Review of Some Recent European Cybersecurity Research and Innovation Projects

Mehmet Ufuk Çağlayan

Abstract—**This paper reviews research from several EU Projects that have addressed cybersecurity using techniques based on Machine Learning, including the security of Mobile Networks and the Internet of Things (IoT). These research projects have considered IoT Gateways and their design, security and performance, the security of digital health systems that are interconnected across Europe to provide health services to pople who travel through the EU, and related issues of the energy consumption and sustainability in Information and Communication Technologies (ICT) and their cybersecurity. The methods used in much of these research projects are based on Machine Learning both for attack detection and dynamic attack mitigation, as well as performance analysis and measurement techniques based on applied probability models.**

Index Terms—**Cybersecurity, Secure Mobile Networks, Machine Learning, IoT Gateways, Secure Health Informatics, Attack Detection, Cyber-Attack Mitigation, IoT Massive Access Problem, Adaptive Network Routing, ICT Sustainability.**

I. INTRODUCTION

Cybersecurity has substantially grown as a research area due to the massive growth of cyberattacks, the increasing interest in the IoT and cyber-physical systems [13], [14], and the European Union's recommendations with regard to security and privacy [15], which is our main area of research interest [10]–[12]. Even when they are unsuccessful, cyberattacks and the additional software needed to offer better security, create additional costs including increased energy consumption in computer systems and network and the resulting greenhouse gases (GHG) [16]–[19]. Hence energy consumption in mobile networks in the presence of attacks has also received attention [20], [21].

Thus several of the International Symposia on Computer and Information Sciences (ISCIS), that were held in Turkey, France, the USA, the UK, and Poland [1]–[8] have covered this important area over more than a decade. Most recently, the ISCIS CyberSecurity 2021 Symposium presented a summary of the work in several projects funded by the European Commision, just as the previous event [9],

The European Commission has funded an increasing number of research and innovation projects on cybersecurity that we will summarize in this paper, namely:

- NEMESYS on the cybersecurity of mobile telephone system [22]–[26],
- The project SDK4ED that mainly focused on energy savings [27], [28] but also considered issues of Cybersecurity and Reliability [29].
- KONFIDO [30]–[33] on the security of communications and data transfers for interconnected European national or regional health services,
- GHOST [34], [35] regarding the security of IoT systems for the home, and the design of secure IoT home gateways,
- SerIoT on the Cybersecurity of IoT systems [36], [37] with a range of applications in supply chains, smart cities, smart manufacturing, and other areas.
- IoTAC, which secures IoT networks by strengthening the protection of gateways and developing techniques such as Botnet detection, system wide vulnerability assessement [38], [39], and the optimization of the massive access to IoT gateways [40], [41].

Much of this research uses principles of probabilistic computing [42]–[46] due to the probabilistic and random nature of attacks themselves. Indeed cyberattacks occur at unpredictable instants, and themselves attempt to hide their own intentions by using random behaviours. It also discusses some results from the SDK4ED project concerning the energy efficient handling of system reliability issues through checkpointing [47], [48].

II. IMPROVING THE SECURITY OF MOBILE TELEPHONY

Cybersecurity of mobile telephony is a fundamental societal issue. The related problems are axacerbated by the fact that most mobile phones offer opportunistic connections [49], [50] 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 [51], [52].

On the other hand, the work described in [53], [54], concerns a form of Distributed Denial of Sevrice (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 witin the EU NEMESYS project [55]–[57] using queueing theoretic methods [58], [59].

Early work on DDoS Attacks [60] had proposed self-aware networks and the Cognitive Packet Network (CPN) [61]–[64] to detect and couter-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 [60], [65]. It was also applied to mitigate worm attacks and to deviate user traffic so as to avoid insecure nodes [66]–[68]. Related issues include the management of keys [69], [70], and the study and mitigation of signalling storms in mobile telephony [52], [53].

The author is with the Department of Computer Engineering, Yaşar University, Bornova, Izmir, Turkey. (E-mail: ufuk.caglayan@yasar.edu.tr) ORCID: 0000-0001-9688-2201

DOI: 10.36244/ICJ.2022.4.10

III. 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 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 [71] presents an overall view and challenges of the project, while in [72] the authors present an analysis of the corresponding user requirements. Such systems have obvious performance optimization issues which are discussed in [73]. Keeping track of the transactions in such a system through blockchains is suggested in [74].

IV. 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 [75], [76].

The Internet of Things (IoT) and its related software systems [77] are rapidly proliferating as their applications expand, with reports [78] indicating that 52% of IoT devices will be low-cost low-maintenance devices that can only perform one task at a time, and unable to handle the types of complex real-time algorithms that are neeed to detect, block and mitigate cyberattacks. Improving the security of cyberphysical systems via systematic approaches have been suggested [79], [80], but industry confirms that it is difficult to load simple IoT devices with foolproof security capabilities [81]. Thus such devices and their wired and wireless interconnections are vulnerable to attacks [82]–[84] such as Denial of Service (DoS) which represent some 20% of IoT attacks [85], where malicious devices generate usless requests that impede normal operation and saturate limited resources, and may also add malware [86], [87].

A single Distributed DoS (DDoS) attack can compromise thousands of devices [88] through Botnets where victims themselves join the attack by being turned into "bots" [89]. An example is the 2016 massive "Mirai" attack that brought down the Domain Name System (DNS) Dyn [90], and blocked access to Netflix, Reddit, Spotify, and Twitter [91], [92] , accessing the equipment of major cybersecurity providers [93], and also congesting IoT and IP networks [94]. Thus as soon as a Botnet attempts an attack, it is crucial to detect it, if possible block it, and especially avoid its propagation and proliferation.

Thus much work has been devoted to what we may call "the first stage" which is essentially comprised of attack detection. The characteristics of Botnet attacks have been analyzed [95], and in [90] capabilities of Mirai has been examined, while in [96] its source code has also been studied, others have suggested that blockchains can be used to protect [97] and much work has involved machine learning models to detect attacks such as KNN, Support Vector Machines (SVM), Decision Trees (DT) and MLP [98], Classification and Regression Trees (CART) [99]; DT, Gradient Boosting and Random Forests [100], Logistic Regression [101] and their comparative performance Tuan et al. [102] . Botnet attack detection via neural networks was also considered [103], [104] including with the and Naive Bayesian Models [105], the LSTM [106], and Convolutional Networks (CNN) [107], also combined with LSTM [108]. In [109] Botnet attacks were detected via a sparse representation framework with a large number of inputs using only normal non-attack traffic as in [110] that uses auto-associative learning with a variant of the Random Neural Network [111] adapted for deep learning [112] that was initially designed for image recognition [113]. The RNN was already used successfully to detect SYN attacks [35] and extended to a wide variety of attacks in [114], based on the function approximation capabilities of the RNN [115].

Thus in [34] 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 [116] based on Deep Learning [117]–[119] with the Random Neural Network [120]–[123] and its extensions [124].

A. Attacks on Battery Power

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 [125], [126].

