Signalling Attacks in Mobile Telephony

Mihajlo Pavloski

Department of Electrical & Electronic Engineering
Imperial College, London, UK,
m.pavloski13@imperial.ac.uk

Abstract. Many emerging Internet of Things devices, gateways and networks, rely either on mobile networks or on Internet Protocols to support their connectivity. However it is known that both types of networks are susceptible to different types of attacks that can significantly disrupt their operations. In particular 3rd and 4th generation mobile networks experience signalling related attacks, such as signalling storms, that have been a common problem in the last decade. This paper presents a generic model of a mobile network that includes different end user behaviours, including possible attacks to the signalling system. We then suggest two attack detection mechanisms, and evaluate them by analysis and simulation based on the generc mobile network model. Our findings suggest that mobile networks can be modified to be able to automatically detect attacks. Our results also suggest that attack mitigation can be carriedout both via the signalling system and on a ”per mobile terminal” basis.

Keywords: signalling storms, denial of service, mathematical modelling, detection, mitigation

1 Introduction

The security of computing systems is based on three basic principles: confidentiality, integrity and availability. System availability of networks and services can be significantly impaired by *Denial of Service* (DoS) attacks which can take various forms which differ according to the technology being considered. Thus DoS attacks for IP (Internet Protocol) networks differ significantly from DoS attacks against mobile networks.

Mobile networks are susceptible to DoS attacks, mostly because of the networks' openness to the Internet, the use of deterministic procedures, and the use of basic design principles based on typical user behaviour. In the last ten years, there were huge advances from an algorithmic, manufacturing ‘and software perspective, pushing forward the innovation of mobile smart devices and applications, which operate over a mobile network - while the network itself did not keep up with the pace. One of the problems caused by these circumstances, is the appearance of DoS attacks known as *signalling storms*, which overload the control plane of the mobile network, unlike many previously known data plane flooding attacks [23, 35].

Network security is ranked as one of the top priorities for future self-aware networks [17], which is why there is well established research in the field. Furthermore, while work in [20, 31] focuses on a general defensive approach against DoS attacks in future networks, signalling storm specific research can roughly be categorised in the following groups: problem definition and attacks classification [4, 28, 29, 39]; measurements in real operating networks [38], [10]; modelling and simulation [1, 24]; impact of attacks on energy consumption [9, 11]; attacks detection and mitigation, using counters [18,19,36], change-point detection techniques [30, 40], IP packet analysis [26], randomisation in RRC's functions [41], software changes in the mobile terminal [7,32], monitoring terminal's bandwidth usage [37], and detection using techniques from Artificial Intelligence [2]. As we look to the future, such as the Internet of Things (IoT), various forms of attacks will also have to be considered [5, 8].

The communication schemes may be opportunistic [**?**, 25] and attacks may use similar opportunistic means to access IoT devices, viruses and worms will continue being important threats [15] and they can diffuse opportunistically through a network [16], video input is one of the uses of the IoT and video encoding [6] can also be specifically targeted by attacks. Thus research needs to remain alert to such developments.

In this paper we mainly use stochastic modelling techniques, in order to represent complex communication protocols, such as the Radio Resource Control (RRC), in simplified mathematic terms. In particular we use open and closed queueing networks with multiple classes of calls. The analysis of these systems is first described by Jackson [27], Basket et al. [3], and Gelenbe [13, 14, 21, 22], among others. A second approach is used through discrete event simulation, whose results in many cases are comparable to queueing network models. More precisely, we are using a specialised Mobile Networks Security Simulator (SECSIM) created by in research group [24].

The remainder of the paper is organised as follows. In Section 2 we present a queueing network model of a generic architecture of a mobile network, and model normal and attack behaviour in Sec 2.2. In Section 3 we present two attack detection techniques, respectively in Section 3.1 and Section 3.2, and a mitigation technique in Section 3.3. Finally, Section 4 concludes the paper.

2 Network model

The proposed model describes a general network architecture, focusing on its radio access part, from the perspective of both, the control and data (user) plane. It's envisioned to represent different mobile network technologies, which is achieved through representing the resource allocation in the data plane as a "black box" where different technologies' sub-models can be plugged in, while keeping the control plane unchanged. The core part of the model consists only the basic elements of the architecture, such as multiple Base Station (BS) nodes connected to a single network controller consisting one Signalling Server (SS) node, and the communication stage nodes.

