References

1. Lippmann, R.P., Fried, D.J., Graf, I., Haines, J.W., Kendall, K.R., McClung, D., Weber, D., Webster, S.E., Wyschogrod, D., Cunningham, R.K., Zissman, M.A.: Evaluating Intrusion Detection Systems: the 1998 DARPA Off-line Intrusion Detection Evaluation. In: DARPA Information Survivability Conference and Exposition, DISCEX 2000 (2000)
2. CERT Statistics (Historical), http://www.cert.org/stats/
3. Internet Security Threat Report - Volume XIV - Executive Summary. Symantec Corporation (2009)
4. Richardson, R.: CSI Survey 2008 - The 13th Annual Computer Crime & Security Survey. Computer Security Institute (2008)
5. Richardson, R.: CSI Survey 2007 - The 12th Annual Computer Crime and Security Survey. Computer Security Institute (2007)
6. X-Force Threat Insight Quarterly - Q4 2008, IBM Internet Security Systems - X-Force (2009)
7. Galetsas, A.: Statistical Data on Network Security. European Commission. Information Society and Media Directorate-General. Emerging Technologies & Infrastructures. Security (2007)
8. Barbará, D., Jajodia, S.: Applications of Data Mining in Computer Security. In: Advances in Information Security, vol. 6. Kluwer Academic Publishers, Dordrecht (2002)
9. Neumann, P.G., Parker, D.B.: A Summary of Computer Misuse Techniques. In: 12th National Computer Security Conference (1989)
10. Rogers, L.R.: Home Computer and Internet User Security. CERT, Software Engineering Institute, Carnegie Mellon University (2005)
11. Goodall, J.R., Lutters, W.G., Komlodi, A.: The Work of Intrusion Detection: Rethinking the Role of Security Analysts. In: Americas Conference on Information Systems (2004)
12. Heady, R., Luger, G., Maccabe, A., Servilla, M.: The Architecture of a Network Level Intrusion Detection System. Technical Report CS90-20. University of New Mexico (1990)
13. Security Terms, https://security.ias.edu/glossary
14. Puketza, N.J., Zhang, K., Chung, M., Mukherjee, B., Olsson, R.A.: A Methodology for Testing Intrusion Detection Systems. IEEE Transactions on Software Engineering 22(10), 719–729 (1996)
15. Woon, I.M.Y., Kankanhalli, A.: Investigation of IS Professionals' Intention to Practise Secure Development of Applications. International Journal of Human-Computer Studies 65(1), 29–41 (2007)

16. Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., Stoner, E.: State of the Practice of Intrusion Detection Technologies. Technical Report CMU/SEI-99-TR-028. Carnegie Mellon University - Software Engineering Institute (2000)
17. Bace, R., Mell, P.: NIST Special Publication on Intrusion Detection Systems. National Institute of Standards and Technology - U.S. Department of Commerce (2001)
18. X-Force 2008, Trend & Risk Report. IBM Internet Security Systems - X-Force (2009)
19. Maloof, M.: Machine Learning and Data Mining for Computer Security. In: Advanced Information and Knowledge Processing. Springer, Heidelberg (2006)
20. Chuvakin, A.: Monitoring IDS. Information Security Journal: A Global Perspective 12(6), 12–16 (2004)
21. Rizza, J.M.: Computer Network Security. Springer, US (2005)
22. Mukherjee, B., Heberlein, L.T., Levitt, K.N.: Network Intrusion Detection. IEEE Network 8(3), 26–41 (1994)
23. Marchette, D.J.: Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint. Information Science and Statistics Springer-Verlag New York, Inc., New York (2001)
24. McHugh, J., Christie, A., Allen, J.: Defending Yourself: The Role of Intrusion Detection Systems. IEEE Software 17(5), 42–51 (2000)
25. Smaha, S.E.: Haystack: an Intrusion Detection System. In: Fourth Aerospace Computer Security Applications Conference (1988)
26. Lindqvist, U., Jonsson, E.: How to Systematically Classify Computer Security Intrusions. In: 1997 IEEE Symposium on Security and Privacy (1997)
27. Khaled, L.: Computer Security and Intrusion Detection. Crossroads 11(1), 2 (2004)
28. Anderson, J.P.: Computer Security Threat Monitoring and Surveillance. Technical Report (1980)
29. Denning, D.E.: An Intrusion-Detection Model. IEEE Transactions on Software Engineering 13(2), 222–232 (1987)
30. Jones, A., Sielken, R.: Computer System Intrusion Detection: A Survey. White Paper. University of Virginia - Computer Science Department (1999)
31. McHugh, J.: Intrusion and Intrusion Detection. International Journal of Information Security 1(1), 14–35 (2001)
32. Debar, H., Dacier, M., Wespi, A.: Towards a Taxonomy of Intrusion-Detection Systems. Computer Networks - the International Journal of Computer and Telecommunications Networking 31(8), 805–822 (1999)
33. Ptacek, T.H., Newsham, T.N.: Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection. White paper. Secure Networks, Inc. (1998)
34. Handley, M., Paxson, V., Kreibich, C.: Network Intrusion Detection: Evasion, Traffic Normalization, and End-to-end Protocol Semantics. In: 10th USENIX Security Symposium (2001)
35. Lazarevic, A., Kumar, V., Srivastava, J.: Intrusion Detection: a Survey. Managing Cyber Threats: Issues, Approaches, and Challenges. Massive Computing 5, 19–78 (2005)
36. Sundaram, A.: An Introduction to Intrusion Detection. Crossroads 2(4), 3–7 (1996)
37. Laskov, P., Düssel, P., Schäfer, C., Rieck, K.: Learning intrusion detection: Supervised or unsupervised? In: Roli, F., Vitulano, S. (eds.) ICIAP 2005. LNCS, vol. 3617, pp. 50–57. Springer, Heidelberg (2005)

38. Balepin, I., Maltsev, S., Rowe, J., Levitt, K.N.: Using specification-based intrusion detection for automated response. In: Vigna, G., Krügel, C., Jonsson, E. (eds.) RAID 2003. LNCS, vol. 2820, pp. 136–154. Springer, Heidelberg (2003)
39. Kemmerer, R.A., Vigna, G.: Intrusion Detection: a Brief History and Overview. Computer 35(4), 27–30 (2002)
40. Verwoerd, T., Hunt, R.: Intrusion Detection Techniques and Approaches. Computer Communications 25(15), 1356–1365 (2002)
41. Kruegel, C., Valeur, F., Vigna, G.: Intrusion Detection and Correlation - Challenges and Solutions. In: Advances in Information Security. Springer, US (2005)
42. Ahlberg, C., Shneiderman, B.: Visual Information Seeking: Tight Coupling of Dynamic Query Filters with Starfield Displays. In: Readings in Information Visualization: using Vision to Think, pp. 244–250. Morgan Kaufmann Publishrs Inc., San Francisco (1999)
43. Becker, R.A., Eick, S.G., Wilks, A.R.: Visualizing Network Data. IEEE Transactions on Visualization and Computer Graphics 1(1), 16–28 (1995)
44. Choi, H., Lee, H., Kim, H.: Fast Detection and Visualization of Network Attacks on Parallel Coordinates. Computers & Security 28(5), 276–288 (2009)
45. Conti, G.: Security Data Visualization: Graphical Techniques for Network Analysis. No Starch Press (2007)
46. Marty, R.: Applied Security Visualization. Addison-Wesley Professional, Reading (2008)
47. Itoh, T., Takakura, H., Sawada, A., Koyamada, K.: Hierarchical Visualization of Network Intrusion Detection Data. IEEE Computer Graphics and Applications 26(2), 40–47 (2006)
48. Conti, G., Abdullah, K.: Passive Visual Fingerprinting of Network Attack Tools. In: 2004 ACM Workshop on Visualization and Data Mining for Computer Security, ACM, Washington (2004)
49. Wilkinson, L.: The Grammar of Graphics. In: Statistics and Computing. Springer, New York (2005)
50. Keim, D.A.: Information Visualization and Visual Data Mining. IEEE Transactions on Visualization and Computer Graphics 8(1), 1–8 (2002)
51. Elmqvist, N., Dragicevic, P., Fekete, J.D.: Rolling the Dice: Multidimensional Visual Exploration using Scatterplot Matrix Navigation. IEEE Transactions on Visualization and Computer Graphics 14(6), 1141–1148 (2008)
52. Iris Dataset - UCI Machine Learning Repository, `http://archive.ics.uci.edu/ml/datasets/Iris`
53. McCulloch, W.S., Pitts, W.: A Logical Calculus of the Ideas Immanent in Nervous Activity. Bulletin of Mathematical Biology 5(4), 115–133 (1943)
54. Hebb, D.: The Organisation of Behaviour. Willey, New York (1949)
55. Haykin, S.: Neural Networks: a Comprehensive Foundation. Macmillan, Basingstoke (1994)
56. Rubner, J., Tavan, P.: A Self-Organizing Network for Principal Component Analysis. Europhysics Letters 10(7), 693–698 (1989)
57. Rubner, J., Schulten, K.: Development of Feature Detectors by Self-Organization. Biological Cybernetics 62(3), 193–199 (1990)
58. Rumelhart, D.E., Zipser, D.: Feature Discovery by Competitive Learning. Parallel Distributed Processing: Explorations in the Microstructure of Cognition. Foundations, vol. 1. MIT Press, Cambridge (1986)