To this effect much research has been devoted to creating viable mathematical models of sensors that incorporate both the data collection, processing and transmission role of sensors, and their consumption of energy from batteries [127]. Computational techniques for large scale system analysis, including both communication or computational steps and energy consumption have also been developed [128].

Important results have been obtained in this respect in our ability to analyze and predict the life-time of sensors with rgard to their available battery power under different assumptions regarding renewable bu unpredictable random source of energy such as photovoltaic, the normal energy consumption of the device, and the impact of attacks that tend

to deplete energy through spurious and undesired processing and transmission on the part of the sensor [129]–[134].

V. THE SERIOT PROJECT

The SerIoT project was started in 2018 [135] and produced important results [136]–[138], [138]–[140]. These have been summarized in a brief article recently published by the EU CORDIS web site [141] under the title "Getting more *intelligent* about Internet security," which we reproduce below.

"Cognitive packets of internet information could revolutionise cybersecurity. Rerouting themselves dynamically and with great agility, they can avoid security threats or breaches in the network.

Most of us are highly aware of the need to protect our personal data on the internet ? our email accounts, bank accounts, health information and so much more. As we rapidly move to the Internet of things (IoT), the "things" requiring protection range from home ovens to sophisticated industrial tools, self-driving cars and remotely operated surgical equipment. Underlying these and more, including military communications and defence, is the electric power grid. Current internet protection is primarily static, detecting and blocking portions of an IoT system under attack but not rerouting information intelligently and avoiding glitches or worse. The EU-funded SerIoT project has delivered an unprecedented adaptive and intelligent solution by the same name. It will ensure IoT networks safely continue business as usual regardless of network conditions.

IoT networks connect sensors and actuators related to a physical system like a factory, vehicle or smart grid with software systems that control the system?s functions. Conventional networks use hardware like routers and switches to direct network traffic. SerIoT relies on cognitive intelligent control based on random neural networks and implements the controls through software-defined networking (SDN). SDN uses software-based technologies to control routers and direct network traffic in the form of internet packets, or blocks of information. This also enables flexible and dynamic configuration of "virtual networks" from physical ones depending on needs at the time. SerIoT added to this flexibility by integrating AI into the packets themselves, creating a patented cognitive packet network (CPN) ... SerIoT introduced self-awareness into SDN through a CPN in which the packets route themselves adaptively via SDN controllers with integrated AI. Attack and security detectors support rerouting of traffic to avoid items or areas that may be insecure due to threats or attacks. Each cognitive packet is thus self-aware, adaptive and intelligent, reacting not only to security issues but also network congestion or changes in energy consumption to improve the IoT system's or network's performance. The background and description of the practical working system have been published."

Wesummarize that SerIoT not only allows the IoT system to operate normally while under attack, but even at such times it saves energy and optimises performance. It can be installed in existing SDN technology, allowing the approach to be ported to many unforeseen applications. SerIoT moves the field of cybersecurity from the static mentality to an active, highly mobile, agile and adaptive system that not only defends against cyberattacks but moves critical traffic away from attack paths ... The (project's) large-scale pilots, including with project partner Deutsche Telecom, targeted the smart grid, which uses the IoT extensively, exploiting smart meters to optimise electricity production and distribution. Smart vehicles and Industry 4.0 robots were also tested. SerIoT is available for demonstration and beta testing by commercial partners and is being exploited in the ongoing Horizon 2020 IOTAC project. SerIoT will ensure that global IoT traffic agilely detours around malicious and natural obstacles large and small, for business as usual."

A. SerIoT Technical Scope

Its technical scope included SerCPN [137], [142], a specific secure network [143] for managing geographically distributed IoT devices and services using the principles of the Cognitive Packet Network (CPN) tested in several experiments [144]–[148]. 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 [149]–[152].

Extensions with a genetic algorithm [153] was also also tested [154]. An interesting development in SerIoT combines energy aware routing [155], [156] and security, and admission control [157].

Adaptive techniques for wireless IoT traffic to achieve better QoS are also found in [158]–[161] and summarized in [162]–[164], [164]–[168], while the RNN with adaptive approaches was shown to offer opportunities for massive video compression [169], [170], as well as for managing Cloud servers [171]. Such adaptive techniques that support the interaction between security metrics, performance and energy consumption were also discussed in a recent paper [172].

B. Energy Aspects

The energy aspects of system performance are also of great interests, and go beyond the questions regarding the energy supplied by batteries. Software systems themselves have to be designed with energy optimization being kept in mind [173].

Similarly it is important to be able to share energy flows between subsystems so that their workload is provisioned in a manner that matches the load on each subsystem [174], [175].

C. System Dynamics

Whenever adaptive techniques are used, the system under consideration is likely to change state in order to reach a better level of system operation. For instance, paths in the system can be changed in response to cyberattacks [176] with impact on security, Quality of Service a well as dependability.

When this occurs the transient behaviour of the system must be considered, which was addressed in several recent papers [177]–[180].

VI. THE IOTAC PROJECT

The subsequent IoTAC project has lead to novel techniques for learning from user traffic and then testing for an attack as described in [181]. In IoTAC, there is 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 [40], [41], [182], [183].

This project has created several novel attack detection techniques for attack detection of Botnets [184], [185]. The most original contribution in this respect has been to show that a large class of stochastic networks, of which the Random Neural Network is an instance, can in fact be used to detect cyberattacks [186].

Due to the role of transients due to the manner in which SDN routers operate, the SerIoT project also examined novel techniques to predict the time it takes to effect significant state changes such as re-routing of traffic in the network, using novel diffusion based techniques

VII. CONCLUSIONS

Frequent and effective cyberattacks on private and public networks, and on information technology infrustructures constantly motivates research on Cybersecurity. Starting with the encryption of massages and data, it has evolved to develop more secure systems through passwords, authentication schemes, firewalls and cryptographic keys. But it has now substantially been revolutionized as a means to detect and mitigate cyberattacks. Software's own specific vulnerabilities [187] have also become critical [176], [188]–[192]. Indeed, static means of Cybersecurity assurance are largely ineffective unless they incorportd real-time methods that can detect and rapidly react to attacks and malicious actions against a system.

Cybersecurity research is now encompassing a far broader approach, and the support of substantial European Union research programs has allowed the field to attain a higher level of maturity that includes performance, energy consumption and higher security levels through self-adaptation and system reconfiguration as demonstrated in the research projects that we have surveyed in this paper.

REFERENCES

[1] E. Gelenbe, *24th International Symposium on Computer and Information Sciences, ISCIS 2009*, 14-16 September 2009, North Cyprus. IEEE, 2009.

[2] E. Gelenbe, R. Lent, G. Sakellari, A. Sacan, I. H. Toroslu, and A. Yazici, *Computer and Information Sciences - Proceedings of the 25th International Symposium on Computer and Information Sciences,* London, UK, September 22-24, 2010, ser. Lecture Notes in Electrical Engineering. Springer, 2010, vol. 62. [Online]. Available: DOI: 10.1007/978-90-481-9794-1

[3] E. Gelenbe and R. Lent, *Eds., Computer and Information Sciences III - 27th International Symposium on Computer and Information Sciences*, Paris, France, October 3-4, 2012. Springer, 2013.

