Cognitive Routing for Improvement of IoT Security

Mateusz Nowak, Sławomir Nowak, Joanna Domańska
Institute of Theoretical and Applied Informatics, PAS
Gliwice, Poland
{mateusz,snowak,joanna}@iitis.pl

***Abstract*—Internet of Things is nowadays growing faster than ever before. Operators are planning or already creating dedicated networks for this type of devices. There is a need to create dedicated solutions for this type of network, especially solutions related to information security. In this article we present a mechanism of security-aware routing, which takes into account the evaluation of trust in devices and packet flows. We use trust relationships between flows and network nodes to create secure SDN paths, not ignoring also QoS and energy criteria. The system uses SDN infrastructure, enriched with Cognitive Packet Networks (CPN) mechanisms. Routing decisions are made by Random Neural Networks, trained with data fetched with Cognitive Packets. The proposed network architecture, implementing the security-by-design concept, was designed and is being implemented within the SerIoT project to demonstrate secure networks for the Internet of Things (IoT).**

***Index Terms*—Internet of Things (IoT), Security, Quality of Service, Energy, Cognitive Packet Network, SerIoT**

I. Introduction

Security in Internet of Things (IoT) in no longer viewed as peripheral issue, but is moved as one of key topics in development of current networking and computer systems. Data gathered by smart devices belong to most sensitive areas, like personal localisation, health data, also business-critical data. IoT networks transmit data used for controlling industrial or municipal facilities. The growing IoT market causes more and more questions about the safety of both IoT devices and the networks transferring data from these devices. Cyberattacks indeed cause very high cost to system operation, including degradation of trust and commercial image of organisations, even if they are detected and mitigated. The owners of 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 [1] and CO_2 impact [2].

One of the key process ensuring reliability of Internet connectivity is routing. Therefore it is continuously the aim of cyber-attacks - according to [3] only in 2017 ca. 14,000 attacks such as hijacking, leaks, spoofing led to data deft, revenue lost and reputation damage. Attacks on the transport service, attacks on the topology service, attacks on the route computation service and attacks on the identity resolution service are categories of routing attacks, classified in [4], and their purpose may be exhausting network resources and deplete bandwidth, and also eavesdropping [5]. Securing the routing itself is a matter of significant research effort (see [6]). Relatively less research activities is devoted to routing as a way of attacks mitigation – the problem is present in mobile ad-hoc networks [7], but recently some works concerning security aware routing in SDN core networks appeared [8].

Traffic Analysis and Anomaly Detection (TA/AD) are normal mechanisms used in computer networks for attack detection and mitigation decisions. We propose routing as an additional security ensuring mechanism, which may be the way of protection of most sensitive parts of the network in situation where the final mitigation decision is not taken by TA/AD yet. Rerouting of traffic likely to be harmful to less sensitive areas of the network to gain time for more thorough analysis or deflecting the flows to honeypots are just examples of using routing as support for cyberdefence.

Exploring possible role of routing as a way of counteracting cyberattacks in computer networks made us to set security-aware path management as one of important goals of the Secure and Safe Internet of Things (SerIoT) project [9] accepted for funding by European Commission. We are focused on novel path management methods within SDN network, based on online cognitive security surveillance and reporting, which establish and dynamically modify paths in a way that enhances security for IoT devices and end users, and offers a high quality of service (QoS) as well as reduced energy usage with required security constraints. The ways of security-focused path management include, among others, gathering various security metrics and – having clues about limited confidence of traffic or particular nodes – re-route traffic which is suspected to be part of cyberattack to less sensitive nodes (eg. to gain time for deeper analysis), changing the paths of network packets to visit the nodes able to do thorough analysis of the security of the packets or omit the nodes for which some suspicion is taken. Thanks to the new developed algorithms and methods we expect to gain better resistance to attacks, increasing level of protection both of network operator's and network customers' devices. Additional reason to focus on SDN was, that the relatively new and promising technology, despite great advances in research and deployment, has still security research in its infancy [10]

A. Related research

The SerIoT Project finds its origins in early work started over a decade ago on Distributed Denial of Service (DDoS)

The authors gratefully acknowledge the support of the SerIoT Research and Innovation Action, funded by the European Commission under the H2020-IOT-2017 Program through Grant Agreement 780139.

