Countering Mobile Signaling Storms with Counters

Erol Gelenbe(✉) and Omer H. Abdelrahman

Department of Electrical and Electronic Engineering,
Imperial College, London SW7 2BT, UK
{e.gelenbe,o.abd06}@imperial.ac.uk

Abstract. Mobile Networks are subject to signaling storms launched by misbehaving applications or malware, which result in bandwidth overload at the cell level and excessive signaling within the mobile operator, and may also deplete the battery power of mobile devices. This paper reviews the causes of signaling storms and proposes a novel technique for storm detection and mitigation. The approach is based on counting the number of successive signaling transitions that do not utilize allocated bandwidth, and temporarily blocking mobile devices that exceed a certain threshold to avoid overloading the network. Through a mathematical analysis, we derive the optimum value of the counter's threshold, which minimizes both the number of misbehaving mobiles and the signaling overload in the network. Simulation results are provided to illustrate the effectiveness of the proposed scheme.

Keywords: Signaling overload · Radio resource control · M2M · IoT · Application malfunctions · Malware · QoS

1 Introduction

There has been significant industry interest worldwide regarding mobile signaling overload or "signaling storms" which have been publicly documented in the real world numerous times [6,10,11,15,31]. Signaling storms can be triggered by various factors, which all lead to a large number of mobile devices making successive connection requests that then time-out because of inactivity, triggering repeated signaling to allocate and de-allocate radio channels and other resources in the network.

This type of behavior on wireless networks can result in abusive bandwidth occupancy, excessive signaling at the mobile operator [2,22], battery dissipation at mobile devices [14], and extra energy consumption in base stations and backbone networks [17,18,34]. If mobile technology is exploited in cyber-physical infrastructures such as the smart grid, or for the Internet of Things (IoT) including vehicular technologies, smart homes, and emergency management systems [20], such signaling storm effects can delay or impair communications which are of vital importance. In IoT and machine to machine (M2M) applications, the

B. Mandler et al. (Eds.) IoT 360° 2015, Part I, LNICST 169, pp. 199–209, 2016.
DOI: 10.1007/978-3-319-47063-4_18

massive number of devices to be supported and actions which may be synchronized, require new efforts to make such networks resilient and reliable [4]. Thus in this paper, we propose and analyze a novel approach that aims to protect cellular networks against signaling storms that can be caused by mobile malware or misbehaving applications.

1.1 Signaling Storms

The vulnerability of mobile networks to signaling denial of service (DoS) attacks is not new. Indeed, early work has identified different ways to attack the control plane of mobile networks, e.g. through paging [35], service requests [37] and radio resource control (RRC) [26,33]. Poorly designed mobile applications are perhaps one of the most common triggers of signaling overloads [6] that lead to performance degradation and even network outages [11,15]. Such "chatty" applications constantly poll the network, even when users are inactive, in order to provide always-on connectivity, background updates [29] and in-application advertisements [10]. Similar problems have been reported with M2M systems that transmit small amounts of data with deterministic intervals [1,25,36]. A common issue with those applications is that developers are not familiar with the control plane of mobile networks, so they build applications without considering their adverse effect on the networks. This has prompted the mobile industry to promote best practices for developing network-friendly applications [7,13,23,24].

Industry guidelines, however, do not provide adequate protection against signaling storms which can be triggered by well-designed applications, when an unexpected event occurs in the Internet. Examples of such events include outages in mobile cloud services [8,31] and in VoIP peer-to-peer networks [9]. During those incidents, a large number of mobile devices attempt to recover connectivity to the application servers, generating significantly more keep-alive messages [5] and an unexpectedly high signaling load in the process.

In addition, signaling storms may occur as a by-product of malicious activity that is not intended to cause a signaling DoS attack. The perpetrators in many of those incidents rely on the Internet to carry out profitable attacks, and therefore it is against their interest to cause disruption in the access to the infrastructure. Examples of such scenarios include: (i) Large-scale malware infections with frequent communications, such as premium SMS dialers, spammers, adware and bot-clients, which are among the top encountered threats on smartphones [28] and have been shown [27] to exhibit resource-inefficient communication patterns. (ii) Unwanted traffic in the Internet [32], including backscatter noise from remote DoS attacks, scanning worms, and spam campaigns, which pose a risk to mobile networks that can be eliminated using middleboxes, but is often not due to carriers' policies [30,38]. (iii) Network outages due to cyber-attacks which could be followed (and hence prolonged) by a signaling storm, due to the large number of user devices that will attempt to reconnect after the service is restored [12].

