Future Research Directions on Energy-Aware Security Mechanisms

Laura Soares
Institute of Informatics
Federal University of Rio Grande do Sul
Porto Alegre, Brazil
lrsoares@inf.ufrgs.br

Jeferson Nobre
Institute of Informatics
Federal University of Rio Grande do Sul
Porto Alegre, Brazil
jcnobre@inf.ufrgs.br

***Abstract*—With the onset of the climate emergency, all areas of human activity are expected to continuously assess their Greenhouse Gas emissions and encourage the use of clean energy as much as possible. The current discussion on green networking in the Network Management research field still needs to be expanded to the adjoined areas, such as Network Security. This document summarizes the security considerations of the existing works on green networking and outlines possible research directions for energy-aware security mechanisms.**

***Index Terms*—security, energy-aware, green networking**

I. Introduction

The United Nations 2030 Agenda for Sustainable Development was established during the Paris Agreement in 2016. Among other goals, it intended to limit the global temperature rise to below 2°C – threshold which would lead to accelerating and irreversible changes to the climate on Earth [1]. Almost ten years have passed after the establishment of the 2030 Agenda, and is a sad agreement among specialists that the global warming will likely exceed 1.5°C still in the 21st century [2]. Human activity has unequivocally contributed to raising the global temperature through the emission of Greenhouse Gasses (GHG) such as carbon dioxide (CO2), of which the burning of fossil fuels (coal, oil, and natural gas) is the principal producer. In 2023, the concentration of CO2 in the atmosphere has increased by about 50% over pre-industrial levels [3]. Therefore, it is crucial that all areas of human activity encourage the use of clean, CO2-free energy sources in their production chain.

Computer networking and the Internet are no exception to the global necessity of reducing CO2 emissions. While the green networking effort is not new, the recent escalation of the climate emergency inevitably led to intensified discussion on the topic of how the network management community can increase energy-efficiency of networking protocols. Some of the recent works on the subject of green networking focus on improving the efficiency of current network mechanisms as means to save energy, such as optimizing the volume of transmitted data and improving congestion control mechanisms to avoid re-transmission [4]. Another promising approach is to alternate high link utilization with power-saving modes in network equipment [5]. Regardless of the approach, the green networking effort must follow from robust measurement frameworks capable of providing comprehensive visibility into the energy consumption of the network.

Despite the advancements on green networking, much of the discussion still needs to be expanded to adjoined research fields, such as network security. Security protocols are some of the more expensive, and are likely to show up in measurement tools as top consumers of energy resources. However, neglecting them in modern applications is simply not possible. Policies and guidelines must take functionality into account, or risk overly penalizing security algorithms. With appropriate energy measurement mechanisms, network administrators can compare energy usage versus security performance of popular network security mechanisms in order to select the appropriate tool for each task. The first step towards efficient energy management should be to avoid the two extremes – saving energy at the cost of endangering the application, and allocating unrestricted resources to secure a much simpler asset. An example widely discussed in both literature and the media is the use of crypto assets, which should be avoided where other mechanisms suffice due to their huge energy consumption [6].

This document primarily focuses on the current security considerations on the existing discussion on green networking, in Section II, and then Section III outlines future research directions for energy-aware network security.

II. Existing Green Networking Research and Their Security Considerations

Concerns about the substantial amount of energy used by the Internet have been showing up in research over the last 20 years or so [7], [8]. The existing work on energy-aware networking range from 2008's Adaptive Link Rate (ALR) solutions [9] to more recent carbon-aware routing metrics [10]. Technology such as Software Defined Networks (SDNs) [11] and Programmable Data Planes [12] also advanced the green networking research.

Recently, green networking also became an emerging topic on leading Internet standards organizations such as the IETF (Internet Engineering Task Force). Two works in progress at the Network Management Research Group (NMRG) are [13], [14]. They provide a initial drafting of relevant measurement attributes and related metrics, such as power consumption under various loads, energy efficiency, and carbon footprint,

each associated with varying networking components. The IAB (Internet Architecture Board) also organized a program to discuss sustainability-related issues within the IETF. Their first workshop took place in December 2022 with the goal of calling attention to the topic, and noted the clear need for standardized metrics [6]. Another draft [15] has a detailed glossary of terms and several sustainability considerations for network, protocol, and application designers. Finally, the IEEE also launched a Special Interest Group about Sustainable Network Operations[1] aiming to encourage the development of solutions on the topic.

Some additional points are the need for specialized energy metrics for virtualized environments. Also worth pointing out is the possibility of decentralized network structures contributing to energy saving since they would spare the packet an unnecessarily long travel to a central server – the same concept is already applied to CDNs. Finally, the current green networking research and discussion needs to be expanded to include more security considerations. So far, most the security concerns are regarding extra attack surface brought by the energy measurement tools and controls. An attacker might use these mechanisms to put resources to sleep in critical moments, drain energy to cause damage [16] such as overheating and battery loss, and finally, to tamper with the energy measurement, which would cause misguided energy saving policies being put in place [13]. Though these are all important considerations, they are security risks for energy-saving mechanisms and not energy-saving techniques for security mechanisms.