59. Pearson, K.: On Lines and Planes of Closest Fit to Systems of Points in Space. Philosophical Magazine 2(6), 559–572 (1901)
60. Hotelling, H.: Analysis of a Complex of Statistical Variables into Principal Components. Journal of Education Psychology 24, 417–444 (1933)
61. Bishop, C.M.: Neural Networks for Pattern Recognition. Oxford University Press, Oxford (1996)
62. Oja, E.: Neural Networks, Principal Components, and Subspaces. International Journal of Neural Systems 1, 61–68 (1989)
63. Oja, E.: Principal Components, Minor Components, and Linear Neural Networks. Neural Networks 5(6), 927–935 (1992)
64. Oja, E.: A Simplified Neuron Model as a Principal Component Analyzer. Journal of Mathematical Biology 15(3), 267–273 (1982)
65. Sanger, D.: Contribution Analysis: a Technique for Assigning Responsibilities to Hidden Units in Connectionist Networks. Connection Science 1(2), 115–138 (1989)
66. Fyfe, C.: A Neural Network for PCA and Beyond. Neural Processing Letters 6(1-2), 33–41 (1997)
67. Oja, E., Ogawa, H., Wangviwattana, J.: Principal Component Analysis by Homogeneous Neural Networks, Part I: The Weighted Subspace Criterion. IEICE Transactions on Information and Systems 75(3), 366–375 (1992)
68. Fyfe, C.: PCA Properties of Interneurons: from Neurobiology to Real World Computing. In: International Conference on Artificial Neural Networks (ICANN 1993). Springer, Heidelberg (1993)
69. Fyfe, C.: Negative Feedback as an Organising Principle for Artificial Neural Networks. PhD Thesis. Strathclyde University (1995)
70. Charles, D., Fyfe, C.: Modelling Multiple-Cause Structure using Rectification Constraints. Network: Computation in Neural Systems 9(2), 167–182 (1998)
71. Fyfe, C., Corchado, E.: Maximum Likelihood Hebbian Rules. In: 10th European Symposium on Artificial Neural Networks, ESANN 2002 (2002)
72. Karhunen, J., Joutsensalo, J.: Representation and Separation of Signals using Nonlinear PCA Type Learning. Neural Networks 7(1), 113–127 (1994)
73. Oja, E., Ogawa, H., Wangviwattana, J.: Learning in Nonlinear Constrained Hebbian Networks. In: International Conference on Artificial Neural Networks (1991)
74. Xu, L.: Least Mean Square Error Reconstruction Principle for Self-organizing Neural-nets. Neural Networks 6(5), 627–648 (1993)
75. Bell, A.J., Sejnowski, T.J.: An Information-Maximization Approach to Blind Separation and Blind Deconvolution. Neural Computation 7(6), 1129–1159 (1995)
76. Girolami, M., Fyfe, C.: Stochastic ICA Contrast Maximisation using OJA's Nonlinear PCA Algorithm. International Journal of Neural Systems 8(5-6), 661 (1999)
77. Friedman, J.H., Tukey, J.W.: A Projection Pursuit Algorithm for Exploratory Data-Analysis. IEEE Transactions on Computers 23(9), 881–890 (1974)
78. Diaconis, P., Freedman, D.: Asymptotics of Graphical Projection Pursuit. The Annals of Statistics 12(3), 793–815 (1984)
79. Fyfe, C., Baddeley, R., McGregor, D.R.: Exploratory Projection Pursuit: an Artificial Neural Network Approach. Research Report/94/160, University of Strathclyde (1994)
80. Corchado, E., MacDonald, D., Fyfe, C.: Maximum and Minimum Likelihood Hebbian Learning for Exploratory Projection Pursuit. Data Mining and Knowledge Discovery 8(3), 203–225 (2004)

81. Corchado, E., Fyfe, C.: Connectionist Techniques for the Identification and Suppression of Interfering Underlying Factors. International Journal of Pattern Recognition and Artificial Intelligence 17(8), 1447–1466 (2003)
82. Corchado, E., Han, Y., Fyfe, C.: Structuring Global Responses of Local Filters Using Lateral Connections. Journal of Experimental & Theoretical Artificial Intelligence 15(4), 473–487 (2003)
83. Seung, H.S., Socci, N.D., Lee, D.: The Rectified Gaussian Distribution. Advances in Neural Information Processing Systems 10, 350–356 (1998)
84. Corchado, E., Burgos, P., del Mar Rodríguez, M., Tricio, V.: A Hierarchical Visualization Tool to Analyse the Thermal Evolution of Construction Materials. In: Luo, Y. (ed.) CDVE 2004. LNCS, vol. 3190, pp. 238–245. Springer, Heidelberg (2004)
85. Corchado, E., Pellicer, M.A., Borrajo, M.L.: A MLHL Based Method to an Agent-Based Architecture. International Journal of Computer Mathematics (2009) (accepted in press)
86. Herrero, Á., Corchado, E., Sáiz, L., Abraham, A.: DIPKIP: A Connectionist Knowledge Management System to Identify Knowledge Deficits in Practical Cases. Computational Intelligence (2009) (accepted in press)
87. Kohonen, T.: The Self-Organizing Map. IEEE 78(9), 1464–1480 (1990)
88. Ritter, H., Martinetz, T., Schulten, K.: Neural Computation and Self-Organizing Maps; An Introduction. Addison-Wesley Longman Publishing Co., Inc., Amsterdam (1992)
89. Oja, M., Kaski, S., Kohonen, T.: Bibliography of Self-Organizing Map (SOM) Papers: 1998-2001 Addendum. Neural Computing Surveys 3(1), 1–156 (2003)
90. Demartines, P., Herault, J.: Curvilinear Component Analysis: A Self-Organizing Neural Network for Nonlinear Mapping of Data Sets. IEEE Transactions on Neural Networks 8(1), 148–154 (1997)
91. Demartines, P.: Analyze de données par réseaux de neurones auto-organizés. Institut National Polytechnique de Grenoble (1994)
92. Franklin, S., Graesser, A.: Is It an Agent, or Just a Program?: A Taxonomy for Autonomous Agents. In: Jennings, N.R., Wooldridge, M.J., Müller, J.P. (eds.) ECAI-WS 1996 and ATAL 1996. LNCS, vol. 1193. Springer, Heidelberg (1997)
93. Russell, S.J., Norvig, P.: Artificial Intelligence: a Modern Approach. Prentice Hall, Englewood Cliffs (1995)
94. Weiss, G.: Multiagent Systems: a Modern Approach to Distributed Artificial Intelligence. MIT Press, Cambridge (1999)
95. Ferber, J.: Multi-agent Systems: an Introduction to Distributed Artificial Intelligence. Addison-Wesley, Reading (1999)
96. Huhns, M.N., Singh, M.P.: A Multiagent Treatment of Agenthood. Applied Artificial Intelligence 13(1-2), 3–10 (1999)
97. Durfee, E.H., Lesser, V.R.: Negotiating Task Decomposition and Allocation Using Partial Global Planning. Distributed Artificial Intelligence, vol. 2. Morgan Kaufmann Publishers Inc., San Francisco (1989)
98. Jennings, N.R., Sycara, K., Wooldridge, M.: A Roadmap of Agent Research and Development. Autonomous Agents and Multi-Agent Systems 1(1), 7–38 (1998)
99. Wooldridge, M.: Agent-based Computing. Interoperable Communication Networks 1(1), 71–97 (1998)
100. Brenner, W., Wittig, H., Zarnekow, R.: Intelligent Software Agents: Foundations and Applications. Springer-Verlag New York, Inc., Secaucus (1998)

