A simulation study on a WSN for emergency management

Lelio Campanile
Mauro Iacono
Fiammetta Marulli
Michele Mastroianni
Dipartimento di Matematica e Fisica
Università degli Studi della Campania
"L. Vanvitelli"
viale Lincoln 5
81100, Caserta, Italy

KEYWORDS

Performance evaluation; Wireless Sensor Networks; emergency management; simulation; ns-3; Internet of Things.

ABSTRACT

Wireless Sensors Networks (WSN) are one of the ways to provide the communication infrastructure for advanced applications based on the Internet of Things (IoT) paradigm. IoT supports high level applications over WSN to provide services in a number of fields. WSN are also suitable to support critical applications, as the supporting technologies are consolidated and standard network services can be used on top of the specific layers. FUrthermore, generic distributed or network-enabled software can be run over the nodes of a WSN.

In this paper we evaluate and compare performances of IEEE 802.11g and 802.11n, two implementations of the popular Wi-Fi technology, to support the deployment and utilization of an energy management support system, used to monitor the field by a team of firefighters during a mission. Evaluation on an example scenario is done by using ns-3, an open network simulator characterized by its realistic details, to understand the actual limitations of the two standards besides theoretical limits.

I. INTRODUCTION

IoT and WSN are an established approach to implement viable and flexible monitoring infrastructures. The evolution of both hardware market and software support enables a variety of applications, spanning from domotics, Industry 4.0 related solutions and smart cities. While the commodity market offers a large choice of products, including low cost ones, the use of these technologies to support critical applications should be carefully planned and related solutions require proper care and choice of components, implementation and integration.

The technology stack that implements the IoT paradigm over WSN is now mature and is, at the state, complex and layered. What happens at the system level is not anymore immediately predictable and dominated by determinism as it was in the first, proprietary or embedded products. In fact, there is a large availability of solutions, so that the performances of the layers chosen in a given architecture cannot be predicted on the basis of the declared performances of components. In order to design critical applications and verify the scenarios in which they will operate, possibly in support of safety and protection of human operators or to lower risk in case of intervention in dangerous sites, a simulation based approach that exploits very detailed models of the technological layers should be preferred as a support and reference, particularly when it is not possible, for the variability of operational conditions and setup or their unpredictability, to proceed with validation on the field.

We focus on the domain of emergency management. In particular, the work described in this paper is a part of a larger research activity that aims at studying an Edge computing based support system for emergency response. In the overall approach, a key role is played by IoT technologies in support of the field action of firefighters inside large buildings. Coverage understanding, as well as technological choices, are of paramount importance in the design process: consequently, as we did not find supporting studies after a thorough analysis of the existing literature, here we present the results of a parametric analysis, that has been conducted in a simple scenario that mimics a large warehouse, a typical case for the application domain, that also has the advantage of having a simple geometry, from which general conclusions can be drawn about technological limitations.

In this paper we verified, by means of simulation, the actual possibilities of IEEE 802.11g and 802.11n in a constrained WSN scenario. These two technologies have been used as part of an emergency management support that aims to assist firefighters while entering and moving in a building in which there is a fire. While the second one offers in theory higher performances,

Communications of the ECMS, Volume 34, Issue 1,
Proceedings, ©ECMS Mike Steglich, Christian Mueller,
Gaby Neumann, Mathias Walther (Editors)
ISBN: 978-3-937436-68-5/978-3-937436-69-2(CD) ISSN 2522-2414

specially on available bandwidth and management, the first is already available in rugged hardware and has more mature commercial implementations, due to its consolidated presence on the market and the feedback resulting from its wide number of installations in different conditions and for different uses. The analysis and the comparison is thus motivated by the need for choosing in a savvy way components according to cost issues, and for solving the make or buy dilemma in critical situations for disposable WSN nodes. The scenario is designed to avoid additional workloads and traffic on a node with respect to the one generated by or directed to the node, to obtain an evaluation that is neutral with respect to routing effects. The emergency management system implements an Edge computing based application over heterogeneous IoT WSN nodes with different characteristics, including Augmented Reality personal support for firefighters that operate on the field and camera based protection solutions for the environments in which they operate: consequently, we explored the potential of these two technologies with synthetic workloads in this perspective.

