PhD in Information Technology and Electrical Engineering
Università degli Studi di Napoli Federico II

PhD Student: Alfredo Nascita

Cycle: XXXVII

Training and Research Activities Report

Year: First

Tutor: prof. Valerio Persico

Date: October 31, 2022

1. Information:

PhD student: Alfredo Nascita
DR number: DR995853
Date of birth: 01/10/1994
Master Science degree: Computer Engineering
University: Università degli Studi di Napoli Federico II
Doctoral Cycle: XXXVII
Scholarship type: UNINA
Tutor: Prof. Valerio Persico

2. Study and training activities:

Activity	Type[1]	Hours	Credits	Dates	Organizer	Certificate[2]
Vehicular Hacking in Akka Technologies	Seminar	1,5	0,3	03/11/21	Prof. D. Cotroneo, Prof. S.P. Romano, Dr. R. Natella, DIETI - Unina	Y
Cyber security in Akka Technologies	Seminar	2	0,4	03/11/21	Prof. D. Cotroneo, Prof. S.P. Romano, Dr. R. Natella, DIETI - Unina	Y
Threat Hunting Essentials	Seminar	2	0,4	03/12/021	Prof. D. Cotroneo, Prof. S.P. Romano, Dr. R. Natella, DIETI - Unina	Y
Connecting the dots: Investigating an APT campaign using Splunk	Seminar	2	0,4	26/11/21	Prof. D. Cotroneo, Prof. S.P. Romano, Dr. R. Natella, DIETI - Unina	Y

Possible Quantum Machine Learning Approaches in HEP	Seminar	2	0,4	12/11/21	Prof. A. S. Cacciapuoti, DIETI - Unina	Y
Single cell omics leverage Machine Learning to dissect tumor microenvironment and cancer immuno editing	Seminar	2	0,4	02/12/21	Prof. Anna Corazza - DIETI, Unina	Y
Threat Hunting Use-Cases	Seminar	2	0,4	13/12/21	Prof. D. Cotroneo, Prof. S.P. Romano, Dr. R. Natella, DIETI - Unina	Y
All roads lead to WebRTC: an introduction to Janus	Seminar	2	0,4	16/12/21	Prof. S.P. Romano, DIETI - Unina	Y
Enel - Digital Innovation e Cyber Security	Seminar	1,5	0,3	01/02/22	Prof. Domenico Cotroneo, DIETI, Unina	Y
Network Security	Course	30	6	09/2022 -	Prof. S.P. Romano, DIETI - Unina	Y
The quest of quantum advantage with a photonics platform	Seminar	1,5	0,3	03/02/22	Dr. Giacomo Ascione, Micol Benetti, Marco Coraggio	Y
Computational analysis of cancer genomes	Seminar	1	0,2	16/02/22	Prof. Michele Ceccarelli	Y
Project Vāc: Can a Text-to-Speech Engine Generate Human Sentiments?	Seminar	1	0,2	28/02/2022	Dip. Fisica, "Ettore Pancini" -	N

(Picariello Lectures)					DIETI, Unina	
RAILS mid-term workshop	Seminar	5	1	25/02/2022	Prof. Valeria Vittorini et al. - DIETI, Unina	Y
Explainable Natural Language Inference	Seminar	1,5	0,3	13/04/22	Prof. Francesco Cutugno, Unina	Y
Ciberconflitti e minacce per la pace e la stabilità internazionale - Riflessioni sulla guerra in Ucraina e oltre	Seminar	2	0,4	05/04/22	Gruppo di Ateneo della Rete delle Università per la Pace (RUniPace UNINA)	Y
IEEE Authorship and Open Access Symposium: Tips and Best Practices to Get Published from IEEE Editors	Seminar	1,5	0,3	30/03/22	IEEE	Y
Malware Reverse Engineering: Foundations	Seminar	2	0,4	16/03/22	Prof. Fabio de Gasperi, Università degli Studi di Roma La Sapienza	Y
Towards a Political Philosophy of AI (Picariello Lectures)	Seminar	2	0,4	11/04/22	Dip. Fisica, "Ettore Pancini" - DIETI, Unina	N
Statistical data analysis for science and engineering	Course	12	4	26/05/22	Prof. Roberto Pietrantuono - DIETI, Unina	Y
Imprenditorialità Accademica	Course	14	4	26/05/22 - 13/07/22	Università degli Studi	Y