Attacks [11] and on using routing with the Cognitive Packet Network protocol (CPN) [12] 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 [13]. More recently, the EU FP7 Project NEMESYS [14] 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 [15]. 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 [16], [17].

In [18], 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 [19] 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 [20] has investigated the use of neural network and machine learning methods to discuss this issue. The research in [21], [22] 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 [23] using techniques from Queuing Theory [24].

KONFIDO [25] 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 [25].

The GHOST project [26] addresses security in the IoT system market [27] for homes, and focuses on the design of a secure home IoT gateway including the attack detection techniques [28], and the analysis of attack methods that try to bring down the energy supply of the devices by draining their batteries [29]. The detection techniques that are proposed are based on Deep Learning [30] and recurrent Random Neural Neworks (RNN) [31] that have been used previously in a variety of applications [32].

B. Background and outline of the SerIoT Project

The SerIoT project started in January of 2018 [9], and further details regarding can also be found in [33]. 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 [34], 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 [35], [36] using measurements that create the system self-awareness [12], [37], [38]. These SDNs will use Cognitive Packets (CP) to search [17], [39] 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 [40] to improve the network overall performance, including all three criteria of high security, good QoS and low energy consumption [41], [42]. Several SerCPN network clusters may be interconnected via end overlay network [43], with adaptive connections to Cloud and Fog servers [44] for network data analysis and visualisation.

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.

Most of routing methods, based on RNN and Cognitive Packets, as well as methods for measurement (or estimation) of factors influencing routing decisions will be also applicable outside SDN, thanks to distributed nature of recurrent RNN.

II. Project objective – Security Aware Routing

One of the objectives of the project is to design, implement and test a secure network infrastructure for the IoT, based on Software Defined Networks (SDN) and a smart SDN-Controller with online cognitive security surveillance and reporting, and with the ability to establish and dynamically modify paths to enhance security for IoT devices and end users, while offering a quasi-optimal level of quality of service (QoS) within the required security constraints. The online cognitive surveillance and path management of the network is based on the CPN (Cognitive Packet Network) principle that was discussed in [45] and detailed in [46]. CPNs routing level implementation and performance is presented in various papers such as [39]. CPN's implementation as an overlay network is discussed in [43], and its use as a software defined network (SDN) is discussed in [47]. The smart SDN network designated "SerIoT CPN network" or SerCPN that we will develop in the SerIoT project, starts with some designs discussed in [47].

The key concept used in the authors' work on novel approach to routing is trust. In general the term might be considered vague, still, there are authors who already defined trust in a way which is also used in the paper. In [48] trust is defined as the "degree of reliability" of nodes in the network. Following the definition in our context, we consider trust as the probability that the cooperating nodes in the network will comply with the security policies enforced in the network and will not act in any malicious way to violence the

security requirements of confidentiality, integrity, availability, authenticity and non-repudiation.

A. Use of CPN within the SerIoT Project

SerCPN is a general secure, QoS aware and energy-aware network solution, suitable for use in various application contexts, and in particular for the IoT domain, such as:

1) IoT-centric virtual network, separated form operator's backbone network.
2) Overlay over the Internet, where resources of public Internet are used in place of leased lines
3) Local communication within large IoT network

B. Design goals of SerCPN

SerCPN utilises and extends the classic SDN approach. It has an architecture of separated data and control planes, and uses the OpenFlow protocol for communication between them.

Decisions about the routes the packets move are made according to the following criteria, ordered by priority:

1) **Security and Safety.** Data must be delivered in reliable way, minimizing the risk of being lost (due to intended attack or accidental failure) or intercepted. This includes protection against hi-jacking the switches and the controller, and against attempts to feed the controller (or other network components) with wrong information.
2) **Quality of Service**. An important criterion for choosing the paths for packet delivery are the QoS parameters such as throughput, delay and jitter and this can be carried out using CPN as well possible using Composite Goal Functions (CGF) [49] that include both security, QoS and possibly energy as indicated below. Indeed, SerCPN must be secure but its QoS must be attractive to customers.
3) **Energy usage**. Energy usage will be taken into account when deciding about packet routes. The load of switches will be adjusted to minimise energy usage, while traffic will be distributed on paths with a view to minimizing the energy consumption per packet or per connection; this can be achieved either by using a heuristic based on CPN [50] or by a computed optimization solution as in [51].