[4] ——, *Information Sciences and Systems 2013 - Proceedings of the 28th International Symposium on Computer and Information Sciences, ISCIS* 2013, Paris, France, October 28-29, 2013, ser. Lecture Notes in Electrical Engineering, vol. 264. Springer, 2013.

[5] O. H. Abdelrahman, E. Gelenbe, G. Görbil, and R. Lent, Eds., *Information Sciences and Systems 2015 - 30th International Symposium on Computer and Information Sciences, ISCIS* 2015, London, UK, 21- 24 September 2015, ser. Lecture Notes in Electrical Engineering, vol. 363. Springer, 2016.

[6] T. Czachórski, E. Gelenbe, and R. Lent, Eds., *Information Sciences and Systems 2014 - Proceedings of the 29th International Symposium on Computer and Information Sciences, ISCIS* 2014, Krakow, Poland, October 27-28, 2014. Springer, 2014.

[7] T. Czachórski, E. Gelenbe, K. Grochla, and R. Lent, Eds., *Computer and Information Sciences - 31st International Symposium, ISCIS* 2016, Kraków, Poland, October 27-28, 2016, *Proceedings*, ser. Communications in Computer and Information Science, vol. 659, 2016.

[8] T. Czachórski, E. Gelenbe, K. Grochla, and R. Lent, "*Computer and Information Sciences: 32nd International Symposium, ISCIS* 2018, Held at the *24th IFIP World Computer Congress, WCC* 2018, Poznan, Poland, September 20-21, 2018, Proceedings," 2018.

[9] E. Gelenbe, P. Campegiani, T. Czachórski, S. K. Katsikas, I. Komnios, L. Romano, and D. Tzovaras, "*Security in computer and information sciences: First International ISCIS Security Workshop* 2018, EURO-CYBERSEC 2018, London, UK, February 26-27, 2018, revised selected papers," 2018.

[10] A. Levi, M. U. Çaglayan, and Ç. K. Koç, "Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure," *ACM Trans. Inf. Syst. Secur.*, vol. 7, no. 1, pp. 21–59, 2004. [Online]. Available: http://doi.acm.org/10.1145/984334.984336

[11] M. Akgün and M. U. Çaglayan, "Towards scalable identification in RFID systems," *Wireless Personal Communications*, vol. 86, no. 2, pp. 403–421, 2016. [Online]. Available: DOI: 10.1007/s11277-015-2936-7

[12] O. Ermis, S. Bahtiyar, E. Anarim, and M. U. Çaglayan, "A key agreement protocol with partial backward confidentiality," *Computer Networks*, vol. 129, pp. 159–177, 2017. [Online]. Available: DOI: 10.1016/j.comnet.2017.09.008

[13] E. Gelenbe and F.-J. Wu, "Large scale simulation for human evacuation and rescue," *Computers & Mathematics with Applications*, vol. 64, no. 12, pp. 3869–3880, 2012.

[14] ——, "Future research on cyber-physical emergency management systems," *Future Internet*, vol. 5, no. 3, pp. 336–354, 2013.

[15] European Commission, "Cybersecurity Policies." [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

[16] H. Jiang, F. Liu, R. K. Thulasiram, and E. Gelenbe, "Guest editorial: Special issue on green pervasive and ubiquitous systems," *IEEE Systems Journal*, vol. 11, no. 2, pp. 806–812, 2017. [Online]. Available: DOI: 10.1109/JSYST.2017.2673218

[17] E. Gelenbe, "Search in unknown random environments," *Physical Review E*, vol. 82, p. 061112, 2010.

[18] O. H. Abdelrahman and E. Gelenbe, "Time and energy in team-based search," *Physical Review E*, vol. 87, no. 3, p. 032125, March 2013.

[19] F. Francois, O. H. Abdelrahman, and E. Gelenbe, "Towards assessment of energy consumption and latency of lte ues during signaling storms," in *Information Sciences and Systems* 2015. Springer, Cham, 2016, pp. 45–55.

[20] O. H. Abdelrahman and E. Gelenbe, "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)*. IEEE, 2016, pp. 154–158.

[21] E. Gelenbe and O. H. Abdelrahman, "An energy packet network model for mobile networks with energy harvesting," *Nonlinear Theory and Its Applications, IEICE*, 2018, vol. 9, no. 3, pp. 1–15, 2018. DOI: 10.1587/nolta.9.1

[22] O. H. Abdelrahman, E. Gelenbe, G. Görbil, and B. Oklander, "Mobile network anomaly detection and mitigation: The nemesys approach," in *Information Sciences and Systems 2013*. Springer International Publishing, 2013, pp. 429–438.

[23] E. Gelenbe, G. Görbil, D. Tzovaras, S. Liebergeld, D. Garcia, M. Baltatu, and G. Lyberopoulos, "Nemesys: Enhanced network security for seamless service provisioning in the smart mobile ecosystem," in *Information Sciences and Systems 2013*. Springer International Publishing, 2013, pp. 369–378.

[24] E. Gelenbe, G. Gorbil, D. Tzovaras, S. Liebergeld, D. Garcia, M. Baltatu, and G. Lyberopoulos, "Security for smart mobile networks: The nemesys approach," in *Privacy and Security in Mobile Systems (PRISMS), 2013 International Conference on*. IEEE, 2013, pp. 1–8.

[25] G. Gorbil, O. H. Abdelrahman, M. Pavloski, and E. Gelenbe, "Storms in mobile networks," arXiv preprint arXiv:1411.1280, 2014.

[26] M. Pavloski and E. Gelenbe, "Mitigating for signalling attacks in umts networks," in *Information Sciences and Systems 2014*. Springer International Publishing, 2014, pp. 159–165.

[27] B. Pernici, M. Aiello, J. Vom Brocke, B. Donnellan, E. Gelenbe, and M. Kretsis, "What is can do for environmental sustainability: a report from caise?11 panel on green and sustainable is," *Communications of the Association for Information Systems*, vol. 30, no. 1, p. 18, 2012.

[28] E. Gelenbe and Y. Caseau, "The impact of information technology on energy consumption and carbon emissions," *ubiquity*, vol. 2015, no. June, pp. 1–15, 2015.

[29] M. G. Siavvas and E. Gelenbe, "Optimum interval for application-level checkpoints," in *CSCloud/EdgeCom*. IEEE, 2019, pp. 145–150.

[30] S. Diamantopoulos, D. Karamitros, L. Romano, L. Coppolino, V. Koutkias, K. Votis, O. Stan, P. Campegiani, D. M. Martinez, M. Nalin et al., "Secure cross-border exchange of health related data: The konfido approach," in *International Conference on Internet and Distributed Computing Systems*. Springer, Cham, 2019, pp. 318–327.

[31] S. Diamantopoulos, M. Nalin, I. Baroni, F. Clemente, G. Faiella, C. Mesaritakis, E. Grivas, J. Rasmussen, J. Petersen, I. Cano, E. Puig- domènech, D. Karamitros, E. Gelenbe, J. Dumortier, M. V. Voronkov, L. Romano, L. Coppolino, V. Koutkias, K. Votis, O. Stan, P. Campegiani, and D. M. Martinez, "Secure cross-border exchange of health related data: The KONFIDO approach," in *EDCC*. IEEE, 2019, pp. 73–74.