This paper is organized as follows: Section II presents related works; Section III presents the operational scenario in which the system is to be deployed and a glance on all its components, to describe the complete framework; Section IV introduces the simulation choices and the characteristics of the simulation; Section V presents the results of the simulation campaigns and a short analysis of the outcomes; Section VI closes the paper with final considerations and future works.

II. BACKGROUND AND RELATED WORK

The growth of IoT technology causes the increasingly pressing need to keep computing close to the user or to the application scenario, while keeping the advantages of Cloud computing available and in the loop. This sums up the potential offered by Cloud computing, Mobile computing and IoT, with the purpose of matching both global requirements in terms of cost management, performances and flexibility of resources, and local requirements such as privacy enforcement and resiliency to network problems. With this in mind, Fog computing paradigm standardizes the Edge approach to computing.

With regard to Fog computing, interesting introductory resources are [24], [26] and [14], that propose complementary approaches to the fundamentals of the topic.

The paradigm and the substanding architecture present a richness of open research challenges, that encompass basic aspects like communication protocols, system organization and architectures [16][28][21], and technological solutions [17], advanced aspects like performance evaluation and verification [10], design methodologies, system and software management [12][11][27], data reduction [4], security [25][29], load balancing [20] or policy-related aspects such as legal implications and risk [13][23]. A useful review paper is [15].

A convenient approach to study and evaluate different network topologies without the need of setting up a physical implementation is network simulation. Due to the richness of aspects and parameters that characterize computer networks, selecting the appropriate network simulator to target is a crucial task for researchers. In order to deep into simulators, an extended description and a comparison table between the most relevant network simulators may be found in [6].

In order to perform large-scale network simulation, one of the most widely used tool is Network Simulator 3 (ns-3). ns-3 is stated as a versatile and complete simulator by many authors, and in some benchmarks related to the study of wireless network it proved to be the fastest simulator in terms of computation time [18]. ns-3 is an open source simulator, released in 2006 [1][22], and may be considered as a replacement of an older tool, called ns-2. The simulation environment is released for most of the modern operating systems, and is written in C++ with an optional Python scripting API. It allows researchers and practitioners to study network protocols (mainly Internet-related) and large-scale networked systems in a controlled environment. ns-3 provides community supported modules for a wide variety of network protocols and components, it supports both simulation and emulation that allows including real network portions, it is designed to support large-scale simulations and it is easily extensible and programmable.

ns-3 generates PCAP traces of simulated models, so researchers can easily study or debug the output with standard tools such as Tcpdump [2] or Wireshark [3]. Additionally, there is also a number of external tools provided by the ns-3 community, in this work we have used extensively the Flow Monitor module [7] for the performance monitoring and the ns-3 Simulation Execution Manager (SEM)[19] to perform multiple simulations in a structured and repeatable manner. A systematic literature review on ns-3 is [6].

III. SCENARIO

The reference scenario concerns a system conceived to support firefighting squads during field operations (from [9]). Firefighters are equipped with a number of sensors to monitor their health conditions, an augmented reality device that enriches their personal view with details on the scene they are observing, and a camera. Besides personal equipment, firefighters deploy on the field additional sensors while moving into the incident location. Such sensors are designed to provide various kind of sensing features: some complex sensors with significant computing power can synthesize elementary sensed data into abstract information and integrate sensed data from other sensors. Sensors and personal equipment are powered by batteries and compose a WSN that connects all devices to an Edge server that runs a field command and control application. For a more complete description of the system and of the personal equipment, the reader can refer to [9].