2.1 Model description

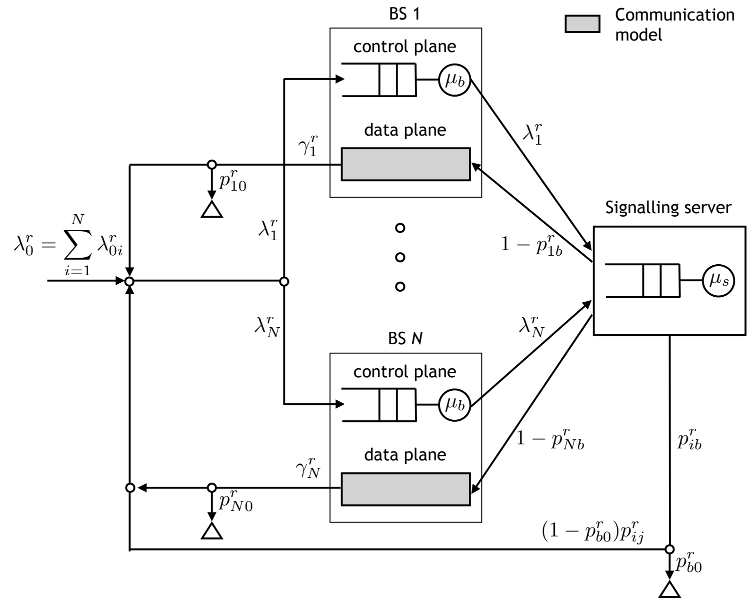

Fig. 1. A model of the radio access part of a mobile network.

An example workflow captured by our model goes as follows. When a mobile terminal wants to communicate, it sends a connection setup request through the control plane of the network, which needs to be processed at the BS and the SS. If admitted, the mobile proceeds to communicate in the data plane of the network, in sessions (each comprising multiple data packets), which we denote as *calls* in the rest of the paper. If a call is blocked, then the mobile may either leave the network or attempt to reconnect with a probability that depends on the type of call. There are two types of calls or connection setup requests in the network: i) normal calls representing traffic from legitimate users or applications, and ii) attack traffic generated by malicious or malfunctioning applications that may overload the network. The network model is open with calls joining and leaving the network, representing for example the arrival and departure of mobiles to WiFi areas. Its parameters are defined in Table 1 where the superscript $r \in \{n, a\}$ denotes the class of a call (normal n or attack a).

We assume calls arrive from outside the network according to independent Poisson processes and the service times in each node are independent and exponentially distributed. Since calls may be blocked at the SS due to congestion, the aggregate arrival processes at different parts of the network are not Poisson. Nevertheless, to simplify matters so as to obtain analytical solutions, we make

Table 1. The main parameters of the model

N	Number of cells covered by one signalling server.
λ_{0i}^r	Rate of new class-r calls joining cell $i \in \{1, \ldots, N\}$, which corresponds to mobile phone activations and handovers by roaming users.
λ_i^r	Rate of class-r connection requests traversing the i-th BS. These include calls joining from outside the network, calls that have been successfully served and return as new calls, and calls that retry connecting after not being admitted at cell j due to insufficient data channels.
λ_s^r	Total rate of class-r calls arriving at the SS, $\lambda_s^r = \sum_{i=1}^N \lambda_i^r$.
γ_i^r	Rate of class-r calls that timed out after being admitted to cell i.
p_{ib}^r	Proportion of class-r calls not admitted for communication at cell i.
p_{b0}^r	Probability that a blocked class-r call leaves the network; p_{b0}^a represents attackers' stubbornness while p_{b0}^n reflects human persistence.
p_{i0}^r	Proportion of class-r calls leaving the network after successful service at cell i.
p_{ij}^r	Proportion of class-r calls joining cell j after being blocked at cell i given that they stay in the network, i.e. $\sum_{j=1}^N p_{ij} = 1$.
μ_b	Class-independent service rate of connection requests in the BS, representing the *cell signalling capacity.*
μ_s	Class-independent service rate of connection requests in the SS, representing the *SS capacity.*
t_0^r	Inactivity timer.

the approximation that all flows within the network are Poisson. The service time distribution for the BS and SS nodes in the signalling stage is same for both classes of calls, because the signalling procedure undertaken by the network does not distinguish call classes. On the other hand, in the communication stage, the service time distribution is distinct for different classes of calls because of the different bandwidth usage behaviour of the normal and malicious calls.