[32] M. Nalin, I. Baroni, G. Faiella, M. Romano, F. Matrisciano, E. Gelenbe, D. M. Martinez, J. Dumortier, P. Natsiavas, K. Votis et al., "The european cross-border health data exchange roadmap: Case study in the italian setting," *Journal of biomedical informatics*, vol. 94, p. 103183, 2019.

[33] P. Natsiavas, G. Mazzeo, G. Faiella, P. Campegiani, J. Dumortier, O. Stan, M. Nalin, D. Mari Martinez, A. Theodouli, K. Moschou et al., "Developing an infrastructure for secure patient summary exchange in the eu context: Lessons learned from the konfido project," *Health Informatics Journal*, vol. 27, no. 2, p. 14604582211021459, 2021.

[34] A. Collen, N. A. Nijdam, J. Augusto-Gonzalez, S. K. Katsikas, K. M. Giannoutakis, G. Spathoulas, E. Gelenbe, K. Votis, D. Tzovaras, N. Ghavami, M. Volkamer, P. Haller, A. Sánchez, and M. Dimas, "Ghost - safe-guarding home iot environments with personalised real-time risk control," in *Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London*, E. Gelenbe, P. Campegiani, T. Czachorski, S. Katsikas, I. Komnios, L. Romano, and D. Tzovaras, Eds. Lecture Notes CCIS No. 821, Springer Verlag, 2018.

[35] O. Brun, Y. Yin, and E. Gelenbe, "Deep learning with dense random neural network for detecting attacks against iot-connected home environments," *Procedia Computer Science*, vol. 134, pp. 458–463, 2018.

[36] A. Frötscher, B. Monschiebl, A. Drosou, E. Gelenbe, M. J. Reed, and M. Al-Naday, "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)*. IEEE, 2019, pp. 1–5.

[37] G. Baldini, P. Fröhlich, E. Gelenbe, Hernandez-Ramos, J. Luis, M. Nowak, S. Nowak, S. Papadopoulos, A. Drosou, and D. Tzovaras, "*Iot network risk assessment and mitigation: The seriot approach*," 2020.

[38] M. Nakip and E. Gelenbe, "Randomization of data generation times improves performance of predictive iot networks," in *IEEE World Forum on Internet of Things (WF IoT)*, July 14-21, 2021, p. 5161. https://wfiot2021.iot.ieee.org, 2021

[39] ——, "Mirai botnet attack detection with auto-associative dense ran- dom neural networks," in *2021 IEEE Global Communications Conference*, vol. 2021. IEEE Communications Society, 2021, pp. 1–6.

[40] E. Gelenbe, M. Nakip, D. Marek, and T. Czachorski, "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*., 2021, pp. 1–6. https://zenodo.org/record/5501822#.YT3bri8itmA

[41] E. Gelenbe and K. Sigman, "Iot traffic shaping and the mas- sive access problem," in *ICC 2022, IEEE International Conference on Communications*, 16–20 May 2022, Seoul, South Korea, no., 2022, pp. 1–6., https://zenodo.org/record/5918301#.YgaCP

[42] E. Gelenbe, "On languages defined by linear probabilistic automata," *Information and Control*, vol. 16, no. 5, pp. 487–501, 1970.

[43] ——, "On the loop-free decomposition of stochastic finite-state systems," *Information and Control*, vol. 17, no. 5, pp. 474–484, 1970.

[44] S. E. Gelenbe, "A realizable model for stochastic sequential machines," *IEEE Trans. Computers*, vol. 20, no. 2, pp. 199–204, 1971.

[45] S. E. Gelenbe and N. Rossi, "Uniform modular realizations and linear machines," *IEEE Trans. Computers*, vol. 20, no. 12, pp. 1616–1617, 1971.

[46] E. Gelenbe, "A unified approach to the evaluation of a class of replacement algorithms," *IEEE Trans. Computers*, vol. 22, no. 6, pp. 611–618, 1973.

[47] M. Siavvas and E. Gelenbe, "Optimum checkpoints for programs with loops," *Simulation Modelling Practice and Theory*, vol. 97, p. 101951, 2019.

[48] M. Siavvas, D. Tsoukalas, M. Jankovic D. Kehagias, A. Chatzigeorgiou, D. Tzovaras, N. Aničic, and E. Gelenbe, "An empirical evaluation of the relationship between technical debt and software security," in *ICIST 2019 Proceedings*, vol. 1, 2019, pp. 199–203.

[49] G. Gorbil and E. Gelenbe, "Opportunistic communications for emergency support systems," *Procedia Computer Science*, vol. 5, pp. 39–47, 2011.

[50] ——, "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*, 2012, pp. 115–124.

[51] G. Gorbil, O. H. Abdelrahman, and E. Gelenbe, "Modeling and analysis of rrc-based signaling storms in 3g networks," *IEEE Transactions on Emerging Topics in Computing, Special Issue on Emerging Topics in Cyber Security*, p. 1-14, January 2015.

[52] F. Francois, O. H. Abdelrahman, and E. Gelenbe, "Feasibility of signaling storms in 3g/umts operational networks," in *International Internet of Things Summit*. Springer, Cham, 2015, pp. 187–198.

[53] M. Pavloski, G. Görbil, and E. Gelenbe, "Bandwidth usage?based detection of signaling attacks," in *Information Sciences and Systems 2015*. Springer, Cham, 2016, pp. 105–114.

[54] O. H. Abdelrahman and E. Gelenbe, "A data plane approach for detecting control plane anomalies in mobile networks," in *International Internet of Things Summit*. Springer, Cham, 2015, pp. 210–221.

[55] E. Gelenbe, O. H. Abdelrahman, and G. Gorbil, "Detection and mitigation of signaling storms in mobile networks," in *2016 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2016, pp. 1–5.

[56] E. Gelenbe and O. H. Abdelrahman, "Countering mobile signaling storms with counters," in *International Internet of Things Summit. Springer, Cham*, 2015, pp. 199–209.

[57] G. Gorbil, O. H. Abdelrahman, M. Pavloski, and E. Gelenbe, "Modeling and analysis of rrc-based signalling storms in 3g networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 1, pp. 113– 127, 2016.

[58] E. Gelenbe, "G-networks with instantaneous customer movement," *Journal of Applied Probability*, vol. 30, no. 3, pp. 742–748, 1993.

[59] J.-M. Fourneau, E. Gelenbe, and R. Suros, "G-networks with multiple classes of negative and positive customers," *Theoretical computer science*, vol. 155, no. 1, pp. 141–156, 1996.

[60] E. Gelenbe and G. Loukas, "A self-aware approach to denial of service defence," *Computer Networks*, vol. 51, no. 5, pp. 1299–1314, 2007.

[61] E. Gelenbe, Z. Xu, and E. Seref, "Cognitive packet networks," in *Conference Tools with Artificial Intelligence, 1999. Proceedings. 11th IEEE International Conference on, Publisher IEEE*, 1999, pp. 47–54.

