Some Current Cybersecurity Research in Europe

Mehmet Ufuk Çağlayan(✉)

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

Abstract. We present a brief summary of the papers that were presented at the Security Workshop 2018 of the International Symposium on Computer and Information Sciences (ISCIS) that was held on February 26, 2018 at Imperial College, London. These papers are primarily based on several research projects funded by the European Commission. The subjects that are covered include the cybersecurity of the Internet of Things (IoT), the security of networked health systems that are used to provide health services, the security of mobile telephony, and the security of software itself. The papers include overall presentations project objectives, plans and achievements, and their specific research findings.

Keywords: Cybersecurity · European Commission · E-health
User requirements · Cryptography · IoT · Network attacks
Attack detection · Random Neural Network · System reliability
Cognitive Packet Routing · Block-chains

1 Introduction

The International Symposia on Computer and Information Sciences (ISCIS) were started by Erol Gelenbe in 1986 in Turkey, and over the years they have been held in Turkey, France, the USA, the UK, and Poland. Examples of ISCIS proceedings [3,13,14,40,41,44,45], include research on a wide range of topics in Computer Science and Engineering, and have typically been published by Springer Verlag in recent years. This first ISCIS 2018 Symposium breaks the tradition and for the first time specializes on Cybersecurity, which has been my own major area of research for many years [5,18,69].

Cybersecurity has now come to the forefront of our interests and concern in Computer Science and Engineering, and in 2017 the European Union published its recommendation for security and privacy. In addition, both the lack of security and the techniques used to defend networks increase the energy consumption in computer systems and networks [34], resulting in an increase of their CO^2 impact and of their operating costs [20,34,67]. Thus the number of research projects funded by the European Commission in this field has significantly increased, and these Proceedings [23] present some of the current trends and outcomes of this research.

E. Gelenbe et al. (Eds.): Euro-CYBERSEC 2018, CCIS 821, pp. 1–10, 2018.
https://doi.org/10.1007/978-3-319-95189-8_1

These Proceedings contain a series of papers regarding research undertaken throughout Europe on Cybersecurity, including five recent projects funded by the European Commission:

- KONFIDO on the security of communications and data transfers for interconnected European national or regional health services,
- GHOST regarding the security of IoT systems for the home, and the design of secure IoT home gateways,
- SerIoT on the Cybersecurity of IoT systems in general with a range of applications in supply chains, smart cities, and other areas,
- NEMESYS concerning the security of mobile networks, and
- SDK4ED concerning the optimisation of software for energy consumption, security and computation time.

It also includes research results from the previous NEMESYS project [4,36,37] and the new SDK4ED project of the European Commission. This symposium's main organiser developed early work on Distributed Denial of Service (DDoS) Attacks [51] and proposed to use the Cognitive Packet Network routing protocol (CPN) [43] as a way to detect DDoS, counter-attack by tracing the attacking traffic upstream, and to use CPN's ACK packets to give "drop orders" to upstream routers that convey the attack [51,73]. This approach was evaluated to detect worm attacks and to forward the users' traffic on routes avoiding infected nodes [77,78], and continued with the study of software viruses [28], the security of cyber-physical systems [1,6,15,29,31,60], the management of cryptographic keys [83,84], and also on control plane attacks on mobile networks [2,65].

2 Security of the Trans-European Health Informatics Network

The first set of papers in this volume emanate from the KONFIDO project which addresses the important issue of providing a secure support to European health systems.

Indeed, 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.

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 [80] presents an overall view and challenges of the project, while in [71] the authors present an analysis of the corresponding user requirements. Such systems have obvious ethics and privacy constraints which are discussed in [19].

A specific physics based technique for generating unique keys for the encryption needs for such systems is discussed in [7]. Keeping track of the transactions in such a system through blockchains is suggested in [10].

3 Contributions to the Security of the IoT

The first paper in the second group of papers concerning the IoT, examines the creation of markets which can exploit the value that the IoT generated provides [66]. Obviously, this will require the protection of privacy and will need that the data 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.

The second paper [11] is an overview of the principles and current achievements of the GHOST project which started in May of 2017 and which runs for three years. The project addresses 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 that is coordinating the project.

