AI and Quality of Service Driven Attack Detection, Mitigation and Energy Optimization: A Review of Some EU Project Results

Mehmet Ufuk Çağlayan(✉)

Department of Computer Engineering, Yaşar University, Bornova, Izmir, Turkey
ufuk.caglayan@yasar.edu.tr

Abstract. This article summarizes briefly the contributions presented in this EuroCyberSecurity Workshop 2021 which is organized as part of the series of International Symposia on Computer and Information Sciences (ISCIS), with the support of the European Commission funded IoTAC Project, that was held on November and in NIce, France, and sponsored by the Institute of Teoretical and Applied Informatics of the Polish Academy of Sciences. It also summarizes some of the research contributions of several EU Projects including NEMESYS, GHOST, KONFIDO, SDK4ED and IoTAC, primarily with a cybersecurity and Machine Learning orientation. Thus subjects covered include the cybersecurity of Mobile Networks and of the Internet of Things (IoT), the design of IoT Gateways and their performance, the security of networked health systems that provide health services to individuals across the EU Member states, as well as the issues of energy consumption by ICT which are becoming increasingly important, including in the cybersecurity perspective, as we focus increasingly on climate change and the needed transition towards highly reduced emissions. Many of the techniques and results discussed in this article are based either on Machine Learning (ML) methods, or on methods for the performance modeling and optimization of networked and distributed computer systems.

Keywords: Internet of Things (IoT) · Cybersecurity · Secure mobile networks · IoT gateways · Secure health informatics · Attack detection · IoT massive access problem · Attack mitigation · Adaptive routing · ICT energy optimization

1 Introduction

The International Symposia on Computer and Information Sciences (ISCIS) were started in 1986 in Turkey by Erol Gelenbe, and held in Turkey, France, the USA, the UK, and Poland with proceedings [4,14–16,38,57,58,60,112] including a wide range of topics published by Springer.

E. Gelenbe et al. (Eds.): EuroCybersec 2021, CCIS 1596, pp. 1–12, 2022.
https://doi.org/10.1007/978-3-031-09357-9_1

This ISCIS CyberSecurity 2021 Symposium that was held in Nice, France, as part of this series, specializes for the second time on Cybersecurity following a previous event [45], which is my main research interest [6,21,90]. Indeed, Cybersecurity is at the forefront of serious technical issues in Computer Science as we transition to highly inter-dependent cyber-physical systems [76], and the European Union published its recommendation for security and privacy [22]. Furthermore, insecurity in systems and networks and the techniques that are used to defend our systems, are also increasing energy consumption in computer systems and network and their CO_2 impact, and the costs of operating them [27,46,86]. Hence energy consumption in mobile network has also received attention [3,42].

Thus the European Commission funded research projects in this field have significantly increased [1] over recent years and this introduction summarizes related research undertaken throughout Europe and includes five recent EC funded projects:

- NEMESYS on the cybersecurity of mobile telephone system [5,52,53,82,101],
- The project SDK4ED that mainly focused on energy savings [87,103] but also considered issues of Cybersecurity and Reliability [109].
- KONFIDO [17,18,96,97] on the security of communications and data transfers for interconnected European national or regional health services,
- GHOST [8,11] regarding the security of IoT systems for the home, and the design of secure IoT home gateways,
- SerIoT on the Cybersecurity of IoT systems [7,31] with a range of applications in supply chains, smart cities, smart manufacturing, and other areas.
- IoTAC, which aims at securing IoT networks by strengthening the protection of gateways using novel techniques such as Botnet detection, system wide vulnerability assessment [93,94], disruptive checkpoints, and assuring the optimization of the massive access to IoT gateways [67,75].

It also discusses some results from the SDK4ED project concerning the energy efficient handling of system reliability issues through checkpointing [107,108].

2 Improving the Security of Mobile Telephony

Cybersecurity of mobile telephony is a fundamental societal issue. The related problems are exacerbate by the fact that most mobile phones offer opportunistic connections [84,85] to WIFI and other wireless networks which are not part of the mobile operators' core infrastructure. This creates vulnerabilities that need to be monitored on the mobile device itself, which is the motivation for the work in [26,81].

