area, it is found that the performance obtained on the NSL-KDD dataset is better compared to the KDD99 and UNSW-NB15 datasets.

In Future Work we will study other feature selection methods combined with more machine learning algorithms applied to real-time data from IoT devices.

REFERENCES

[1] Atzori, L., Iera, A., Morabito, G. (2010). The Internet of Things: A survey. Computer Network, 54(15): 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[2] Weiser, M. (1991). The computer for the 21st century. Scientific American, 265(3): 94-105.

[3] Sedjelmaci, H., Senouci, S.M., Al-Bahri, M. (2016). Lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology. IEEE ICC - Mobile and Wireless Networking Symposium. https://doi.org/10.1109/ICC.2016.7510811

[4] Raza, S., Wallgren, L., Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks, 11(8): 2661-2674. https://doi.org/10.1016/j.adhoc.2013.04.014

[5] Anand, A., Patel, B. (2012). An overview on intrusion detection system and types of attacks it can detect considering different protocols. International Journal of Advanced Research in Computer Science and Software Engineering, 2(8): 94-98.

[6] Rajasegarar, S., Leckie, C., Palaniswami M. (2008). Anomaly detection in wireless sensor networks. IEEE Wireless Communications, 15(4): 34-40. https://doi.org/10.1109/MWC.2008.4599219

[7] Li, W.C., Yi, P., Wu, Y., Pan, L., Li, J.H. (2014). A new intrusion detection system based on KNN classification algorithm in wireless sensor network. Journal of Electrical and Computer Engineering, 2014: 8 pages. http://dx.doi.org/10.1155/2014/240217

[8] Thanigaivelan, N.K., Nigussie, E., Kanth, R.K., Virtanen, S., Isoaho, J. (2016). Distributed internal anomaly detection system for Internet-of-Things. 13th IEEE Annual Consumer Communications & Networking Conference (CCNC). https://doi.org/10.1109/CCNC.2016.7444797

[9] Summerville, D.H., Zach, K.M., Chen, Y. (2015). Ultra-lightweight deep packet anomaly detection for Internet of Things devices. 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC). https://doi.org/10.1109/PCCC.2015.7410342

[10] Huang, S.H. (2003). Dimensionality reduction in automatic knowledge acquisition: A simple greedy search approach. IEEE Transactions on Knowledge and Data Engineering, 15(6): 1364-1373. https://doi.org/10.1109/TKDE.2003.1245278

[11] Zhao, K., Ge, L. (2013). A survey on the Internet of Things security. in Int'l Conf. on Computational Intelligence and Security (CIS), pp. 663-667. https://doi.org/10.1109/CIS.2013.145

[12] Leo, M., Battisti, F., Carli, M., Neri, A. (2014). A federated architecture approach for internet of things security. in Euro Med Telco Conference (EMTC), pp. 1-5. https://doi.org/10.1109/ EMTC. 2014. 6996632

[13] Oh, D., Kim, D., Ro, W.W. (2014). A malicious pattern detection engine for embedded security systems in the Internet of Things. Sensors, 14(12): 24188-24211. https://dx.doi.org/10.3390/s141224188

[14] Sherasiya, T., Upadhyay, H., Patel, H.B. (2016). A survey: Intrusion detection system for Internet of Things. International Journal of Computer Science and Engineering (IJCSE), 5(2): 91-98.

[15] Zarpelão, B.B., Miani, R.S., de Alvarenga, S.C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84(C): 25-37. http://dx.doi.org/10.1016/j.jnca.2017.02.009

[16] Alrajeh, N.A., Khan, S., Shams, B. (2013). Intrusion detection systems in wireless sensor networks: A review. International Journal of Distributed Sensor Networks, 2013: 7 pages. https://doi.org/10.1155/2013/167575

[17] Liao, H.J., Richard Lin, C.H., Lin, Y.C., Tung, K.Y. (2013). Review intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, 36(1): 16-24. https://doi.org/10.1016/j.jnca.2012.09.004

[18] Maharaj, N., Khanna, P. (2014). A comparative analysis of different classification techniques for intrusion detection system. International Journal of Computer Applications, 95(17): 22-26. http://dx.doi.org/10.5120/16687-6806

[19] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.L., Iorkyase, E., Tachtatzis, C., Atkinson, P. (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. 2016 International Symposium on Networks, Computers and Communications (ISNCC). https://doi.org/10.1109/ISNCC.2016.7746067

[20] Roman, R., Zhou, J.Y., Lopez, J. (2006). Applying intrusion detection systems to wireless sensor networks. In IEEE Consumer Communications & Networking Conference (CCNC 2006), pp. 640-644. https://doi.org/10.1109/CCNC.2006.1593102

[21] KDD cup 99 Intrusion detection dataset. http://kdd.ics.uci.edu/databases /kddcup99/ kddcup.data_10_percent.gz, accessed on March 1, 2019.

[22] NSL-KDDDataset, https://www.unb.ca/cic/datasets/nsl.html, accessed on March 1, 2019.

[23] Nour, M., Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). Military Communications and Information Systems Conference (MilCIS). https://doi.org/10.1109/MilCIS.2015.7348942

[24] Hasan, M.A.M., Nasser, M., Ahmad, S., Molla, K.I. (2016). Feature selection for intrusion detection using random forest. Journal of Information Security, 7(3): 129-140. https://doi.org/10.4236/jis.2016.73009

[25] Paliwal, S., Gupta, R. (2012). Denial of-service, probing & remote to user (R2L) attack detection using genetic algorithm. International Journal of Computer Applications, 60(19): 57-62. https://doi.org/10.5120/9813-4306