Related to this project, another paper uses machine learning methods for the detection of network attacks on IoT gateways [9] based on Deep Learning [61] with the Random Neural Network [12,25,26]. Related to the GHOST project, other recent work published elsewhere, discusses the effect and mitigation of attacks on the batteries which supply the power of many light-weight IoT network nodes [38].

The following paper, also emanating from the GHOST project, discusses the use of novel blockchain techniques to enhance the security of IoT systems [68].

The final paper in this section is a description of the new SerIoT project that was started in 2018 [17]. Further details regarding this project can be found in a forthcoming paper [35]. Among its technical objectives is the design of SerCPN [16], a specific network for managing geographically distributed IoT devices using the principles of the Cognitive Packet Network (CPN) and using Software Defined Neyworks that has been tested in several experiments [42,43,46,47,49]. CPN uses "Smart" Packets (SPs) to search [1] for paths and measure QoS while the network is in operation, via Reinforcement Learning using a Random Neural Network [24], 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. The end user, which may be a source node or a decision making software package for a QoS Class, receives many such ACKs and takes the decision to switch to the one offering the best security or quality of service, or to stay with the current path [30,39,48]. An extension using genetic algorithms [27,50] was implemented [70], a version for overlay networks [8] and a related system for Cloud computing [81,82] were also tested.

An interesting development in SerIoT will combine energy aware routing [52,53] and security in a Software Defined Network (SDN) approach [21,22,32].

It could also address admission control [58] as a means to improve security. Adaptive techniques for the management of wireless IoT device traffic to achieve better QoS will also be used by SerIoT [54–56,72].

4 Improving the Security of Mobile Telephony

The final two papers in this volume address the cybersecurity of mobile telephony. Many mobile phones also offer opportunistic connections [64] to WIFI and other wireless networks. This creates vulnerabilities that need to be constantly monitored on the mobile device itself, which is the motivations for the work in [62] which investigates machine learning techniques to this effect.

On the other hand, the work described in [74] is a comprehensive review of the work of the author and of his colleagues [63], regarding attacks on the signalling plane of the core network of the mobile network operator, and especially the mitigation of such attacks. This work was conducted in the context of the European Commission funded project NEMESYS [75,76] and makes extensive use of methods from the theory of Queueing Networks [57].

5 Conclusions

The reality of diverse, numerous and powerful cyber attacks has allowed the field of Cybersecurity to transition from an area concerned primarily with cryptography and the management of cryptographic keys, to a far broader field concerned with all forms of attacks on our cyber-infrastructure. These developments are illustrated by the diversity of the research and contributions presented in this volume. Subtending all these issues is the security of the software modules that we use in all the systems we develop and use. Thus the final paper in this volume relates to a static analysis approach to test and verify the security of software [79] which emanates from the European Commission's funded SDK4ED research project. An important area that is left out of this volume concerns the integrated security of physical and cyber systems [33,59].

We believe that the field has entered a new phase of substantial activity, and its support through funding from the European Commission illustrates the importance and vigour of European Research in Cybersecurity.

References

1. Abdelrahman, O.H., Gelenbe, E.: Time and energy in team-based search. Phys. Rev. E **87**(3), 032125 (2013)
2. Abdelrahman, O.H., Gelenbe, E.: Signalling storms in 3G mobile networks. In: IEEE International Conference on Communications, ICC 2014, Sydney, Australia, 10–14 June 2014, pp. 1017–1022. IEEE (2014). https://doi.org/10.1109/ICC.2014.6883453