On the other hand, the work described in [2,102], concerns a form of Distributed Denial of Service (DDoS) attacks on the signalling plane of the core mobile network which are caused by malicious software which is deposited in the mobile devices. Related work conducted within the EU NEMESYS project [41,43,83] using queueing theoretic methods [25,34].

Early work on DDoS Attacks [65] had proposed self-aware networks and the Cognitive Packet Network (CPN) [39,77,80] to detect and counter-attack against DDoS, by identifying sources of attacks by following upstream the attacking traffic, using CPN's ACK packets to "drop" attacking traffic at upstream routers [65,100]. It was also applied to mitigate worm attacks and to deviate user traffic so as to avoid insecure nodes [37,104,105]. Related issues include the management of keys [114,115], and the study and mitigation of signalling storms in mobile telephony [26,102].

3 Security of the Trans-European Health Informatics Network

Large numbers of travellers from one European country to another sometimes need to access health services in the country they are visiting. These health services are typically based on a national model, or a regional model inside a given country such as Italy. Thus the KONFIDO project addressed the important issue of providing a secure support to European health systems.

The corresponding informatics systems, with their patient data bases are also nationally or regionally based, so that when the medical practitioner in one country or region is required to diagnose and treat a visitor from some other region or country, she/he will need to access the patient's data remotely. KONFIDO's aim is to improve the cybersecurity of such systems, while improving also their inter-operability across countries and regions in Europe.

Thus the work in [111] presents an overall view and challenges of the project, while in [98] the authors present an analysis of the corresponding user requirements. Such systems have obvious performance optimization issues which are discussed in [72]. Keeping track of the transactions in such a system through blockchains is suggested in [9].

4 Contributions to the Security of the IoT

To exploit the value that the IoT generated provides requires the protection of privacy and in many cases data will have to be rendered strongly anonymous. It will also require specific security not just for the IoT devices and networks, but also for the IoT data repositories in the Cloud and their access networks. These aspects are complicated by the simplicity of many IoT devices which cannot be integrated in complex distributed communication infrastructures that would require communications to be synchronized or schedules [10,74].

Thus in [11] an overview of the principles and achievements of the GHOST project are presented, which started in May of 2017 and which ran for three years. The project addressed safe-guarding home IoT environments through appropriate software that can be installed on home IoT gateways, and it also creates a prototype and test-bed using specific equipment from the TELEVES company.

Related to this project, machine learning methods were developed for the detection of network attacks on IoT gateways [8] based on Deep Learning

[78,79,106] with the Random Neural Network [32,33,35,54] and its extensions [89]. Related to the GHOST project, other recent work discusses the effect and mitigation of attacks on the batteries which supply the power of many light-weight IoT network nodes [55].

The SerIoT project that was started in 2018 [19] also produced valuable results [48]. Its technical scope included SerCPN [29,30], a specific secure network [49] for managing geographically distributed IoT devices and services using the principles of the Cognitive Packet Network (CPN) tested in several experiments [28,59,61,62,64]. CPN uses "Smart" Packets (SPs) to search for paths and measure QoS while the network is in operation, via Reinforcement Learning using a Random Neural Network, and based on the QoS Goal pursued by the end user. When an SP reaches its destination, its measurements are returned by an ACK packet to the intermediate nodes of the path that was identified by the SP, and to the end user, providing the QoS offered by the path that the SP travelled. Source nodes receive ACKs and take the decision to switch to the path that offers the best security or quality of service [50,51,56,63].

Extensions with a genetic algorithm [36] was also tested [92]. An interesting development in SerIoT combines energy aware routing [40,66] and security, and admission control [73]. Adaptive techniques for wireless IoT traffic to achieve better QoS are also found in [68–70,99] and summarized in [20,91], while the RNN with adaptive approaches was shown to offer opportunities for massive video compression [12,13], as well as for managing Cloud servers [113]. Such adaptive techniques that support the interaction between security metrics, performance and energy consumption were also discussed in a paper in this volume [71].

The subsequent IoTAC project has lead to incremental techniques for learning from user traffic and then testing for an attack as described in [95]. In IoTAC, there was also substantial work on dealing with severe performance issues due to the large flows of IoT packets towards gateways from thousands of IoT devices, so that the resulting Massive Access Problem (MAP) has to be mitigated with novel traffic shaping techniques [47].