[62] S. E. Gelenbe, "Cognitive packet network," Oct. 12 2004, uS Patent 6,804,201.

[63] E. Gelenbe, "Steps toward self-aware networks," *Communications of the ACM*, vol. 52, no. 7, pp. 66–75, 2009.

[64] E. Gelenbe and Y. Cao, "Autonomous search for mines," *European Journal of Operational Research*, vol. 108, no. 2, pp. 319–333, 1998.

[65] G. Oke, G. Loukas, and E. Gelenbe, "Detecting denial of service attacks with bayesian classifiers and the random neural network," in *Fuzzy Systems Conference*, 2007. FUZZ-IEEE 2007. IEEE International. IEEE, 2007, pp. 1–6.

[66] E. Gelenbe, "Dealing with software viruses: a biological paradigm," *Information security technical report*, vol. 12, no. 4, pp. 242–250, 2007.

[67] G. Sakellari, L. Hey, and E. Gelenbe, "Adaptability and failure resilience of the cognitive packet network," *DemoSession of the 27th IEEE Conference on Computer Communications (INFOCOM2008)*, Phoenix, Arizona, USA, 2008.

[68] G. Sakellari and E. Gelenbe, "Adaptive resilience of the cognitive packet network in the presence of network worms," *Proceedings of the NATO Symposium on C3I for Crisis, Emergency and Consequence Management*, pp. 11–12, 2009.

[69] C.-M. Yu, G.-K. Ni, Y. Chen, E. Gelenbe, and S.-Y. Kuo, "Top-k query result completeness verification in sensor networks," in *Communications Workshops (ICC)*, 2013 IEEE International Conference on. IEEE, 2013, pp. 1026–1030.

[70] C. Yu, G. Ni, I. Chen, E. Gelenbe, and S. Kuo, "Top- k query result completeness verification in tiered sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 1, pp. 109–124, 2014. [Online]. Available: http://dx.doi.org/10.1109/TIFS.2013.2291326

[71] M. Staffa, L. Sgaglione, G. Mazzeo, L. Coppolino, S. D'Antonio, L. Romano, E. Gelenbe, O. Stan, S. Carpov, E. Grivas et al., "An openncp-based solution for secure ehealth data exchange," *Journal of Network and Computer Applications*, vol. 116, pp. 65–85, 2018.

[72] P. Natsiavas, J. Rasmussen, M. Voss-Knude, K. Votis, L. Coppolino, P. Campegiani, I. Cano, D. Marí, G. Faiella, F. Clemente et al., "Comprehensive user requirements engineering methodology for secure and interoperable health data exchange," *BMC medical informatics and decision making*, vol. 18, no. 1, pp. 1–16, 2018.

[73] E. Gelenbe and M. Pavloski, "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.

[74] L. Castaldo and V. Cinque, "Blockchain-based logging for the cross-border exchange of ehealth data in europe," in Euro-CYBERSEC, ser. *Communications in Computer and Information Science*, vol. 821. Springer, 2018, pp. 46–56.

[75] E. Gelenbe and K. Sevcik, "Analysis of update synchronization for multiple copy data bases," *IEEE Transactions on Computers*, no. 10, pp. 737–747, 1979.

[76] A. Chesnais, E. Gelenbe, and I. Mitrani, "On the modeling of parallel access to shared data," *Communications of the ACM*, vol. 26, no. 3, pp. 196–202, 1983.

[77] R. Buyya, S. N. Srirama, G. Casale, R. Calheiros, Y. Simmhan, B. Varghese, E. Gelenbe, B. Javadi, L. M. Vaquero, M. A. Netto et al., "A manifesto for future generation cloud computing: Research directions for the next decade," *ACM Computing Surveys (CSUR)*, vol. 51, no. 5, pp. 1–38, 2019.

[78] Cisco, "Cisco annual internet report (2018–2023)." [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[79] G. Matta, S. Chlup, A. M. Shaaban, C. Schmittner, A. Pinzenöhler, E. Szalai, and M. Tauber, "Risk management and standard compliance for cyber-physical systems of systems," *Infocommunications Journal*, vol. 13, no. 2, pp. 32–39, June 2021. [Online]. Available: DOI: 10.36244/ICJ.2021.2.5

[80] S. Maksuti, M. Zsilak, M. Tauber, and J. Delsing, "Security and autonomic management in system of systems," *Infocommunications Journal*, vol. 13, no. 3, pp. 66–75, September 2021. [Online]. Available: DOI: 10.36244/ICJ.2021.3.7

[81] "Hp study reveals 70 percent of Internet of Things devices vulnerable to attack," Accessed on 25.01.2022. [Online]. Available: https://www.securityweek.com/70-iot-devices-vulnerable-cyberattacks-hp

[82] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.

[83] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[84] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[85] S. Benzarti, B. Triki, and O. Korbaa, "A survey on attacks in Internet of Things based networks," in *2017 International conference on engineering & MIS (ICEMIS)*. IEEE, 2017, pp. 1–7.

[86] CISA, "Understanding Denial-of-Service attacks." [Online]. Available: https://us-cert.cisa.gov/ncas/tips/ST04-015

[87] G. Carl, G. Kesidis, R. Brooks, and S. Rai, "Denial-of-Service attack-detection techniques," *IEEE Internet Computing*, vol. 10, no. 1, pp. 82–89, 2006.

[88] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer networks*, vol. 44, no. 5, pp. 643–666, 2004.

[89] D. Goodin, "100,000-strong Botnet built on router 0-day could strike at any time," *Ars Technica*, December 2017. [Online]. Available: https://arstechnica.com/information-technology/2017/12/100000-strong-botnet-built-on-router-0-day-could-strike-at-any-time/

[90] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim, and J. N. Kim, "An in-depth analysis of the mirai botnet," in *2017 International Conference on Software Security and Assurance (ICSSA)*. IEEE, 2017, pp. 6–12.

[91] J. Biggs, "Hackers release source code for a powerful DDoS app called Mirai," *TechCrunch*, October 2018. [Online]. Available: https://techcrunch.com/2016/10/10/hackers-release-source-code-for-a-powerful-ddos-app-called-mirai/

[92] R. Hackett, "Why a hacker dumped code behind colossal website-trampling botnet," *Fortune*, October 2016. [Online]. Available: https://finance.yahoo.com/news/why-hacker-dumped-code-behind-145847907.html

[93] N. Statt, "How an army of vulnerable gadgets took down the web today," *The Verge*, October 2016. [Online]. Available: https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained

[94] B. Tushir, H. Sehgal, R. Nair, B. Dezfouli, and Y. Liu, "The impact of dos attacks onresource-constrained iot devices: A study on the mirai attack," arXiv preprint *arXiv:2104.09041*, 2021.

[95] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet," in *Proceedings of the 26th USENIX Security Symposium*, 2017. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[96] H. Sinanović and S. Mrdovic, "Analysis of mirai malicious software," in *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE, 2017, pp. 1–5.

