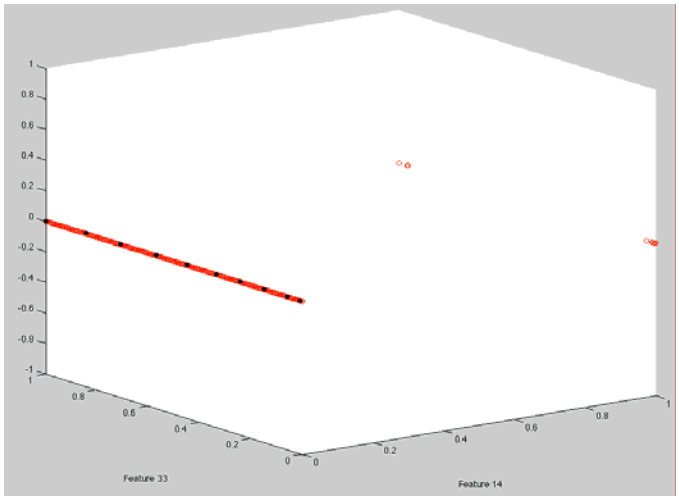

Figure 5: FCM Clustering results using 2 features

The outlier data (anomaly) may be investigated further (for frequency, features, and contents) to make sure it is a serious attack and, if necessary, may be used to update or train misuse intrusion detection signature data files to detect similar attacks in the future. Signature data files can be updated by using several machine learning methods as reported in [30].

V. Future Directions

Intrusion detection techniques are continuously evolving, with the goal of improving the security and protection of networks and computer infrastructures. Despite the promising nature of fuzzy clustering-based anomaly IDS, as well as its relatively long existence, there still exist several open issues regarding these systems.

For future research, how to determine the appropriate number of clusters remains an open problem. Moreover, other data mining techniques, such as support vector machine, evolutionary computing, outlier detection, may be introduced into IDS. Comparisons of various data mining techniques will provide clues for constructing more effective

hybrid Artificial Neural Networks for detection intrusions. Further, as many of the features are correlated, a study can be made of the variation in detection rate and accuracy with different sets of features.

Over the years, numerous techniques, models, and full-fledged intrusion detection systems have been proposed and built in the commercial and research sectors; however, there is no globally acceptable standard/metric for evaluating an intrusion detection system. Therefore, one of the open challenges is the development of a general systematic methodology, or a set of metrics, that can be used to fairly evaluate intrusion detection systems.

The 1998 and 1999 intrusion detection evaluations from DARPA/MIT Lincoln Labs have been shown to be inappropriate for simulating actual network environments [40]. Therefore, there is a critical need to build a more appropriate evaluation dataset. The methodology for generating the evaluation dataset should not only simulate realistic network conditions, but also be able to generate datasets that have normal traffic interlaced with anomalous traffic.

VI. Conclusion and Discussions

We proposed an anomaly detection system based on fuzzy clustering for updating signature files of a misuse detection system. Fuzzy clustering integrates the advantage of fuzzy set theory and conventional clustering algorithms so that the improved algorithm can identify zero-day attacks (anomalies), which conventional misuse network intrusion detection would fail to detect. Once new attacks are detected, then this information could be used to update the signature files of the misuse intrusion detection system. Experimental results reveal that the proposed system can detect anomalies in the traffic data and could be a suitable candidate for future intrusion detection systems. Therefore implementing a signature-based intrusion detection engine should improve the detection engine's performance.

An increasing problem in today's corporate networks is the threat posed by insiders, although configuring an intrusion detection system to detect internal attacks is very difficult. The greatest challenge lies in creating a good rule set for detecting "internal" attacks or anomalies. Different network users require different degrees of access to different services, servers, and systems for their work, thus making it extremely difficult to define and create user- or system-specific usage profiles.

Acknowledgements

We would like to thank the authors of [30] for sharing the intrusion data and the related papers, which helped us to finish the research in a timely manner.

References:

[1] J. P. Anderson. Computer Security Threat Monitoring and Surveillance. Technical report, James P Anderson Co., Fort Washington, Pennsylvania, April 1980.

[2] D. E. Denning. An Intrusion Detection Model. In IEEE Transactions on Software Engineering, pp. 222-228, February 1997.

[3] Alvaro Herrero, Emilio Corchado, Maria Pellicer and Ajith Abraham, MOVIH-IDS: A Mobile-Visualization Hybrid Intrusion Detection System, Neurocomputing Journal, Elsevier Science, Netherlands, Volume 72, Issues 13-15, pp. 2775-2784, 2009.