The whole system can be described in terms of three

classes of nodes:

- *Personal Support* (PS): equipment that each fireman wears, including various sensors (e.g. vital parameters, audio, thermal, chemical), an AR visor including a camera, and a local computing device that manages all sensing;
- *Simple Sensor* (SS): there are ordinary WSN nodes with some local computing capability, mainly used for managing interactions with the rest of the system and preprocessing data;
- *Intelligent Sensor* (IS): there are nodes equipped with multiple sensors and can perform significant local computing on sensed data and execute generic tasks, with the possibility of offloading from other nodes and towards other nodes or the Edge server.

The PS nodes may also generate AR additional graphics, and process sensed information to produce comprehensive abstract local status information and interacts with the rest of the system.

In the system designed, the SS nodes can be put directly under the control of PS or IS nodes in order to augment their capabilities, but in this paper we will simplify the problem by only considering the case in which all nodes are directly under the control of the Edge server, in order to evaluate network performances.

The SS nodes, in normal operating conditions, generate a light and regular network traffic towards the Edge server, and IS nodes send larger and less regular network workloads. The PS nodes, besides generating large and non regular traffic, also deals with an additional traffic due to video information, and receive traffic from the Edge server. Furthermore, IS and PS nodes, when available energy on their board is lower than a given threshold, start delegating computing tasks to the Edge server, in order to extend their own active lifetime. For this reason, more intense data traffic is generated on the WSN after an initial reconfiguration and status synchronization data traffic. A similar situation happens (in the opposite traffic direction) whenever IS or PS nodes need to reload software images and/or reconfiguration parameters, which are loaded from the Edge server.

In the next section some simulation-based analyses are presented about the proposed solution, and in the section V some preliminary results are shown.

IV. MODELING AND SIMULATION

Before implementing the real network, wide simulation campaigns are needed in order to assess the technology to be used (WiFi, LoWPAN, etc.). The platform chosen for simulation is ns-3, because of its versatility and simulation performance. As a first attempt to simulate the network, standard WiFi technologies are simulated, such as IEEE 802.11g and 802.11n.

The choice of WiFi technologies is due to their diffusion and performance in term of throughput and data rate; on the other hand, this kind of devices are more power consuming than others (e.g., LoWPAN). Moreover, the outdated 802.11g technology is taken into consideration due to the larger availability of industrial rugged devices than 802.11n.

TABLE I: Values of simulation parameters

Parameters	**Values**
WiFi Protocol	[802.11g, 802.11n]
N. of nodes	[3, 4, 5, 6, 7, 8, 9, 10 , 11, 12, 13, 14]
Datarate	[3Mbps, 5Mbps, 7Mbps]

The used topology is a simple grid with the same horizontal and vertical distance between rows and columns. The Edge server is placed in the upper left corner and the second deployed mode is the Access Point (AP), while the other nodes are placed in rows, with F nodes per row. The distance between rows is ΔX, and the distance between columns is ΔY (see Fig. 2). All nodes directly communicate with the Edge server (see Fig. 3). Obviously, the diagonal of grid is the maximum distance from the grid server to the node (worst case). The version of ns-3 used is 3.30.1, compiled and the simulation ran on a macbook pro 15" equipped with an Intel core i7 2.8GHz with 16Gb of RAM and macOS Mojave 10.14.5.

The ns-3 modules used to set up the simulation are showed in Table II.

The simulation campaigns were aimed at obtaining different metrics for evaluating the performance of the entire network. The metrics that have been taken into consideration are the total throughput that the server can manage, or rather the maximum data flow it can receive, the throughput that each node can manage singularly and finally a derived metric, the number of nodes that are able to guarantee a throughput greater than a threshold value.

In order to obtain the best and most complete simulation results, we decided to run the simulations by varying different parameters:

- *WiFi protocol*: the protocols set in the simulations. We used 802.11 family protocol at level 1 and 2 of the ISO/OSI protocol stack.
- *number of nodes*: the number of simultaneous nodes in each simulation. We used IPv6 protocol at level 3 of the ISO/OSI protocol stack.
- *Datarate*: the continuous dataflow that the node transmits to the Edge Server. We used the UDP protocol at the level 4 of the ISO/OSI protocol stack.