The flow of calls in the above model could be expressed in a closed form as follows. The total arrival rate of class-r connection requests at BS i is the sum of the rates of i) new calls, ii) returning calls that timed out, and iii) calls that were blocked at a cell j by the SS and are attempting to connect at cell i:

$$\lambda_i^r = \underbrace{\lambda_{0i}^r}_{\text{new calls}} + \underbrace{\gamma_i^r(1 - p_{i0}^r)}_{\substack{\text{reconnecting after}\\ \text{timeout}}} + \underbrace{\sum_{j=1}^{N} \lambda_j^r p_{jb}^r (1 - p_{b0}^r) p_{ji}^r}_{\substack{\text{joining after being blocked}\\ \text{at cell } j \text{ due to congestion}}} \,, \qquad (1)$$

where the proportion of blocked calls p_{ib}^r and the rate of admitted calls that has timed out γ_i^r depend on λ_j^r, $\forall j$. The model as presented is suitable for modelling different mobile technologies under an attack. More details, and a comparison of the attacks' influence on two groups of technologies, are presented in [34].

2.2 User behaviour model

An important part of the network model is the user behaviour model. In general, the two classes of calls have different service time distributions. A normal call, for example web browsing traffic, would usually happen in bursts which would occupy the channel for a longer period. Contrary, attack calls would usually transfer only a small portion of data in order to trigger quick bandwidth allocations and deallocations. The two patterns are depicted on Fig. 2 with T^n denoting the *normal session duration* and T^a the *attack session duration*, and s and q respectively denoting "service" and "quiet" periods. In this part we need to estimate the average session duration $E[T^r] = 1/\mu^r$.

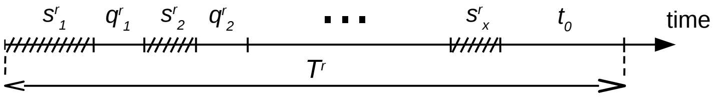

Fig. 2. The user behaviour model describing the duration of a single data session T^r of class r.

Fig. 2 could be translated to a Markov Chain model as in Fig. 3, using the states: service (S), quiet (Q), and end of session (F). The transitions among S and Q states are controlled with α^r, and β^r, where $1/\alpha^r$ is the average communication time of a class-r burst, and $1/\beta^r$ is the average duration of a quiet (inactivity) period, regarding class-r calls. The timeout rate is given with $\tau = 1/t_0$.

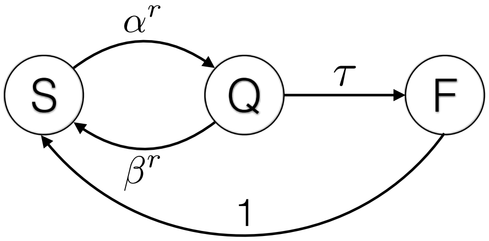

Fig. 3. State diagram of the user behaviour model.

Let us denote with Π_i the probability of the session being in one of the states $\{S, Q, F\}$. The average session duration could be found using the following ratio:

$$\frac{\Pi_S + \Pi_Q + \Pi_F}{1 + E[T^r]} = \Pi_F.$$

Solving the balance equations yields the state probabilities in equilibrium, and the above equation solves to:

$$(\mu^r)^{-1} = E[T^r] \equiv \frac{1}{\mu^r} = \frac{1}{\alpha^r} + \frac{1}{\tau} + \frac{\beta^r}{\alpha^r \tau}. \tag{2}$$

In the above expression, one can see that when the timeout is very short, with $\tau \to \infty$, the average session duration tends to the communication time of a single burst $1/\alpha^r$. Modifying the α^r and β^r parameters, this modelling approach can be used to investigate different traffic types, and different attack patterns.

3 Detection and mitigation

In this Section, we first present two real-time storm detection mechanisms based on counting channel allocations and monitoring bandwidth usage. Both are tested in the SECSIM simulator. The mitigation mechanism employs an idea of using a adjustable inactivity timer, and is tested with the model in Section 2.

3.1 Counter detection

Description. The *Counter detection mechanism* enables detection of signalling storms per mobile terminal in real-time. It is based on counting the repetitive bandwidth allocations of same channel type (eg. a shared FACH or dedicated DCH channel in a 3G UMTS network). It is envisioned as a lightweight mechanism that should not impose any processing, storage, and memory problems if implemented on a mobile terminal.