2 The Model

We represent the set of normal and malicious mobile calls in the system at time t by a state $s(t) = (b, B, C, A_1, a_1, ..., A_i, a_i, ...; t)$ where:

- b is the number of mobiles which are in low bandwidth mode,
- B is the number of normal mobiles which are in high bandwidth mode,
- C is the number of normal mobiles that have started to transfer or receive data or voice in high bandwidth mode,
- A_i is the number of attacking mobiles which are in high bandwidth mode and have undergone a time-out for $i-1$ times,
- a_i is the number of attacking mobiles which have entered low bandwidth mode from high bandwidth mode after i time-outs.

We assume a Poisson arrival process of rate λ of new mobile activations or calls, and a call that is first admitted in state b then requests high bandwidth at rate r. Note that r^{-1} can be viewed as the average time it takes a call to make its first high bandwidth request to the network. With probability $\bar{\alpha} = 1 - \alpha$ such a call will be of normal type and will enter state B, while with probability α it will be an attacking call and will request high bandwidth and hence enter state A_1 indicating the first request for bandwidth that is made by a defectively operating application or malware that can contribute to a storm. Thus, α is a metric that represents the fraction of all activations that are attacking or mobiles which contain malware or a deficient application.

Once a call enters state A_1, since it is misbehaving, it will not start a communication and will time-out after some time of average value τ^{-1}. Note that the time-out is a parameter that is set by the operator for all the mobile devices so that they will not occupy the high bandwidth mode if they are actually not making use of it, and in practice it is of the order of a few seconds. After entering state a_1, the call may be detected as being anomalous, and will be removed or blocked from the system at rate β_1, where β_1^{-1} is the average time it takes the detector to identify that this call has the potential to contribute to a storm, and to block the device from making further connections. However, it is very unlikely that the system is so smart that it can make this decision correctly regarding the call so early in the game, so typically $\beta_1 \simeq 0$ and the call will manage to request high bandwidth and then enter state A_2 at rate r. Proceeding in the same manner, in state A_i the anomalous call will again not start a normal communication, so it will eventually time-out after an average time τ and enter state a_i, and so on.

Now with regard to normal calls, a normally operating mobile in high bandwidth mode B may transition to the communicating mode C at rate κ, signifying that transmission or reception has started, or it will transition back to the low bandwidth mode at a rate τ that signifies a time-out. From state C the call's activity may be interrupted, as when a mobile device stops sending or receiving data to/from a web site, in which case the call will return to state B at rate μ. Similarly, the call may end at rate δ, leaving the system. The parameters κ, μ and δ can represent a wide range of normal mobile usage patterns. For example,

Table 1. State transitions in the model.

Transition	Rate	Cause
$b \to b+1$	λ	network activation (attach)
$(b,B) \to (b-1, B+1)$	$br\bar{\alpha}$	new normal call
$(B,C) \to (B-1, C+1)$	$B\kappa$	start sending or receiving traffic
$(b,B) \to (b+1, B-1)$	$B\tau$	time-out for a normal call
$C \to C-1$	$C\delta$	end of a normal call
$(B,C) \to (B+1, C-1)$	$C\mu$	stop sending or receiving traffic
$(b,A_1) \to (b-1, A_1+1)$	$br\alpha$	new attack call
$(a_{i-1},A_i) \to (a_{i-1}-1, A_i+1)$	$a_{i-1}r$	i-th superfluous transition of an attack call, $i>1$
$(a_i,A_i) \to (a_i+1, A_i-1)$	$A_i\tau$	i-th time-out of an attack call, $i \geq 1$
$a_i \to a_i - 1$	$a_i\beta_i$	attack call blocked after i time-outs, $i \geq 1$

a web browsing session or call normally lasts for several minutes or even hours (thus δ is typically very small), but may include several downloading and reading times, with mean of μ^{-1} and κ^{-1}, respectively; in this case, the time-out operates only while the user is reading, taking the state from B to b.

With the above assumptions, Table 1 shows the possible transitions from the state $s(t)$. Note that all of the state transitions which are not indicated in the table are simply the ones where the state is unchanged, and furthermore note that apart from the first case, the state transition rates are population dependent.