101. Bird, S.D.: Toward a Taxonomy of Multi-agent Systems. International Journal of Man-Machine Studies 39(4), 689–704 (1993)
102. Wooldridge, M., Jennings, N.R.: Intelligent Agents: Theory and Practice. Knowledge Engineering Review 10(2), 115–152 (1995)
103. Leake, D., Wilson, D.: When experience is wrong: Examining CBR for changing tasks and environments. In: Althoff, K.-D., Bergmann, R., Branting, L.K. (eds.) ICCBR 1999. LNCS (LNAI), vol. 1650, p. 218. Springer, Heidelberg (1999)
104. Aamodt, A., Plaza, E.: Case-Based Reasoning - Foundational Issues, Methodological Variations, and System Approaches. AI Communications 7(1), 39–59 (1994)
105. Mantaras, R.L.D., McSherry, D., Bridge, D., Leake, D., Smyth, B., Craw, S., Faltings, B., Maher, M.L., Cox, M.T., Forbus, K., Keane, M., Aamodt, A., Watson, I.: Retrieval, Reuse, Revision, and Retention in Case-Based Reasoning. The Knowledge Engineering Review 20(3), 215–240 (2005)
106. Kolodner, J.: Case-based Reasoning. Morgan Kaufmann Publishers Inc., San Francisco (1993)
107. Reinartz, T., Iglezakis, I., Berghofer, T.R.: Review and Restore for Case-Base Maintenance. Computational Intelligence 17(2), 214–234 (2001)
108. Eskin, E., Arnold, A., Prerau, M., Portnoy, L., Stolfo, S.: A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data. In: Barbará, D., Jajodia, S. (eds.) Applications of Data Mining in Computer Security, pp. 77–101. Kluwer, Dordrecht (2002)
109. SNORT - Open Source Network Intrusion Prevention and Detection System, `http://snort.org/`
110. Noel, S., Wijesekera, D.: Modern Intrusion Detection, Data Mining, and Degrees of Attack Guilt. In: Barbará, D., Jajodia, S. (eds.) Applications of Data Mining in Computer Security, pp. 1–31. Kluwer Academic Publishers, Dordrecht (2002)
111. Julisch, K.: Data Mining for Intrusion Detection: A Critical Review. In: Barbará, D., Jajodia, S. (eds.) Applications of Data Mining in Computer Security. Advances in Information Security, pp. 33–62. Kluwer Academic Publishers, Dordrecht (2002)
112. Ye, N., Chen, Q.: Attack-norm Separation for Detecting Attack-induced Quality Problems on Computers and Networks. Quality and Reliability Engineering International 23(5), 545–553 (2007)
113. Eleazar, E.: Anomaly Detection over Noisy Data using Learned Probability Distributions. In: Seventeenth International Conference on Machine Learning. Morgan Kaufmann Publishers Inc., San Francisco (2000)
114. Lane, T., Brodley, C.E.: Temporal Sequence Learning and Data Reduction for Anomaly Detection. ACM Transactions on Information and System Security 2(3), 295–331 (1999)
115. Katos, V.: Network Intrusion Detection: Evaluating Cluster, Discriminant, and Logit Analysis. Information Sciences 177(15), 3060–3073 (2007)
116. Sarasamma, S.T., Zhu, Q.A.: Min-Max Hyperellipsoidal Clustering for Anomaly Detection in Network Security. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics 36(4), 887–901 (2006)
117. Wu, N., Zhang, J.: Factor-Analysis Based Anomaly Detection and Clustering. Decision Support Systems 42(1), 375–389 (2006)
118. Engelhardt, D.: Directions for Intrusion Detection and Response: a Survey. Electronics and Surveillance Research Laboratory, Defence Science and Technology Organisation, Department of Defence, Australian Government (1997)

119. Blustein, J., Fu, C.L., Silver, D.L.: Information Visualization for an Intrusion Detection System. In: Sixteenth ACM Conference on Hypertext and Hypermedia. ACM Press, New York (2005)
120. Goodall, J.R.: User Requirements and Design of a Visualization for Intrusion Detection Analysis. In: Sixth Annual IEEE SMC Information Assurance Workshop, IAW 2005 (2005)
121. Withall, M., Phillips, I., Parish, D.: Network Visualisation: a Review. IET Communications 1(3), 365–372 (2007)
122. Pongsiri, J., Parikh, M., Raspopovic, M., Chandra, K.: Visualization of Internet Traffic Features. In: 12th International Conference of Scientific Computing and Mathematical Modeling (1999)
123. Cox, K.C., Eick, S.G., He, T.: 3D Geographic Network Displays. ACM SIGMOD Record 25(4), 50–54 (1996)
124. Koutsofios, E.E., North, S.C., Truscott, R., Keim, D.A.: Visualizing Large-Scale Telecommunication Networks and Services. In: Conference on Visualization 1999. IEEE Computer Society Press, San Francisco (1999)
125. Dodge, M., Kitchin, R.: Atlas of Cyberspace. Addison-Wesley, Reading (2001)
126. Mansmann, F., Keim, D.A., North, S.C., Rexroad, B., Sheleheda, D.: Visual Analysis of Network Traffic for Resource Planning, Interactive Monitoring, and Interpretation of Security Threats. IEEE Transactions on Visualization and Computer Graphics 13(6), 1105–1112 (2007)
127. Claffy, K., Hyun, Y., Keys, K., Fomenkov, M., Krioukov, D.: Internet Mapping: From Art to Science. In: Conference For Homeland Security, Cybersecurity Applications & Technology (2009)
128. MRTG: The Multi Router Traffic Grapher, `http://www.mrtg.org`
129. Nyarko, K., Capers, T., Scott, C., Ladeji-Osias, K.A.: Network Intrusion Visualization with NIVA, an Intrusion Detection Visual Analyzer with Haptic Integration. In: Capers, T. (ed.) 10th Symposium on Haptic Interfaces for Virtual Environment and Teleoperator Systems, HAPTICS 2002 (2002)
130. Wood, A., Mountain, S.R., Denver, C.O., Practical, G.G.: Intrusion Detection: Visualizing Attacks in IDS Data. GIAC GCIA Practical, SANS Institute (2003)
131. Koike, H., Ohno, K.: SnortView: Visualization System of Snort Logs. In: 2004 ACM Workshop on Visualization and Data Mining for Computer Security. ACM Press, Washington (2004)
132. Abdullah, K., Lee, C.P., Conti, G., Copeland, J.A., Stasko, J.: IDS RainStorm: Visualizing IDS Alarms. In: IEEE Workshop on Visualization for Computer Security (VizSEC 2005). IEEE Computer Society, Los Alamitos (2005)
133. Koike, H., Ohno, K., Koizumi, K.: Visualizing Cyber Attacks Using IP Matrix. In: IEEE Workshop on Visualization for Computer Security (VizSEC 2005). IEEE Computer Society, Los Alamitos (2005)
134. Axelsson, S., Sands, D.: Understanding Intrusion Detection through Visualization. In: Advances in Information Security, vol. 24. Springer, Heidelberg (2006)
135. Foresti, S., Agutter, J., Livnat, Y., Moon, S., Erbacher, R.: Visual Correlation of Network Alerts. IEEE Computer Graphics and Applications 26(2), 48–59 (2006)
136. Analysis Console for Intrusion Databases (ACID), `http://www.andrew.cmu.edu/user/rdanyliw/snort/snortacid.html`
137. Kim, H., Kang, I., Bahk, S.: Real-time Visualization of Network Attacks on High-speed Links. IEEE Network 18(5), 30–39 (2004)

