European Cybersecurity Research and the SerIoT Project

Joanna Domańska, Mateusz Nowak, Sawomir Nowak, and Tadeusz Czachórski(✉)

IITIS Polish Academy of Science, Gliwice, Poland
tadek@iitis.pl

Abstract. This paper briefly reviews some recent research in Cybersecurity in Europe funded by the European Commission in areas such as mobile telephony, networked health systems, the Internet of Things. We then outline the objectives of the SerIoT Project which started in 2018 to address the security needs of fields such as Smart Cities, Smart Transportation Systems, Supply Chains and Industrial Informatics.

Keywords: Cybersecurity · European Commission · E-Health
Smart Cities · IoT · Network attacks · Random Neural Network
Cognitive packet routing

1 Introduction

Viewed for a long time as a peripheral issue, Cybersecurity is now at the forefront of everyday computer system and network operations, and of research in Computer Science and Engineering. Indeed cyberattacks, even when they are detected and mitigated, have a very large cost to systems operations including the degradation of the commercial image or trust of the and in 2017 the European Union published its recommendation for security and privacy. In addition, the organisations that operate systems that come under cyberattack can not only lose market share and lose the trust of the end users, but they also have to increase their operating costs both in terms of means to defend themselves but also in increased energy consumption and operating costs [31] and CO^2 impact [17,60].

The SerIoT Project [14] finds its origins in early work started over a decade ago on Distributed Denial of Service (DDoS) Attacks [25,44] and on using routing with the Cognitive Packet Network protocol (CPN) [38] to detect DDoS, and trace the attacking traffic so as to use CPN's ACK packets to drop the attacking traffic packets at upstream routers that carry the attacking traffic, and also detect worm attacks [65,69–71]. More recently, the EU FP7 Project NEMESYS [3,33,34] provided the opportunity to examine the cybersecurity of mobile networks including the control plane which is used to establish and keep track of calls. Since the control plane is a critical element that enables the mobile network to function, some attacks aim in particular at this part of the system [2,58].

T. Czachórski et al. (Eds.): ISCIS 2018, CCIS 935, pp. 166–173, 2018.
https://doi.org/10.1007/978-3-030-00840-6_19

Further work on the security of cyber-physical systems has considered vulnerabilities that address the physical infrastructure, the decision algorithms that manage the system when it operates normally or under threat, and the communication system used to convey data, information and commands between different system components [1,4,12,26,28,53].

2 European Research in Cybersecurity in Recent Years

In [20], some recent research on cybersecurity in Europe has been summarised regarding the several projects funded by the European Commission. A core issue that diffuses through all layers of information technology concerns cybersecurity for mobile telephony. Because most modern mobile phones offer opportunistic access [57] to WIFI and other wireless networks, the resulting security vulnerabilities should be constantly monitored both at the network and control plane levels, and in the mobile device. Thus recent [55] has investigated the use of neural network and machine learning methods to discuss this issue. The research in [56,66], addresses attacks that manipulate the signalling plane of the backbone network and directly concerns the mobile network operator as well as the end user, and the project NEMESYS addressed many of these issues [67,68] using techniques from Queuing Theory [11,49].

KONFIDO [73] concentrates on the security of communications and data transfers for interconnected European national or regional health services. Since travellers from European countries must often access health services in another European country, the health informatics systems will have to access remote patient data in a secure manner [73] and the related technical and ethical issues are addressed in a series of recent papers [5,8,16].

The GHOST project [9] addresses security in the IoT system market [59] for homes, and focuses on the design of a secure home IoT gateway including the attack detection techniques [7], and the analysis of attack methods that try to bring down the energy supply of the devices by draining their batteries [35]. The detection techniques that are proposed are based on Deep Learning [54] and recurrent Random Neural Neworks [22,23] that have been used previously in a variety of applications [10,51]. GHOST also investigates blockchain based methods to track and improve the security of the home IoT system [61].

3 The SerIoT Project

The SerIoT project started in January of 2018 [14], and further details regarding can also be found in a forthcoming paper [32]. The project's Technical Objectives include means to understand the threats to a IoT based economy and understand how distributed ledgers (Blockchain) may improve IoT based systems. It will design and implement virtualised self-aware honeypots to attract and analyse attacks.