C. Routing Criteria

In the case of a SDN based implementation for SerCPN, routing decisions are reflected by creating appropriate rules for given flows. The routing decisions will be taken by an "oracle", which is fed with security, QoS and energy data, which will be stored in a Cognitive Security Memory (CSM). As in CPN [45] [46] the "oracle" will be implemented using Random Neural Networks (RNN) [52] which will specifically exploit a real-time learning algorithm such as Reinforcement Learning (RL). RNNs will be placed in the controller plugin, and the CSM data will be used in the RNN learning process. Let us note that the RL based learning process of CPN not only exploits the ongoing measurement data, but it also generates data such as the comparison between short or long-term history regarding measurements, and the QoS, Energy or Security state of paths [49] that may be exploited by the analytics modules of SerCPN.

CSM data will belong to three groups, according to the criteria listed in II-B. A detailed list of used values, as well as their meaning for final evaluation of paths and intermediate nodes will be worked out during the timeline of the project. We will evaluate the:

We will focus on, and obtain, quantitative metrics and evaluations, and these values will be used for learning by the RNNs, and transferred for exploitation by the analytics modules of SerIoT. There exist many methods and approaches to traffic classification and threats detection, eg. [53] or [54] to list just few. The choice of advanced threats detection methods will be done in later stage of the work, however we can list introductory list of actions, which will give us quantitative view at level of trust to network devices and network traffic.

1) Estimation of security (trust level) of devices connected to given SerIoT forwarder (SFE – see Sec. III) — likeliness of being the source or destination of the attack. This group includes preventive actions. Simple verifications may include the verification of default credentials, also the fingerprinting the firmware version against latest security patches installed and more advanced – automatic active penetration testing of connected devices (one time or periodic).
2) Security (trust level) of the SFEs – likeliness of the node being attacked and disabled or intercepted. Actions similar to group 1 are considered here, as well as we may use the availability rate of the nodes, independently of the reasons such as attacks or technical failure, as a way to modify the trust level of a node.
3) Security (trust level) of particular flows. Here we have a wide group of methods. Simple (lightweight) indications that a given flow might be a part of an attack include prevention without using statistics, e.g.:
   - Checking if the source or destination of the flow is on the public blacklist of IP addresses known to be sources of attack,
   - Detection of a bitrate exceeding predefined threshold,
   - Detection of access to random IP addresses (IP scan),
   - Detection of non-standard use of protocols (ssh, DNS, NTP etc.).

   At the end of the project we however intend to use also advanced techniques comparing traffic statistics with patterns of attacks using methods of mathematical statistics or artificial intelligence.
4) QoS parameters provided by particular paths. Throughput of given links, delay and jitter, as well as loss rates should be measured and forwarded to the CM.
5) Power consumption of particular nodes for specific measured traffic values.

Thus the factors listed above in 1) through 5) will be used to

create the Cognitive Goal Function for SerCPN optimisation.

D. Formal Representation of CGF

Cognitive Goal Function $G(f,P)$ takes numerical non-negative real values, f denotes a flow (traffic identified by its source address, source port, destination address, destination port), and P denotes some specific path in the network. Thus, the values of $G(.,.)$ result from the flow to which it applies and from the path used by the flow. A large value of $G(.,.)$ means that the particular flow f should not use the path P. It may be caused by a risky flow, which we do not want in the sensitive node belonging to P, or in contrary - by the suspicious node, which should rather not be carrying a sensitive flow f. In any case, the decision system should look for a new path for a flow F, resulting in lower value of $G(.,.)$. Of course, complete $G(.,.)$ function will also take into account QoS and Energy.

Now, let e denote some forwarding element or network node. We define the *Trust Level* $T(f,e)$, again as a non-negative number that says how much we can trust f when it flows through e, or reciprocally, how much f itself can trust e. We define also the *Sensitivity* of e when it is carrying f; again this is a reciprocal property which say something about how the security of f is affected by transiting through e, or how an insecure flow f can affect a node e, and it is again a non-negative number.