138. Lau, S.: The Spinning Cube of Potential Doom. Communications of the ACM 47(6), 25–26 (2004)
139. The Shoki Packet Hustler, http://shoki.sourceforge.net/hustler/
140. Plonka, D.: FlowScan: A Network Traffic Flow Reporting and Visualization Tool. In: 14th USENIX Conference on System Administration. USENIX Association, New Orleans (2000)
141. Abdullah, K., Lee, C., Conti, G., Copeland, J.A.: Visualizing Network Data for Intrusion Detection. In: Sixth Annual IEEE Information Assurance Workshop - Systems, Man and Cybernetics (2005)
142. Stockinger, K., Bethel, E.W., Campbell, S., Dart, E., Wu, K.: Detecting Distributed Scans using High-Performance Query-Driven Visualization. In: 2006 ACM/ IEEE Conference on Supercomputing. ACM, Tampa (2006)
143. Conti, G., Grizzard, J., Ahamad, M., Owen, H.: Visual Exploration of Malicious Network Objects Using Semantic Zoom, Interactive Encoding and Dynamic Queries. In: IEEE Workshop on Visualization for Computer Security (VizSEC 2005). IEEE Computer Society, Los Alamitos (2005)
144. Taylor, T., Brooks, S., McHugh, J.: NetBytes Viewer: An Entity-Based NetFlow Visualization Utility for Identifying Intrusive Behavior. In: Workshop on Visualization for Computer Security (VizSEC 2007). Mathematics and Visualization. Springer, Heidelberg (2008)
145. Cheung, S., Crawford, R., Dilger, M., Frank, J., Hoagland, J., Levitt, K., Rowe, J., Staniford-Chen, S., Yip, R., Zerkle, D.: The Design of GrIDS: A Graph-based Intrusion Detection System. Technical Report CSE-99-2. University of California at Davis. Computer Science Department (1999)
146. Yin, X., Yurcik, W., Adam, S.: VisFlowCluster-IP: Connectivity-Based Visual Clustering of Network Hosts. In: 21st IFIP International Information Security Conference (SEC 2006), Karlstad, Sweden (2006)
147. Pearlman, J., Rheingans, P.: Visualizing Network Security Events Using Compound Glyphs from a Service-Oriented Perspective. In: Workshop on Visualization for Computer Security (VizSEC 2007). Mathematics and Visualization. Springer, Heidelberg (2008)
148. Höglund, A.J., Hätönen, K.: Computer Network User Behaviour Visualisation using Self Organizing Maps. In: 8th International Conference on Artificial Neural Networks (ICANN 1998), vol. 2. IEEE, Los Alamitos (1998)
149. Girardin, L.: An Eye on Network Intruder-Administrator Shootouts. In: 1st Workshop on Intrusion Detection and Network Monitoring 1. USENIX Association, Santa Clara (1999)
150. Girardin, L., Brodbeck, D.: A Visual Approach for Monitoring Logs. In: 12th USENIX Conference on System Administration. USENIX Association, Boston (1998)
151. Labib, K., Vemuri, V.: Application of Exploratory Multivariate Analysis for Network Security. In: Vemuri, V. (ed.) Enhancing Computer Security with Smart Technology, pp. 229–261. CRC Press, Boca Raton (2005)
152. Kayacik, H.G., Zincir-Heywood, A.N.: Using Self-Organizing Maps to Build an Attack Map for Forensic Analysis. In: ACM 2006 International Conference on Privacy, Security and Trust (PST 2006). ACM, Markham (2006)
153. KDD Cup 1999 Dataset (1999), http://archive.ics.uci.edu/ml/databases/kddcup99/kddcup99.html

154. Elkan, M.: Results of the KDD 1999 Classifier Learning Contest (1999), http://www-cse.ucsd.edu/users/elkan/clresults.html
155. Kumar, G., Devaraj, D.: Network Intrusion Detection using Hybrid Neural Networks. In: International Conference on Signal Processing, Communications and Networking, ICSCN 2007 (2007)
156. Solka, J.L., Marchette, D.J., Wallet, B.C.: Statistical Visualization Methods in Intrusion Detection. In: 32nd Symposium on the Interface. Computing Science and Statistics, vol. 32 (2000)
157. Estrin, D., Handley, M., Heidemann, J., McCanne, S., Ya, X., Yu, H.: Network Visualization with Nam, the VINT Network Animator. IEEE Computer Magazine 33(11), 63–68 (2000)
158. D'Amico, A., Larkin, M.: Methods of Visualizing Temporal Patterns in and Mission Impact of Computer Security Breaches. In: DARPA Information Survivability Conference & Exposition II (DISCEX 2001) (January 2001)
159. Erbacher, R.F., Frincke, D.: Visual Behavior Characterization for Intrusion and Misuse Detection. In: Visual Data Exploration and Analysis Conference. SPIE Proceedings Series, vol. 4302 (2001)
160. Erbacher, R.F., Garber, M.: Visualization Techniques for Intrusion Behavior Identification. In: Sixth Annual IEEE SMC Information Assurance Workshop, IAW 2005 (2005)
161. Teoh, S.T., Ma, K.-L., Wu, S.F., Jankun-Kelly, T.J.: Detecting Flaws and Intruders with Visual Data Analysis. IEEE Computer Graphics and Applications 24(5), 27–35 (2004)
162. McPherson, J., Ma, K.-L., Krystosk, P., Bartoletti, T., Christensen, M.: PortVis: a Tool for Port-Based Detection of Security Events. In: 2004 ACM Workshop on Visualization and Data Mining for Computer Security. ACM Press, Washington (2004)
163. Lakkaraju, K., Yurcik, W., Lee, A.J.: NVisionIP: Netflow Visualizations of System State for Security Situational Awareness. In: 2004 ACM Workshop on Visualization and Data Mining for Computer Security. ACM, Washington (2004)
164. Abad, C., Li, Y., Lakkaraju, K., Yin, X., Yurcik, W.: Correlation Between NetFlow System and Network Views for Intrusion Detection. In: Workshop on Link Analysis, Counter-terrorism, and Privacy. Lake Buena Vista, FL (2004)
165. Lee, C.P., Trost, J., Gibbs, N., Raheem, B., Copeland, J.A.: Visual Firewall: Real-time Network Security Monitor. In: IEEE Workshop on Visualization for Computer Security (VizSEC 2005). IEEE Computer Society, Los Alamitos (2005)
166. Oline, A., Reiners, D.: Exploring Three-Dimensional Visualization for Intrusion Detection. In: IEEE Workshop on Visualization for Computer Security (VizSEC 2005). IEEE Computer Society, Los Alamitos (2005)
167. Muelder, C., Ma, K.-L., Bartoletti, T.: A Visualization Methodology for Characterization of Network Scans. In: IEEE Workshop on Visualization for Computer Security (VizSEC 2005), IEEE Computer Society, Los Alamitos (2005)
168. Krasser, S., Conti, G., Grizzard, J., Gribschaw, J., Owen, H.: Real-time and Forensic Network Data Analysis Using Animated and Coordinated Visualization. In: Sixth Annual IEEE SMC Information Assurance Workshop, IAW 2005 (2005)
169. Fink, G.A., Muessig, P., North, C.: Visual Correlation of Host Processes and Network Traffic. In: IEEE Workshop on Visualization for Computer Security (VizSEC 2005). IEEE Computer Society, Los Alamitos (2005)

