behavioral activities comprehensively, and detecting anomaly more effectively.

Acknowledgment

We would like thank Jiang Wang for his insightful comments and helpful suggestions on this paper. This work was supported by National Natural Science Foundation of China (Grant No. 71571186 and 71471176) and China Postdoctoral Science Foundation (No. 2016M593018)

References

[1] Hong, J., Kim, J., & Cho, J. (2009). *The Trend of the Security Research for the Insider Cyber Threat*. *Security Technology*. Springer Berlin Heidelberg.

[2] Nellikar, S. (2010). Insider threat simulation and performance analysis of insider detection algorithms with role based models. *University of Illinois at Urbana-Champaign*.

[3] Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2017). Automated insider threat detection system using user and role-based profile assessment. *IEEE Systems Journal, 11(2)*, 503-512.

[4] Myers, J., Grimaila, M. R., & Mills, R. F. (2009). Towards insider threat detection using web server logs, 1-4.

[5] Eldardiry, H., Bart, E., Liu, J., Hanley, J., Price, B., & Brdiczka, O. (2013). Multi-domain information fusion for insider threat detection. *IEEE Security and Privacy Workshops*, *42*, 45-51. IEEE Computer Society.

[6] Anderson, G. F., Selby, D. A., & Ramsey, M. (2007). Insider attack and real-time data mining of user behavior. *Ibm Journal of Research & Development, 51(3.4)*, 465-475.

[7] Nguyen, N., Reiher, P., & Kuenning, G. H. (2003). Detecting insider threats by monitoring system call activity. *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, pp. 45-52).

[8] Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015). Caught in the act of an insider attack: detection and assessment of insider threat. *Proceedings of IEEE International Symposium on Technologies for Homeland Security.*

[9] Park, J. S., & Giordano, J. (2006). Role-based profile analysis for scalable and accurate insider-anomaly detection. *Proceedings of IPCCC 2006 IEEE International Performance, Computing, and Communications Conference, Vol. 2,* (pp. 7-470).

[10] Senator, T. E., Goldberg, H. G., Memory, A., Young, W. T., Rees, B., & Pierce, R., *et al.* (2013). Detecting insider threats in a real corporate database of computer usage activity. *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp.1393-1401). ACM.

[11] Magklaras, G. B., & Furnell, S. M. (2001). *Events: Insider Threat Prediction Tool: Evaluating the Probability of IT Misuse*. Elsevier Advanced Technology Publications.

[12] Aggarwal, C. C. (2013). Outlier analysis. 75-99.

[13] Eberle, W., & Holder, L. (2009). Insider threat detection using graph-based approaches. *Proceedings of Cybersecurity* Applications *& Technology Conference for Homeland Security*, *Vol. 6*, (pp. 237-241). IEEE Computer Society.

[14] Parveen, P., Evans, J., Thuraisingham, B., Hamlen, K. W., & Khan, L. (2012). Insider threat detection using stream mining and graph mining. *Proceedings of IEEE Third International Conference on Privacy, Security, Risk and Trust* (pp. 1102-1110).

[15] Liu, F. T., Ting, K, M., & Zhou, Z. H. (2012). Isolation-based anomaly detection. *ACM Transactions on Knowledge Discovery from Data, 6(1),* 1-39.

[16] Breunig, M. M. (2000). LOF: Identifying density-based local outliers. *ACM SIGMOD Record, 29(2)*, 93-104.