Assuming that all the rates that are indicated are the parameters of independent and identically distributed exponential random variables, and that the probability α corresponds to successively independent and identically distributed events, the above model has an exact equilibrium solution [16,19] that can be easily calculated, and thus can provide the joint probability distribution of the state $s(t)$. However the rate parameters r and μ are actually congestion dependent. This means that they will essentially dependent on the number of calls in each of the states because for a total amount of bandwidth in the system at a base station level of say W, the total amount of bandwidth available may be expressed as some value $W^* = W - w_1(b + \sum_i a_i) - w_2(B + \sum_i A_i) - w_3 C$ where w_1, w_2 and w_3 denote the bandwidth allocated per low bandwidth, inactive high bandwidth and active high bandwidth requests, respectively. Thus in reality the rate r will be "slowed down" as W^* becomes smaller since requests will be delayed or will even remain unsatisfied. The matter is of course more complex, because not only the bandwidth allocation itself but the error probabilities in the channel will be affected by the amount of bandwidth that is already allocated and thus the channel holding time μ^{-1} will also depend on W^*.

A schematic diagram of the model is presented in Fig. 1(a), showing the states $s(t) \in \{b, B, C, a_1, A_1, \ldots, a_i, A_i, \ldots\}$, possible transitions, and rates at which *each* of the calls in one state will transition to another state. Assuming that the transition rates r and μ do *not* depend on the number of mobiles that are

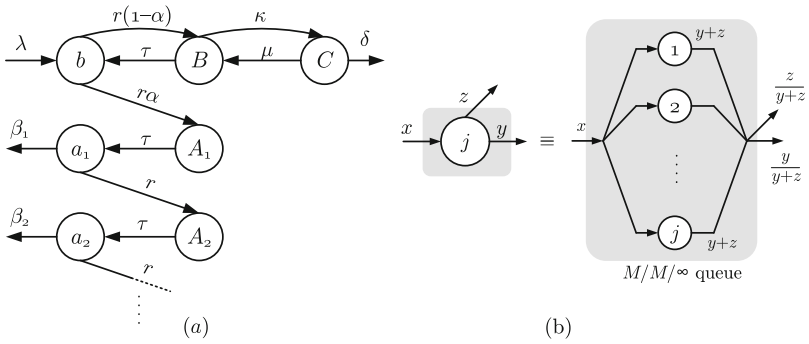

Fig. 1. (a) A schematic diagram of the state transition model for the number of normal and attacking calls in the network. (b) An $M/M/\infty$ queueing representation of a node j with arrival rate x and transition rates (for each of the calls in j) y and z; the ratios $y/(y+z)$ and $z/(y+z)$ denote the transition probabilities from state j

using the bandwidth, calls act independently of each other so that the evolution of the number of calls in any of the states can be represented by an equivalent $M/M/\infty$ queueing model as shown in Fig. 1(b).

2.1 Traffic Equations and Equilibrium Probability Distribution

The arrival rate of calls into each of the possible states may be written as Λ_j where $j \in \{b, B, C, A_1, a_1, ..., A_i, a_i, ...\}$ which satisfy a system of linear equations. Specifically, the rates at which calls enter the attack states are simply:

$$\begin{aligned} \Lambda_{a_i} &= \Lambda_{A_i}, \\ \Lambda_{A_1} &= \alpha\Lambda_b, \\ \Lambda_{A_i} &= \Lambda_{a_{i-1}} \frac{r}{r+\beta_{i-1}} = \alpha\Lambda_b \prod_{l=1}^{i-1} \frac{r}{r+\beta_l}, \ i > 1 \end{aligned} \tag{1}$$

where Λ_b is the rate at which calls enter state b which is calculated as follows. The rates at which calls enter the normal operating states are described by the linear equations:

$$\begin{aligned} \Lambda_b &= \lambda + \frac{\tau}{\tau+\kappa}\Lambda_B, \\ \Lambda_B &= (1-\alpha)\Lambda_b + \frac{\mu}{\mu+\delta}\Lambda_C, \\ \Lambda_C &= \frac{\kappa}{\kappa+\tau}\Lambda_B, \end{aligned} \tag{2}$$

so that $\Lambda_B = \gamma\Lambda_b$, where $\gamma = \frac{1-\alpha}{1-\frac{\mu\kappa}{(\mu+\delta)(\kappa+\tau)}}$, and:

$$\Lambda_b = \frac{\lambda}{1 - \frac{\tau}{\tau+\kappa}\gamma} = \frac{\lambda}{1 - \frac{\tau(1-\alpha)}{\tau+\kappa-\frac{\mu\kappa}{\mu+\delta}}}, \quad \Lambda_B = \frac{\lambda\gamma}{1 - \frac{\tau}{\tau+\kappa}\gamma}, \quad \Lambda_C = \frac{\kappa\lambda\gamma}{\kappa + \tau(1-\gamma)}. \quad (3)$$