3. Abdelrahman, O.H., Gelenbe, E., Görbil, G., Lent, R. (eds.): Information Sciences and Systems 2015. LNEE, vol. 363. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-319-22635-4
4. 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. LNEE, vol. 264, pp. 429–438. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-01604-7_42
5. Akgün, M., Çaglayan, M.U.: Towards scalable identification in RFID systems. Wirel. Pers. Commun. **86**(2), 403–421 (2016). https://doi.org/10.1007/s11277-015-2936-7
6. Akinwande, O.J., Bi, H., Gelenbe, E.: Managing crowds in hazards with dynamic grouping. IEEE Access **3**, 1060–1070 (2015)
7. Akriotou, M., et al.: Random number generation from a secure photonic physical unclonable hardware module. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 28–37. Springer, Heidelberg (2018)
8. Brun, O., Wang, L., Gelenbe, E.: Big data for autonomic intercontinental communications. IEEE Trans. Sel. Areas Commun. **34**(3), 575–583 (2016)
9. Brun, O., et al.: Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 79–89. Springer, Heidelberg (2018)
10. 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, Heidelberg (2018)
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, Heidelberg (2018)
12. 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)
13. Czachórski, T., Gelenbe, E., Grochla, K., Lent, R. (eds.): Computer and Information Sciences. CCIS, vol. 659. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-47217-1
14. 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
15. Desmet, A., Gelenbe, E.: Graph and analytical models for emergency evacuation. In: 2013 IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM 2013 Workshops, San Diego, CA, USA, March 18–22, 2013, pp. 523–527 (2013). https://doi.org/10.1109/PerComW.2013.6529552
16. Domanska, J., Czachòrski, T., Nowak, M., Nowak, S., Gelenbe, E.: Sercpn: smart software defined network for IoT (2018, to appear)
17. 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, Heidelberg (2018)
18. 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
19. Faiella, G., et al.: Building an ethical framework for cross-border applications: the KONFIDO project. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 38–45. Springer, Heidelberg (2018)

20. François, F., Abdelrahman, O.H., Gelenbe, E.: Impact of signaling storms on energy consumption and latency of LTE user equipment. In: 17th IEEE International Conference on High Performance Computing and Communications, HPCC 2015, 7th IEEE International Symposium on Cyberspace Safety and Security, CSS 2015, and 12th IEEE International Conference on Embedded Software and Systems, ICESS 2015, New York, NY, USA, 24–26 August 2015, pp. 1248–1255 (2015). https://doi.org/10.1109/HPCC-CSS-ICESS.2015.84
21. François, F., Gelenbe, E.: Optimizing secure SDN-enabled inter-data centre overlay networks through cognitive routing. In: 24th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, MASCOTS 2016, London, United Kingdom, 19–21 September 2016, pp. 283–288 (2016). https://doi.org/10.1109/MASCOTS.2016.26
22. François, F., Gelenbe, E.: Towards a cognitive routing engine for software defined networks. In: 2016 IEEE International Conference on Communications, ICC 2016, Kuala Lumpur, Malaysia, 22–27 May 2016, pp. 1–6 (2016). https://doi.org/10.1109/ICC.2016.7511138
23. Gelenbe, E., Campegiani, P., Czachorski, T., Katsikas, S., Komnios, I., Romano, L., Tzovaras, D. (eds.): Proceedings of the Security Workshop: Recent Cybersecurity Research in Europe. Lecture Notes CCIS. Springer, Berlin (2018)
24. Gelenbe, E.: Random neural networks with negative and positive signals and product form solution. Neural Comput. **1**(4), 502–510 (1989)
25. Gelenbe, E.: Réseaux neuronaux aléatoires stables. Comptes Rendus de l'Académie des sciences. Série 2 **310**(3), 177–180 (1990)
26. Gelenbe, E.: Learning in the recurrent random neural network. Neural Comput. **5**(1), 154–164 (1993)
27. Gelenbe, E.: Genetic algorithms with analytical solution. In: Proceedings of the 1st Annual Conference on Genetic Programming, pp. 437–443. MIT Press (1996)
28. Gelenbe, E.: Dealing with software viruses: a biological paradigm. Inf. Secur. Techn. Rep. **12**(4), 242–250 (2007)
29. Gelenbe, E.: Steady-state solution of probabilistic gene regulatory networks. Phys. Rev. E **76**(1), 031903 (2007)
30. Gelenbe, E.: Steps toward self-aware networks. Commun. ACM **52**(7), 66–75 (2009)
31. Gelenbe, E.: Search in unknown random environments. Phys. Rev. E **82**(6), 061112 (2010)
32. Gelenbe, E.: A software defined self-aware network: the cognitive packet network. In: IEEE 3rd Symposium on Network Cloud Computing and Applications, NCCA 2014, Rome, Italy, 5–7 February 2014, pp. 9–14 (2014). https://doi.org/10.1109/NCCA.2014.9
33. Gelenbe, E., Bi, H.: Emergency navigation without an infrastructure. Sensors **14**(8), 15142–15162 (2014)
34. Gelenbe, E., Caseau, Y.: The impact of information technology on energy consumption and carbon emissions. Ubiquity **2015**(June), 1 (2015)
35. 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
36. Gelenbe, E., Görbil, G., Tzovaras, D., Liebergeld, S., Garcia, D., Baltatu, M., Lyberopoulos, G.: NEMESYS: enhanced network security for seamless service provisioning in the smart mobile ecosystem. In: Gelenbe, E., Lent, R. (eds.) Information Sciences and Systems 2013. LNEE, pp. 369–378. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-01604-7_36