Now we define the *Rejection Factor* of the flow f in the node e $R(f,e)$. It indicates how much the flow f is "unwanted" in the forwarder e.

$$R(f,e) = \begin{cases} 0 & \text{if SE(f,e)} \leq \text{TF(f,e)} \ , \\ SE(f,e) - TF(f,e) & \text{SE(f,e)} > \text{TF(f,e)}, \end{cases}$$

We can also define the cumulative Rejection Factor (RF) that links flows to paths, simply by looking at the effect of a path P, as it is related to the nodes e that it contains, for instance:

$$RF(f,P) = \sum_{e \in P} R(f,e), \text{ or } R(f,P) = \max_{e \in P} R(f,e). \quad (1)$$

The RF serves as the security component of $G(.,.)$, while we would like to include also QoS and energy when we consider the *Goal Function* that will be used in our RL based routing scheme. To achieve that, we can a relatively simple form such as:

$$G(f,P) = \alpha RF(f,P) + \beta Q(f,P) + \gamma E^o(f,P), \quad (2)$$

where $Q(.,.)$ is the quality of service component of CGF, resulting mainly from the delay measured by CP on the individual links and $E^o(f,P)$ is the energy component whose value is obtained from the energy consumed by the node for each transmitted packet. In turn α, β, γ are non-negative constants that indicate the relative importance within the Goal $G(.,.)$ of Security, QoS and Energy consumption.

As already mentioned, the value of CGF obtained in Eq.2 is used in Reinforcement Learning algorithm with Random Neural Networks.

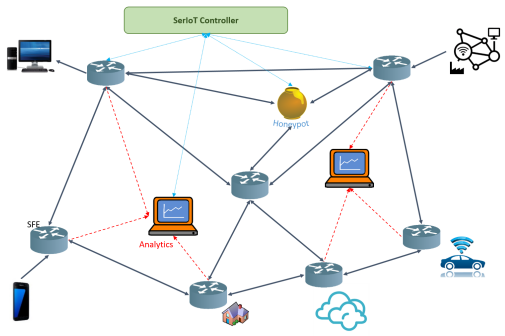

Fig. 1. An example of a basic SerCPN network (single domain)

III. Architecture of the SerCPN network

The proposed routing solutions will be implemented as extension of classic SDN network. We will introduce new SerCPN's components, able to perform actions necessary to reach the project's goals, especially smart security aware routing. Main components of SerCPN include:

1) SerCPN Forwarding Element (SFE),
2) SerCPN Controller(s),
3) SerIoT Analytics Module will exploit data collected by SerCPN,
4) SerIoT Honeypots will also attempt to attract attacks and inform SerCPN about the network state.

SerCPN's Forwarding Element (SFE) is a basic component of the network. It is a Network Forwarding Element (NFE, referred often imprecisely as SDN switch or SDN router) modified for the needs of SerCPN. SFE performs regular packet switching according to OpenFlow rules. In addition, SFE will use the CPNs approach to perform tasks related to gathering security, QoS and energy usage data.

The SerCPN controller will be standard SDN controller (we chose ONOS – https://onosproject.org/), accompanied by SerCPN Routing Engine (SRE). Heart of SRE is RNN-based Cognitive Routing Module taking the routing decisions according to method outlined in Sec. II-D.

The aim of the **SerIoT Analytics Module** (SAM) is to provide evaluation of flows in the SerCPN by statistical comparison with historical data. Flows having characteristics different than expected may be blocked, or directed towards a Honeypot, or put under observation for a later decision. ion in the project.

The SerIoT Honeypot (SH) is a system which mimics the functions of certain devices; it is connected to SerCPN and analyzes the attacks that are conducted on itself. It can be taken over by an attacker without any harm to other nodes of SerCPN.

IV. Implementation of data acquisition and routing decisions

The SerCPN Routing Engine (SRE) will be distributed in one or more SDN controllers as a plugin module, using the

RNNs to implement the decision oracles, enabling a semi-distributed way of taking decisions, but using the advantages of the semi-centralisation of the SDN architecture. Linking specific RNNs to SFEs will reflect the physical network topology. The role of a single RNN will be to specify, at the time of decision making, which output node should be used for a given SFE, regarding a flow having a given destination. Data will be gathered by the SRE in two ways:

1) in the form of Smart Packets (SPs).
2) via controller, which gathers data from monitoring or analytic entities

SerIoT, following the CPN concept uses Cognitive Packets that travel from one node to another towards their destination, gathering measured data that is provided by the nodes that are visited. Normally, the path of the CPs is provided by the SFEs of the nodes visited by the CPs, and the path of ACKs is source routed from the destination node back to the source. Thus in CPN each of the nodes visited by a CP is able to receive and copy from the corresponding ACK (acknowledgement packets) the data that was collected by a CP on its path. Such nodes can then store and exploit the data that has been collected by each CP that visited the node. In SerCPN the approach is modified, as sending of CPs and routing over the network is controlled by a controller and SRE, so ACK packets, instead of travelling via the network using the route back to the source node, go to the SRE, which makes use if their content to decide about routing.