					di Napoli Federico II	
Network Traffic Measurement and Analysis (TMA) PhD Scool	Doctoral School - Seminar	16	3,2	27-28/06/22	University of Twente Enschede, NL	Y
eXplainable AI Summer School (XAISS)	Doctoral School	30	5	29/08/22 - 02/09/22	University of Delft, Delft, NL	Y
Accelerated Deep Learning via Efficient, Compressed and Managed Communication	Seminar	1	0,2	03/05/22	Prof. Antonio Pescapè, DIETI, Unina	Y
Machine Learning for Science and Engineering Research	Course	20	5	20/06/22 - 01/07/22	Proff. A. Corazza, F. Isgrò, R. Prevete, C. Sansone - DIETI, Dr. G. Pezzulo - CNR	Y

1) Courses, Seminar, Doctoral School, Research, Tutorship
2) Choose: Y or N

2.1. Study and training activities - credits earned

	Courses	Seminars	Research	Tutorship	Total
Bimonth 1	0	3,1	7	0	10,1
Bimonth 2	6	2	3	0	11
Bimonth 3	0	1,8	7	0	8,8
Bimonth 4	4	3,4	4	0	11,4
Bimonth 5	7	0	3	0	10
Bimonth 6	7	0	5	0	12
Total	24	10,3	29	0	63,3
Expected	30 - 70	10 - 30	80 - 140	0 – 4.8	

3. Research activity:

During my first PhD year, I deepened the motivations, applications, and issues of Network Traffic Analysis (NTA) with a specific focus on the explainability of models and tools developed to face several related problems.

Network traffic analysis is a critical process based on collecting and examining network data to understand and improve the performance of communication networks. Several practical activities are integral parts of this process and are becoming increasingly important in today's challenging network scenario. Nowadays, network traffic has profoundly changed compared with previous years (both in terms of composition and volume) and its analysis poses unprecedented challenges making all the approaches proposed over the years less and less viable. As an example, the now pervasive use of cryptographic protocols prevents the effectiveness of deep packet inspection, one of the most widely used approaches in the past [1]. Moreover, today's traffic is highly heterogeneous (different apps, services, users, and devices) and constantly evolves. These are just some of the reasons underlying the need for the design of new tools for effective and efficient management of traffic and to meet increasingly stringent requirements.
In recent years, artificial intelligence-based approaches have emerged as a solution to the problems described and are increasingly being used to solve NTA problems. In particular, Deep Learning (DL) approaches represent the new frontier for traffic analysis tools. A key feature of these tools is their ability to work directly with *raw traffic data*, which makes them particularly suitable for handling traffic dynamicity without continuous model adapting. The essentially *data-driven* nature of such network tools, however, also constitutes their main weakness since it raises serious questions of interpretability and confidence in their results and thus, in the management policies they suggest.
In other words, there is a very strong need for network operators to obtain, along with the outcomes of these new NTA tools, explanations of their behavior to increase confidence in their outputs and to act in a timely and confident manner to implement network management policies.
In order to cope with the current limitations of DL approaches, eXplainable Artificial Intelligence (XAI) has recently been proposed in many different contexts with the purpose of shedding light on the decision mechanisms of artificial intelligence approaches and revealing the logic behind their decisions. More specifically, Defense Advanced Research Projects Agency (DARPA) [2], launched its program for XAI in 2017, with the aim of shaping new learning processes that (a) produce better explainable models, (b) design effective explanation interfaces, and (c) understand the psychological requirements for appropriate explanations.

In light of all the above considerations, the focus of my research is the design and implementation of new tools for traffic analysis driven by XAI analyses. In other words, the main goal is to obtain better-performing and more secure network tools by employing the insights gained from explainability analyses and the valuable information they can provide. Another objective is to understand the models' decisions, ensuring that they are based on valid and objective evidence (the model is *right for the right reasons*) to increase user trust and promote their adoption in real network scenarios.

To achieve such goals, I defined a theoretical framework involving several steps, starting from the collection of network data and the following training of AI-based models that solve a specific traffic NTA task. After these two paramount steps, the next phase involves the design and application of XAI techniques to interpret the models from different perspectives (input importance, internal operations, and components...). All the new knowledge produced in this phase (both about particular models under investigation and about the problem more generally) is the input for the final phase where the models are optimized and refined, to produce a better version of the tools along the chosen optimization directions.

During this first year, I followed this theoretical framework to tackle the problem of mobile Traffic Classification (TC) which is considered a key prerequisite for secure network management. In fact, detailed knowledge of the traffic traversing the network enables a series of activities ranging from security to accurate management of resources and the detection of intrusions and anomalies.