Figure 1 summarizes the ISO/OSI protocol stack setup used in simulations. We execute the simulation with all possible combinations of value, shown in table I, for the above parameters. We then had 72 different simulation scenarios run for the subsequent analysis of the results and evaluation of performance.

V. RESULTS

Keeping in mind that some of the simulated nodes (particularly PS nodes) are part of the gear of firemen in a crisis area, the dispatched simulation campaigns are aimed to detect expected performance values. First of all, it is needed to know how many PS nodes may be used in the crisis area (i.e. how many firemen can work

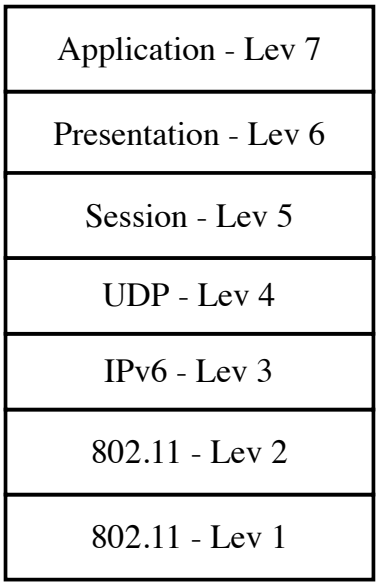

Fig. 1. The ISO/OSI stack used in simulations

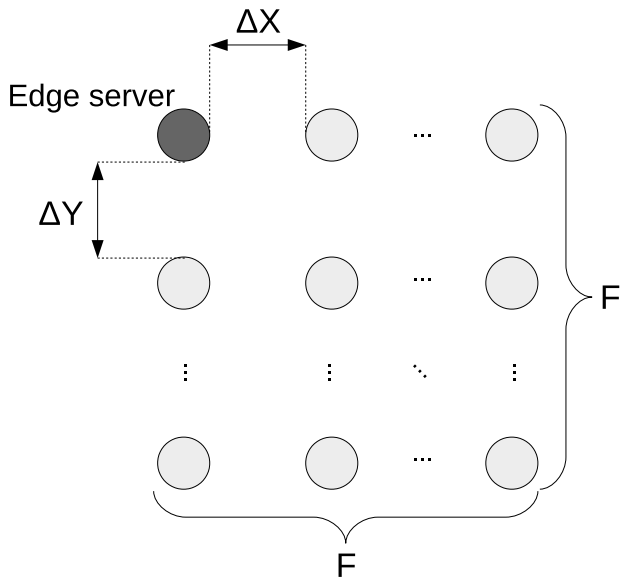

Fig. 2. Spatial configuration of the network and related parameters

TABLE II: Used ns-3 modules for the simulation setup

Modules	**Description**
Internet	general IP, TCP and UDP protocols implementation
IPv6	IPv6 protocol implementation
Mobility	a model that helps to allocate devices
Spectrum	it aims at providing support for modeling the frequency-dependent aspects of communications [5]
Propagation Loss	modeling of propagation loss and propagation delay
Wi-Fi	implementation of ns-3 models for wi-fi (IEEE 802.11)
Flow Monitor	the module uses probes, installed in network nodes, to track the packets exchanged by the nodes to measure the performance of network protocols [8]
Application	modeling different applications at ISO/OSI level 7

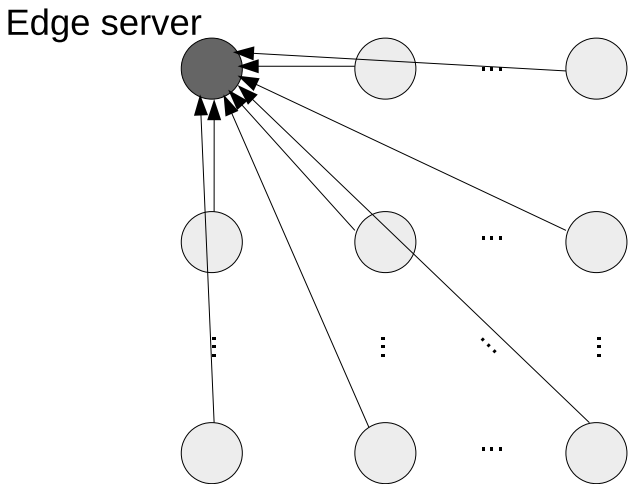

Fig. 3. Structure of the connections and information flow considered for the experiments