5 Conclusions

The existence of frequent and effective cyberattacks on public networks and information technology infrastructures motivates education and research on Cybersecurity. The field that started with the need to encrypt data and create secure systems through strong means for security such as passwords, authentication schemes, firewalls and cryptographic keys, has now substantially evolved towards the detection and mitigation of cyberattacks. In addition issues with respect to software's own specific vulnerabilities [23] and the need to detect and mitigate such properties has also become important [23,24,44,88,109,110].

Indeed, we now realize that hoping to use static means of defence in Cybersecurity is largely ineffective unless it is accompanied by real-time techniques that rapidly react to possible malicious actions or attempts to attack a system.

Thus the field of Cybersecurity research has now entered a far broader phase with much more substantial activity. Its support through several European Union

research programs demonstrates a new level of maturity that attempts to attain higher levels of performance and effectiveness through self-adaptation and system reconfiguration.

References

1. https://www.grantsoffice.com/Portals/0/funded/issues/FUNDEDOct2021.pdf
2. Abdelrahman, O.H., Gelenbe, E.: A data plane approach for detecting control plane anomalies in mobile networks. In: Mandler, B., et al. (eds.) IoT360 2015. LNICST, vol. 169, pp. 210–221. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47063-4_19
3. Abdelrahman, O.H., Gelenbe, E.: A diffusion model for energy harvesting sensor nodes. In: 2016 IEEE 24th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), pp. 154–158. IEEE (2016)
4. Abdelrahman, O.H., Gelenbe, E., Gorbil, G., Lent, R. (eds.): Information Sciences and Systems 2015. LNEE, vol. 363. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-22635-4
5. Abdelrahman, O.H., Gelenbe, E., Görbil, G., Oklander, B.: Mobile network anomaly detection and mitigation: the NEMESYS approach. In: Gelenbe, E., Lent, R. (eds.) Information Sciences and Systems 2013, pp. 429–438. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-01604-7_42
6. Akgün, M., Çaglayan, M.U.: Towards scalable identification in RFID systems. Wireless Pers. Commun. **86**(2), 403–421 (2016). https://doi.org/10.1007/s11277-015-2936-7
7. Baldini, G., et al.: IoT network risk assessment and mitigation: the SerIoT approach (2020)
8. Brun, O., Yin, Y., Gelenbe, E.: Deep learning with dense random neural network for detecting attacks against IoT-connected home environments. Procedia Comput. Sci. **134**, 458–463 (2018)
9. Castaldo, L., Cinque, V.: Blockchain-based logging for the cross-border exchange of eHealth data in Europe. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 46–56. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-95189-8_5
10. Chesnais, A., Gelenbe, E., Mitrani, I.: On the modeling of parallel access to shared data. Commun. ACM **26**(3), 196–202 (1983)
11. Collen, A., et al.: GHOST - safe-guarding home IoT environments with personalised real-time risk control. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 68–78. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-95189-8_7
12. Cramer, C., Gelenbe, E., Bakircloglu, H.: Low bit-rate video compression with neural networks and temporal subsampling. Proc. IEEE **84**(10), 1529–1543 (1996)
13. Cramer, C.E., Gelenbe, E.: Video quality and traffic QoS in learning-based subsampled and receiver-interpolated video sequences. IEEE J. Sel. Areas Commun. **18**(2), 150–167 (2000)
14. Czachórski, T., Gelenbe, E., Grochla, K., Lent, R. (eds.): ISCIS 2016. CCIS, vol. 659. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47217-1
15. Czachórski, T., Gelenbe, E., Grochla, K., Lent, R. (eds.): ISCIS 2018. CCIS, vol. 935. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-00840-6