III. Future Research on Energy-Aware Network Security

As the research on green networking progresses, it naturally expands to adjoined fields such as energy-aware security. Security mechanisms from all layers of the network protocol stack are widely considered as overhead since they often increase both computational and energy demands of a system. However, to dismiss security concerns on the modern-day Internet is unthinkable. The available alternative energy-wise is to use the appropriate mechanism for each task without either over-provisioning it or failing to allocate enough resources. In the following we present a non-exhaustive list of possible research challenges regarding energy-aware security mechanisms, outlined from the existing works on green networking:

i *How can the energy consumption of existing network security mechanisms be measured?* This research challenge borrows from the general research on green networking for the assessment of metrics and the frameworks capable of providing them.

ii *Which of these metrics are up for industry-wide standardization?* Security protocols often have greater costs if compared with other networking protocols. Energy consumption metrics should take functionality into account to avoid compromising security properties.

iii *Is it possible to perform a cost-benefit analysis comparing performance with energy usage, to assess if energy can be saved with little harm to safety and functionality?*

iv *How to best compare two or more security mechanisms to assess which one is best for a task, energy-wise?* This broad research challenge encompasses the previous items, depending on the definition of categories and metrics for comparison regarding both security and energy usage.

These research directions will be further explored in a PhD program at UFRGS. We believe the answers to these questions can help expanding the security considerations in the current green networking discussion, contributing to the broader goal of reducing the carbon footprint of the Internet.

[1] https://cnom.committees.comsoc.org/sustainable-network-operations-sno/

References

[1] D. I. Armstrong McKay, A. Staal, J. F. Abrams, R. Winkelmann, B. Sakschewski, S. Loriani, I. Fetzer, S. E. Cornell, J. Rockström, and T. M. Lenton, "Exceeding 1.5 c global warming could trigger multiple climate tipping points," *Science*, vol. 377, no. 6611, p. eabn7950, 2022.

[2] IPCC, "Summary for policymakers," in *Climate Change 2023: Synthesis Report. Contribution of Working Groups I, II and III to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change*, Core Writing Team, H. Lee and J. Romero, Ed. Geneva, Switzerland: IPCC, 2023, pp. 1–34, archived from the original on 8 April 2024 at https://tinyurl.com/dmy2dzxy. Retrieved 9 April 2024.

[3] FRIEDLINGSTEIN P. et al., "Global carbon budget 2023," *Earth System Science Data*, vol. 15, pp. 5301—5369, 2023, https://doi.org/10.5194/essd-15-5301-2023.

[4] A. Clemm and C. Westphal, "Challenges and opportunities in green networking," in *2022 IEEE 8th International Conference on Network Softwarization (NetSoft)*. IEEE, 2022, pp. 43–48.

[5] C. Westphal and A. Clemm, "Optimization framework for green networking," in *2023 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2023, pp. 581–585.

[6] J. Arkko, C. Perkins, and S. Krishnan, "Report from the iab workshop on environmental impact of internet applications and systems, 2022," 2024. [Online]. Available: https://datatracker.ietf.org/doc/rfc9547

[7] D. Otten, A. Brundiers, T. Schüller, and N. Aschenbruck, "Green segment routing for improved sustainability of backbone networks," in *2023 IEEE 48th Conference on Local Computer Networks (LCN)*. IEEE, 2023, pp. 1–9.

[8] A. P. Bianzino, C. Chaudet, D. Rossi, and J.-L. Rougier, "A survey of green networking research," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 1, pp. 3–20, 2010.

[9] C. Gunaratne, K. Christensen, B. Nordman, and S. Suen, "Reducing the energy consumption of ethernet with adaptive link rate (alr)," *IEEE Transactions on Computers*, vol. 57, no. 4, pp. 448–461, 2008.

[10] S. El-Zahr, P. Gunning, and N. Zilberman, "Exploring the benefits of carbon-aware routing," *Proceedings of the ACM on Networking*, vol. 1, no. CoNEXT3, pp. 1–24, 2023.

[11] B. G. Assefa and Ö. Özkasap, "Resdn: A novel metric and method for energy efficient routing in software defined networks," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 736–749, 2020.

[12] J. A. Brito, J. I. Moreno, L. M. Contreras, and M. B. Caamaño, "Architecture and methodology for green mec services using programmable data planes in 5g and beyond networks," in *2024 IFIP Networking Conference (IFIP Networking)*. IEEE, 2024, pp. 738–743.

[13] A. Clemm, C. Westphal, J. Tantsura, L. Ciavaglia, M.-P. Odini, and C. Pignataro, "Challenges and opportunities in management for green networking," 2024. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-nmrg-green-ps

[14] A. Clemm, C. Pignataro, E. Schooler, L. Ciavaglia, A. Rezaki, G. Mirsky, and J. Tantsura, "Green networking metrics for environmentally sustainable networking," 2023. [Online]. Available: https://datatracker.ietf.org/doc/draft-cx-green-green-metrics/00/

[15] C. Pignataro, A. Rezaki, and H. ElBakoury, "Environmental sustainability terminology and concepts," 2024. [Online]. Available: https://datatracker.ietf.org/doc/draft-pignataro-green-enviro-sust-terminology/00/

[16] A. Merlo, M. Migliardi, and L. Caviglione, "A survey on energy-aware security mechanisms," *Pervasive and Mobile Computing*, vol. 24, pp. 77–90, 2015.