in crisis area) without causing performance decay. In order to do this, tests have been conducted varying the numbers of involved nodes. The nodes feed the Edge server with data streams of different data rates (3, 5 and 7 Mbps). For a correct understanding of the results we want to emphasize that in the simulations all the nodes involved start transmitting at maximum speed at the same time. The next figures show throughput values for both IEEE 802.11g (Figure 4) and 802.11n (Figure 5) devices.

Looking at the results, it is clear that the throughput given by IEEE 802.11g is widely inadequate. In fact, Figure 4 shows that, even with a 3 Mbps data stream, the throughput is very low also with a low number of nodes. Figure 5, instead, shows that IEEE 802.11n is really promising, allowing sufficient performance, up to 8 PS nodes with a data stream of 3 Mbps.

Established that 802.11g is inadequate for implementation of the designed system, the focus shifts on 802.11n. The analysis continues with another simulation campaign, in which the number of nodes that are "up" (i.e. nodes that are able to make use of data rate/2) is evaluated. The following Figure 6 shows that, with a data rate of 3 Mbps, 8 nodes are fully available; with a data rate of 7 Mbps, at least 5 nodes may be fully available.

The next graph, in Figure 7, is also more interesting, and shows the mean performance of PS nodes versus total number of nodes. In this Figure it is easy to see

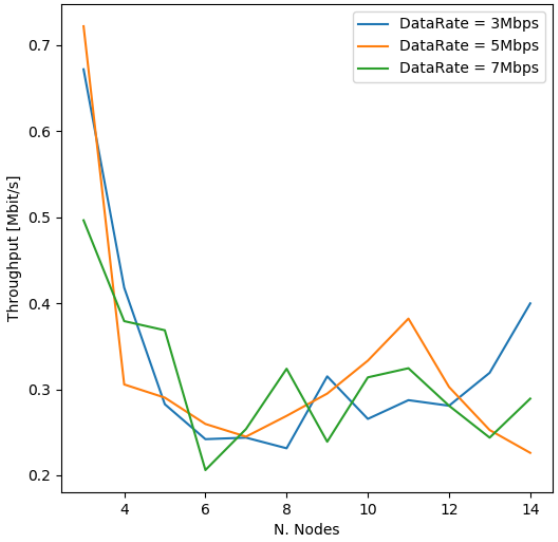

Fig. 4. Throughput of the network when using IEEE 802.11g

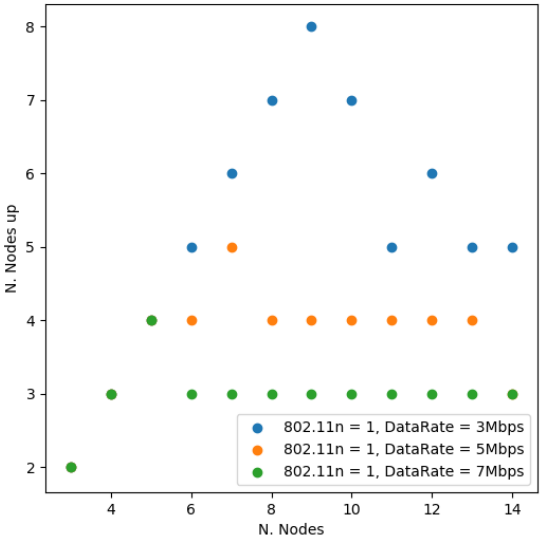

Fig. 6. Nodes "up" versus total number of nodes (IEEE 802.11n)