16. Czachórski, T., Gelenbe, E., Lent, R. (eds.): Information Sciences and Systems 2014. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-09465-6
17. Diamantopoulos, S., et al.: Secure cross-border exchange of health related data: the KONFIDO approach. In: Montella, R., Ciaramella, A., Fortino, G., Guerrieri, A., Liotta, A. (eds.) IDCS 2019. LNCS, vol. 11874, pp. 318–327. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34914-1_30
18. Diamantopoulos, S., et al.: Secure cross-border exchange of health related data: the KONFIDO approach. In: EDCC, pp. 73–74. IEEE (2019)
19. Domanska, J., Gelenbe, E., Czachorski, T., Drosou, A., Tzovaras, D.: Research and innovation action for the security of the internet of things: the SerIoT project. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 101–118. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-95189-8_10
20. Du, J., Jiang, C., Gelenbe, E., Zhang, H., Ren, Y.: Traffic offloading in software defined ultra-dense networks. In: Ultra-Dense Networks: Principles and Applications, p. 164 (2020)
21. Ermis, O., Bahtiyar, S., Anarim, E., Çaglayan, M.U.: A key agreement protocol with partial backward confidentiality. Comput. Netw. **129**, 159–177 (2017). https://doi.org/10.1016/j.comnet.2017.09.008
22. European Commission: Cybersecurity Policies. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies
23. Filus, K., Boryszko, P., Domańska, J., Siavvas, M., Gelenbe, E.: Efficient feature selection for static analysis vulnerability prediction. Sensors **21**, 1113 (2021). https://doi.org/10.3390/s21041133
24. Filus, K., Siavvas, M., Domańska, J., Gelenbe, E.: The random neural network as a bonding model for software vulnerability prediction. In: Calzarossa, M.C., Gelenbe, E., Grochla, K., Lent, R., Czachórski, T. (eds.) MASCOTS 2020. LNCS, vol. 12527, pp. 102–116. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-68110-4_7
25. Fourneau, J.M., Gelenbe, E., Suros, R.: G-networks with multiple classes of negative and positive customers. Theoret. Comput. Sci. **155**(1), 141–156 (1996)
26. Francois, F., Abdelrahman, O.H., Gelenbe, E.: Feasibility of signaling storms in 3G/UMTS operational networks. In: Mandler, B., et al. (eds.) IoT360 2015. LNICST, vol. 169, pp. 187–198. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47063-4_17
27. Francois, F., Abdelrahman, O.H., Gelenbe, E.: Towards assessment of energy consumption and latency of LTE UES during signaling storms. In: Abdelrahman, O.H., Gelenbe, E., Gorbil, G., Lent, R. (eds.) Information Sciences and Systems 2015. LNEE, vol. 363, pp. 45–55. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-22635-4_4
28. Francois, F., Gelenbe, E.: Optimizing secure SDN-enabled inter-data centre overlay networks through cognitive routing. In: 2016 IEEE 24th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS), pp. 283–288. IEEE (2016)
29. Fröhlich, P., Gelenbe, E., Fiołka, J., Checinski, J., Nowak, M., Filus, Z.: Smart SDN management of fog services to optimize QoS and energy. Sensors **21**, 3105 (2021). https://doi.org/10.3390/s21093105
30. Rutkowski, L., Scherer, R., Korytkowski, M., Pedrycz, W., Tadeusiewicz, R., Zurada, J.M. (eds.): ICAISC 2020. LNCS (LNAI), vol. 12415. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-61401-0