The project will design SerCPN [13], a network that manages specific distributed IoT devices based on the Cognitive Packet Network (CPN). It will use the implementation of Software Defined Networks (SDN) based on CPN [18,19,29] using measurements that create the system self-awareness [37–40,42]. These SDNs will use "Smart" Packets (SP) to search [1,27] for secure multi-hop routes having good quality of service (QoS) and measure their security and performance, and will use Reinforcement Learning with Random Neural Networks [21] to improve the network overall performance, including all three criteria of high security, good QoS and low energy consumption [36,41]. It may be possible to extend these schemes with genetic algorithms which use an analogy between network paths and genotypes [24,43,63]. Several SerCPN network clusters may be interconnected via end overlay network [6], with adaptive connections to Cloud and Fog servers [74,75] for network data analysis and visualisation.

Combining energy aware routing and QoS [45,46] with security, we can also address network admission [50] to enhance security. Wireless IoT device traffic may also be specifically monitored and adaptively routed in a similar manner as it accesses SerCPN [47,48,64].

The project will deliver a number of platforms that comprise the main technical outputs of the project, including Platforms for (i) IoT Data Acquisition, (ii) Ad-hoc Anomaly Detection, (iii) Interactive Visual Analytics and Decision Support Tools, and (iv) Mitigation and Counteraction that will orchestrate, synchronise and implement the decisions taken by the various components.

4 SerIoT: Use Cases and Future Work of the Project

The SerIoT project's outcomes will be evaluated in a number of significant use cases. These include four main areas. The first one is Surveillance, where physical security in bus depots will be monitored through the infrastructure of OASA which is the largest transport authority in Greece. The second one involves Intelligent Transport Systems in Smart Cities, in particular in areas such as collision avoidance, where we will demonstrate how SerIoT can enhance the cybersecurity of such systems with infrastructures proveded by OASA, Austria-Tech (ATECH), and TECNALIA for vehicle safety. The third use case will involve Flexible Manufacturing Systems (Industry 4.0), which will monitor physical attacks to wireless sensor networks in Industry 4.0 with the help of DT/T-Sys., for situations related to automated warehouses where different attack vectors may be used for breaking or jamming communication lines. The fourth use case will address Food Chains which require end-to-end security through multiple communication channels, including device authentication, detection and avoidance of DDoS and replication attacks, and detection of functionality anomalies and disabling of IoT devices. In the food chain, IoT devices may be critical to notify perishability of food items that use visually readable labels by IoT devices to trigger indicators for shop managers and customers, offering "on board sensing and communications" for food. This Use Case will be supported by third parties. We take into account diverse, numerous and powerful cyber attacks.

Thus the confrontation in SerIoT of the physical world with issues of Cybersecurity, creates a rich opportunity to move forward from traditional work in this area that focuses on cryptography and the management of cryptographic keys [15,62,76,77], or the security of software [72] and physical structures [30,52], to broad issues regarding security and system efficiency in the presence of cyberattacks to the integrated cyber and physical infrastructure.

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., 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 International Publishing, Cham (2013)
4. Akinwande, O.J., Bi, H., Gelenbe, E.: Managing crowds in hazards with dynamic grouping. IEEE Access **3**, 1060–1070 (2015)
5. Akriotou, M., Mesaritakis, C., Grivas, E., Chaintoutis, C., Fragkos, A., Syvridis, D.: Random number generation from a secure photonic physical unclonable hardware module. In: Gelenbe, E., et al. (eds.) Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop. CCIS, vol. 821. Springer, Cham (2018)
6. Brun, O., Wang, L., Gelenbe, E.: Big data for autonomic intercontinental communications. IEEE Trans. Sel. Areas Commun. **34**(3), 575–583 (2016)
7. Brun, O., Yin, Y., Gelenbe, E., Kadioglu, Y.M., Augusto-Gonzalez, J., Ramos, M.: Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments. In: Gelenbe, E. (ed.) Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop. CCIS, vol. 821. Springer, Cham (2018)
8. Castaldo, L., Cinque, V.: Blockchain based logging for the cross-border exchange of ehealth data in Europe. Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop. CCIS, vol. 821. Springer, Cham (2018)
9. Collen, A., et al.: Ghost - safe-guarding home IoT environments with personalised real-time risk control. In: Gelenbe, E., et al. (eds.) Recent Cyber security Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Communications in Computer and Information Science, vol. 821. Springer, Cham (2018)
10. 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)
11. Czachórski, T., Gelenbe, E., Lent, R.: Information Sciences and Systems. Springer International Publishing, Cham (2014)
12. 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, 18–22 March 2013, pp. 523–527 (2013). https://doi.org/10.1109/PerComW.2013.6529552