170. Ren, P., Gao, Y., Li, Z.C., Chen, Y., Watson, B.: IDGraphs: Intrusion Detection and Analysis Using Histographs. In: IEEE Workshop on Visualization for Computer Security (VizSEC 2005). IEEE Computer Society, Los Alamitos (2005)
171. Ren, P., Gao, Y., Li, Z.C., Chen, Y., Watson, B.: IDGraphs: Intrusion Detection and Analysis Using Stream Compositing. IEEE Computer Graphics and Applications 26(2), 28–39 (2006)
172. Goodall, J.R., Lutters, W.G., Rheingans, P., Komlodi, A.: Focusing on Context in Network Traffic Analysis. IEEE Computer Graphics and Applications 26(2), 72–80 (2006)
173. Muelder, C., Ma, K.-L., Bartoletti, T.: Interactive visualization for network and port scan detection. In: Valdes, A., Zamboni, D. (eds.) RAID 2005. LNCS, vol. 3858, pp. 265–283. Springer, Heidelberg (2006)
174. D'Amico, A.D., Goodall, J.R., Tesone, D.R., Kopylec, J.K.: Visual Discovery in Computer Network Defense. IEEE Computer Graphics and Applications 27(5), 20–27 (2007)
175. Goodall, J.R., Tesone, D.R.: Visual Analytics for Network Flow Analysis. In: Cybersecurity Applications & Technology Conference for Homeland Security. IEEE Press, Los Alamitos (2009)
176. Fischer, F., Mansmann, F., Keim, D.A., Pietzko, S., Waldvogel, M.: Large-scale network monitoring for visual analysis of attacks. In: Goodall, J.R., Conti, G., Ma, K.-L. (eds.) VizSec 2008. LNCS, vol. 5210, pp. 111–118. Springer, Heidelberg (2008)
177. Shneiderman, B.: Tree Visualization with Tree-maps: a 2-D Space-filling Approach. ACM Transactions on Graphics 11(1), 92–99 (1992)
178. Phan, D., Gerth, J., Lee, M., Paepcke, A., Winograd, T.: Visual Analysis of Network Flow Data with Timelines and Event Plots. In: Workshop on Visualization for Computer Security (VizSEC 2007). Mathematics and Visualization. Springer, Heidelberg (2008)
179. Shoch, J.F., Hupp, J.A.: The "Worm" Programs - Early Experience with a Distributed Computation. Communications of the ACM 25(3), 172–180 (1982)
180. Crosbie, M., Dole, B., Ellis, T., Krsul, I., Spafford, E.: IDIOT Users Guide. Technical Report CSD-TR-96-050. Department of Computer Sciences. Purdue University (1996)
181. Jensen, K.: Coloured Petri Nets and the Invariant Method. Theoretical Computer Science 14, 317–336 (1981)
182. Petri, C.A.: Kommunikation mit Automaten. Institut für Instrumentelle Mathematik, Schriften des IMM Nr. 2 (1962)
183. Vert, G., Frincke, D.A., McConnell, J.C.: A Visual Mathematical Model for Intrusion Detection. In: 21st National Information Systems Security Conference (1998)
184. Atkison, T., Pensy, K., Nicholas, C., Ebert, D., Atkison, R., Morris, C.: Case Study: Visualization and Information Retrieval Techniques for Network Intrusion Detection. In: Joint Eurographics- IEEE TCVG Symposium on Visualization (VisSym 2001). Computer Science. Springer, Heidelberg (2001)
185. Ebert, D.S., Shaw, C.D., Zwa, A., Starr, C.: Two-handed Interactive Stereoscopic Visualization. In: IEEE 7th Conference on Visualization 1996. IEEE Computer Society Press, San Francisco (1996)
186. Takada, T., Koike, H.: Tudumi: Information Visualization System for Monitoring and Auditing Computer Logs. In: Sixth International Conference on Information Visualisation (2002)

187. Teoh, S.T., Ma, K.L., Wu, S.F., Zhao, X.: Case Study: Interactive Visualization for Internet Security. In: IEEE Conference on Visualization (Vis 2002). IEEE Computer Society, Boston (2002)
188. Fisk, M., Smith, S.A., Weber, P., Kothapally, S., Caudell, T.: Immersive Network Monitoring. In: 2003 Passive and Active Measurement Workshop (2003)
189. Ball, R., Glenn, A.F., North, C.: Home-centric Visualization of Network Traffic for Security Administration. In: 2004 ACM Workshop on Visualization and Data Mining for Computer Security. ACM, Washington (2004)
190. Erbacher, R.F., Christensen, K., Sundberg, A.: Designing Visualization Capabilities for IDS Challenges. In: IEEE Workshop on Visualization for Computer Security (VizSEC 2005). IEEE Computer Society, Los Alamitos (2005)
191. Komlodi, A., Rheingans, P., Utkarsha, A., Goodall, J.R., Amit, J.: A User-Centered Look at Glyph-Based Security Visualization. In: IEEE Workshop on Visualization for Computer Security (VizSEC 2005). IEEE Computer Society, Los Alamitos (2005)
192. Kim, S.S., Reddy, A.L.N.: A Study of Analyzing Network Traffic as Images in Real-time. In: IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2005 (March 2005)
193. Kisner, T., Essoh, A., Kaderali, F.: Visualisation of Network Traffic using Dynamic Co-occurrence Matrices. In: Second International Conference on Internet Monitoring and Protection, ICIMP 2007 (2007)
194. Onut, I.-V., Ghorbani, A.A.: SVision: A Novel Visual Network-Anomaly Identification Technique. Computers & Security 26(3), 201–212 (2007)
195. Samak, T., Ghanem, S., Ismail, M.A.: On the Efficiency of Using Space-filling Curves in Network Traffic Representation. In: IEEE INFOCOM Workshop (2008)
196. Paxson, V.: Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks: the International Journal of Computer and Telecommunications Networking 31(23-24), 2435–2463 (1999)
197. Bro Intrusion Detection System, `http://bro-ids.org/`
198. tcpdump/libpcap, `http://www.tcpdump.org/`
199. Lippmann, R., Haines, J.W., Fried, D.J., Korba, J., Das, K.: The 1999 DARPA Off-line Intrusion Detection Evaluation. Computer Networks 34(4), 579–595 (2000)
200. Lippmann, R., Haines, J.W., Fried, D.J., Korba, J., Das, K.: Analysis and Results of the 1999 DARPA Off-Line Intrusion Detection Evaluation. In: Debar, H., Mé, L., Wu, S.F. (eds.) RAID 2000. LNCS, vol. 1907, p. 162. Springer, Heidelberg (2000)
201. Stolfo, S., Prodromidis, A.L., Tselepis, S., Lee, W., Fan, D.W., Chan, P.K.: JAM: Java Agents for Meta-Learning over Distributed Databases. In: Third International Conference on Knowledge Discovery and Data Mining (1997)
202. Reilly, M., Stillman, M.: Open Infrastructure for Scalable Intrusion Detection. In: 1998 IEEE Information Technology Conference (1998)
203. Spafford, E.H., Zamboni, D.: Intrusion Detection Using Autonomous Agents. Computer Networks: The International Journal of Computer and Telecommunications Networking 34(4), 547–570 (2000)
204. Hegazy, I.M., Al-Arif, T., Fayed, Z.T., Faheem, H.M.: A Multi-agent Based System for Intrusion Detection. IEEE Potentials 22(4), 28–31 (2003)
205. Gorodetski, V., Kotenko, I., Karsaev, O.: Multi-Agent Technologies for Computer Network Security: Attack Simulation, Intrusion Detection and Intrusion Detection Learning. Computer Systems Science and Engineering 18(4), 191–200 (2003)