CPs will be used for data which is not available otherwise, such as delay on the link or total delay between two adjacent nodes including the delay inside nodes, and for data which can be sent by nodes directly (asynchronously or by request) but which are less urgent (e.g. energy usage). CPs aggregate the data from many nodes on their path and send them back to controller in a single message, reducing the potential communication overhead.

V. Conclusions

SerIoT project is aimed at enhancing a wide spectrum of security methods dedicated to IoT world which is developing rapidly. Still, main focus of mechanisms presented in the paper, contributed by authors to SerIoT project, is at novel routing methods, which take into account also ensuring security of data delivery, in aspects of reliability and integrity. The influence of routing decision on protection level of IoT devices connected to the multipath core network and the network appliances themselves has not yet been examined.

In SerIoT we are developing the multi-criteria routing, not only security-aware, but also including QoS and energy awareness rules, and using Random Neural Networks to achieve the goals. The security part will explore the concept of confidence to particular devices and network flows, based on measurements which are achievable in SDN network. The characteristics of network traffic from IoT devices will enable us to define risks and symptoms of malicious behaviour more precisely than in network of a general nature, and the dedicated module processing the security-related information from various sources can be adapted to new threats and attack vectors. Thus, the use of the RNN module provides a smart tool for effective decision making in a dynamically changing environment.

We are also introducing the network architecture following security-by-design approach. In the times of networks carrying more and more sensitive information, either very private or business-critical it is vital to develop security aspects of networking and we hope to add a significant contribution to the area of designing networks which are not only efficient but also safe and secure. The architecture is SDN-based. SDN is emerging technology, making management task easier thanks to detaching control plane from data plane. Neural Network based decision engine is however designed in a way enabling using the approach also in classical architecture.

References

[1] E. Gelenbe and Y. Caseau, "The impact of information technology on energy consumption and carbon emissions," *Ubiquity*, vol. 2015, no. June, p. 1, 2015.

[2] F. François, O. H. Abdelrahman, and E. Gelenbe, "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, August 24-26, 2015*, pp. 1248–1255, 2015.

[3] E. Hanselman, "Manrs project study report," tech. rep., 451 Research, Commissioned by Internet Society, August 2017.

[4] M. Hollick, C. Nita-Rotaru, and P. Papadimitratos, "Toward a taxonomy and attacker model for secure routing protocols," *ACM SIGCOMM Computer Communication Review*, vol. 47, 2017.

[5] E. B. Eskca, O. Abuzaghleh, P. Joshi, S. Bondugula, and T. Nakayama, "Software defined networks security: An analysis of issues and solutions," *International Journal of Scientific & Engineering Research*, vol. 6, 2015.

[6] A. Herzberg, M. Hollick, and A. Perrig, "Secure Routing for Future Communication Networks (Dagstuhl Seminar 15102)," *Dagstuhl Reports*, vol. 5, no. 3, pp. 28–40, 2015.

[7] P. Lokulwar, V. Shelkhe, and M. Ghonge, *Security Aware Routing Protocol for Manet*. LAP Lambert Academic Publishing, 2012.

[8] M. Wang, J. Liu, J. Mao, H. Cheng, J. Chen, and C. Qi, "RouteGuardian: Constructing Secure Routing Paths in Software-Defined Networking," *Tsinghua Science and Technology*, vol. 4, no. 22, pp. 400–412, 2017.

[9] 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, EURO Cybersec 2018* (E. Gelenbe, P. Campegiani, T. Czachorski, S. Katsikas, I. Komnios, L. Romano, and D. Tzovaras, eds.), Lecture Notes CCIS No. 821, Springer Verlag, 2018.

[10] H. Zhang, Z. Cai, Q. Liu, Q. Xiao, Y. Li, and C. F. Cheang, "A survey on security-aware measurement in sdn," *Security and Communication Networks*, vol. 2018, 2018.

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

[12] E. Gelenbe, R. Lent, and A. Nunez, "Self-aware networks and qos," *Proceedings of the IEEE*, vol. 92, no. 9, pp. 1478–1489, 2004.

[13] G. Sakellari and E. Gelenbe, "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.