Decision making. The mechanism requires two input parameters: the time instances of bandwidth allocation and the type of bandwidth allocation, which are stored in memory for the duration of a time window of length t_w. A decision of an attack being detected is simply taken when the number of repetitions reaches a predefined threshold called *counter threshold* - n. The length of the window t_w is chosen such that $t_w > n \cdot t_I$, where t_I the duration of the inactivity timer of the attacked state. The upper limit of t_w is set according the memory and storage capacities of the device on which it is implemented.

Evaluation. Fig. 4 shows the performance of the described detection algorithm using a ROC curve, as calculated with the SECSIM simulator. A threshold of n=3 could be a suitable choice resulting in around 40% true positive detection p_{tp} and less than 0.2% false positive detection p_{fp}.

3.2 Bandwidth monitoring detection

The *Bandwidth monitoring detection mechanism* uses a simple idea of tracking the bandwidth usage of each mobile terminal in a given sliding time window, and calculating a cost function to estimate the likelihood of a terminal performing a signalling attack. It's based on previous analyses which showed that signalling storms are inefficient bandwidth users. The mechanism monitors two input parameters: the total time that the terminal spends while allocated bandwidth within a given time window t_w (denoted with t_D, and t_F respectively for DCH and FACH states in 3G UMTs), and the time which the mobile terminal is allocated bandwidth but does not transfer any data in a time window t_w (denoted with t_{Di} and t_{Fi}). Whenever resources are de/allocated, the detector calculates the ratio $\frac{t_{Fi}+t_{Di}}{t_F+t_D}$, which is then rolled in time using the Exponential Weighted Moving Average (EWMA) algorithm as:

$$C[k] = \alpha \frac{t_{Fi}[k] + t_{Di}[k]}{t_F[k] + t_D[k]} + (1-\alpha)C[k-1], \tag{3}$$

where $k \in \mathbb{N} > 0$ is the index of the state change, $0 \leq \alpha \leq 1$ is a weight parameter and $C[0] = \frac{t_{Fi}[0]+t_{Di}[0]}{t_F[0]+t_D[0]}$ is the initial cost value. As defined, C is between 0 and 1 with values closer to 1 indicating higher probability of an attack.

Decision making. For decision making, we define two thresholding rules, and a rule based on the cost function. Observing the cost C, and having calculated an average C_{avg} over all historical C values, a simple rule of $C \geq \beta C_{avg}$ can be used to detect an attack. A second rule is using an *upper threshold* θ^+ above which we make a decision of an attack. This rule helps in detecting attacks with very small attack rate, for which the cost function rule cannot be used, because $\beta C_{avg} > 1$. A second threshold is defined as *lower threshold* θ^- below which we assume a normal behaviour of the mobile terminal. The θ^- rule helps in protecting mobiles with normal behaviour of high activity, which are assigned a low value of C_{avg}. Setting up these thresholds should be based on offline traffic analysis by the mobile operators.

Evaluation. The performance of the Bandwidth monitoring detection algorithm is depicted with the ROC curve on Fig. 4, which combines the p_{fp} and p_{tp} metrics. Values in the top-left corner of the graph are most desirable, as it produces the highest true positive and lowest false positive detection probabilities. The simulation results suggest that $\alpha = 0.3$ is the most suitable value, producing 95% true positive and 0.04% false positive detection.

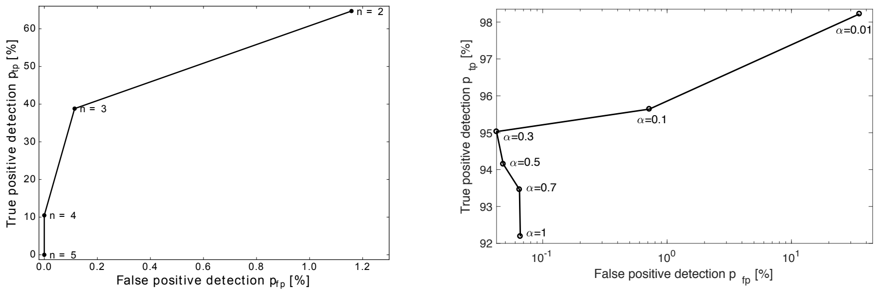

Fig. 4. ROC curves of the counter detector (left), and bandwidth detector (right).