31. Frötscher, A., Monschiebl, B., Drosou, A., Gelenbe, E., Reed, M.J., Al-Naday, M.: Improve cybersecurity of c-its road side infrastructure installations: the SerIoT-secure and safe IoT approach. In: 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE), pp. 1–5. IEEE (2019)
32. Gelenbe, E.: Random neural networks with negative and positive signals and product form solution. Neural Comput. **1**(4), 502–510 (1989)
33. Gelenbe, E.: Stability of the random neural network model. Neural Comput. **2**(2), 239–247 (1990)
34. Gelenbe, E.: G-networks with signals and batch removal. Probab. Eng. Inf. Sci. **7**(3), 335–342 (1993)
35. Gelenbe, E.: Learning in the recurrent random neural network. Neural Comput. **5**(1), 154–164 (1993)
36. Gelenbe, E.: Genetic algorithms with analytical solution. In: Proceedings of the 1st Annual Conference on Genetic Programming, pp. 437–443. MIT Press (1996)
37. Gelenbe, E.: Dealing with software viruses: a biological paradigm. Inf. Secur. Tech. Rep. **12**(4), 242–250 (2007)
38. Gelenbe, E.: The 24th International Symposium on Computer and Information Sciences, ISCIS 2009, 14–16 September 2009. IEEE (2009)
39. Gelenbe, E.: Steps toward self-aware networks. Commun. ACM **52**(7), 66–75 (2009)
40. Gelenbe, E.: Energy packet networks: ICT based energy allocation and storage. In: Rodrigues, J.J.P.C., Zhou, L., Chen, M., Kailas, A. (eds.) GreeNets 2011. LNICST, vol. 51, pp. 186–195. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-33368-2_16
41. Gelenbe, E., Abdelrahman, O.H.: Countering mobile signaling storms with counters. In: Mandler, B., et al. (eds.) IoT360 2015. LNICST, vol. 169, pp. 199–209. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47063-4_18
42. Gelenbe, E., Abdelrahman, O.H.: An energy packet network model for mobile networks with energy harvesting. Nonlinear Theory Its Appl. IEICE **9**(3), 1–15 (2018) https://doi.org/10.1587/nolta.9.1
43. Gelenbe, E., Abdelrahman, O.H., Gorbil, G.: Detection and mitigation of signaling storms in mobile networks. In: 2016 International Conference on Computing, Networking and Communications (ICNC), pp. 1–5. IEEE (2016)
44. Gelenbe, E., Boryszko, P., Siavvas, M., Domanska, J.: Optimum checkpoints for time and energy. In: 2020 28th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), pp. 1–8. IEEE (2020)
45. Gelenbe, E., et al. (eds.): Euro-CYBERSEC 2018. CCIS, vol. 821. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-95189-8
46. Gelenbe, E., Caseau, Y.: The impact of information technology on energy consumption and carbon emissions. Ubiquity **2015**, 1–15 (2015)
47. Gelenbe, E., Czachorski, T., Marek, D., Nakıp, M.: Mitigating the massive access problem in the internet of things. In: Gelenbe, E., et al. (Eds.) EuroCybersec 2021, CCIS 1596, pp. 118–132. Springer, Cham (2022)
48. Gelenbe, E., Domanska, J., Czachorski, T., Drosou, A., Tzovaras, D.: Security for internet of things: the SerIoT project. In: Proceedings of the International Symposium on Networks, Computers and Communications. IEEE, June 2018
49. Gelenbe, E., Domanska, J., Frohlich, P., Nowak, M., Nowak, S.: Self-aware networks that optimize security, QoS and energy. Proc. IEEE **108**(7), 1150–1167 (2020)

50. Gelenbe, E., Gellman, M.: Can routing oscillations be good? The benefits of route-switching in self-aware networks. In: 2007 15th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, pp. 343–352. IEEE (2007)
51. Gelenbe, E., Gellman, M.: Oscillations in a bio-inspired routing algorithm. In: 2007 IEEE International Conference on Mobile Adhoc and Sensor Systems, pp. 1–7. IEEE (2007)
52. Gelenbe, E., et al.: NEMESYS: enhanced network security for seamless service provisioning in the smart mobile ecosystem. In: Gelenbe, E., Lent, R. (eds.) Information Sciences and Systems 2013, pp. 369–378. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-01604-7_36
53. Gelenbe, E., et al.: Security for smart mobile networks: the NEMESYS approach. In: 2013 International Conference on Privacy and Security in Mobile Systems (PRISMS), pp. 1–8. IEEE (2013)
54. Gelenbe, E., Hussain, K.F.: Learning in the multiple class random neural network. IEEE Trans. Neural Networks **13**(6), 1257–1267 (2002)
55. Gelenbe, E., Kadioglu, Y.M.: Energy life-time of wireless nodes with network attacks and mitigation. In: Proceedings of ICC 2018, 20–24 May 2018, W04: IEEE Workshop on Energy Harvesting Wireless Communications. IEEE (2018)
56. Gelenbe, E., Lent, R.: Power-aware ad hoc cognitive packet networks. Ad Hoc Netw. **2**(3), 205–216 (2004)
57. Gelenbe, E., Lent, R. (eds.): Computer and Information Sciences III - 27th International Symposium on Computer and Information Sciences, Paris, France, 3–4 October 2012. Springer, London (2013). https://doi.org/10.1007/978-1-4471-4594-3
58. Gelenbe, E., Lent, R. (eds.): Information Sciences and Systems 2013 - Proceedings of the 28th International Symposium on Computer and Information Sciences, ISCIS 2013, Paris, France, 28–29 October 2013, Lecture Notes in Electrical Engineering, vol. 264. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-01604-7
59. Gelenbe, E., Lent, R., Montuori, A., Xu, Z.: Cognitive packet networks: QoS and performance. In: 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, MASCOTS 2002, Proceedings, pp. 3–9. IEEE (2002)
60. Gelenbe, E., Lent, R., Sakellari, G., Sacan, A., Toroslu, I.H., Yazici, A.: Computer and Information Sciences - Proceedings of the 25th International Symposium on Computer and Information Sciences, London, UK, 22–24 September 2010. LNEE, vol. 62. Springer, Dordrecht (2010). https://doi.org/10.1007/978-90-481-9794-1
61. Gelenbe, E., Lent, R., Xu, Z.: Design and performance of cognitive packet networks. Perform. Eval. **46**(2), 155–176 (2001)
62. Gelenbe, E., Lent, R., Xu, Z.: Measurement and performance of a cognitive packet network. Comput. Netw. **37**(6), 691–701 (2001)
63. Gelenbe, E., Lent, R., Xu, Z.: Towards networks with cognitive packets. In: Goto, K., Hasegawa, T., Takagi, H., Takahashi, Y. (eds.) Performance and QoS of Next Generation Networking, pp. 3–17. Springer, London (2001). https://doi.org/10.1007/978-1-4471-0705-7_1
64. Gelenbe, E., Liu, P.: QoS and routing in the cognitive packet network. In: Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, WoWMoM 2005, pp. 517–521. IEEE (2005)
65. Gelenbe, E., Loukas, G.: A self-aware approach to denial of service defence. Comput. Netw. **51**(5), 1299–1314 (2007)