[97] Z. Ahmed, S. M. Danish, H. K. Qureshi, and M. Lestas, "Protecting IoTs from Mirai Botnet attacks using blockchains," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1–6.

[98] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," in *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018, pp. 29–35.

[99] C. S. Htwe, Y. M. Thant, and M. M. S. Thwin, "Botnets attack detection using machine learning approach for iot environment," in *Journal of Physics: Conference Series*, vol. 1646, no. 1. IOP Publishing, 2020, p. 012101.

[100] M. Banerjee and S. Samantaray, "Network traffic analysis basediot botnet detection using honeynet data applying classification techniques," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 17, no. 8, 2019.

[101] A. O. Prokofiev, Y. S. Smirnova, and V. A. Surov, "A method to detect internet of things botnets," in *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE, 2018, pp. 105–108.

[102] T. A. Tuan, H. V. Long, R. Kumar, I. Priyadarshini, N. T .K. Sonetal., "Performance evaluation of botnet ddos attack detection using machine learning," *Evolutionary Intelligence*, pp. 1–12, 2019.

[103] I. Letteri, M. Del Rosso, P. Caianiello, and D. Cassioli, "Performance of botnet detection by neural networks in software-defined networks." in *ITASEC: Proceedings of the Second Italian Conference on Cyber Security*, Milan, Italy, 6-9 February, 2018.

[104] S. Sriram, R. Vinayakumar, M. Alazab, and K. Soman, "Network flow based iot botnet attack detection using deep learning," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2020, pp. 189–194.

[105] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based iot-botnet attack detection with sequential architecture," *Sensors*, vol. 20, no. 16, p. 4372, 2020.

[106] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the Internet of Things using deep learning approaches," in *2018 international joint conference on neural networks (IJCNN)*. IEEE, 2018, pp. 1–8.

[107] J. Liu, S. Liu, and S. Zhang, "Detection of iot botnet based on deep learning," in *2019 Chinese Control Conference (CCC)*. IEEE, 2019, pp. 8381–8385.

[108] G. D. L. T. Parra, P. Rad, K.-K. R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *Journal of Network and Computer Applications*, vol. 163, p. 102662, 2020.

[109] C. Tzagkarakis, N. Petroulakis, and S. Ioannidis, "Botnet attack detection at the iot edge based on sparse representation," in *2019 Global IoT Summit (GIoTS)*. IEEE, 2019, pp. 1–6.

[110] M. Nakip and E. Gelenbe, "MIRAI botnet attack detection with auto-associative dense random neural network," in *IEEE Global Communications Conference (Globecom)*, 2021, pp. 1–6.

[111] E. Gelenbe, "Random neural networks with negative and positive signals and product form solution," *Neural Computation*, vol. 1, no. 4, pp. 502–510, 1989.

[112] E. Gelenbe and Y. Yin, "Deep learning with random neural networks," in *2016 International Joint Conference on Neural Networks (IJCNN)*, 2016, pp. 1633–1638.

[113] E. Gelenbe and Y. Yin, "Deep learning with dense random neural networks," in *International Conference on Man–Machine Interactions*. Springer, 2017, pp. 3–18.

[114] E. Gelenbe and M. Nakıp, "G-networks can detect different types of cyberattacks," in *MASCOTS'22: 30th International Symposium on the Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, IEEE Computer Society*. IEEEXplore, pp. 1–6.

[115] E. Gelenbe, Z.-H. Mao, and Y.-D. Li, "Function approximation with spiked random networks," *IEEE Trans. Neural Networks*, vol. 10, no. 1, pp. 3–9, 1999.

[116] O. Brun, Y. Yin, and E. Gelenbe, "Deep learning with dense random neural network for detecting attacks against iot-connected home environments," *Procedia Computer Science*, vol. 134, pp. 458–463, 2018.

[117] E. Gelenbe and Y. Yin, "Deep learning with random neural networks," in *2016 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2016, pp. 1633–1638.

[118] ——, "Deep learning with dense random neural networks," in *International Conference on Man–Machine Interactions*. Springer, Cham, 2017, pp. 3–18.

[119] W. Serrano, E. Gelenbe, and Y. Yin, "The random neural network with deep learning clusters in smart search," *Neurocomputing*, vol. 396, pp. 394–405, 2020.

[120] E. Gelenbe, "Random neural networks with negative and positive signals and product form solution," *Neural computation*, vol. 1, no. 4, pp. 502–510, 1989.

[121] ——, "Stability of the random neural network model," *Neural computation*, vol. 2, no. 2, pp. 239–247, 1990.

[122] ——, "Learning in the recurrent random neural network," *Neural Computation*, vol. 5, no. 1, pp. 154–164, 1993.

[123] E. Gelenbe and K. F. Hussain, "Learning in the multiple class random neural network," *IEEE Transactions on Neural Networks*, vol. 13, no. 6, pp. 1257–1267, 2002.

[124] D. Konar, E. Gelenbe, S. Bhandary, A. D. Sarma, and A. Cangi, "Random quantum neural networks (RQNN) for noisy image recognition," CoRR, vol. abs/2203.01764, 2022.

[125] E. Gelenbe, "Energy packet networks: adaptive energy management for the cloud," in *CloudCP'12: Proceedings of the 2nd International Workshop on Cloud Computing Platforms. ACM*, 2012, pp. 1–5. **DOI**: 10.1145/2168697.2168698

[126] E. Gelenbe and Y. M. Kadioglu, "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.

[127] E. Gelenbe and E. T. Ceran, "Energy packet networks with energy harvesting," *IEEE Access*, vol. 4, pp. 1321–1331, 2016.

[128] Y. M. Kadioglu and E. Gelenbe, "Product-form solution for cascade networks with intermittent energy," *IEEE Systems Journal*, vol. 13, no. 1, pp. 918–927, 2018.

[129] E. Gelenbe and Y. M. Kadioglu, "Energy loss through standby and leakage in energy harvesting wireless sensors," in *2015 IEEE 20th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD)*. IEEE, 2015, pp. 231– 236.

[130] Y. M. Kadioglu and E. Gelenbe, "Packet transmission with k energy packets in an energy harvesting sensor," in *Proceedings of the 2nd International Workshop on Energy-Aware Simulation*, 2016, pp. 1–6.

[131] E. Gelenbe and Y. M. Kadioglu, "Performance of an autonomous energy harvesting wireless sensor," in *Information sciences and systems 2015. Springer, Cham*, 2016, pp. 35–43.

[132] Y. M. Kadioglu and E. Gelenbe, "Wireless sensor with data and energy packets," in *2017 IEEE international conference on communications workshops (ICC Workshops)*. IEEE, 2017, pp. 564–569.

[133] E. Gelenbe and Y. M. Kadioglu, "Energy life-time of wireless nodes with network attacks and mitigation," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2018, pp. 1–6.

[134] ——, "Battery attacks on sensors," in *EuroCybersec 2018: International symposium on computer and information sciences, Security Workshop*. Springer, 2018.