Since we assume that the transition rates r and μ do *not* depend on the number of mobiles in the system, calls act independently of each other so that the *average number* of calls in each of the states is the *average arrival rate* of calls into the state, multiplied by the *average time* spent by a call in that state. We will present here only results for the attacking states, since we are interested in mitigating the storm. We first note that the average time spent by a mobile in state a_i is $(r+\beta_i)^{-1}$ and in A_i is τ^{-1}, so that the average number of mobiles in equilibrium N_j in each of the attacking states becomes:

$$\begin{aligned} N_{A_1} &= \frac{\alpha\Lambda_b}{\tau}, \\ N_{A_i} &= \frac{\alpha\Lambda_b}{\tau}\prod_{l=1}^{i-1}\frac{r}{r+\beta_l}, \ i > 1, \\ N_{a_i} &= \frac{\alpha\Lambda_b}{r+\beta_i}\prod_{l=1}^{i-1}\frac{r}{r+\beta_l}, \ i \geq 1. \end{aligned} \quad (4)$$

As a consequence, the total average number of malicious calls becomes:

$$N_\alpha = \sum_{i=1}^{\infty}[N_{a_i} + N_{A_i}] = \alpha\Lambda_b \sum_{i=1}^{\infty}\Big[(\frac{1}{\tau} + \frac{1}{r+\beta_i})\prod_{l=1}^{i-1}\frac{r}{r+\beta_l}\Big]. \quad (5)$$

2.2 Optimum Counter for Mitigation

Although choosing a relatively small value of the time-out of the order of a few seconds can be useful, we see that some additional mechanism needs to be inserted to mitigate the effect of signaling storms. Therefore we suggest that a counter value n be selected so that as long as the number of successive times that the mobile uses the time-out is less than n, then the mobile remains attached to the network. However as soon as this number reaches n, then the mobile is detached after a time of average value β^{-1}. Thus β^{-1} can be viewed as the decision time plus the physical detachment time that is needed.

A large value of n will improve the chances of *correctly* detecting a misbehaving mobile user, providing the system with full confidence to activate the mitigation policy. If n is small we may have false positives, requiring analysis of the users behavior with other ongoing connections, or checking some data plane attributes such as destination IP addresses or port numbers that may be associated with malicious activities. Thus the higher the n, the faster the decision can be to disconnect the mobile, i.e. β increases with the threshold n, with a slope or derivative with respect to n expressed as $\beta^{'}$.

Based on this principle, and with reference to our earlier definition of β_i, we have:

$$\beta_i = \begin{cases} 0, & 1 \leq i < n, \\ \beta(n), & i \geq n \end{cases} \quad (6)$$

so that storm mitigation is activated when high bandwidth is requested n successive times, each followed by a time-out. Using the previous analysis, the average number of malicious calls becomes:

$$N_\alpha = \alpha \Lambda_b [(n - 1 + \frac{r}{\beta})(\frac{1}{\tau} + \frac{1}{r}) + \frac{1}{\tau}] \tag{7}$$

while the resulting signaling load from the attack is given by the total rate of malicious transitions between low and high bandwidth states:

$$\Lambda_\alpha = \alpha \Lambda_b + \sum_{i=1}^{\infty} [\Lambda_{a_i} + \Lambda_{A_i}] = \alpha \Lambda_b [2n + 1 + \frac{2r}{\beta}] \tag{8}$$

With some further simple analysis we can show that the value n^* that minimizes *both* N_α and Λ_α, is the value that satisfies:

$$\beta(n^*)^2 \approx r.\beta^{'}(n^*). \tag{9}$$

As an example, consider a detection rate that increases linearly with the threshold according to $\beta(n) = mn,\ m > 0$. In this case, the optimum value of the counter's threshold is obtained by solving the quadratic equation $m^2 n^2 = rm$ which yields:

$$n^* = \sqrt{r/m}.$$

We see that n^* decreases with m, which means that the optimum threshold becomes smaller when the network is more able (i.e. larger m) to detect malicious connections using data plane attributes. This simple example illustrates how the proposed counter-based approach can be optimized when deployed in conjunction with detection systems [3] that analyze IP packets to identify attacks.