[14] 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*, pp. 429–438, Springer International Publishing, 2013.

[15] O. H. Abdelrahman and E. Gelenbe, "Signalling storms in 3g mobile networks," in *IEEE International Conference on Communications, ICC 2014, Sydney, Australia, June 10-14, 2014*, pp. 1017–1022, IEEE, 2014.

[16] A. Desmet and E. Gelenbe, "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.

[17] E. Gelenbe, "A diffusion model for packet travel time in a random multihop medium," *ACM Transactions on Sensor Networks (TOSN)*, vol. 3, no. 2, p. 10, 2007.

[18] E. Gelenbe, P. Campegiani, T. Czachórski, S. Katsikas, I. Komnios, L. Romano, and D. Tzovaras, eds., *Proceedings of the 2018 ISCIS Security Workshop: Recent Cybersecurity Research in Europe*, vol. 821, Lecture Notes CCIS, Springer Verlag, 2018.

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

[20] D. Geneiatakis, G. Baldini, I. N. Fovino, and I. Vakalis, "Towards a mobile malware detection framework with the support of machine learning," 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.

[21] M. Pavloski, "Signalling attacks in mobile telephony," 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.

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

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

[24] T. Czachórski, E. Gelenbe, and R. Lent, *Information Sciences and Systems 2014*. Springer International Publishing, 2014.

[25] M. Staffa, L. Coppolino, L. Sgaglione, E. Gelenbe, I. Komnios, E. Grivas, O. Stan, and L. Castaldo, "Konfido: An openncp-based secure ehealth data exchange system," 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.

[26] 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.

[27] M. Horváth and L. Buttyán, "Problem domain analysis of iot-driven secure data markets," 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.

[28] O. Brun, Y. Yin, E. Gelenbe, Y. M. Kadioglu, J. Augusto-Gonzalez, and M. Ramos, "Deep learning with dense random neural networks for detecting attacks against iot-connected home environments," 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.

[29] 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, 2018.

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

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

[32] E. Gelenbe and C. Cramer, "Oscillatory corticothalamic response to somatosensory input," *Biosystems*, vol. 48, no. 1, pp. 67–75, 1998.

[33] 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.

[34] J. Domanska, T. Czachòrski, M. Nowak, S. Nowak, and E. Gelenbe, "Sercpn: Smart software defined network for iot," in *To appear*, 2018.

[35] E. Gelenbe, "A software defined self-aware network: The cognitive packet network," in *IEEE 3rd Symposium on Network Cloud Computing and Applications, NCCA 2014, Rome, Italy, February 5-7, 2014*, pp. 9–14, 2014.

[36] F. François and E. Gelenbe, "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, September 19-21, 2016*, pp. 283–288, 2016.

[37] 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.

[38] 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*, pp. 517–521, IEEE, 2005.

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

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

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

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

[43] O. Brun, L. Wang, and E. Gelenbe, "Big data for autonomic intercontinental communications," *IEEE Transactions on Selected Areas in Communications*, vol. 34, no. 3, pp. 575–583, 2016.

[44] L. Wang, O. Brun, and E. Gelenbe, "Adaptive workload distribution for local and remote clouds," in *Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on*, pp. 003984–003988, IEEE, 2016.

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

[46] E. Gelenbe, "Cognitive packet network," *US Patent 6,804,201*, 2004.

[47] F. François and E. Gelenbe, "Towards a cognitive routing engine for software defined networks," in *ICC 2016*, pp. 1–6, IEEE Xplore, 2016.

[48] S. Devisri and C. Balasubramaniam, "Secure routing using trust based mechanism in wireless sensor networks(wsns)," *International Journal of Scientific & Engineering Research*, vol. 4, 2013.

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

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

[51] E. Gelenbe and C. Morfopoulou, "A framework for energy-aware routing in packet networks," *Computer Journal*, vol. 54, no. 6, pp. 850–859, 2011.

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

[53] M. Min, L. Xiao, C. Xie, M. Hajimirsadeghi, and N. B. Mandayam, "Defense against advanced persistent threats in dynamic cloud storage: A colonel blotto game approach," *CoRR*, vol. abs/1801.06270, 2018.

[54] P. Foremski, C. Callegari, and M. Pagano, "Waterfall: Rapid identification of ip flows using cascade classification," in *International Conference on Computer Networks*, pp. 14–23, Springer, 2014.