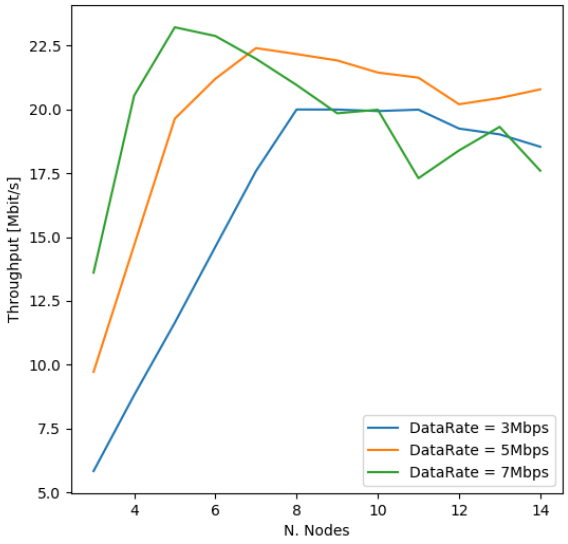

Fig. 5. Throughput of the network when using IEEE 802.11n

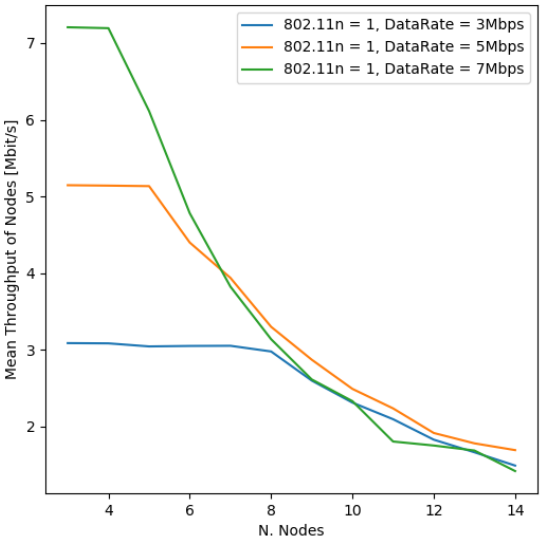

Fig. 7. Mean throughput of nodes versus total number of nodes (IEEE 802.11n)

that, with a data stream of 3 Mbps, up to 8 PS nodes may be used at the same time.

The same test has been performed also on a network based on IEEE 802.11g devices. The results, shown in Figure 8, confirm that 802.11g is not able to perform well enough for the case study; in fact, throughput decays quickly, even when using a little number of PS nodes.

VI. CONCLUSIONS

In this paper, the network simulator ns-3 is used to study the performance of an Edge system conceived to support an advanced emergency management system. This system, based on three different types of sensors (personal, base and intelligent sensors) is simulated considering the possible implementation based on IEEE 802.11g or 802.11n network devices. A large test campaign has been performed, and the results show that 802.11g is inadequate for implementation, whilst 802.11n shows promising results. In this case, it is possible to use up to eight PS nodes with a data rate of 3 Mbps, which may be acceptable for the purpose of the system.

Future work includes extending simulation using different network technologies, such as LoWPAN, and

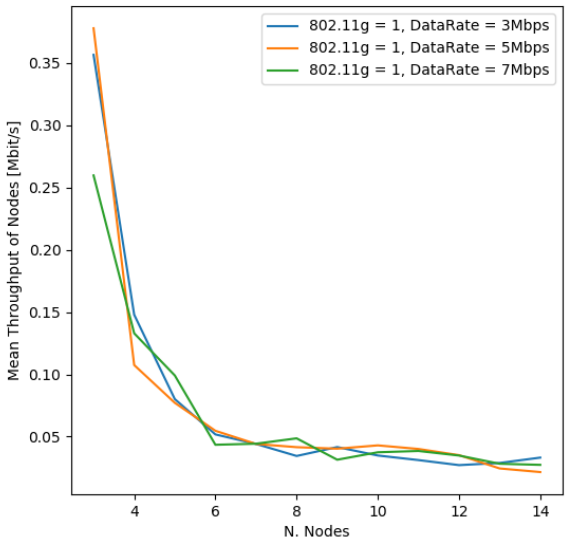

Fig. 8. Mean throughput of nodes versus total number of nodes (IEEE 802.11g)

deepening into the model to study the effect of different policies on the nodes behaviour. Furthermore, energy management in the sensor network will be considered, as well as more complex routing policies.