3 Simulation Experiments

In this section we evaluate the performance of the joint detection and mitigation approach that we have proposed using the mobile network simulator described in [21,22]. We illustrate how the proposed scheme allows quick reaction to malicious signaling behaviors or to malfunctioning applications, by showing the temporal behavior of network signaling load and delay during normal operation and then during an attack which is being detected and mitigated with our approach. However, we have not addressed the problem of how to set the parameters of the mathematical model based on the average mobile user profile and network configurations, so as to optimize the counter's threshold using Eq. (9); we leave this issue for future work.

The results that we present were obtained by simulating 500 mobile devices, each running the detection and mitigation mechanism, in an area of $2 \times 2\,\mathrm{km}^2$ which is covered by 7 UMTS base stations connected to a single radio network controller (RNC). All mobiles join the network at the beginning of the simulation, and generate web browsing traffic following a model based on industry recommendations and web metrics released by Google. We assume 20 % of the mobiles

are malicious or compromised, which overload the RNC by causing superfluous promotions to the high bandwidth DCH state. The service times in the RNC have been artificially increased in order to simulate overload conditions with a small number of mobiles.

In Fig. 2, the signaling misbehavior starts gradually between 2800 and 4000 s from the beginning of the simulation, rather than suddenly, in order to prevent artifacts such as a huge spike of signaling load due to many devices attacking at the same time. Also, for the purpose of showing the effect of the storm and the proposed countermeasure, we activate the mitigation mechanism at 7000 s.

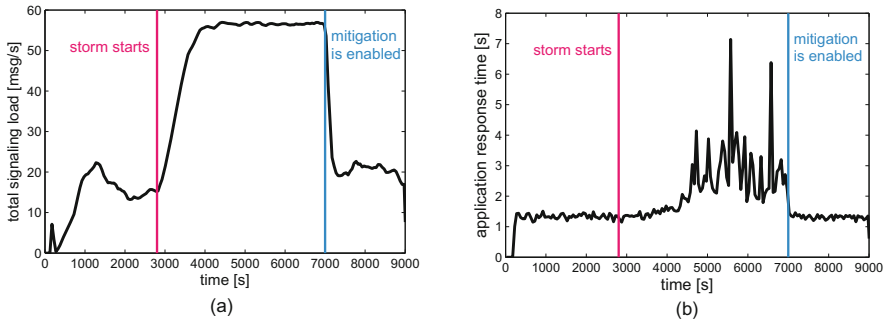

Fig. 2. Simulation results: (a) total signaling load at the RNC, and (b) application response time. The mitigation mechanism is activated at 7000 s to allow the storm to develop and to show the effectiveness of the approach. The counter's threshold was set experimentally to $n = 3$ based on performance.

Figure 2(a) shows the number of signaling messages sent and received per second by the RNC as captured during a simulation run. The application response time at a normal mobile is shown in Fig. 2(b), which is the duration between when the user requests a web page and when all of the web page is received. The results are obtained by using an averaging window of size 50 s. It can be observed that the signaling load increases significantly as a result of the attack, which in turn increases the time it takes for a mobile to acquire a radio channel to send and receive data, leading to higher latency and jitter. However, the proposed detection and mitigation scheme is able to quickly identify and mitigate the attack, effectively recovering the average response time for the normal users to the level they had before the storm.

4 Conclusions

Mobile operators have recently experienced an exponential growth in mobile data traffic, coupled with a greater surge in signaling loads which degrade the quality of service for users. These signaling storms will continue to pose challenges to operators, especially with the expected wide deployment of M2M and

IoT applications over cellular networks, due to the massive number of devices to be supported, the fact that those devices may act in a synchronized manner, and the absence of the human-in-the-loop in most applications. As the demand for always-on connectivity increases from mobile and M2M applications, signaling storms can become a significant show stopper, particularly from the perspective of the response time requirements of applications, hence underscoring the need for new approaches to make networks more resilient and reliable.