3.3 Dynamic timer mitigation

Mobile networks today use a fixed value for the inactivity timer with possible manual corrections for specific situations, which we consider to not be the optimal approach. While it plays an important role in controlling radio resource allocation, being a trade-off parameter between the bandwidth reuse and number of connections, this section examines if it could possibly play a similar role controlling the impact of a signalling attack on the network. For this, we propose a *dynamic inactivity timer* which is set as a function of the network load, and use the model described in Section 2 to study its performance.

One possible approach is to increase the timer linearly with the load on the signalling server, after a signalling load threshold value θ is reached:

$$t_0(\lambda_s) = \begin{cases} t_0^{min} & \lambda_s \leq \theta, \\ \frac{(t_0^{max} - t_0^{min})}{\lambda_s^{max} - \theta} \cdot (\lambda_s - \theta) + t_0^{min} & \lambda_s > \theta, \end{cases}$$

where λ_s^{max} is the maximum allowed load on the signalling server, θ is a load threshold and t_0^{min} and t_0^{max} are the minimum and maximum values that the timer can take. In real operating network, these parameters need to be estimated from statistical observations.

Results. Using the model in Section 2 we select a data plane model with $m = 20$ non-sharing data channels, such as in 3G UMTS Rel. 99, modelled as M/M/m/m Markov chain [33]. The rest of the parameters are selected as follows: λ_0^n=1, p_0^n=0.9, p_0^a=0.1, p_{b0}^n=0.9, p_{b0}^a=0.3, λ_e=0.05, t_0=2s (static), t_0^{max} =60s, t_0^{min} =2s, λ_s^{max}=5calls/s θ=3calls/s.

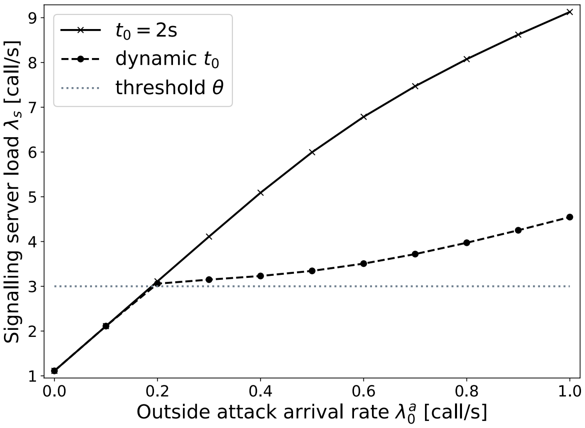

Fig. 5. Signalling server load for static and dynamic inactivity timer.

Fig. 5 shows the comparison of a static and dynamic inactivity timer for varying network load. The dynamic timer activates when the threshold load θ is reached and manages to lower the resulting network load, compared to the static approach. Although the timer can play a control role, it cannot completely mitigate a signalling storm. One downside of using this approach is increasing the portion of normal calls that don't get a service. Therefore, the timer controls the trade-off between the signalling load in the network and the number of unserviced normal calls.

4 Conclusions

This paper has briefly explained the ongoing research in the field of mobile networks security, looking at in particular, signalling related attacks. It introduced a generic mathematical model of the radio access part of a network, which can be used to model different mobile technologies, and different user patterns. The model was afterwards used to examine an attack mitigation technique using a modified inactivity timer. The two proposed attack detection mechanisms were implemented in a simulation environment and their evaluation showed satisfactory results of 95% true positive and 0.04% false positive detection. Recent work has used the Random Neural Network [12] for attack detection [2] and we expect that further results will become available with similar machine learning techniques.

References

1. Abdelrahman, O.H., Gelenbe, E.: Signalling storms in 3G mobile networks. In: IEEE International Conference on Communications (ICC'14), Communication and Information Systems Security Symposium. pp. 1023 –1028. Sydney, Australia (Jun 2014)
2. Abdelrahman, O.H.: Detecting network-unfriendly mobiles with the random neural network. Probability in the Engineering and Informational Sciences pp. 514–531 (2016)
3. Baskett, F., Chandy, K.M., Muntz, R.R., Palacios, F.G.: Open, closed, and mixed networks of queues with different classes of customers. J. ACM pp. 248–260 (Apr 1975)
4. Choi, Y., hyun Yoon, C., Kim, Y.S., Heo, S.W., Silvester, J.A.: The impact of application signaling traffic on public land mobile networks. IEEE Communications Magazine pp. 166–172 (2014)
5. Collen, A., Nijdam, N., Augusto-Gonzalez, J., Katsikas, S., Giannoutakis, K., Spathoulas, G., Gelenbe, E., Votis, K., Tzovaras, D., Ghavami, N., Volkamer, M., Haller, P., Sanchez, A., Dimas, M.: Ghost - safe-guarding home iot environments with personalised real-time risk control. In: Gelenbe, E., Campegiani, P., Czachorski, T., Katsikas, S., Komnios, I., Romano, L., Tzovaras, D. (eds.) Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Lecture Notes CCIS No. 821, Springer Verlag (2018)

