An attacker can send a malicious signal at any instance. Suppose that the attacker decides to send k=20 malicious signals at different instances. Assume that the IDS is set to perform m=15 checks during the interval. Our goal is to calculate the probability that IDS detects x=4 malicious signals. We perform 10,000 experiments where each experiment consists of 1000 simulated runs.

The histogram of the resulting probabilities is presented in Fig. 5. For the reference, we calculate the theoretical probability p(4) using Equation 1. As shown in Fig. 5, the histogram is centered symmetrically around the theoretical probability.

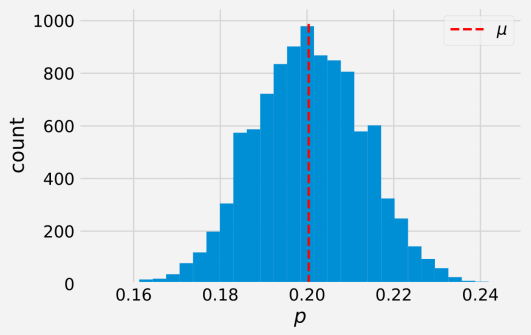

Fig. 5 A numerical simulation with a total of 10^7 runs. The parameters of the simulation are n=100, m=15, k=20, and x=4. The value μ = 0.2 is the theoretical probability obtained from Equation 1

In addition, we calculated the expected number of detected attacks in the same scenario as above using the direct approach and Equation 3. Using the direct approach, we obtain:

$$E[X] = \sum_{x=0}^{k} x.\frac{\binom{k}{x}\binom{n-k}{m-x}}{\binom{n}{m}} = \sum_{x}^{20} x.\frac{\binom{20}{x}\binom{80}{15-x}}{\binom{100}{15}} = 3 \quad (11)$$

A more efficient approach to calculate the expected number of attacks is given by us in Equation 1:

$$E[X] = \frac{k.m}{n} = \frac{20.15}{100} = 3 \quad (12)$$

It follows from the above comparisons that the direct approach and the one provided by us yield the same results. We observe that the experimental results support the theoretical findings from the previous section.

IV. Conclusion

The widespread adoption of network-based technologies has increased the potential for damage caused by a malicious attack on a network. Both the frequency and the severity of network attacks have risen over the past decade. As a result, it has become essential to develop effective intrusion detection systems. In this paper, we provide a probabilistic framework to analyze the detection rate of malicious attacks. We carried out careful theoretical and experimental analyses of the research problem. We developed the formula for calculating the intrusion detection rate for a fixed set of parameters. Given an interval of time that is divided into discrete instances at which the attacks can occur we can calculate the probability of IDS detecting x attacks via Equation 1. In addition, the expected number of detected attacks is also calculated via Equation 3. The theoretical results were tested and validated through numerical experiments. The outcome of the experiments confirmed the original theoretical results. We note that even with a simple strategy such as uniform sampling the probability of detecting at least one malicious attack is high given a small number of checks: the intrusion detection rate is nearly 0.9 when checking only 15% of time instances. The detection rate reaches 1 when checking 30% of time instances.

We believe that the probabilistic framework developed in this paper would be of use to IDS experts. For a network-based IDS that is checking the incoming packets in real time the computational cost of analyzing the entire traffic flow can be prohibitively expensive. So, checking only a probabilistically sampled fraction of the network traffic would allow the IDS to handle its task. However, checking only a fraction of the traffic introduces a probability of missing an attack. We hope to provide a better understanding of the likelihood of detecting an attack by an IDS and improve the design of the system. In practical terms, the results of this paper help IDS designers achieve appropriate detection rates while maintaining a low false alarm rate.

The groundwork that has been laid out in this paper can be used for future research into understanding of the probabilities related to intrusion detection. We believe that there are multiple avenues for future research that stem from the present work. The key assumption of our study is the uniform distribution of attacks and checks. However, it does not cover all the intrusion scenarios. It would be necessary to address other attack and detection patterns in future research.

References

[1] K. N. Sevis and E. Seker, "Cyber warfare: terms, issues, laws and controversies," 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security), Jun. 2016, doi:10.1109/cybersecpods.2016.7502348.

[2] G. De Masi, "The impact of topology on Internet of Things: A multidisciplinary review," 2018 Advances in Science and Engineering Technology International Conferences (ASET), Feb. 2018, doi:10.1109/icaset.2018.8376837.

[3] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702–2733, 2019, doi: 10.1109/comst.2019.2910750.

[4] Ventures C. Cybersecurity jobs report. Herjavec Group. 2017 May;1.

[5] A. Borkar, A. Donode, and A. Kumari, "A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)," 2017 International Conference on Inventive Computing and Informatics (ICICI), Nov. 2017, doi:10.1109/icici.2017.8365277.

[6] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems," IEEE Access, vol. 7, pp. 46595–46620, 2019, doi: 10.1109/access.2019.2909807.

[7] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16–24, Jan. 2013, doi:10.1016/j.jnca.2012.09.004.