VII. ACKNOWLEDGEMENTS

This work has been partially funded by the internal competitive funding program "VALERE: VAnviteLli pEr la RicErca" of Università degli Studi della Campania "Luigi Vanvitelli" and by project "Attrazione e Mobilità dei Ricercatori" Italian PON Programme (PON_AIM 2018 num. AIM1878214-2).

References

[1] NS3. `https://www.nsnam.org/`. Accessed: 2019-06-03.

[2] Tcpdump. `https://www.tcpdump.org/`. Accessed: 2019-06-03.

[3] Wireshark. `https://www.wireshark.org/`. Accessed: 2019-06-03.

[4] M. Aazam and E.-N. Huh. Fog computing and smart gateway based communication for Cloud of Things. pages 464–470, 2014.

[5] N. Baldo and M. Miozzo. Spectrum-aware channel and phy layer modeling for ns3. In *Proceedings of the Fourth International ICST Conference on Performance Evaluation Methodologies and Tools*, VALUETOOLS '09, pages 2:1–2:8, ICST, Brussels, Belgium, Belgium, 2009. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[6] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni. Computer network simulation with ns-3: A systematic literature review. *Electronics*, 9(2):272, Feb 2020.

[7] G. Carneiro, P. Fortuna, and M. Ricardo. Flowmonitor - a network monitoring framework for the network simulator 3 (ns-3). ACM, 5 2010.

[8] G. Carneiro, P. Fortuna, and M. Ricardo. Flowmonitor - a network monitoring framework for the network simulator 3 (ns-3). ACM, 5 2010.

[9] E. Cavalieri d'Oro, S. Colombo, M. Gribaudo, M. Iacono, D. Manca, and P. Piazzolla. Modeling and evaluating a complex Edge computing based systems: An emergency management support system case study. *Internet of Things*, 6:100054, 2019.

[10] M. Chiang and T. Zhang. Fog and IoT: An overview of research opportunities. *IEEE Internet of Things Journal*, 3(6):854–864, Dec 2016.

[11] A. V. Dastjerdi and R. Buyya. Fog computing: Helping the Internet of Things realize its potential. *Computer*, 49(8):112–116, Aug 2016.

[12] M. Desertot, C. Escoffier, and D. Donsez. Towards an autonomic approach for edge computing: Research articles. *Concurr. Comput. : Pract. Exper.*, 19(14):1901–1916, Sept. 2007.

[13] C. Esposito, A. Castiglione, F. Pop, and K. K. R. Choo. Challenges of connecting Edge and Cloud computing: A security and forensic perspective. *IEEE Cloud Computing*, 4(2):13–17, March 2017.

[14] M. Ficco, C. Esposito, Y. Xiang, and F. Palmieri. Pseudo-dynamic testing of realistic Edge-Fog Cloud ecosystems. *IEEE Communications Magazine*, 55(11):98–104, Nov 2017.

[15] M. Hajibaba and S. Gorgin. A review on modern distributed computing paradigms: Cloud computing, Jungle computing and Fog computing. *Journal of Computing and Information Technology*, 22(2):69–84, 2014.

[16] Z. Hao, E. Novak, S. Yi, and Q. Li. Challenges and software architecture for Fog computing. *IEEE Internet Computing*, 21(2):44–53, Mar. 2017.

[17] M. B. A. Karim, B. I. Ismail, W. M. Tat, E. M. Goortani, S. Setapa, J. Y. Luke, and H. Ong. Extending Cloud resources to the Edge: Possible scenarios, challenges, and experiments. In *2016 International Conference on Cloud Computing Research and Innovations (ICCCRI)*, pages 78–85, May 2016.