66. Gelenbe, E., Mahmoodi, T.: Distributed energy-aware routing protocol. In: Gelenbe, E., Lent, R., Sakellari, G. (eds.) Computer and Information Sciences II, pp. 149–154. Springer, London (2011). https://doi.org/10.1007/978-1-4471-2155-8_18
67. Gelenbe, E., Nakip, M., Marek, D., Czachorski, T.: Diffusion analysis improves scalability of IoT networks to mitigate the massive access problem. In: IEEE MASCOTS 2021: 29th International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems, pp. 1–6 (2021). https://zenodo.org/record/5501822#.YT3bri8itmA
68. Gelenbe, E., Ngai, E.C.H.: Adaptive QoS routing for significant events in wireless sensor networks. In: 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2008, pp. 410–415. IEEE (2008)
69. Gelenbe, E., Ngai, E.C.: Adaptive random re-routing in sensor networks. In: Proceedings of the Annual Conference of ITA (ACITA 2008), 16–18 September, pp. 348–349 (2008)
70. Gelenbe, E., Ngai, E.C., Yadav, P.: Routing of high-priority packets in wireless sensor networks. In: IEEE Second International Conference on Computer and Network Technology. IEEE (2010)
71. Gelenbe, E., Nowak, M.P., Frohlich, P., Fiolka, J., Checinski, J.: Energy, QoS and security aware services at the edge. In: Gelenbe, E., et al. (Eds.) EuroCybersec 2021, CCIS 1596, pp. 102–117. Springer, Cham (2022)
72. Gelenbe, E., Pavloski, M.: Performance of a security control scheme for a health data exchange system. In: IEEE International Black Sea Conference on Communications and Networking, 26–29 May 2020, Virtual Conference (2020)
73. Gelenbe, E., Sakellari, G., D'arienzo, M.: Admission of QoS aware users in a smart network. ACM Trans. Auton. Adapt. Syst. (TAAS) **3**(1), 4 (2008)
74. Gelenbe, E., Sevcik, K.: Analysis of update synchronization for multiple copy data bases. IEEE Trans. Comput. **10**, 737–747 (1979)
75. Gelenbe, E., Sigman, K.: IoT traffic shaping and the massive access problem. In: ICC 2022, IEEE International Conference on Communications, Seoul, South Korea, 16–20 May 2022, pp. 1–6 (2022). https://zenodo.org/record/5918301#.YgaCP
76. Gelenbe, E., Wu, F.J.: Future research on cyber-physical emergency management systems. Future Internet **5**(3), 336–354 (2013)
77. Gelenbe, E., Xu, Z., Seref, E.: Cognitive packet networks. In: 11th IEEE International Conference on Conference Tools with Artificial Intelligence, Proceedings, pp. 47–54. Publisher IEEE (1999)
78. Gelenbe, E., Yin, Y.: Deep learning with random neural networks. In: 2016 International Joint Conference on Neural Networks (IJCNN), pp. 1633–1638. IEEE (2016)
79. Gelenbe, E., Yin, Y.: Deep learning with dense random neural networks. In: Gruca, A., Czachórski, T., Harezlak, K., Kozielski, S., Piotrowska, A. (eds.) ICMMI 2017. AISC, vol. 659, pp. 3–18. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-67792-7_1
80. Gelenbe, S.E.: Cognitive packet network, uS Patent 6,804,201, 12 October 2004
81. Gorbil, G., Abdelrahman, O.H., Gelenbe, E.: Modeling and analysis of RRC-based signaling storms in 3G networks. IEEE Trans. Emerg. Top. Comput., 14 (2015). Special Issue on Emerging Topics in Cyber Security
82. Gorbil, G., Abdelrahman, O.H., Pavloski, M., Gelenbe, E.: Storms in mobile networks. arXiv preprint arXiv:1411.1280 (2014)