[135] J. Domanska, E. Gelenbe, T. Czachorski, A. Drosou, and D. Tzovaras, "Research and innovation action for the security of the internet of things: The seriot project," in *Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London*, E. Gelenbe, P. Campegiani, T. Czachorski, S. Katsikas, I. Komnios, L. Romano, and D. Tzovaras, Eds. Lecture Notes CCIS No. 821, Springer Verlag, 2018.

[136] E. Gelenbe, J. Domanska, T. Czachorski, A. Drosou, and D. Tzovaras, "Security for internet of things: The seriot project," in *International Symposium on Networks, Computers and Communications, Proceedings of the. IEEE*, June 2018.

[137] P. Fröhlich, E. Gelenbe, J. Fiołka, J. Checinski, M. Nowak, and Z. Filus, "Smart sdn management of fog services to optimize qos and energy," *Sensors*, vol. 21, no. p. 3105, 2021. **DOI**: 10.3390/s21093105

[138] P. Frohlich, E. Gelenbe, and M. P. Nowak, "Smart sdn management of fog services," in *GIOTS 2020: Global IoT Summit 2020, IEEE Communications Society*, 1-5 June 2020, Dubin, Ireland. TechRxiv, 2020.

[139] E. Gelenbe, P. Frohlich, Nowak, Mateusz, S. Papadopoulos, Protogerou, Aikaterini, A. Drosou, and D. Tsovaras, "Iot network attack detection and mitigation," in T*he 9th Mediterranean Conference on Embedded Computing (MECO'2020)*, June 8-11, 2020, Budva, Montenegro, 2020, pp. 1–6.

[140] P. Fröhlich, E. Gelenbe, and M. Nowak, "Reinforcement learning and energy-aware routing," in *Proceedings ACM SIGCOMM 4th FlexNets Workshop on Flexible Networks: Artificial Intelligence Supported Network Flexibility and Agility*, 2021, pp. 26–31.

[141] E. C. H2020, "Getting more "intelligent"about internet security." [Online]. Available: https://cordis.europa.eu/article/id/436278-getting-more-intelligent-about-internet-security

[142] P. Frohlich and E. Gelenbe, "Optimal fog services placement in sdn iot network using random neural networks and cognitive network map," in *The 19th International Conference on Artificial Intelligence and Soft Computing*, Zakopane, PL, Springer LNAI, vol. 12415., 2020, pp. 78–89. **DOI**: 10.1007/978-3-030-61401-0

[143] E. Gelenbe, J. Domanska, P. Frohlich, M. Nowak, and S. Nowak, "Self-aware networks that optimize security, qos and energy," *Proceedings of the IEEE*, vol. 108, no. 7, pp. 1150–1167, 2020.

[144] E. Gelenbe, R. Lent, and Z. Xu, "Measurement and performance of a cognitive packet network," *Computer Networks*, vol. 37, no. 6, pp. 691–701, 2001.

[145] ——, "Design and performance of cognitive packet networks," *Performance Evaluation*, vol. 46, no. 2, pp. 155–176, 2001.

[146] E. Gelenbe, R. Lent, A. Montuori, and Z. Xu, "Cognitive packet networks: Qos and performance," in *Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 2002. MASCOTS 2002. Proceedings. 10th IEEE International Symposium on. IEEE*, 2002, pp. 3–9.

[147] E. Gelenbe and P. Liu, "Qos and routing in the cognitive packet network," in *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a. IEEE*, 2005, pp. 517–521.

[148] F. Francois and E. Gelenbe, "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)*. IEEE, 2016, pp. 283–288.

[149] E. Gelenbe, R. Lent, and Z. Xu, "Towards networks with cognitive packets," in *Performance and QoS of next generation networking*. Springer, 2001, pp. 3–17.

[150] E. Gelenbe and R. Lent, "Power-aware ad hoc cognitive packet networks," *Ad Hoc Networks*, vol. 2, no. 3, pp. 205–216, 2004.

[151] E. Gelenbe and M. Gellman, "Oscillations in a bio-inspired routing algorithm," in *2007 IEEE International Conference on Mobile Adhoc and Sensor Systems*. IEEE, 2007, pp. 1–7.

[152] ——, "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*. IEEE, 2007, pp. 343–352.

[153] E. Gelenbe, "Genetic algorithms with analytical solution," in *Proceed- ings of the 1st annual conference on genetic programming*. MIT Press, 1996, pp. 437–443.

[154] P. Liu and E. Gelenbe, "Recursive routing in the cognitive packet network," in *Testbeds and Research Infrastructure for the Development of Networks and Communities*, 2007. TridentCom 2007. 3rd International Conference on. IEEE, 2007, pp. 1–6.

[155] E. Gelenbe and T. Mahmoodi, "Energy-aware routing in the cognitive packet network," *Energy*, pp. 7–12, 2011.

[156] ——, "Distributed energy-aware routing protocol," in Computer and Information Sciences II. Springer London, 2012, pp. 149–154.

[157] E. Gelenbe, G. Sakellari, and M. D'arienzo, "Admission of qos aware users in a smart network," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 3, no. 1, pp. 1–28, 2008.

[158] E. Gelenbe and E. C.-H. Ngai, "Adaptive qos routing for significant events in wireless sensor networks," in *2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*. IEEE, 2008, pp. 410–415.

[159] E. Gelenbe and E. C. Ngai, "Adaptive random re-routing in sensor networks," *Proceedings of the Annual Conference of ITA (ACITA'08)* September 16, vol. 18, pp. 348–349, 2008.

[160] E. C. Ngai, E. Gelenbe, and G. Humber, "Information-aware traffic reduction for wireless sensor networks," in *Local Computer Networks*, 2009. LCN 2009. IEEE 34th Conference on. IEEE, 2009, pp. 451–458.

[161] E. Gelenbe, E. C. Ngai, and P. Yadav, "Routing of high-priority packets in wireless sensor networks," *IEEE Second International Conference on Computer and Network Technology*, IEEE, 2010.

[162] N. Li, X. Hu, E. Ngai, and E. Gelenbe, "Cooperative wire-less edges with composite resource allocation in hierarchical networks," in *2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM)*, 2021, pp. 1–6.
DOI: 10.1109/HEALTHCOM49281.2021.9398997

[163] J. Du, C. Jiang, E. Gelenbe, H. Zhang, and Y. Ren, "Traffic offloading in software defined ultra-dense networks," *Ultra-Dense Networks: Principles and Applications*, p. 164, 2020.

[164] J. Du, E. Gelenbe, C. Jiang, H. Zhang, and Y. Ren, "Contract design for traffic offloading and resource allocation in heterogeneous ultra-dense networks," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2457–2467, 2017.

[165] J. Du, E. Gelenbe, C. Jiang, H. Zhang, Y. Ren, and H. V. Poor, "Peer prediction-based trustworthiness evaluation and trustworthy service rating in social networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1582–1594, 2018.

[166] J. Du, C. Jiang, E. Gelenbe, L. Xu, J. Li, and Y. Ren, "Distributed data privacy preservation in iot applications," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 68–76, 2018.

[167] J. Du, C. Jiang, E. Gelenbe, H. Zhang, Y. Ren, and T. Q. Quek, "Double auction mechanism design for video caching in heterogeneous ultra-dense networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 3, pp. 1669–1683, 2019.