206. Miller, P., Inoue, A.: Collaborative Intrusion Detection System. In: 22nd International Conference of the North American Fuzzy Information Processing Society, NAFIPS 2003 (2003)
207. Gorodetsky, V., Karsaev, O., Samoilov, V., Ulanov, A.: Asynchronous alert correlation in multi-agent intrusion detection systems. In: Gorodetsky, V., Kotenko, I., Skormin, V.A. (eds.) MMM-ACNS 2005. LNCS, vol. 3685, pp. 366–379. Springer, Heidelberg (2005)
208. Dasgupta, D., Gonzalez, F., Yallapu, K., Gomez, J., Yarramsettii, R.: CIDS: An Agent-based Intrusion Detection System. Computers & Security 24(5), 387–398 (2005)
209. Cougaar: Cognitive Agent Architecture, `http://cougaar.org/`
210. Debar, H., Curry, D., Feinstein, B.: The Intrusion Detection Message Exchange Format (IDMEF). IETF RFC 4765 (2007)
211. Gowadia, V., Farkas, C., Valtorta, M.: PAID: A Probabilistic Agent-Based Intrusion Detection System. Computers & Security 24(7), 529–545 (2005)
212. Tsang, C.-H., Kwong, S.: Multi-agent Intrusion Detection System in Industrial Network using Ant Colony Clustering Approach and Unsupervised Feature Extraction. In: 2005 IEEE International Conference on Industrial Technology (ICIT 2005) (2005)
213. Mukkamala, S., Sung, A.H., Abraham, A.: Hybrid Multi-agent Framework for Detection of Stealthy Probes. Applied Soft Computing 7(3), 631–641 (2007)
214. Jansen, W.A., Karygiannis, T., Marks, D.G.: Applying Mobile Agents to Intrusion Detection and Response. US Department of Commerce, Technology Administration, National Institute of Standards and Technology (1999)
215. Asaka, M., Taguchi, A., Goto, S.: The Implementation of IDA: An Intrusion Detection Agent System. In: 11th Annual Computer Security Incident Handling Conference (June 1999)
216. De Queiroz, J.D., da Costa Carmo, L.F.R., Pirmez, L.: Micael: An Autonomous Mobile Agent System to Protect New Generation Networked Applications. In: Second International Workshop on Recent Advances in Intrusion Detection, RAID 1999 (1999)
217. Mell, P., Marks, D., McLarnon, M.: A Denial-of-service Resistant Intrusion Detection Architecture. Computer Networks: The International Journal of Computer and Telecommunications Networking 34(4), 641–658 (2000)
218. Krügel, C., Toth, T., Kirda, E.: SPARTA: a Mobile Agent Based Instrusion Detection System. In: IFIP TC11 WG11.4 First Annual Working Conference on Network Security: Advances in Network and Distributed Systems Security. IFIP Conference Proceedings, vol. 206. Kluwer, Dordrecht (2001)
219. Dasgupta, D., Brian, H.: Mobile Security Agents for Network Traffic Analysis. In: DARPA Information Survivability Conference & Exposition II, DISCEX 2001 (February 2001)
220. Helmer, G., Wong, J.S.K., Honavar, V.G., Miller, L.: Automated Discovery of Concise Predictive Rules for Intrusion Detection. Journal of Systems and Software 60(3), 165–175 (2002)
221. Helmer, G., Wong, J.S.K., Honavar, V., Miller, L., Wang, Y.: Lightweight Agents for Intrusion Detection. Journal of Systems and Software 67(2), 109–122 (2003)
222. Li, C., Song, Q., Zhang, C.: MA-IDS Architecture for Distributed Intrusion Detection using Mobile Agents. In: 2nd International Conference on Information Technology for Application, ICITA 2004 (2004)

223. Marks, D.G., Mell, P., Stinson, M.: Optimizing the Scalability of Network Intrusion Detection Systems Using Mobile Agents. Journal of Network and Systems Management 12(1), 95–110 (2004)
224. Deeter, K., Singh, K., Wilson, S., Filipozzi, L., Vuong, S.T.: APHIDS: A mobile agent-based programmable hybrid intrusion detection system. In: Karmouch, A., Korba, L., Madeira, E.R.M. (eds.) MATA 2004. LNCS, vol. 3284, pp. 244–253. Springer, Heidelberg (2004)
225. Alam, M.S., Gupta, A., Wires, J., Vuong, S.T.: APHIDS++: Evolution of A programmable hybrid intrusion detection system. In: Magedanz, T., Karmouch, A., Pierre, S., Venieris, I.S. (eds.) MATA 2005. LNCS, vol. 3744, pp. 22–31. Springer, Heidelberg (2005)
226. Kolaczek, G., Pieczynska-Kuchtiak, A., Juszczyszyn, K., Grzech, A., Katarzyniak, R.P., Nguyen, N.T.: A mobile agent approach to intrusion detection in network systems. In: Khosla, R., Howlett, R.J., Jain, L.C. (eds.) KES 2005. LNCS (LNAI), vol. 3682, pp. 514–519. Springer, Heidelberg (2005)
227. Foukia, N.: IDReAM: Intrusion Detection and Response Executed with Agent Mobility Architecture and Implementation. In: Fourth International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS 2005). ACM, The Netherlands (2005)
228. Alim, A.S.A., Ismail, A.S., Ahmed, S.H.: IDSUDA: An Intrusion Detection System Using Distributed Agents. Journal of Computer Networks and Internet Research 5(1), 1–11 (2005)
229. Wang, H.Q., Wang, Z.Q., Zhao, Q., Wang, G.F., Zheng, R.J., Liu, D.X.: Mobile agents for network intrusion resistance. In: Shen, H.T., Li, J., Li, M., Ni, J., Wang, W. (eds.) APWeb Workshops 2006. LNCS, vol. 3842, pp. 965–970. Springer, Heidelberg (2006)
230. Ma, K.-L.: Visualization for Security. ACM SIGGRAPH Computer Graphics 38(4), 4–6 (2004)
231. Erbacher, R.F., Walker, K.L., Frincke, D.A.: Intrusion and Misuse Detection in Large-scale Systems. IEEE Computer Graphics and Applications 22(1), 38–47 (2002)
232. Corchado, E., Wu, X., Oja, E., Herrero, Á., Baruque, B. (eds.): HAIS 2009. LNCS, vol. 5572. Springer, Heidelberg (2009)
233. Medsker, L.R.: Hybrid Intelligent Systems. Kluwer Academic Publishers, Dordrecht (1995)
234. Ron, S., Frederic, A. (eds.): Connectionist-Symbolic Integration: From Unified to Hybrid Approaches. Lawrence Erlbaum Associates, Inc., Mahwah (1997)
235. Tran, C., Abraham, A., Jain, L.: Decision Support Systems using Hybrid Neurocomputing. Neurocomputing 61, 85–97 (2004)
236. Bridges, S.M., Vaughn, R.B.: Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection. In: National Information Systems Security Conference (NISSC) (2000)
237. Marin, J.A., Ragsdale, D., Surdu, J.: A Hybrid Approach to Profile Creation and Intrusion Detection. In: DARPA Information Survivability Conference and Exposition II (DISCEX 2001) (2001)
238. Botha, M., Solms, R.v., Perry, K., Loubser, E., Yamoyany, G.: The Utilization of Artificial Intelligence in a Hybrid Intrusion Detection System. In: 2002 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology, Port Elizabeth, South Africa. ACM International Conference Proceedings Series, vol. 30 (2002)