[4] T. Lunt. Detecting intruders in computer systems. In Proceedings of the 1993 Conference on Auditing and Computer Technology, 1993.

[5] K. Jackson, Intrusion Detection Systems (IDS): Product Survey, Los Alamos National Laboratory, LA-UR-99-3883, 1999.

[6] H. Debar, M. Dacier, and A. Wespi, Towards Taxonomy of Intrusion Detection Systems, Computer Networks, 31(8):805-822, April 1999.

[7] Kumar. Classification and Detection of Computer Intrusions. PhD Thesis, Department of Computer Science, Purdue University, August 1995.

[8] W. Lee and S.J. Stolfo, Data Mining Approaches for Intrusion Detection, *7th USENIX Security Symposium*, 1998, pp.79-94.

[9] M. Mohajerani, A. Moeini and M. Kianie, NFIDS: A Neuro-fuzzy Intrusion Detection System, *Proceedings of the10th IEEE International Conference on Electronics*, Circuits and Systems, 2003, pp348-351.

[10] W.D.Wang and S. Bridges, Genetic Algorithm Optimization of Membership Functions for Mining Fuzzy Association Rules, *Proceedings of the 7th International Conference on Fuzzy Theory & Technology*, Atlantic City, NJ, 2000, pp131-134.

[11] Stanifor, Hoagland and McAlerney, "Practical Automated Detection of Stealthy PortScans", Journal of Computer Security, 2002, vol. 10, no. 1, pp. 105-136

[12] M. V. Mahoney and P.K. Chan, "PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic", Technical report, Florida Tech., CS-2001-4, 2001

[13] M. Mahoney, "Network Traffic Anomaly Detection Based on Packet Bytes", Proc. ACM. Symposium on Applied Computing, 2003, pp. 346-350

[14] H. Yang, F. Xie, and Y. Lu, "Clustering and Classification Based Anomaly Detection", Lecture Notes in Computer Science, 2006, vol. 4223, pp. 1611-3349.

[15] J.S. Balasubramaniyan, J.O. Garcia-Fernandez, et al., "An Architecture for Intrusion Detection using Autonomous Agents", in Proceedings of the 14th IEEE ACSAC 1998, Scottsdale, AZ, USA, pp. 13-24.

[16] D. Ourston, S. Matzner, et al., "Coordinated Internet attacks: responding to attack complexity", Journal of Computer Security, 2004, vol. 12, pp. 165-190.

[17] J.S. Sherif, R. Ayers, and T. G. Dearmond, "Intrusion Detedction: the art and the practice", Part 1. Information Management and Computer Security, 2003, vol. 11, no. 4, pp. 175-186.

[18] J.S. Sherif and R. Ayers, "Intrusion detection: methods and systems", Part II. Information Management and Computer Security, 2003, vol. 11, no. 5, pp. 222-229

[19] R. A. Kemmerer and G. Vigna, "Intrusion detection: a brief history and overview," Security and Privacy a Supplement to IEEE Computer, April 2002

[20] Lunt T., Jagannathan R., Lee R., Whitehurst A., Listgarten S., *Knowledge based Intrusion Detection*, In Proceedings of the Annual AI Systems in Government Conference (1989), Washington DC.

[21] Shieh S., Gligor V., *A pattern-oriented intrusion detection model and its applications*, In Proceedings of

Symposium on Security and Privacy (1991), Oakland, CA, pp. 327--342.

[22] Kumar S., Spafford E., *A Pattern Matching Model for Misuse Intrusion Detection*, In Proceedings of the National Computer Security Conference, Baltimore, Coast TR 95-06 (1994), pp.11--21.

[23] Sandhya Peddabachigari, Ajith Abraham, Crina Grosan and Johnson Thomas, Modeling Intrusion Detection System Using Hybrid Intelligent Systems, Journal of Network and Computer Applications, Elsevier Science, Volume 30, Issue 1, pp. 114-132, 2007.

[24] Anderson J.P., *Computer Security Threat Monitoring and Surveillance*. Technical report, James P. Anderson Co., Fort Washington, Pennsylvania, 1980.

[25] Heberlein L.T., Levitt K.N. and Mukherjee B.*A Method To Detect Intrusive Activity in a Networked Environment*, In Proceedings of the 14th National Computer Security Conference (1991), pp. 362--371.

[26] Lunt T., Jagannathan R., Lee R., Whitehurst A., Listgarten S., *Knowledge based Intrusion Detection*, In Proceedings of the Annual AI Systems in Government Conference (1989), Washington DC.