6. Cramer, C.E., Gelenbe, E.: Video quality and traffic qos in learning-based subsampled and receiver-interpolated video sequences. IEEE Journal on Selected Areas in Communications pp. 150–167 (2000)
7. Delosières, L., Sánchez, A.: Information Sciences and Systems 2014: Proceedings of the 29th International Symposium on Computer and Information Sciences, chap. DroidCollector: A Honeyclient for Collecting and Classifying Android Applications, pp. 175–183. Springer International Publishing, Cham (2014)
8. Domanka, J., Gelenbe, E., Czachorski, T., Drosou, A., Tzovaras, D.: Research and innovation action for the security of the internet of things: The seriot project. In: Gelenbe, E., Campegiani, P., Czachorski, T., Katsikas, S., Komnios, I., Romano, L., Tzovaras, D. (eds.) Proceedings of the 2018 ISCIS Security Workshop, Imperial College London. Lecture Notes CCIS No. 821, Springer Verlag (2018)
9. Francois, F., Abdelrahman, O.H., Gelenbe, E.: Impact of signaling storms on energy consumption and latency of LTE user equipment. In: Proceedings of the 7th IEEE International Symposium on Cyberspace safety and security (CSS15). New York (Aug 2015)
10. Francois, F., Abdelrahman, O.H., Gelenbe, E.: Feasibility of signaling storms in 3G/UMTS operational networks. In: Internet of Things. IoT Infrastructures: Second International Summit, IoT 360 2015, Rome, Italy, October 27-29, 2015. Revised Selected Papers, Part I. pp. 187–198. Springer International Publishing (2016)
11. Francois, F., Abdelrahman, O.H., Gelenbe, E.: Towards assessment of energy consumption and latency of lte ues during signaling storms. In: Information Sciences and Systems 2015, pp. 45–55. Springer (2016)
12. Gelenbe, E.: Reseaux neuronaux aletoires stables. Comptes rendus de l'Acadmie des sciences. Srie 2, Mcanique, Physique, Chimie, Sciences de l'univers, Sciences de la Terre 310(3), 177–180 (1990)
13. Gelenbe, E.: Probabilistic models of computer systems. Acta Informatica 12(4), 285–303 (1979)
14. Gelenbe, E.: Product-form queueing networks with negative and positive customers. Journal of Applied Probability pp. 656–663 (1991)
15. Gelenbe, E.: Dealing with software viruses: a biological paradigm. information security technical report pp. 242–250 (2007)
16. Gelenbe, E.: A diffusion model for packet travel time in a random multi-hop medium. ACM Transactions on Sensor Networks (TOSN) p. 10 (2007)
17. Gelenbe, E.: Self-aware networks. In: Self-Adaptive and Self-Organizing Systems (SASO), 2011 Fifth IEEE International Conference on. pp. 227–234. IEEE (2011)
18. Gelenbe, E., Abdelrahman, O.H.: Countering mobile signaling storms with counters. Proc. Intl Conf. on Cyber Physical Systems, IoT and Sensors Networks (Cyclone), Rome, Italy (2015)
19. Gelenbe, E., Abdelrahman, O.H., Gorbil, G.: Detection and mitigation of signaling storms in mobile networks. In: Computing, Networking and Communications (ICNC), 2016 International Conference on. pp. 1–5. IEEE (2016)
20. Gelenbe, E., Loukas, G.: A self-aware approach to denial of service defence. Comput. Netw. pp. 1299–1314 (Apr 2007)
21. Gelenbe, E., Mitrani, I.: Analysis and synthesis of computer systems, vol. 4. World Scientific (2010)
22. Gelenbe, E., Muntz, R.R.: Probabilistic models of computer systemspart i (exact results). Acta Informatica 7(1), 35–60 (1976)
23. Gorbil, G., Abdelrahman, O.H., Gelenbe, E.: Storms in mobile networks. In: Proceedings of the 9th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet'14). pp. 119–126 (Sep 2014)