239. Sindhu, S.S.S., Ramasubramanian, P., Kannan, A.: Intelligent multi-agent based genetic fuzzy ensemble network intrusion detection. In: Pal, N.R., Kasabov, N., Mudi, R.K., Pal, S., Parui, S.K. (eds.) ICONIP 2004. LNCS, vol. 3316, pp. 983–988. Springer, Heidelberg (2004)
240. Middlemiss, M., Dick, G.: Feature Selection of Intrusion Detection Data Using a Hybrid Genetic Algorithm/KNN Approach. In: Design and Application of Hybrid Intelligent Systems, pp. 519–527. IOS Press, Amsterdam (2003)
241. Mukkamala, S., Sung, A.H., Abraham, A.: Intrusion Detection Using an Ensemble of Intelligent Paradigms. Journal of Network and Computer Applications 28(2), 167–182 (2005)
242. Kholfi, S., Habib, M., Aljahdali, S.: Best Hybrid Classifiers for Intrusion Detection. Journal of Computational Methods in Science and Engineering 6(2), 299–307 (2006)
243. Toosi, A.N., Kahani, M.: A New Approach to Intrusion Detection Based on an Evolutionary Soft Computing Model using Neuro-Fuzzy Classifiers. Computer Communications 30(10), 2201–2212 (2007)
244. Tsang, C.-H., Kwong, S., Wang, H.: Genetic-Fuzzy Rule Mining Approach and Evaluation of Feature Selection Techniques for Anomaly Intrusion Detection. Pattern Recognition 40(9), 2373–2391 (2007)
245. Peddabachigari, S., Abraham, A., Grosan, C., Thomas, J.: Modeling Intrusion Detection System Using Hybrid Intelligent Systems. Journal of Network and Computer Applications 30(1), 114–132 (2007)
246. Abadeh, M.S., Habibi, J., Lucas, C.: Intrusion Detection using a Fuzzy Genetics-based Learning Algorithm. Journal of Network and Computer Applications 30(1), 414–428 (2007)
247. Yuehui, C., Ajith, A., Bo, Y.: Hybrid Flexible Neural-tree-based Intrusion Detection Systems. International Journal of Intelligent Systems 22(4), 337–352 (2007)
248. Shon, T., Moon, J.: A Hybrid Machine Learning Approach to Network Anomaly Detection. Information Sciences 177(18), 3799–3821 (2007)
249. Goldring, T.: Scatter (and Other) Plots for Visualizing User Profiling Data and Network Traffic. In: 2004 ACM Workshop on Visualization and Data Mining for Computer Security. ACM Press, Washington (2004)
250. Labib, K., Vemuri, V.R.: Detecting and Visualizing Denial-of-Service and Network Probe Attacks Using Principal Component Analysis. In: Third Conference on Security and Network Architectures, SAR 2004 (2004)
251. Labib, K., Vemuri, V.R.: An Application of Principal Component Analysis to the Detection and Visualization of Computer Network Attacks. Annals of Telecommunications 61(1-2), 218–234 (2006)
252. Jianqiang, X., Dickerson, J.E., Dickerson, J.A.: Fuzzy Feature Extraction and Visualization for Intrusion Detection. In: 12th IEEE International Conference on Fuzzy Systems, vol. 2 (2003)
253. GGobi, `http://www.ggobi.org/`
254. Taylor, C., Alves-Foss, J.: NATE - Network Analysis of Anomalous Traffic Events, A Low-Cost Approach. In: New Security Paradigms Workshop (2001)
255. Shyu, M.L., Chen, S.C., Sarinnapakorn, K., Chang, L.: A Novel Anomaly Detection Scheme Based on Principal Component Classifier. In: IEEE Foundations and New Directions of Data Mining Workshop, pp. 172–179 (2003)
256. Lakhina, A., Papagiannaki, K., Crovella, M., Diot, C., Kolaczyk, E.D., Taft, N.: Structural Analysis of Network Traffic Flows. In: Joint International Conference on Measurement and Modeling of Computer Systems. ACM Press, New York (2004)

257. Bouzida, Y., Gombault, S.: Eigenconnections to Intrusion Detection. In: 19th IFIP International Information Security Conference. IFIP International Federation for Information Processing, vol. 147. Springer, Boston (2004)
258. Kuchimanchi, G.K., Phoha, V.V., Balagani, K.S., Gaddam, S.R.: Dimension Reduction using Feature Extraction Methods for Real-time Misuse Detection Systems. In: Fifth Annual IEEE SMC Information Assurance Workshop (2004)
259. Kurosawa, S., Nakayama, H., Nei, K., Jamalipour, A., Nemoto, Y.: A Self-adaptive Intrusion Detection Method for AODV-based Mobile Ad Hoc Networks. In: IEEE International Conference on Mobile Adhoc and Sensor Systems (2005)
260. Wang, W., Battiti, R.: Identifying Intrusions in Computer Networks with Principal Component Analysis. In: First International Conference on Availability, Reliability and Security, ARES 2006 (2006)
261. Ramah, K.H., Ayari, H., Kamoun, F.: Traffic anomaly detection and characterization in the tunisian national university network. In: Boavida, F., Plagemann, T., Stiller, B., Westphal, C., Monteiro, E. (eds.) NETWORKING 2006. LNCS, vol. 3976, pp. 136–147. Springer, Heidelberg (2006)
262. Venkatachalam, V., Selvan, S.: Performance Comparison of Intrusion Detection System Classifiers using Various Feature Reduction Techniques. International Journal of Simulation 9(1), 30–39 (2008)
263. Corchado, E., Herrero, Á.: Neural Visualization of Network Traffic Data for Intrusion Detection. Applied Soft Computing (2010) (accepted with changes)
264. Case, J., Fedor, M.S., Schoffstall, M.L., Davin, C.: Simple Network Management Protocol (SNMP). IETF RFC 1157 (1990)
265. Davin, J., Galvin, J., McCloghrie, K.: SNMP Administrative Model. IETF RFC 1351 (1992)
266. Vulnerability Statistics Report. Cisco Secure Consulting (2000)
267. Case, J., McCloghrie, K., Rose, M., Waldbusse, S.: Introduction to Version 2 of the Internet-standard Network Management Framework. IETF RFC 1441 (1993)
268. The Top 10 Most Critical Internet Security Threats (2000-2001 Archive). SANS Institute (2001)
269. Northcutt, S., Cooper, M., Fredericks, K., Fearnow, M., Riley, J.: Intrusion Signatures and Analysis. New Riders Publishing, Thousand Oaks (2001)
270. Myerson, J.M.: Identifying Enterprise Network Vulnerabilities. International Journal of Network Management 12(3), 135–144 (2002)
271. Mauro, D.R., Schmidt, K.J.: Essential SNMP. O'Reilly Media, Inc., Sebastopol (2001)
272. Perkins, D.T.: SNMP Versions. The Simple Times 5(1), 13–14 (1997)
273. Blumenthal, U., Wijnen, B.: Security Features of SNMPv3. The Simple Times 5(1), 8–12 (1997)
274. SNMP MIB, `http://edocs.bea.com/snmpagnt/v210/mibref/1tmib.html`
275. McCloghrie, K., Rose, M.: Management Information Base for Network Management of TCP/IP-based Internets: MIB-II. IETF RFC 1213 (1991)
276. Postel, J.: IAB Official Protocol Standards. IETF RFC 1100 (1989)
277. Staniford, S., Hoagland, J.A., McAlerney, J.M.: Practical Automated Detection of Stealthy Portscans. Journal of Computer Security 10(1-2), 105–136 (2002)
278. Malowidzki, M.: GetBulk Worth Fixing. The Simple Times 10(1), 3–6 (2002)