[27] Liepins G.E., Vaccaro H.S., *Anomaly Detection: Purpose and Framework*, In Proceedings of the 12th National Computer Security Conference (1989), pp. 495--504.

[28] Porras P.A., Kemmerer R.A., *Penetration State Transition Analysis: A Rule-Based Intrusion Detection Approach*, In Eighth Annual Computer Security Applications Conference (1992), pp.220--229.

[29] Ajith Abraham, Ravi Jain, Johnson Thomas and Sang Yong Han, D-SCIDS: Distributed Soft Computing Intrusion Detection Systems, Journal of Network and Computer Applications, Elsevier Science, Volume 30, Issue 1, pp. 81-98, 2007.

[30] Abraham A., Grosan, C. and Martin-Vide, C, Evolutionary Design of Intrusion Detection Programs, International Journal of Network Security, Vol.4, No.3, pp. 328-339, 2007.

[31] Jose F.Nieves., "Data clustering for anomaly detection in Network intrusion detection", Research Alliance in Math and Science August 14, 2009,pp.1-12

[32] Nani Yasmin1, Anto Satriyo Nugroho2, Harya Widiputra3,"Optimized Sampling with Clustering Approach for Large Intrusion Detection Data", International Conference on Rural Information and Communication Technology 2009 Pp.56-60

[33] S. L. Gerhad munz and G. Carle, "Traffic anomaly detection using kmeans clustering," *Proc. of GI/ITG-Workshop MMBnet*, 2007.

[34] S. H. Oh and W. S. Lee, "An anomaly intrusion detection method by clustering normal user behaviour," *International journal of Computer and Security*, vol. 22, 2003.

[35] J. E. Dickerson and J. A. Dickerson, "Fuzzy network profiling for intrusion detection," *Proc. of International Conference of the North American Fuzzy Information Processing Society*, 2005.

[36] J. U. Hn Shah and A. Joshi, "Fuzzy clustering for intrusion detection," *Proc. of IEEE International conference on Fuzzy Systems*, 2003.

[37] J. Y. S. Zhao and L. V. Saxton, "A study on fuzzy intrusion detection," *Proc. of Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security, SPIE*, 2005.

[38] O. L. John E. Dickerson, Iukka Juslin and J. A. Dickerson, "Fuzzy intrusion detection," *Proc. of IFSA World Congress and 20th North American Fuzzy Information Processing Society (NAFIPS) international Conference*, 2001.

[39] Bezdek, J. C., Pattern Recognition with Fuzzy Objective Function Algorithms, New York: Plenum Press, 1981.

[40] J. McHugh, Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection, *ACM Transactions on information and System Security* 3 (200), pp. 262-294

Author Biographies

Anish Abraham Padath received his BS from Mahatma Gandhi University, India (1992), Masters Degree in Computer Application from Bharathidasan University, India (1996) and Masters Degree in Information Management (Specialized in Information Assurance and Security) from University of Washington (2011).

Mr. Padath is a member of the Association of Computing Machinery (ACM). He has over 15 years experience in System Analysis and Management, Risk Assessment, Security, Healthcare application support, and Implementation of various healthcare projects. Currently he manages and maintains the employee health application for the University of Washington Seattle Campus, which includes employees at University of Washington Medical Center, Harborview Medical Center and Hall Health Primary Care Center. He is also responsible for developing procedures and reports to ensure the completeness, consistency and integrity of the database.

Barbara Endicott-Popovsky has an MBA from the University of Washington (1972, 1985), an MS in Information Systems Engineering from Seattle Pacific University (1987) and PhD in Computer Science from the University of Idaho (2007).

She is the Director for the Center of Information Assurance and Cybersecurity at the University of Washington, designated by the NSA/DHS as a Center for Academic Excellence in Information Assurance Education and Research. She holds a joint faculty appointment with the Information School and the School of Urban Design and Planning--Critical Infrastructure, following a 20-year industry career marked by executive and consulting positions in IT architecture and project management. Her research interests fall under the umbrella of managing/mitigating network risks: deception, governance and network forensic readiness.

Ms. Endicott-Popovsky is a member of the IEEE, a founding member of the NW Regional Computer ForensicsCooperative, Principal Investigator on numerous grants, producer of the televised Unintended Consequences of the Information Age Lecture series. She has served on organizing committees for the International Workshop on Systematic Approaches to Digital Forensic Engineering and the Recent Advances in Intrusion Detection (RAID) conference and on the editorial board of a Special Edition of the Journal on Educational Resources in Computing.