This research activity led to a journal publication [J2], made in collaboration with other members of the research group, where we propose a new traffic classifier optimized in several respects.

In this work, we exploited XAI to interpret, and improve multimodal DL approaches that solve multiple (visibility) TC tasks via multitask learning, focusing on encrypted traffic. Pursuing these goals, we design, implement, and evaluate an evolved multimodal multitask DL traffic classifier, attained in multiple refinement steps driven by XAI, producing an evolved version of a recently proposed classifier [3].

Our evaluation was performed on the public ISCX VPN-NONVPN dataset [4] of human-generated traffic labeled according to three different TC tasks, namely encapsulation, traffic type, and application recognition.

In detail, we employed two interpretability methods (i.e. Deep SHAP [5] and Integrated Gradients [6]) to provide global explanations and quantify the contribution of each modality in solving each task and the rationale for each considered modality, fed with transport-layer payload or fields extracted from packet-sequences, respectively. Driven by interpretability outcomes, we designed a better-performing and "earlier" version of our traffic classifier. Such an optimized proposal was then investigated in terms of reliability, namely how much we can trust its prediction confidence, via calibration analysis. Leveraging label smoothing we designed a novel version of the classifier that halves the calibration error on all three tasks, obtaining a significant gain in reliability, without a significant loss in performance. Finally, we investigated three techniques to reduce the model size aiming at improving its feasibility: knowledge distillation, pruning, and quantization. Pruning turned out to be the best compression technique and led us to the final version. The final classifier, obtained with successive XAI-aided refinements, represents an evolved version of the starting architecture in terms of the investigated aspects of interest: performance, interpretability, reliability, and memory occupation.

Besides this research activity, I carried out various study and research activities with a specific focus on attack classification and malware detection that lead to the publications [C1] and [C2].

In particular, I dealt with the classification of attacks performed in Internet of Things (IoT) networks. This topic is particularly important since IoT devices expose several vulnerabilities, and so the effective and timely identification of attacks against them calls for novel intelligent tools. More precisely, in the work [C1] we employed state-of-the-art DL approaches, also comparing them with more traditional Machine Learning approaches. Taking into account the specific nature of considered malicious/benign traffic, we extended the input commonly used for mobile TC in order to exploit information extracted from the network-layer header and payload. Furthermore, we exploited a well-known XAI approach, *Occlusion Analysis*, to shed light on the working principles of DL investigated models and quantify the impact on the performance of some input known to introduce bias (e.g. IP addresses and ports), witnessing the importance of not considering them in operational scenarios to not obtain misleading results and inflated performance.

On the same line, I studied malware traffic analysis since, with the huge popularity of mobile-app services, malicious software is growing at a rapid pace. Accordingly, the interest of the scientific community in DL solutions for detecting and classifying malware traffic is increasing. Accordingly, in the work [C2], we provided an assessment of the performance of several data-driven strategies to detect and classify Android malware traffic considering both flat and hierarchical approaches. We evaluate the hierarchical approach since

it allows us to exploit model and data parallelism and to break down the classification problem to address it in a more targeted manner.

Another important topic I studied is *class incremental learning* applied to mobile TC. This approach aims to extend an already trained classifier without the need for retraining it. Such an approach is critical to coping with the rapid growth experienced in the mobile traffic scenario where new apps are daily released. The architectures resulting from this approach suffer from two complementary problems: forgetting, i.e. the progressively losing of accumulated knowledge, and intransigence, i.e. the inability to learn new knowledge. The specific reasons that lead to these two problems are not fully known and therefore guidelines are currently lacking to mitigate them. Also in this case, explainability analyses are key to understanding the changes that models undergo as new applications are added and working to ensure that old knowledge remains solid while learning how to classify new applications.

These research activities allowed me to extend my knowledge about recent NTA problems which today are solved with data-driven approaches and therefore require an adequate analysis of explainability to be able to safely support network operators and suggest appropriate action policies for operators. In future work, therefore, I propose to deepen these aspects under the lens of explainability with the aim of designing and implementing more effective and efficient network traffic analysis by exploiting the insights of the explainability analysis.

In parallel with the above-mentioned activities a collaboration with the National Institute of Textile Engineering and Research (NITER) of the University of Dhaka has led to the paper [J1] where we provided a comprehensive survey regarding Blockchain and Software Defined Network technologies. We focused on their integration to jointly take advantage of their features and fulfill the need for stronger security and privacy. Additionally, we covered the application fields of these technologies both individually and combined and discuss the open issues and potential directions for future avenues regarding the integration of these promising technologies.