37. Gelenbe, E., Gorbil, G., Tzovaras, D., Liebergeld, S., Garcia, D., Baltatu, M., Lyberopoulos, G.: 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)
38. Gelenbe, E., Kadioglu, Y.M.: Energy life-time of wireless nodes with network attacks and mitigation. In: Proceedings of W04: IEEE Workshop on Energy Harvesting Wireless Communications. ICC 2018, 20–24 May 2018. IEEE (2018)
39. Gelenbe, E., Lent, R.: Power-aware ad hoc cognitive packet networks. Ad Hoc Netw. **2**(3), 205–216 (2004)
40. Gelenbe, E., Lent, R. (eds.): Computer and Information Sciences III. Springer, Cham (2013). https://doi.org/10.1007/978-1-4471-4594-3
41. Gelenbe, E., Lent, R. (eds.): Information Sciences and Systems 2013, vol. 264. Springer, Cham (2013). https://doi.org/10.1007/978-1-4471-4594-3
42. Gelenbe, E., Lent, R., Montuori, A., Xu, Z.: Cognitive packet networks: QoS and performance. In: Proceedings of 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, MASCOTS 2002, pp. 3–9. IEEE (2002)
43. Gelenbe, E., Lent, R., Nunez, A.: Self-aware networks and QoS. Proc. IEEE **92**(9), 1478–1489 (2004)
44. Gelenbe, E., Lent, R., Sakellari, G. (eds.): Computer and Information Sciences II. Springer, Cham (2011). https://doi.org/10.1007/978-1-4471-2155-8
45. Gelenbe, E., Lent, R., Sakellari, G., Sacan, A., Toroslu, I.H., Yazici, A. (eds.): Computer and Information Sciences. LNEE, vol. 62. Springer, Cham (2010). https://doi.org/10.1007/978-90-481-9794-1
46. Gelenbe, E., Lent, R., Xu, Z.: Design and performance of cognitive packet networks. Perform. Evol. **46**(2), 155–176 (2001)
47. Gelenbe, E., Lent, R., Xu, Z.: Measurement and performance of a cognitive packet network. Comput. Netw. **37**(6), 691–701 (2001)
48. 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, Heidelberg (2001). https://doi.org/10.1007/978-1-4471-0705-7_1
49. Gelenbe, E., Liu, P.: Qos and routing in the cognitive packet network. In: Sixth IEEE International Symposium on World of Wireless Mobile and Multimedia Networks, WoWMoM 2005, pp. 517–521. IEEE (2005)
50. Gelenbe, E., Liu, P., Laine, J.: Genetic algorithms for route discovery. IEEE Trans. Syst. Man Cybern. Part B (Cybern.) **36**(6), 1247–1254 (2006)
51. Gelenbe, E., Loukas, G.: A self-aware approach to denial of service defence. Comput. Netw. **51**(5), 1299–1314 (2007)
52. Gelenbe, E., Mahmoodi, T.: Energy-aware routing in the cognitive packet network. In: ENERGY, pp. 7–12 (2011)
53. 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
54. 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)
55. Gelenbe, E., Ngai, E.C.: Adaptive random re-routing in sensor networks. In: Proceedings of the Annual Conference of ITA (ACITA08), 16–18 September 2008, pp. 348–349 (2008)