Thus we have suggested a novel mitigation approach for signaling storms, that maintains a counter for each active mobile device, either within the device or at the network signaling server. If the counter exceeds a certain threshold, indicating excessive radio resource control requests, the mobile device is temporarily blocked to avoid overloading the signaling plane. We developed a mathematical model which examines the role of the time-out and computes the counter's threshold that minimizes both signaling load and number of misbehaving devices. Simulation results illustrate these behaviors, showing that the counter-based technique restores the signaling load and application response times to their values before the storm began.

Acknowledgments. We thank Mihajlo Pavloski and Gokce Gorbil for the simulation results, and the EU FP7 project NEMESYS (Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem), grant agreement no. 317888, for financial support.

References

1. 3GPP: Study on machine-type communications (MTC) and other mobile data applications communications enhancements (release 12) (2013). 3GPP TR 23.887. http://www.3gpp.org/DynaReport/23887.htm
2. Abdelrahman, O.H., Gelenbe, E.: Signalling storms in 3G mobile networks. In: Proceedings of IEEE International Conference on Communications (ICC), pp. 1017–1022, Sydney (2014). doi:10.1109/ICC.2014.6883453
3. Abdelrahman, O.H., Gelenbe, E.: A data plane approach for detecting control plane anomalies in mobile networks. In: Proceedings of International Conference on Cyber Physical Systems, IoT and Sensors Networks (Cyclone), Rome (2015)
4. Abdelrahman, O.H., Gelenbe, E., Gorbil, G., Oklander, B.: Mobile network anomaly detection and mitigation: the NEMESYS approach. In: Gelenbe, E., Lent, R. (eds.) Information Sciences and Systems 2013. Lecture Notes in Electrical Engineering, vol. 264, pp. 429–438. Springer, Switzerland (2013). doi:10.1007/978-3-319-01604-7_42
5. Amrutkar, C., Hiltunen, M., Jim, T., Joshi, K., Spatscheck, O., Traynor, P., Venkataraman, S.: Why is my smartphone slow? on the fly diagnosis of underperformance on the mobile internet. In: Proceedings of 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 1–8. IEEE Computer Society, Budapest (2013). doi:10.1109/DSN.2013.6575301
6. Arbor Networks: Worldwide infrastructure security report (2014). http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf
7. AT&T: Best practices for 3G and 4G app development. Whitepaper (2012). http://developer.att.com/static-assets/documents/library/best-practices-3g-4g-app-development.pdf

8. Choi, Y., Yoon, C.H., Kim, Y.S., Heo, S.W., Silvester, J.: The impact of application signaling traffic on public land mobile networks. IEEE Commun. Mag. **52**(1), 166–172 (2014). doi:10.1109/MCOM.2014.6710079
9. Coluccia, A., D'alconzo, A., Ricciato, F.: Distribution-based anomaly detection via generalized likelihood ratio test: a general maximum entropy approach. Comput. Netw. **57**(17), 3446–3462 (2013). doi:10.1016/j.comnet.2013.07.028
10. Corner, S.: Angry birds + android + ads = network overload (2011). http://www.itwire.com/business-it-news/networking/47823
11. Donegan, M.: Operators urge action against chatty apps. Light Reading Report (2011). http://www.lightreading.com/operators-urge-action-against-chatty-apps/d/d-id/687399
12. Ericsson: High availability is more than five nines (2014). http://www.ericsson.com/real-performance/wp-content/uploads/sites/3/2014/07/high-avaialbility.pdf
13. Ericsson: A smartphone app developers guide: Optimizing for mobile networks. Whitepaper (2014). http://www.ericsson.com/res/docs/2014/smartphone-app-dev-guide.pdf
14. Francois, F., Abdelrahman, O.H., Gelenbe, E.: Impact of signaling storms on energy consumption and latency of LTE user equipment. In: Proceedings of 7th IEEE International Symposium on Cyberspace safety and security (CSS), New York (2015)
15. Gabriel, C.: DoCoMo demands Google's help with signalling storm (2012). http://www.rethink-wireless.com/2012/01/30/docomo-demands-googles-signalling-storm.htm
16. Gelenbe, E.: The first decade of G-networks. Eur. J. Oper. Res. **126**(2), 231–232 (2000)
17. Gelenbe, E., Mahmoodi, T.: Energy-aware routing in the cognitive packet network. In: ENERGY, Venice (2011)
18. Gelenbe, E., Morfopoulou, C.: A framework for energy-aware routing in packet networks. Comput. J. **54**(6), 850–859 (2011)
19. Gelenbe, E., Timotheou, S.: Random neural networks with synchronized interactions. Neural Comput. **20**(9), 2308–2324 (2008)
20. Gelenbe, E., Wu, F.J.: Large scale simulation for human evacuation and rescue. Comput. Math. Appl. **64**(12), 3869–3880 (2012)
21. Gorbil, G., Abdelrahman, O.H., Gelenbe, E.: Storms in mobile networks. In: Proceedings of 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet), Montreal, pp. 119–126 (2014). doi:10.1145/2642687.2642688
22. Gorbil, G., Abdelrahman, O.H., Pavloski, M., Gelenbe, E.: Modeling and analysis of RRC-based signalling storms in 3G networks. IEEE Trans. Emerg. Topics Comput. **4**(1), 113–127 (2016). doi:10.1109/TETC.2015.2389662
23. GSMA: Smarter apps for smarter phones, version 4.0 (2014). http://www.gsma.com/newsroom/wp-content/uploads//TS-20-v4-0.pdf
24. Jiantao, S.: Analyzing the network friendliness of mobile applications. Technical report, Huawei (2012). http://www.huawei.com/ilink/en/download/HW_146595
25. Ksentini, A., Hadjadj-Aoul, Y., Taleb, T.: Cellular-based machine-to-machine: overload control. IEEE Netw. **26**(6), 54–60 (2012). doi:10.1109/MNET.2012.6375894
26. Lee, P.P., Bu, T., Woo, T.: On the detection of signaling DoS attacks on 3G wireless networks. In: Proceedings of 26th IEEE Internatioanl Conference on Computer Communications (INFOCOM), pp. 1289–1297 (2007). doi:10.1109/INFCOM.2007.153