References:

[1] A. Dainotti, A. Pescapé and K. C. Claffy, *Issues and future directions in traffic classification*, IEEE Network 26 (1) (2012) 35–40.

[2] D. Gunning and D. Aha, "*DARPA's explainable artificial intelligence (XAI) program*", AI Magazine, vol. 40, no. 2, pp. 44–58, 2019.

[3] G. Aceto, D. Ciuonzo, A. Montieri and A. Pescapé. *"DISTILLER: Encrypted traffic classification via multimodal multitask deep learning"*, Journal of Network and Computer Applications, 183, 102985, 2021.

[4] G. Draper-Gil, A. H. Lashkari, M. Mamun, and A. A. Ghorbani, "Characterization of encrypted and VPN traffic using time-related features," 2nd International Conference on Information Systems Security and Privacy (ICISSP), pp. 407–414, 2016.

[5] M. Sundararajan, A. Taly, and Q. Yan. *"Axiomatic attribution for deep networks"*, International Conference on Machine Learning (ICML), 2017.

[6] S. M. Lundberg and S.-I. Lee, *"A unified approach to interpreting model predictions"* in NIPS'17 Proceedings of the 31st International Conference on Neural Information Processing Systems, 2017.

4. Research products

Conference Papers:

[C1] Machine and Deep Learning Approaches for IoT Attack Classification, Alfredo Nascita, Francesco Cerasuolo, Davide Di Monda, Jonas Thern Aberia Garcia, Antonio Montieri, and Antonio Pescapè. INFOCOM 10th International Workshop on Security and Privacy in Big Data (BigSecurity) - published

[C2] A Comparison of Machine and Deep Learning Models for Detection and Classification of Android Malware Traffic, Giampaolo Bovenzi, Francesco Cerasuolo, Antonio Montieri, Alfredo Nascita, Valerio Persico, Antonio Pescapé, ISCC 2nd IEEE International Workshop on Distributed Intelligent Systems (DistInSys) - published

[C3] Can XAI Tools Interpret Traffic Classifiers based on Deep Learning?, Alfredo Nascita, Antonio Montieri, Giuseppe Aceto, Domenico Ciuonzo, Valerio Persico, Antonio Pescapé, *Secondo Convegno Nazionale CINI sull'Intelligenza Artificiale* (NOT indexed in Scopus or ISI Web of Science) - *published*

Journal Papers:

[J1] On the Integration of Blockchain and SDN: Overview, Applications, and Future Perspectives - Anichur Rahman, Antonio Montieri, Dipanjali Kundu, Md Razaul Karim, Md Jahidul Islam, Sara Umme, Alfredo Nascita, Antonio Pescapé, *Springer's Journal of Network and Systems Management, Special Issue on Blockchains and Distributed Ledgers in Network and Service Management* - published

[J2] Improving Performance, Trust, and Feasibility in Multitask Traffic Classification with XAI, Alfredo Nascita, Antonio Montieri, Giuseppe Aceto, Valerio Persico, Antonio Pescapé, submitted to *IEEE Transactions on Network and Service Management (TNSM)* 2022 - submitted

5. Conferences and seminars attended

INFOCOM 10th International Workshop on Security and Privacy in Big Data (BigSecurity) 2022, Virtual, 2-5 May 2022
Presentation of the Article*: [C1] Machine and Deep Learning Approaches for IoT Attack Classification*

ISCC 2nd IEEE International Workshop on "Distributed Intelligent Systems" (DistInSys) 2022, Virtual, 30 June - 3 July 2022
Presentation of the Article*: [C2] A Comparison of Machine and Deep Learning Models for Detection and Classification of Android Malware Traffic*
Ital-IA 2022, Secondo Convegno Nazionale CINI sull'Intelligenza Artificiale, Virtual, 9-11 February 2022
Presentation of the Article*: [C3] Can XAI Tools Interpret Traffic Classifiers based on Deep Learning?*

Network Traffic Measurement and Analysis (TMA) PhD Scool, Unversity of Twente, Enschede, NL, 26-28 June 2022
Presentation of the Poster: *Towards the Interpretability of Deep Learning Traffic Classifiers via XAI Techniques*

6. Activity abroad:

I have not carried out any activity abroad during my first PhD year.

7. Tutorship

I have not carried out any tutorship during my first PhD year.