13. Domanska, J., Czachòrski, T., Nowak, M., Nowak, S., Gelenbe, E.: Sercpn: smart software defined network for IoT (2018). (To appear)
14. 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. (eds.) Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Communications in Computer and Information Science, vol. 821. Springer, Cham (2018)
15. 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
16. Faiella, G., et al.: Building an ethical framework for cross-border applications: the konfido project. In: Gelenbe, E., et al. (eds.) Recent Cyber security Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Communications in Computer and Information Science, vol. 821. Springer, Cham (2018)
17. 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 Aug 2015, pp. 1248–1255 (2015). https://doi.org/10.1109/HPCC-CSS-ICESS.2015.84
18. 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 Sept 2016, pp. 283–288 (2016). https://doi.org/10.1109/MASCOTS.2016.26
19. 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
20. Gelenbe, E. et al. (eds.): Proceedings of the 2018 ISCIS Security Workshop: Recent Cybersecurity Research in Europe, vol. 821. Lecture Notes CCIS, Springer (2018)
21. Gelenbe, E.: Random neural networks with negative and positive signals and product form solution. Neural Comput. **1**(4), 502–510 (1989)
22. Gelenbe, E.: Réseaux neuronaux aléatoires stables. Comptes Rendus de l'Académie des sciences. Série 2 **310**(3), 177–180 (1990)
23. Gelenbe, E.: Learning in the recurrent random neural network. Neural Comput. **5**(1), 154–164 (1993)
24. Gelenbe, E.: Genetic algorithms with analytical solution. In: Proceedings of the 1st Annual Conference on Genetic Programming, pp. 437–443. MIT Press (1996)
25. Gelenbe, E.: Dealing with software viruses: a biological paradigm. Inf. Sec. Tech. Rep. **12**(4), 242–250 (2007)
26. Gelenbe, E.: Steady-state solution of probabilistic gene regulatory networks. Phys. Rev. E **76**(1), 031903 (2007)
27. Gelenbe, E.: Steps toward self-aware networks. Commun. ACM **52**(7), 66–75 (2009)
28. Gelenbe, E.: Search in unknown random environments. Phys. Rev. E **82**, 061112 (2010)
29. 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 Feb 2014, pp. 9–14 (2014). https://doi.org/10.1109/NCCA.2014.9

30. Gelenbe, E., Bi, H.: Emergency navigation without an infrastructure. Sensors **14**(8), 15142–15162 (2014)
31. Gelenbe, E., Caseau, Y.: The impact of information technology on energy consumption and carbon emissions. Ubiquity **2015**(June), 1 (2015)
32. 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 (2018)
33. 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. Lecture Notes in Electrical Engineering, vol 264. Springer International Publishing, Cham (2013)
34. 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)
35. 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
36. Gelenbe, E., Lent, R.: Power-aware ad hoc cognitive packet networks. Ad Hoc Netw. **2**(3), 205–216 (2004)
37. 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)
38. Gelenbe, E., Lent, R., Nunez, A.: Self-aware networks and qos. Proc. IEEE **92**(9), 1478–1489 (2004)
39. Gelenbe, E., Lent, R., Xu, Z.: Design and performance of cognitive packet networks. Perform. Eval. **46**(2), 155–176 (2001)
40. Gelenbe, E., Lent, R., Xu, Z.: Measurement and performance of a cognitive packet network. Comput. Netw. **37**(6), 691–701 (2001)
41. 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, Cham (2001)
42. 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)
43. Gelenbe, E., Liu, P., Laine, J.: Genetic algorithms for route discovery. IEEE Trans. Syst. Man Cybern. Part B (Cybernetics) **36**(6), 1247–1254 (2006)
44. Gelenbe, E., Loukas, G.: A self-aware approach to denial of service defence. Comput. Netw. **51**(5), 1299–1314 (2007)
45. Gelenbe, E., Mahmoodi, T.: Energy-aware routing in the cognitive packet network. Energy, pp. 7–12 (2011)
46. Gelenbe, E., Mahmoodi, T.: Distributed energy-aware routing protocol. In: Computer and Information Sciences II, pp. 149–154. Springer, London (2012)
47. 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, 2008. MASS 2008, pp. 410–415. IEEE (2008)
48. 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)