279. Sprenkels, R., Martin-Flatin, J.P.: Bulk Transfers of MIB Data. Technical Report SSC/1999/009. Communication Systems Division. Swiss Federal Institute of Technology Lausanne (1999)
280. Herrero, Á., Corchado, E., Pellicer, M.A., Abraham, A.: MOVIH-IDS: A Mobile-Visualization Hybrid Intrusion Detection System. Neurocomputing 72(13-15), 2775–2784 (2009)
281. Carrascosa, C., Bajo, J., Julián, V., Corchado, J.M., Botti, V.: Hybrid Multi-agent Architecture as a Real-Time Problem-Solving Model. Expert Systems with Applications: An International Journal 34(1), 2–17 (2008)
282. Bratman, M.E.: Intentions, Plans and Practical Reason. Harvard University Press, Cambridge (1987)
283. Herrero, Á., Corchado, E., Gastaldo, P., Zunino, R.: Neural Projection Techniques for the Visual Inspection of Network Traffic. Neurocomputing 72(16-18), 3649–3658 (2009)
284. Babu, S., Subramanian, L., Widom, J.: A Data Stream Management System for Network Traffic Management. In: Workshop on Network-Related Data Management (NRDM 2001) (2001)
285. Herrero, Á., Corchado, E.: Traffic data preparation for a hybrid network IDS. In: Corchado, E., Abraham, A., Pedrycz, W. (eds.) HAIS 2008. LNCS (LNAI), vol. 5271, pp. 247–256. Springer, Heidelberg (2008)
286. Dreger, H., Feldmann, A., Paxson, V., Sommer, R.: Operational Experiences with High-Volume Network Intrusion Detection. In: 11th ACM Conference on Computer and Communications Security. ACM Press, New York (2004)
287. Wireshark, `http://www.wireshark.org`
288. Cisco IOS NetFlow, `http://www.cisco.com/web/go/netflow`
289. Corchado, J.M., Laza, R.: Constructing Deliberative Agents with Case-Based Reasoning Technology. International Journal of Intelligent Systems 18(12), 1227–1241 (2003)
290. Pellicer, M.A., Corchado, J.M.: Development of CBR-BDI Agents. International Journal of Computer Science and Applications 2(1), 25–32 (2005)
291. Bajo, J., Corchado, J.M., Rodríguez, S.: Intelligent guidance and suggestions using case-based planning. In: Weber, R.O., Richter, M.M. (eds.) ICCBR 2007. LNCS (LNAI), vol. 4626, pp. 389–403. Springer, Heidelberg (2007)
292. Hammond, K.J.: Case-based Planning: Viewing Planning as a Memory Task. Academic Press Professional, Inc., London (1989)
293. Spalzzi, L.: A Survey on Case-Based Planning. Artificial Intelligence Review 16(1), 3–36 (2001)
294. Zambonelli, F., Jennings, N.R., Wooldridge, M.: Developing Multiagent Systems: the Gaia Methodology. ACM Transactions on Software Engineering and Methodology 12(3), 317–370 (2003)
295. Bevilacqua, A.: A Dynamic Load Balancing Method on A Heterogeneous Cluster of Workstations. Informatica 23(1) (1999)
296. Schaerf, A., Shoham, Y., Tennenholtz, M.: Adaptive Load Balancing: A Study in Multi-Agent Learning. Journal of Artificial Intelligence Research 2, 475–500 (1995)
297. Noronha Nassif, L., Marcos Nogueira, J., Vinicius de Andrade, F., Ahmed, M., Karmouch, A., Impey, R.: Job Completion Prediction in Grid using Distributed Case-based Reasoning. In: 14th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprise (2005)

298. Mahoney, M.V., Chan, P.K.: An analysis of the 1999 dARPA/Lincoln laboratory evaluation data for network anomaly detection. In: Vigna, G., Krügel, C., Jonsson, E. (eds.) RAID 2003. LNCS, vol. 2820, pp. 220–237. Springer, Heidelberg (2003)
299. McHugh, J.: Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 Darpa Off-line Intrusion Detection System Evaluation as Performed by Lincoln Laboratory. ACM Transactions on Information and System Security 3(4), 262–294 (2000)
300. DARPA Intrusion Detection Evaluation, http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/index.html
301. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., Vázquez, E.: Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges. Computers & Security 28(1-2), 18–28 (2009)
302. Ranum, M.J.: Experiences Benchmarking Intrusion Detection Systems. NFR Security Technical Publications (2001)
303. Egan, J.P.: Signal Detection Theory and ROC-analysis. Series in Cognition and Perception. Academic Press, London (1975)
304. Mueller, P., Shipley, G.: Dragon Claws its Way to the Top. Network Computing 20, 45–67 (2001)
305. Athanasiades, N., Abler, R., Levine, J., Owen, H., Riley, G.: Intrusion Detection Testing and Benchmarking Methodologies. In: First IEEE International Workshop on Information Assurance (2003)
306. Maheshkumar, S., Gursel, S.: Why Machine Learning Algorithms Fail in Misuse Detection on KDD Intrusion Detection Data Set. Intelligent Data Analysis 8(4), 403–415 (2004)
307. Brugger, S.T., Chow, J.: An Assessment of the DARPA IDS Evaluation Dataset Using Snort. Technical Report. Department of Computer Science - UC Davis (2007)
308. Bermúdez-Edo, M., Salazar-Hernández, R., Díaz-Verdejo, J.E., García-Teodoro, P.: Proposals on assessment environments for anomaly-based network intrusion detection systems. In: López, J. (ed.) CRITIS 2006. LNCS, vol. 4347, pp. 210–221. Springer, Heidelberg (2006)
309. Haines, J.W., Rossey, L.M., Lippmann, R.P., Cunningham, R.: Extending the DARPA Off-Line Intrusion Detection Evaluations. In: DARPA Information Survivability Conference and Exposition II, vol. 1 (2001)
310. Alessandri, D.: Using rule-based activity descriptions to evaluate intrusion-detection systems. In: Debar, H., Mé, L., Wu, S.F. (eds.) RAID 2000. LNCS, vol. 1907, p. 183. Springer, Heidelberg (2000)
311. Mueller, P., Shipley, G.: To Catch a Thief. Network Computing 20 (2001)
312. Newman, D., Snyder, J., Thayer, R.: Crying Wolf: False Alarms Hide Attacks. Network World (2002)
313. Network Intrusion Prevention System Tests, http://nsslabs.com/ips
314. Maxion, R.A., Tan, K.M.C.: Benchmarking Anomaly-based Detection Systems. In: International Conference on Dependable Systems and Networks (DSN 2000) (2000)
315. Mell, P., Hu, V., Lippmann, R.: An Overview of Issues in Testing Intrusion Detection Systems. NIST Interagency Reports. National Institute of Standards and Technology - Information Technology Laboratory (2003)
316. Vigna, G., Robertson, W., Balzarotti, D.: Testing Network-Based Intrusion Detection Signatures Using Mutant Exploits. In: 11th ACM Conference on Computer and Communications Security. ACM Press, Washington (2004)
317. Marti, R.: THOR: A Tool to Test Intrusion Detection Systems by Variations of Attacks. Diploma Thesis. ETH Zurich (2002)

318. Herrero, Á., Corchado, E., Gastaldo, P., Zunino, R.: A comparison of neural projection techniques applied to intrusion detection systems. In: Sandoval, F., Prieto, A.G., Cabestany, J., Graña, M. (eds.) IWANN 2007. LNCS, vol. 4507, pp. 1138–1146. Springer, Heidelberg (2007)
319. SOM Toolbox for Matlab, http://www.cis.hut.fi/projects/somtoolbox/
320. Goodall, J.R., Lutters, W.G., Rheingans, P., Komlodi, A.: Preserving the Big Picture: Visual Network Traffic Analysis with TNV. In: IEEE Workshop on Visualization for Computer Security (VizSEC 2005). IEEE Computer Society, Los Alamitos (2005)
321. Mukkamala, S., Janoski, G., Sung, A.: Intrusion Detection Using Neural Networks and Support Vector Machines. In: 2002 International Joint Conference on Neural Networks, IJCNN 2002 (February 2002)
322. Qiao, Y., Xin, X.W., Bin, Y., Ge, S.: Anomaly Intrusion Detection Method Based on HMM. Electronics Letters 38(13), 663–664 (2002)
323. Liao, Y.H., Vemuri, V.R.: Use of K-Nearest Neighbor Classifier for Intrusion Detection. Computers & Security 21(5), 439–448 (2002)
324. Yi, M.K., Hwang, C.S.: Intrusion-tolerant intrusion detection system. In: Chen, H., Moore, R., Zeng, D.D., Leavitt, J. (eds.) ISI 2004. LNCS, vol. 3073, pp. 476–483. Springer, Heidelberg (2004)
325. Shneiderman, B.: The Eyes Have It: a Task by Data Type Taxonomy for Information Visualizations. In: IEEE Symposium on Visual Languages (1996)