24. Gorbil, G., Abdelrahman, O.H., Pavloski, M., Gelenbe, E.: 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 pp. 1–14 (Jan 2015)
25. Gorbil, G., Gelenbe, E.: Opportunistic communications for emergency support systems. Procedia Computer Science pp. 39–47 (2011)
26. Gupta, A., Verma, T., Bali, S., Kaul, S.: Detecting ms initiated signaling ddos attacks in 3g/4g wireless networks. 2013 Fifth International Conference on Communication Systems and Networks (COMSNETS) pp. 1–60 (jan 2013)
27. Jackson, J.R.: Jobshop-like queueing systems. Management Science pp. 131–142 (1963)
28. Kambourakis, G., Kolias, C., Gritzalis, S., Park, J.H.: Dos attacks exploiting signaling in umts and ims. Comput. Commun. pp. 226–235 (March 2011)
29. Kotapati, K., Liu, P., Sun, Y., LaPorta, T.F.: Intelligence and Security Informatics: IEEE International Conference on Intelligence and Security Informatics, ISI 2005, Atlanta, GA, USA, May 19-20, 2005. Proceedings, chap. A Taxonomy of Cyber Attacks on 3G Networks, pp. 631–633. Springer Berlin Heidelberg, Berlin, Heidelberg (2005)
30. Lee, P.P.C., Bu, T., Woo, T.: On the detection of signaling DoS attacks on 3G wireless networks. In: Proceedings - IEEE INFOCOM. pp. 1289–1297 (2007)
31. Loukas, G., Oke, G., Gelenbe, E., et al.: Defending against denial of service in a self-aware network: A practical approach. In: NATO Symposium on Information Assurance for Emerging and Future Military Systems. Ljubljana, Slovenia (2008)
32. Mulliner, C., Liebergeld, S., Lange, M., Seifert, J.P.: Taming Mr Hayes: Mitigating signaling based attacks on smartphones. In: Proceedings of the International Conference on Dependable Systems and Networks (2012)
33. Pavloski, M.: A performance approach to mobile security. In: 2016 IEEE 24th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS). pp. 325–330 (Sept 2016)
34. Pavloski, M.: Performance analysis of mobile networks under signalling storms. Ph.D. thesis, Imperial College London (2017)
35. Pavloski, M., Gelenbe, E.: Signaling attacks in mobile telephony. In: Proceedings of the 11th International Conference on Security and Cryptography (SECRYPT'14). pp. 206–212 (aug 2014)
36. Pavloski, M., Görbil, G., Gelenbe, E.: Counter based detection and mitigation of signalling attacks. In: Obaidat, M.S., Lorenz, P., Samarati, P. (eds.) SECRYPT 2015 - Proceedings of the 12th International Conference on Security and Cryptography, Colmar, Alsace, France, 20-22 July, 2015. pp. 413–418. SciTePress (2015)
37. Pavloski, M., Görbil, G., Gelenbe, E.: Information Sciences and Systems 2015: 30th International Symposium on Computer and Information Sciences (ISCIS 2015), chap. Bandwidth Usage—Based Detection of Signaling Attacks, pp. 105–114. Springer International Publishing, Cham (2016)
38. Qian, F., Wang, Z., Gerber, A., Mao, Z.M., Sen, S., Spatscheck, O.: Characterizing radio resource allocation for 3g networks. In: Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement. pp. 137–150. IMC '10, ACM, New York, NY, USA (2010)
39. Ricciato, F., Coluccia, A., DAlconzo, A.: A review of DoS attack models for 3G cellular networks from a system-design perspective. Computer Communications pp. 551 – 558 (2010)

40. Wang, H., Zhang, D., Shin, K.G.: Change-point monitoring for the detection of DoS attacks. IEEE Transactions on Dependable and Secure Computing pp. 193–208 (Oct 2004)
41. Wu, Z., Zhou, X., Yang, F.: Defending against DoS attacks on 3G cellular networks via randomization method. In: Educational and Information Technology (ICEIT), 2010 International Conference on. pp. V1–504–V1–508 (2010)