83. Gorbil, G., Abdelrahman, O.H., Pavloski, M., Gelenbe, E.: Modeling and analysis of RRC-based signalling storms in 3G networks. IEEE Trans. Emerg. Top. Comput. **4**(1), 113–127 (2016)
84. Gorbil, G., Gelenbe, E.: Opportunistic communications for emergency support systems. Procedia Comput. Sci. **5**, 39–47 (2011)
85. Gorbil, G., Gelenbe, E.: Resilience and security of opportunistic communications for emergency evacuation. In: Proceedings of the 7th ACM Workshop on Performance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks, pp. 115–124 (2012)
86. Jiang, H., Liu, F., Thulasiram, R.K., Gelenbe, E.: Guest editorial: special issue on green pervasive and ubiquitous systems. IEEE Syst. J. **11**(2), 806–812 (2017). https://doi.org/10.1109/JSYST.2017.2673218
87. Kadioglu, Y.M., Gelenbe, E.: Product-form solution for cascade networks with intermittent energy. IEEE Syst. J. **13**(1), 918–927 (2019)
88. Kehagias, D., Jankovic, M., Siavvas, M., Gelenbe, E.: Investigating the interaction between energy consumption, quality of service, reliability, security, and maintainability of computer systems and networks. SN Comput. Sci. **2**(1), 1–6 (2021)
89. Konar, D., Gelenbe, E., Bhandary, S., Sarma, A.D., Cangi, A.: Random quantum neural networks (RQNN) for noisy image recognition. CoRR abs/2203.01764 (2022)
90. Levi, A., Çaglayan, M.U., Koç, Ç.K.: Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure. ACM Trans. Inf. Syst. Secur. **7**(1), 21–59 (2004). https://doi.org/10.1145/984334.984336
91. Li, N., Hu, X., Ngai, E., Gelenbe, E.: Cooperative wireless edges with composite resource allocation in hierarchical networks. In: 2020 IEEE International Conference on E-Health Networking, Application & Services (HEALTHCOM), pp. 1–6 (2021). https://doi.org/10.1109/HEALTHCOM49281.2021.9398997
92. Liu, P., Gelenbe, E.: Recursive routing in the cognitive packet network. In: 3rd International Conference on Testbeds and Research Infrastructure for the Development of Networks and Communities, TridentCom 2007, pp. 1–6. IEEE (2007)
93. Nakip, M., Gelenbe, E.: MIRAI botnet attack detection with auto-associative dense random neural networks. In: 2021 IEEE Global Communications Conference, vol. 2021, pp. 1–6. IEEE Communications Society (2021)
94. Nakip, M., Gelenbe, E.: Randomization of data generation times improves performance of predictive IoT networks. In: IEEE World Forum on Internet of Things (WF IoT), 14–21 July 2021, p. 5161 (2021). https://wfiot2021.iot.ieee.org
95. Nakip, M., Gelenbe, E.: Botnet attack detection with incremental online learning. In: In: Gelenbe, E., et al. (Eds.) EuroCybersec 2021, CCIS 1596, pp. 51–60. Springer, Cham (2022)
96. Nalin, M., et al.: The European cross-border health data exchange roadmap: case study in the Italian setting. J. Biomed. Inform. **94**, 103183 (2019)
97. Natsiavas, P., et al.: Developing an infrastructure for secure patient summary exchange in the EU context: lessons learned from the KONFIDO project. Health Inform. J. **27**(2) (2021). 14604582211021460
98. Natsiavas, P., et al.: Comprehensive user requirements engineering methodology for secure and interoperable health data exchange. BMC Med. Inform. Decis. Mak. **18**(1), 1–16 (2018)
99. Ngai, E.C., Gelenbe, E., Humber, G.: Information-aware traffic reduction for wireless sensor networks. In: IEEE 34th Conference on Local Computer Networks, LCN 2009, pp. 451–458. IEEE (2009)