[168] J. Du, E. Gelenbe, C. Jiang, Z. Han, and Y. Ren, "Auction-based data transaction in mobile networks: Data allocation design and performance analysis," *IEEE Transactions on Mobile Computing*, vol. 19, no. 5, pp. 1040–1055, 2019.

[169] C. Cramer, E. Gelenbe, and H. Bakircloglu, "Low bit-rate video compression with neural networks and temporal subsampling," *Proceedings of the IEEE*, vol. 84, no. 10, pp. 1529–1543, 1996.

[170] C. E. Cramer and E. Gelenbe, "Video quality and traffic qos in learning-based subsampled and receiver-interpolated video sequences," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 2, pp. 150– 167, 2000.

[171] L. Wang and E. Gelenbe, "Adaptive dispatching of tasks in the cloud," *IEEE Transactions on Cloud Computing*, vol. 6, no. 1, pp. 33–45, 2018.

[172] E. Gelenbe, M. P. Nowak, P. Frohlich, J. Fiolka, and J. Checinski, "Energy, qos and security aware services at the edge," in *EuroCyber-Sec2021*. Springer, Cham, 2022.

[173] E. Gelenbe and M. Siavvas, "Minimizing energy and computation in long-running software," *Applied Sciences*, vol. 11, no. 3, p. 1169, 2021.

[174] E. Gelenbe and Y. Zhang, "Performance optimization with energy packets," *IEEE Systems Journal*, vol. 13, no. 4, pp. 3770–3780, 2019.

[175] ——, "Sharing energy for optimal edge performance," in *International Conference on Current Trends in Theory and Practice of Informatics*. Springer, Cham, 2020, pp. 24–36.

[176] D. Kehagias, M. Jankovic, M. Siavvas, and E. Gelenbe, "Investigating the interaction between energy consumption, quality of service, reliability, security, and maintainability of computer systems and networks," *SN Computer Science*, vol. 2, no. 1, pp. 1–6, 2021.

[177] T. Czachorski, E. Gelenbe, G. S. Kuaban, and D. Marek, "A time-dependent routing model of software defined networks," in *The Second International Workshop on Stochastic Modeling and Applied Research of Technology: SMARTY* 2020, August 16-20, 2020, Karelian Research Center, Russian Academy of Sciences, Petrozavodsk, CEUR Workshop Proceedings, vol. 2792. ISSN: 1613-0073, 2020, pp. 38–56.

[178] T. Czachórski, E. Gelenbe, G. S. Kuaban, and D. Marek, "Time-dependent performance of a multi-hop software defined network," *Applied Sciences*, vol. 11, no. 6, p. 2469, 2021.

[179] T. Czachórski, E. Gelenbe, and D. Marek, "Software defined network dynamics via diffusions," in *Symposium on Modelling, Analysis, and Simulation of Computer and Telecommunication Systems*. Springer, Cham, 2021, pp. 29–47.

[180] T. Czachórski, E. Gelenbe, G. S. Kuaban, and D. Marek, "Optimizing energy usage for an electric drone," in *International ISCIS Security Workshop*. Springer, Cham, 2022, pp. 61–75.

[181] M. Nakip and E. Gelenbe, "Botnet attack detection with incremental online learning," in *EuroCyberSec2021*. Springer, Cham, 2022.

[182] E. Gelenbe, T. Czachorski, D. Marek, and M. Nakıp, "Mitigating the massive access problem in the internet of things," in *EuroCyber-Sec2021*. Springer, Cham, 2022.

[183] E. Gelenbe, M. Nakip, and T. Czachorski, "Improving massive access to iot gateways," *Performance Evaluation*, p. 102308, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166531622000219

[184] M. Nakip and E. Gelenbe, "Mirai botnet attack detection with auto-associative dense random neural networks," in *2021 IEEE Global Communications Conference*, vol. 2021. IEEE Communications Society, 2021, pp. 1–6.

[185] ——, "Botnet attack detection with incremental online learning," in *International ISCIS Security Workshop*. Springer, Cham, 2022, pp. 51–60.

[186] E. Gelenbe and M. Nakip, "G-networks can detect different types of cyberattacks," in *MASCOTS 2022: IEEE 30th International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems*, no., 2022, pp. 1–6.
https://zenodo.org/record/6969827#.Yu6fc

[187] K. Filus, P. Boryszko, J. Domanska, M. G. Siavvas, and E. Gelenbe, "Efficient feature selection for static analysis vulnerability prediction," *Sensors*, vol. 21, no. 4, p. 1133, 2021.

[188] M. Siavvas and E. Gelenbe, "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)*. IEEE, 2019, pp. 145–150.

[189] E. Gelenbe, P. Boryszko, M. Siavvas, and J. Domanska, "Optimum checkpoints for time and energy," in *2020 28th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*. IEEE, 2020, pp. 1–8.

[190] K. Filus, M. Siavvas, J. Domańska, and E. Gelenbe, "The random neural network as a bonding model for software vulnerability prediction," in *Symposium on Modelling, Analysis, and Simulation of Computer and Telecommunication Systems, Workshop*. Springer, Cham, 2021, pp. 102–116.

[191] K. Filus, P. Boryszko, J. Domańska, M. Siavvas, and E. Gelenbe, "Efficient feature selection for static analysis vulnerability prediction," *Sensors*, vol. 21, no. p. 1133, 2021. **DOI**: 10.3390/s21041133

[192] M. Siavvas, D. Kehagias, D. Tzovaras, and E. Gelenbe, "A hierarchical model for quantifying software security based on static analysis alerts and software metrics," *Software Quality Journal*, vol. 29, no. 2, pp. 431–507, 2021.

Mehmet Ufuk Çağlayan holds a BS and MS in CS from METU (Ankara), and the PhD from Northwestern University, USA. He is Professor and Head of the Department of Computer Engineerng at Yaşar University in Izmir, Turkey. Previously Professor of Computer Engineering at Boğaziçi University, Turkey's most selective university. His research includes Computer and Network Security, Computer Communications, Computer Networks and Internet, Wireless and Mobile Networks, Distributed Systems, Operating Systems, Software Engineering, Software Design and Software Project Management. In 1979-81 he served as Instructor in the Department of Electrical Engineering and Computer Science, North-western University and in 1978-79 he was Instructor in Mathematics at DePaul University in Chicago. In 1981-87 he was an Assistant Professor of Computer Science and Engineering at King Fahd University of Petroleum and Minerals, in Dhahran, Saudi Arabia. He joined Boğaziçi University in 1987 as an Assistant Professor, and on leave of absence in 1989-91 was a Computer Scientist at BASF AG, Ludwigshafen, Germany. Author of some two-hundred publications, full Professor since 1999, he Coordinated the nationally funded TAM Project, aiming to increase the PhD graduates in Computer Engineering at his university and in Turkey. In 2000-04 he served as Chair of the Department of Computer Engineering of Boğaziçi University. He graduated several PhDs who are faculty in Turkey's leading universities and many Master's students.