PhD in Information Technology and Electrical Engineering

Università degli Studi di Napoli Federico II

PhD Student: Saeed Javanmardi

XXXIV Cycle

Training and Research Activities Report – Second Year

Tutor: Prof. Antonio Pescapè

Add the following items according to the meeting we had today.

Concerning the structure of the document, use the Section number as is. Use the sub-contents indicated with a letter only as a suggestion for your content (a free form text is preferable)

1. **Information**

   I am Saeed Javanmardi; I received a M.Sc. Degree in Computer Engineering at Azad University (IRAN) in July 2012. I am a PhD student attending the XXXIV Cycle of the ITEE PhD program at the Department of Information Technology and Electrical Engineering of the University of Napoli Federico II. My tutor is Prof. Antonio Pescapè. I am currently part of the COMICS research group, studying in the field of security aware IoT application scheduling.

2. **Study and Training activities**
   a. Courses
      i. *Matlab fundamental, Professor Agostino De Marco, 20 hours, 27/04/2020, 2 Credit*.
      ii. *Design and implementation of augmented reality software, Dr. Domenico Amalfitano, 20 hours, June 3th 2020 till June 23th 2020, 4 Credit*.
      iii. *Computer networks II, Professor Giorgio Ventre, November 2019, 2.4 Credit*.
      iv. *Digital Forensics' methods, practices and tools, Dr. Giovanni Cozzolino, 3, 5, 6, 9 and 10 November 2020, 3 credit.*

   b. Seminars
      i. *Cybersecurity and fuzzing for Robots, Blockchain, and more, Dr. Antonio Ken Iannillo, Dr. Roberto Natella, 13/01/2020, 0.2 Credit*.
      ii. *Flexible two echelon location routing for supply networks, Professor Claudia Archetti, 8 November 2019, 0.2 Credit*.
      iii. *A dynamic and probabilistic orienteering problem*, Professor Claudia Archetti, 8 November 2019, 0.2 Credits.
      iv. *Lo Spazio cybernetico come dominio bellico, Gian piero siroli, 15 November 2019, 0.4 Credit*.
      v. *How to get published with IEEE, IEEE advancing technology for humanity, 04/20/2020, 0.4 Credit*
      vi. *Intelligenza artificiale ed etica: la ricerca in IA alla prova delle sfide etiche, daniele amoroso, piero bonatti, prevete, serafini, schiaffonati, guidotti, December 2019, Credit 1.6*

   c. Credit summary:

	Credits year 1								Credits year 2							
		1	2	3	4	5	6			1	2	3	4	5	6	
	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary	Estimated	bimonth	bimonth	bimonth	bimonth	bimonth	bimonth	Summary
Modules	18		6	2	3.8	2.4		**14**	9	2.4		2		4	3	**11**
Seminars	13		0.5	0.4	0.9	0.9	2.6	**5.3**	6	1.6	0.4	0.4		0.4		**2.8**
Research	34		7	7	7	9	9	**39**	42		7	7	7	9	10	**40**
	65	0	14	9.4	12	12	12	**59**	57	1.6	7.4	9.4	7	13	10	**54**

3. Research activity

My research activity is entitled “FPSTS: A Security Driven Task Scheduling Approach for SDN-based IoT–Fog Networks”. Fog computing is a paradigm to overcome the cloud computing limitations which provides low latency to the users’ applications for the Internet of Things (IoT). Software-defined networking (SDN) is a practical networking infrastructure that provides a great capability in managing network flows. SDN switches are powerful devices, which can be used as fog devices/fog gateways simultaneously. Hence, fog devices are more vulnerable to several attacks. TCP SYN flood attack is one of the most common denial of service attacks, in which a malicious node produces many half-open TCP connections on the targeted computational nodes so as to break them down. Motivated by this, in the second year, I applied SDN envision IoT–Fog networks to address TCP SYN flood attacks. In this way, I propose FPSTS, a security-aware task scheduler in IoT-fog networks. FPSTS puts forward a fuzzy-based multi-objective particle swarm Optimization approach to aggregate optimal computing resources and provide a proper level of security protection into one synthetic objective to find a single proper answer. I perform extensive simulations on IoT-based scenario to show that the FPSTS algorithm significantly outperforms state-of-the-art algorithms.