100. Oke, G., Loukas, G., Gelenbe, E.: Detecting denial of service attacks with Bayesian classifiers and the random neural network. In: IEEE International Fuzzy Systems Conference, FUZZ-IEEE 2007, pp. 1–6. IEEE (2007)
101. Pavloski, M., Gelenbe, E.: Mitigating for signalling attacks in UMTS networks. In: Czachórski, T., Gelenbe, E., Lent, R. (eds.) Information Sciences and Systems 2014, pp. 159–165. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-09465-6_17
102. Pavloski, M., Görbil, G., Gelenbe, E.: Bandwidth usage—based detection of signaling attacks. In: Abdelrahman, O.H., Gelenbe, E., Gorbil, G., Lent, R. (eds.) Information Sciences and Systems 2015. LNEE, vol. 363, pp. 105–114. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-22635-4_9
103. Pernici, B., Aiello, M., Vom Brocke, J., Donnellan, B., Gelenbe, E., Kretsis, M.: What is can do for environmental sustainability: a report from CAiSE? 11 panel on green and sustainable is. Commun. Assoc. Inf. Syst. **30**(1), 18 (2012)
104. Sakellari, G., Gelenbe, E.: Adaptive resilience of the cognitive packet network in the presence of network worms. In: Proceedings of the NATO Symposium on C3I for Crisis, Emergency and Consequence Management, pp. 11–12 (2009)
105. Sakellari, G., Hey, L., Gelenbe, E.: Adaptability and failure resilience of the cognitive packet network. In: DemoSession of the 27th IEEE Conference on Computer Communications (INFOCOM2008), Phoenix, Arizona, USA (2008)
106. Serrano, W., Gelenbe, E., Yin, Y.: The random neural network with deep learning clusters in smart search. Neurocomputing **396**, 394–405 (2020)
107. Siavvas, M., et al.: An empirical evaluation of the relationship between technical debt and software security. In: ICIST 2019 Proceedings, vol. 1, pp. 199–203 (2019)
108. Siavvas, M., Gelenbe, E.: Optimum checkpoints for programs with loops. Simul. Model. Pract. Theory **97** (2019)
109. Siavvas, M., Gelenbe, E.: Optimum interval for application-level checkpoints. In: 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 145–150. IEEE (2019)
110. Siavvas, M., Kehagias, D., Tzovaras, D., Gelenbe, E.: A hierarchical model for quantifying software security based on static analysis alerts and software metrics. Software Qual. J. **29**(2), 431–507 (2021). https://doi.org/10.1007/s11219-021-09555-0
111. Staffa, M., et al.: An openNCP-based solution for secure eHealth data exchange. J. Netw. Comput. Appl. **116**, 65–85 (2018)
112. Tugcu, T., Caglayan, M.U., Alagoz, F., Gelenbe, E.: New Trends in Computer Networks: 20th International Symposium on Computer and Information Sciences. World Scientific, September 2005. https://doi.org/10.1142/p415
113. Wang, L., Gelenbe, E.: Adaptive dispatching of tasks in the cloud. IEEE Trans. Cloud Comput. **6**(1), 33–45 (2018)
114. Yu, C., Ni, G., Chen, I., Gelenbe, E., Kuo, S.: Top-k query result completeness verification in tiered sensor networks. IEEE Trans. Inf. Forensics Secur. **9**(1), 109–124 (2014). https://doi.org/10.1109/TIFS.2013.2291326
115. Yu, C.M., Ni, G.K., Chen, Y., Gelenbe, E., Kuo, S.Y.: Top-k query result completeness verification in sensor networks. In: 2013 IEEE International Conference on Communications Workshops (ICC), pp. 1026–1030. IEEE (2013)