49. Gelenbe, E., Pujolle, G.: Introduction aux réseaux de files d'attente. Edition Hommes et Techniques et Techniques, Eyrolles (1982)
50. 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)
51. Gelenbe, E., Sungur, M., Cramer, C., Gelenbe, P.: Traffic and video quality with adaptive neural compression. Multimed. Syst. **4**(6), 357–369 (1996). https://doi.org/10.1007/s005300050037
52. Gelenbe, E., Wu, F.J.: Large scale simulation for human evacuation and rescue. Comput. Math. Appl. **64**(12), 3869–3880 (2012)
53. Gelenbe, E., Wu, F.J.: Future research on cyber-physical emergency management systems. Future Internet **5**(3), 336–354 (2013)
54. Gelenbe, E., Yin, Y.: Deep learning with random neural networks. In: 2016 International Joint Conference on Neural Networks (IJCNN). IEEE, July 2016
55. 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.) Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Lecture Notes CCIS, vol. 821, Springer (2018)
56. 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**(1), 113–127 (2016)
57. Gorbil, G., Gelenbe, E.: Opportunistic communications for emergency support systems. Procedia Comput. Sci. **5**, 39–47 (2011)
58. 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
59. Horváth, M., Buttyán, L.: Problem domain analysis of iot-driven secure data markets. In: Gelenbe, E. et al., (eds.) Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Lecture Notes CCIS, vol. 821, Springer (2018)
60. 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
61. Kouzinopoulos, C.S. et al.: Using blockchains to strengthen the security of internet of things. In: Gelenbe, E. et al., (eds.) Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Lecture Notes CCIS. vol. 821, Springer (2018)
62. 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
63. 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, 2007. TridentCom 2007, pp. 1–6. IEEE (2007)
64. Ngai, E.C., Gelenbe, E., Humber, G.: Information-aware traffic reduction for wireless sensor networks. In: IEEE 34th Conference on Local Computer Networks, 2009. LCN 2009, pp. 451–458. IEEE (2009)

65. 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, 2007. FUZZ-IEEE 2007, pp. 1–6. IEEE (2007)
66. Pavloski, M.: Signalling attacks in mobile telephony. In: Gelenbe, E. et al., (eds.) Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Lecture Notes CCIS No. 821, Springer (2018)
67. Pavloski, M., Gelenbe, E.: Mitigating for signalling attacks in umts networks. In: Information Sciences and Systems 2014, pp. 159–165. Springer International Publishing (2014)
68. 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
69. 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)
70. Sakellari, G., Gelenbe, E.: Demonstrating cognitive packet network resilience to worm attacks. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, pp. 636–638. ACM (2010)
71. Sakellari, G., Hey, L., Gelenbe, E.: Adaptability and failure resilience of the cognitive packet network. In: Demo Session of the 27th IEEE Conference on Computer Communications (INFOCOM2008), Phoenix, Arizona, USA (2008)
72. Siavvas, M., Gelenbe, E., Kehagias, D., Tzovaras, D.: Static analysis-based approaches for secure software development. In: Gelenbe, E. et al., (eds.) Proceedings of the 2018 ISCIS Security Workshop: Recent Cybersecurity Research in Europe. vol. 821. Lecture Notes CCIS, Springer (2018)
73. Staffa, M. et al.: An openncp-based secure ehealth data exchange system. In: Gelenbe, E. et al., (eds.) Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Lecture Notes CCIS No. 821, Springer (2018)
74. 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)
75. Wang, L., Gelenbe, E.: Adaptive dispatching of tasks in the cloud. IEEE Trans. Cloud Comput. **6**(1), 33–45 (2018)
76. 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
77. 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)