[8] Y. Afek, A. Bremler-Barr, and S. L. Feibish, "Zero-Day Signature Extraction for High-Volume Attacks," IEEE/ACM Transactions on Networking, vol. 27, no. 2, pp. 691–706, Apr. 2019, doi:10.1109/tnet.2019.2899124.

[9] R. Samrin and D. Vasumathi, “Review on anomaly based network intrusion detection system,” 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), Dec. 2017, doi:10.1109/iceeccot.2017.8284655.

[10] S. Oshima, T. Nakashima, and Y. Nishikido, “Extraction for Characteristics of Anomaly Accessed IP Packets Based on Statistical Analysis,” Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007), Nov. 2007, doi: 10.1109/iihmsp.2007.4457652.

[11] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A Deep Learning Approach to Network Intrusion Detection,” IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, Feb. 2018, doi: 10.1109/tetci.2017.2772792.

[12] M. H. Ahmadzadegan, A. A. Khorshidvand, and M. G. Valian, “Low-rate false alarm intrustion detection system with genetic algorithm approach,” 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), Nov. 2015, doi:10.1109/kbei.2015.7436188.

[13] S. Naseer et al., “Enhanced Network Anomaly Detection Based on Deep Neural Networks,” IEEE Access, vol. 6, pp. 48231–48246, 2018, doi: 10.1109/access.2018.2863036.

[14] F. Kamalov and F. Thabtah, “A Feature Selection Method Based on Ranked Vector Scores of Features for Classification,” Annals of Data Science, vol. 4, no. 4, pp. 483–502, Jul. 2017, doi: 10.1007/s40745-017-0116-1.. 6, pp. 48231–48246, 2018, doi:10.1109/access.2018.2863036.

[15] F. Kamalov, “Generalized feature similarity measure,” Annals of Mathematics and Artificial Intelligence, vol. 88, no. 9, pp. 987–1002, May 2020, doi: 10.1007/s10472-020-09700-8.

[16] F. Thabtah and F. Kamalov, “Phishing Detection: A Case Analysis on Classifiers with Rules Using Machine Learning,” Journal of Information & Knowledge Management, vol. 16, no. 04, p. 1750034, Nov. 2017, doi: 10.1142/s0219649217500344.

[17] F. Kamalov and H. H. Leung, “Outlier Detection in High Dimensional Data,” Journal of Information & Knowledge Management, vol. 19, no. 01, p. 2040013, Mar. 2020, doi: 10.1142/s0219649220400134.

[18] A. Garg and P. Maheshwari, “A hybrid intrusion detection system: A review,” 2016 10th International Conference on Intelligent Systems and Control (ISCO), Jan. 2016, doi: 10.1109/isco.2016.7726909.

[19] C.-M. Ou, “Host-based Intrusion Detection Systems Inspired by Machine Learning of Agent-Based Artificial Immune Systems,” 2019 IEEE International Symposium on INnovations in Intelligent SysTems and Applications (INISTA), Jul. 2019, doi:10.1109/inista.2019.8778269.

[20] M. Ahmed, R. Pal, Md. M. Hossain, Md. A. N. Bikas, and Md. K. Hasan, “NIDS: A Network Based Approach to Intrusion Detection and Prevention,” 2009 International Association of Computer Science and Information Technology - Spring Conference, 2009, doi:10.1109/iacsit-sc.2009.96.

[21] Jianning Mai, A. Sridharan, Chen-Nee Chuah, Hui Zang, and Tao Ye, “Impact of Packet Sampling on Portscan Detection,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 12, pp. 2285–2298, Dec. 2006, doi: 10.1109/jsac.2006.884027.

[22] Rong Cong, Jie Yang, and Gang Cheng, “Research of sampling method applied to traffic classification,” 2010 IEEE 12th International Conference on Communication Technology, Nov. 2010, doi:10.1109/icct.2010.5689208.

[23] J. M. C. Silva, P. Carvalho, and S. R. Lima, “Analysing traffic flows through sampling: A comparative study,” 2015 IEEE Symposium on Computers and Communication (ISCC), Jul. 2015, doi:10.1109/iscc.2015.7405538.

[24] I. Paredes-Oliva, P. Barlet-Ros, and J. Sole-Pareta, “Scan detection under sampling: a new perspective,” Computer, vol. 46, no. 4, pp. 38–44, Apr. 2013, doi: 10.1109/mc.2013.70.

[25] K. Bartos, M. Rehak, and V. Krmicek, “Optimizing flow sampling for network anomaly detection,” 2011 7th International Wireless Communications and Mobile Computing Conference, Jul. 2011, doi:10.1109/iwcmc.2011.5982728.

[26] G. Androulidakis, V. Chatzigiannakis, and S. Papavassiliou, “Network anomaly detection and classification via opportunistic sampling,” IEEE Network, vol. 23, no. 1, pp. 6–12, Jan. 2009, doi:10.1109/mnet.2009.4804318.

[27] D. Brauckhoff, B. Tellenbach, A. Wagner, M. May, and A. Lakhina, “Impact of packet sampling on anomaly detection metrics,” Proceedings of the 6th ACM SIGCOMM conference on Internet measurement, Oct. 2006, doi: 10.1145/1177080.1177101.