27. Li, J., Pei, W., Cao, Z.: Characterizing high-frequency subscriber sessions in cellular data networks. In: Proceedings of IFIP Networking Conference, Brooklyn, pp. 1–9 (2013)
28. Maslennikov, D.: Mobile malware evolution: Part 6. Technical report, Kaspersky Lab (2013). https://securelist.com/analysis/publications/36996/mobile-malware-evolution-part-6/
29. NSN Smart Labs: Understanding smartphone behavior in the network. White paper (2011). http://networks.nokia.com/system/files/document/nsn_smart_labs_white_paper.pdf
30. Qian, Z., Wang, Z., Xu, Q., Mao, Z.M., Zhang, M., Wang, Y.M.: You can run, but you can't hide: exposing network location for targeted DoS attacks in cellular networks. In: Proceedings of Network and Distributed System Security Symposium (NDSS), San Diego, pp. 1–16 (2012)
31. Redding, G.: OTT service blackouts trigger signaling overload in mobile networks (2013). https://blog.networks.nokia.com/mobile-networks/2013/09/16/ott-service-blackouts-trigger-signaling-overload-in-mobile-networks/
32. Ricciato, F.: Unwanted traffic in 3G networks. ACM SIGCOMM Comput. Commun. Rev. **36**(2), 53–56 (2006). doi:10.1145/1129582.1129596
33. Ricciato, F., Coluccia, A., D'Alconzo, A.: A review of DoS attack models for 3G cellular networks from a system-design perspective. Comput. Commun. **33**(5), 551–558 (2010). doi:10.1016/j.comcom.2009.11.015
34. Sakellari, G., Morfopoulou, C., Mahmoodi, T., Gelenbe, E.: Using energy criteria to admit flows in a wired network. In: Gelenbe, E., Lent, R. (eds.) Computer and Information Sciences III, pp. 63–72. Springer, London (2013). doi:10.1007/978-1-4471-4594-3_7
35. Serror, J., Zang, H., Bolot, J.C.: Impact of paging channel overloads or attacks on a cellular network. In: Proceedings of 5th ACM Workshop Wireless Security (WiSe 2006), New York, pp. 75–84 (2006). doi:10.1145/1161289.1161304
36. Shafiq, M.Z., Ji, L., Liu, A.X., Pang, J., Wang, J.: A first look at cellular machine-to-machine traffic: large scale measurement and characterization. SIGMETRICS Perf. Eval. Rev. **40**(1), 65–76 (2012). doi:10.1145/2318857.2254767
37. