IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 9, May 2023

Deep Transfer Learning for IoT Attack Detection

Prof. Abdul Khadar A, Sanjay Yadav S, Mohammed Huzaifa B, Vayalpad Mohammad Thouhid

Department of Information Science and Engineering,
SJC Institute of Technology, Chikkaballapur, Karnataka, India

Abstract: *The digital revolution has substantially changed our lives in which Internet-of-Things (IoT) plays a prominent role. The rapid development of IoT to most corners of life, however, leads to various emerging cybersecurity threats. Therefore, detecting and preventing potential attacks in IoT networks have recently attracted paramount interest from both academia and industry. Among various attack detection approaches, machine learning-based methods, especially deep learning, have demonstrated great potential thanks to their early detecting capability. However, these machine learning techniques only work well when a huge volume of data from IoT devices with label information can be collected. Nevertheless, the labeling process is usually time consuming and expensive, thus, it may not be able to adapt with quick evolving IoT attacks in reality. In this paper, we propose a novel deep transfer learning (DTL) method that allows to learn from data collected from multiple IoT devices in which not all of them are labeled. Specifically, we develop a DTL model based on two AutoEncoders (AEs). The first AE (AE1) is trained on the source datasets (source domains) in the supervised mode using the label information and the second AE (AE2) is trained on the target datasets (target domains) in an unsupervised manner without label information. The transfer learning process attempts to force the latent representation (the bottleneck layer) of AE2 similarly to the latent representation of AE1. After that, the latent representation of AE2 is used to detect attacks in the incoming samples in the target domain. We carry out intensive experiments on nine recent IoT datasets to evaluate the performance of the proposed model. The experimental results demonstrate that the proposed DTL model significantly improves the accuracy in detecting IoT attacks compared to the baseline deep learning technique and two recent DTL approaches.*

Keywords: Deep transfer learning, IoT, cyberattack detection, AutoEncoder

REFERENCES

[1] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, D. I. Kim, and Z. Han, ‘‘Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey,’’ IEEE Commun. Surveys Tuts., vol. 18, no. 4, pp. 2546–2590, Jun. 2016.

[2] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, J. Davis Guarnizo, and Y. Elovici, ‘‘Detection of unauthorized IoT devices using machine learning techniques,’’ 2017, arXiv:1709.04647. [Online]. Available: http://arxiv.org/abs/1709.04647

[3] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, ‘‘N-BaIoT—Network-based detection of iot botnet attacks using deep autoencoders,’’ IEEE Pervasive Comput., vol. 17, no. 3, pp. 12–22, Jul./Sep. 2018.

[4] I. Ahmed, A. P. Saleel, B. Beheshti, Z. A. Khan, and I. Ahmad, ‘‘Security in the Internet of Things (IoT),’’ in Proc. 4th HCT Inf. Technol. Trends (ITT), Oct. 2017, pp. 84–90.

[5] N. Vlajic and D. Zhou, ‘‘IoT as a land of opportunity for DDoS hackers,’’
Computer, vol. 51, no. 7, pp. 26–34, Jul. 2018.

[6] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ‘‘DDoS in the IoT: Mirai and other botnets,’’ Computer, vol. 50, no. 7, pp. 80–84, 2017.

[7] R. Gow, F. A. Rabhi, and S. Venugopal, ‘‘Anomaly detection in complex real world application systems,’’ IEEE Trans. Netw. Service Manage., vol. 15, no. 1, pp. 83–96, Mar. 2018.

[8] S. Khattak, N. R. Ramay, K. R. Khan, A. A. Syed, and S. A. Khayam, ‘‘A taxonomy of botnet behavior, detection, and defense,’’ IEEE Commun. Surveys Tuts., vol. 16, no. 2, pp. 898–924, 2nd Quart., 2014.

DOI: 10.48175/IJARSCT-10384

[9] J. Dromard, G. Roudiere, and P. Owezarski, ‘‘Online and scalable unsu- pervised network anomaly detection method,’’ IEEE Trans. Netw. Service Manage., vol. 14, no. 1, pp. 34–47, Mar. 2017.

[10] H. Bahsi, S. Nomm, and F. B. La Torre, ‘‘Dimensionality reduction for machine learning based IoT botnet detection,’’ in Proc. 15th Int. Conf. Control, Autom., Robot. Vis. (ICARCV), Nov. 2018, pp. 1857–1862.

[11] C. Zhang and R. C. Green II, ‘‘Communication security in Internet of Thing: Preventive measure and avoid DDoS attack over IoT network,’’ in Proc. 18th Symp. Commun. Netw., Alexandria, VA, USA, Apr. 2015, pp. 8–15.

[12] C. Dietz, R. L. Castro, J. Steinberger, C. Wilczak, M. Antzek, A. Sperotto, and A. Pras, ‘‘IoT-botnet detection and isolation by access routers,’’ in Proc. 9th Int. Conf. Netw. Future (NOF), Nov. 2018, pp. 88–95.

[13] M. Nobakht, V. Sivaraman, and R. Boreli, ‘‘A host-based intrusion detec- tion and mitigation framework for smart home IoT using OpenFlow,’’ in Proc. 11th Int. Conf. Availability, Rel. Secur. (ARES), Salzburg, Austria, Aug. 2016, pp. 147–156.

[14] J. Ceron, K. Steding-Jessen, C. Hoepers, L. Granville, and C. Margi, ‘‘Improving IoT botnet investigation using an adaptive network layer,’’ Sensors, vol. 19, no. 3, p. 727, Feb. 2019.

[15] L. Vu, V. L. Cao, Q. U. Nguyen, D. N. Nguyen, D. T. Hoang, and E. Dutkiewicz, ‘‘Learning latent distribution for distinguishing network traffic in intrusion detection system,’’ in Proc. IEEE Int. Conf. Commun. (ICC), May 2019, pp. 1–6.

DOI: 10.48175/IJARSCT-10384