56. Gelenbe, E., Ngai, E.C., Yadav, P.: Routing of high-priority packets in wireless sensor networks. IEEE Second International Conference on Computer and Network Technology. IEEE (2010)
57. Gelenbe, E., Pujolle, G.: Introduction aux réseaux de files d'attente. Edition Hommes et Techniques et Techniques, Eyrolles (1982)
58. Gelenbe, E., Sakellari, G., D'arienzo, M.: Admission of QoS aware users in a smart network. ACM Trans. Auton. Adapt. Syst. **3**(1), 4 (2008)
59. Gelenbe, E., Wu, F.J.: Large scale simulation for human evacuation and rescue. Comput. Math. Appl. **64**(12), 3869–3880 (2012)
60. Gelenbe, E., Wu, F.J.: Future research on cyber-physical emergency management systems. Future Internet **5**(3), 336–354 (2013)
61. Gelenbe, E., Yin, Y.: Deep learning with random neural networks. In: Bi, Y., Kapoor, S., Bhatia, R. (eds.) IntelliSys 2016. LNNS, vol. 16, pp. 450–462. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-56991-8_34
62. Geneiatakis, D., Baldini, G., Fovino, I.N., Vakalis, I.: Towards a mobile malware detection framework with the support of machine learning. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 119–129. Springer, Heidelberg (2018)
63. Gorbil, G., Abdelrahman, A.H., Pavloski, M., Gelenbe, E.: Modeling and analysis of RRC-based signaling storms in 3G networks. IEEE Trans. Emerg. Topics Comput. 4, 113–127 (2016)
64. Gorbil, G., Gelenbe, E.: Opportunistic communications for emergency support systems. Procedia Comput. Sci. **5**, 39–47 (2011)
65. Görbil, G., Abdelrahman, O.H., Gelenbe, E.: Storms in mobile networks. In: Mueller, P., Foschini, L., Yu, R. (eds.) Q2SWinet'14, Proceedings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks, Montreal, QC, Canada, September 21–22, 2014, pp. 119–126. ACM (2014). https://doi.org/10.1145/2642687.2642688
66. Horváth, M., Buttyán, L.: Problem domain analysis of IoT-driven secure data markets. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 57–67. Springer, Heidelberg (2018)
67. 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
68. Kouzinopoulos, C.S., et al.: Using blockchains to strengthen the security of internet of things. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 90–100. Springer, Heidelberg (2018)
69. 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
70. Liu, P., Gelenbe, E.: Recursive routing in the cognitive packet network. In: TridentCom 2007 3rd International Conference on Testbeds and Research Infrastructure for the Development of Networks and Communities, pp. 1–6. IEEE (2007)
71. Natsiavas, P., et al.: User requirements elicitation for secure and interoperable health data exchange. In: Gelenbe, E., et al. (eds.) Recent Cybersecurity Research in Europe. CCIS, vol. 821. Springer, Berlin (2018)
72. 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)

73. Oke, G., Loukas, G., Gelenbe, E.: Detecting denial of service attacks with Bayesian classifiers and the random neural network. In: IEEE International Conference on Fuzzy Systems Conference, FUZZ-IEEE 2007, pp. 1–6. IEEE (2007)
74. Pavloski, M.: Signalling attacks in mobile telephony. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 130–141. Springer, Heidelberg (2018)
75. 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
76. Pavloski, M., Gelenbe, E.: Signaling attacks in mobile telephony. In: SECRYPT 2014 - Proceedings of the 11th International Conference on Security and Cryptography, Vienna, Austria, 28–30 August 2014, pp. 206–212 (2014). https://doi.org/10.5220/0005019802060212
77. 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)
78. Sakellari, G., Hey, L., Gelenbe, E.: Adaptability and failure resilience of the cognitive packet network. DemoSession of the 27th IEEE Conference on Computer Communications (INFOCOM2008), Phoenix, Arizona, USA (2008)
79. Siavvas, M., Gelenbe, E., Kehagias, D., Tzovaras, D.: Static analysis-based approaches for secure software development. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 142–157. Springer, Heidelberg (2018)
80. Staffa, M., et al.: Konfido: An openncp-based secure ehealth data exchange system. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 11–27. Springer, Heidelberg (2018)
81. Wang, L., Brun, O., Gelenbe, E.: Adaptive workload distribution for local and remote clouds. In: 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 003984–003988. IEEE (2016)
82. Wang, L., Gelenbe, E.: Adaptive dispatching of tasks in the cloud. IEEE Trans. Cloud Comput. **6**(1), 33–45 (2018)
83. 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
84. 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)