E-mail: 9422512@mail.dyu.edu.tw

DARPA
dataset   k-means

:

[1]   (:)
[2]

[3]
[4]   (:)
[5] Agrawal, R., Gehrke, J. Gunopulos, D. and Rahavan, P., "Automatic subspace clustering of high dimensional data for data mining applications," Proceedings of International Conference on Management of Data, Seattle, Washington, pp. 94-105, 1998.
[6] Ankerst, M., Breunig, M., Kriegel, H.P. and Sander J., "OPTICS:Ordering points to identify the clustering structure," Proceedings of ACM-SIGMOD International Conference Management of Data, Philadelphia, PA, pp. 49-60, 1999.
[7] Arne, V., " ACK Tunneling trojans", May. 2000. URL: http://ntsecurity.nu/papers/acktunneling/ [8] Borders, K. and Prakash, A., " Web tap:detecting covert web traffic," Proceedings of the 11th ACM Conference on Computer and Communications Security, pp. 110-120, 2004.
[9] Cabuk, S., Brodley, C.E., Shields, C., " IP covert timing channels:design and detection," Proceedings of the 11th ACM Conference on Computer and Communications Security, pp. 178-187, 2004.
[10] CERT/CC, " CERT/CC Statistics 1988-2004," Oct. 2004. URL: https://www.cert.org/stats/cert_stats.html [11] Craig. H.R., "Covert channels in the TCP/IP suite," Nov. 1996. URL: http://www.firstmonday.dk/issues/issue2_5/rowland/ [12] DARPA Intrusion Detection

Evaluation, " 1998 DARPA intrusion detection evaluation data set overview," 1998. URL: http://www.ll.mit.edu/IST/ideval/data/1998/1998_data_index.html [13] Dash, M., Liu, M. and Xu, X., "1+1>2':Merging distance and density based cluster," Proceedings of 7th International Conference on Database Systems for Advanced Applications, Hong Kong, pp. 18-20, Apr. 2001.

[14] Department of Defence, "Department of defence trusted computer system evaluation criteria," DoD standard, DOD 5200.28-STD, Dec. 1983.

[15] Forte, D., " Covert channels:covering ' malicious' traffic," Network Security, Vol. 2003, Iss. 4, 2003.

[16] Guralnik, V., Karypis, G., " A scalable algorithm for clustering sequential data," Proceedings of IEEE International Conference on Data Mining, pp. 179-186, Nov. 2001.

[17] Helmer, G., Wong, J. and Madaka, S., "Anomalous intrusion detection system for hostile Java applets," Journal of System and Software, Vol. 55, Iss. 3, pp. 273-286, 2001.

[18] Huang, Z., "Extensions to the k-means algorithm for clustering large data sets with categorical values," Data Mining and Knowledge Discovery, Vol. 2, pp. 283-304, 1998.

[19] Jain, A.K., Murty, M.N. and Flynn, P.J., " Data clustering:a review," ACM Computing Surveys, Vol. 31, Iss. 3, pp. 264-323, 1999.

[20] Jin, H., Leung, K.S., Wong, M.L. and Xu, Z.B., " Scalable model-based cluster analysis using clustering features," Pattern Recognition, Vol. 38, Iss. 5, pp. 637-649, 2005.

[21] Juan M, E.T., Pedro, G.T., Jesus E, D.V., "Anomaly detection methods in wired networks: a survey and taxonomy," Computer Communications, Vol. 27, Iss. 16, pp. 1569-1584, 2004.

[22] Kamran, A., "Covert channel analysis and data hiding in TCP/IP," Department of Electrical and Computer Engineering University of Toronto, 2002.

[23] KDD Cup 1999 Data, 1999. URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html/ [24] Kemmerer, R.A., "A practical approach to identifying storage and timing channels: twenty years later," Proceedings of 18th Computer Security Applications Conference, pp. 109 - 118, Dec. 2002.

[25] Kieltyka, P., "ICMP Shell," Feb. 2002. URL: http://icmpshell.sourceforge.net/ [26] Lampson, B.W., "A note on the confinement problem," Communications of the ACM, Vol. 16, No. 10, pp. 613-615, Oct. 1973.