[18] A. R. Khan, S. M. Bilal, and M. Othman. A performance comparison of open source network simulators for wireless networks. In *2012 IEEE International Conference on Control System, Computing and Engineering*, pages 34–38, Nov 2012.

[19] D. Magrin, D. Zhou, and M. Zorzi. A simulation execution manager for ns-3: Encouraging reproducibility and simplifying statistical analysis of ns-3 simulations. In *Proceedings of the 22nd International ACM Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, MSWIM '19, page 121–125, New York, NY, USA, 2019. Association for Computing Machinery.

[20] J. Oueis, E. Strinati, and S. Barbarossa. The Fog balancing: Load distribution for small cell Cloud computing. volume 2015, 2015.

[21] H. D. Park, O.-G. Min, and Y.-J. Lee. Scalable architecture for an automated surveillance system using Edge computing. *J. Supercomput.*, 73(3):926–939, Mar. 2017.

[22] G. F. Riley and T. R. Henderson. *The ns-3 Network Simulator*, pages 15–34. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[23] R. Roman, J. Lopez, and M. Mambo. Mobile Edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, 2016.

[24] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu. Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 3(5):637–646, Oct 2016.

[25] J. Shropshire. Extending the Cloud with Fog: Security challenges & opportunities. 2014.

[26] L. Vaquero and L. Rodero-Merino. Finding your way in the fog: Towards a comprehensive definition of fog computing. *Computer Communication Review*, 44(5):27–32, 2014.

[27] M. Villari, M. Fazio, S. Dustdar, O. Rana, and R. Ranjan. Osmotic computing: A new paradigm for Edge/Cloud integration. *IEEE Cloud Computing*, 3(6):76–83, Nov 2016.

[28] S. Yi, Z. Hao, Z. Qin, and Q. Li. Fog computing: Platform and applications. In *2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*, pages 73–78, Nov 2015.

[29] S. Yi, Z. Qin, and Q. Li. Security and privacy issues of fog computing: A survey. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9204:685–695, 2015.

AUTHOR BIOGRAPHIES

LELIO CAMPANILE is a PhD. student at Dipartimento di Matematica e Fisica, Università degli Studi della Campania "L. Vanvitelli", Caserta, Italy, where he has been a technician, a network administrator and an expert for many local and regional projects, and is a member of the Data and Computer Science group. He holds a M. Sc Degree in Computer Science. His email is lelio.campanile@unicampania.it.

MAURO IACONO is an Associate Professor in Computing Systems at Dipartimento di Matematica e Fisica, Università degli Studi della Campania "L. Vanvitelli", Caserta, Italy, where he leads the Computer Science section of the Data and Computer Science research group. His research activity is mainly centered on the field of performance modeling of complex computer-based systems, with a special attention for multiformalism modeling techniques. His email is mauro.iacono@unicampania.it. More information about his activities is available at his website http://www.mauroiacono.com.

FIAMMETTA MARULLI is an Assistant Professor in Computing Systems at Dipartimento di Matematica e Fisica, Università degli Studi della Campania "L. Vanvitelli", Caserta, Italy. She works in the Data and Computer Science research group. Her research interests lie in Cognitive Computing and Artificial Intelligence methodologies applied to Deep Neural Networks design for Natural Language Processing (NLP), Data Analytics and Cyber-Physical Systems Security (CPSS) applications. Her email is fiammetta.marulli@unicampania.it.

MICHELE MASTROIANNI is currently the Data Protection Officer of Università degli Studi della Campania "L. Vanvitelli", Caserta, Italy, and is also a research associate at Dipartimento di Matematica e Fisica of the same University, with the Data and Computer Science research group. He holds a M. Sc. degree in Electrical Engineering and a Ph.D. degree in Management Engineering, and has been Network Manager at the same University, project leader and expert for many local, regional and national technical projects. He also teaches Computer Science courses at Vanvitelli university. His email is michele.mastroianni@unicampania.it.