Recent advances in smart devices and communication technologies are fuelling the Internet of Things (IoT) paradigm, which is characterized by the pervasive presence around people of (interconnected and uniquely addressable) things, able to measure and modify the environment and communicate with each other. Accordingly, technology leaders, governments, and researchers are putting serious efforts to develop solutions enabling wide IoT deployment in order to support a variety of applications impacting a number of different scenarios (e.g. healthcare, industry 4.0, smart home). Often, resource-constrained things are required to interact with service platforms in order to benefit from their computation, storage, and networking capability on request. While on the one hand referring to cloud services is the natural choice, on the other hand, some classes of applications may suffer from the performance figures that cloud platforms may guarantee in terms of provided QoS (e.g. due to latency to reach far-away cloud data centers). To address this issue, fog computing has been proposed, which provide the tools to mitigate cloud QoS shortcomings at the expenses of not having available virtually infinite resources of cloud data centers. In fact, fog computing is a cutting edge solution, which leverages near-user (possibly cooperating) edge devices (fog devices) rather than a single (far-away) cloud data center to supply computing services to IoT applications. Hence, fog infrastructures allow for supporting IoT application requirements to reduce both delay and network utilization. Usually, cloud data centers still take part in composing the overall fog architectures, but are accessed only in case of need (i.e. when the fog nodes capabilities are not enough). In the context of fog computing, resource management is a challenging issue to be considered. Task scheduling is the major part of a resource management unit that aims to assign a set of tasks to fog devices. To this end, the task scheduler—possibly located at different places in a fog architecture, such as fog gateways, fog devices, cloud gateway or cloud data center—decompresses the jobs into a set of (independent) tasks, and then it assigns them to the fog devices.

Besides their requirements in terms of QoS, IoT and related fog infrastructures are prone to security and privacy concerns due to the critical nature of the contexts the applications are deployed in and the generated data (e.g., smart home, healthcare etc.). These concerns potentially derive from low-cost hardware and software design choices of IoT devices (e.g. unsafe update mechanism, outdated component, etc.) or lack of adequate security protection. Thus, malicious users have shifted the main target of daily-released malware, now pointing to

infect IoT services and make them unavailable, leveraging the manifold and significant weaknesses generated by the IoT context. IoT and fog devices are both susceptible to be hacked by malicious users. These devices may be even incorporated in botnets, thus unwillingly participating to the attack after they have been compromised (e.g., taking part to Distributed Denial of Service DDoS attacks which aim at disrupting targeted server/service by overwhelming the target with a flood of malicious Internet traffic). As the Software-defined networking (SDN) provides flexible network programmability and logically centralized control (through a global view of the network), this paradigm is able to provide the tools for effectively detecting and containing network security problems that recently is used in IoT-fog networks. Indeed, SDN represents a good fit for the fog environment as fog devices and gateways have the capabilities to implement this paradigm. In accordance with the context above, intelligent and efficient solutions are required to detect and protect against DDoS attacks in their IoT-fog networks. However considering task scheduling efficiency and security poses a non-trivial challenge to task scheduling algorithms that are required to strike a balance between these two distinct objectives. As fog environments have dynamic features in which the characteristics of elements change continuously, techniques to jointly preserve trust and security in such dynamic environments are required.

The scheduler I devised considers the dynamic behaviour of distributed systems and uses two trust degrees obtained from Threshold Random Walk with Credit-Based connection rate-limiting (TRW-CB) and Rate Limiting algorithms— i.e. one of the most prominent source-based attack mitigation strategies available—to deal with TCP SYN flood DDoS attacks. My proposal jointly merges security issues and task scheduling with the aid of multi-objective PSO and multi-criteria decision-making algorithms. FPSTS solves multi objective task scheduling problem to jointly maximize security and efficiency of quality of services (QoS) such as delay in IoT-fog networks. It also leverages SDN programmability and centralized network features to enforce attack mitigation mechanisms against the TCP SYN flood DDoS attacks: in case of detection of requests from devices identified as malicious, the requests are not taken into account. In other words, FPSTS addresses security issues inside the scheduler. More specifically, FPSTS assigns the most suitable resources to the tasks based on the current status of the resources and incoming tasks. FPSTS focuses on assigning applications' tasks among fog devices, considering the trustworthiness of fog devices, and end-user devices. Thus, FPSTS strikes a balance between efficiency and security objectives.

4. Products

a. Publications

i. Javanmardi, Saeed, et al. "FPSTS: A Security Driven Task Scheduling Approach for SDN-based IoT–Fog Networks", It is ready to be submitted to an ISI journal.

ii. Javanmardi, Saeed, et al. "FPFTS: A joint fuzzy particle swarm optimization mobility-aware approach to fog task scheduling algorithm for Internet of Things devices." Software: Practice and Experience (2020).