[27] Lars, B., " HTTP Tunnel," Oct. 2004. URL: http://www.nocrew.org/software/ httptunnel.html/ [28] MacQueen, J., "Some methods for classification and analysis of multivariate observations," Proceedings of Fifth Berkeley Symposium on Mathematical Statistics and Probability, pp. 288-297, 1967.

[29] Mahoney, M.V., " Network traffic anomaly detection based on packet bytes," Proceedings of the 2003 ACM Symposium on Applied Computing, pp. 346-350, 2003.

[30] Mannila, H., Toivonen, H. and Verkamo, A.I., " Discovery of frequent episodes in event sequences," Data Mining and Knowledge Discovery, Vol. 1, Iss. 3, 1997.

[31] Marin, J.A., Ragsdale, D.J. and Surdu, J.R., "A hybrid approach to profile creation and intrusion detection," Proceedings of the DARPA Information Survivability Conference and Exposition, pp. 69-76, 2001.

[32] Mark, O., "A discussion of covert channels and steganography," Mar. 2002. URL: http://www.sans.org/rr/papers/12/678.pdf [33] Meade, F.G., "A guide to understanding covert channel analysis of trusted systems," National Computer Security Center, Nov. 1993. URL: http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-030.html [34] Mirkovic, J., Prier, G. and Reiher, P., "Source-end DDos defence," Second IEEE International Symposium on Network Computing and Applications, pp. 171-178, Apr. 2003.

[35] Moskowitz, I.S., Newman, R.E., Crepeau, D.P. and Miller, A.R., " Covert channel and anonymizing networks," Proceedings of the 2003 ACM workshop on Privacy in the electronic society, pp. 79-88, 2003.

[36] Ofir, A., "ICMP usage in scanning:The complete know-how," Jun. 2001. URL: http://www.sys-security.com/archive/papers/ICMP_Scanning_v3.0.pdf [37] Oh, S.H., Won, S.L., " An anomaly intrusion detection method by clustering normal user behavior," Computer & Secuirty, Vol. 22, No. 7, pp. 596-612, 2003.

[38] Portnoy, L., Eskin, E. and Stolfo, S.J., "Intrusion detection with unlabeled data using clustering," Proceedings of the ACM CCS Workshop on Data Mining for Security Applications, 2001.

[39] Qin, M. and Hwang, K., " Frequent episode rules for Internet anomaly detection," Proceedings of The Third IEEE International Symposium on Network Computing and Applications, pp. 161-168, 2004.

[40] Qu, H., Su, P. and Feng, D., " A typical noisy covert channel in the IP protocol," 38th Annual 2004 International Carnahan Conference on Security Technology, pp. 189-192, 2004.

[41] Robert, F.E., Kenneth, L.W. and Deborah, A.F., "Intrusion and misuse detection in large-scale system," IEEE Transactions on Systems, Vol. 27, No. 3, pp. 38-49, Feb. 2002.

[42] Smith, J.C., "Covert shells," Nov. 2000. URL: http://www.giac.org/practical/GSEC/J_Christian_Smith_GSEC.pdf [43] Smith, R., Bivens, A. and Embrechts, M., "Clustering approaches for anomaly based intrusion detection," Walter Lincoln Hawkins Graduate Research Conference, 2002.

[44] Symantec Taiwan, "Symantec network security threat research," Sep. 2004. URL:
http://www.symantec.com.tw/region/tw/avcenter/10187537_SIST_es_CH.pdf [45] Turkeli, Y., Ercil, A., Sezerman, O.U., " Effect feature extraction and feature selection on expression data from epithelial ovarian cancer," Proceedings of the 25th Annual International Conference of the IEEE, Vol. 4, pp. 3559-3562, 2003.

[46] Vapnik V.N., Statistical Learning Theory. New York:Wiley, 1998.

[47] Verwoerd, T. and Hunt, R., "Intrusion detection techniques and approaches," Computer Communications, Vol. 25, Iss. 15, pp. 1356-1365, 2002.

[48] Ward, J.H., " Hierarchical grouping to optimize an objective function," Journal of the American Statistical Association, Vol. 58, No. 301, pp. 236-244, 1963.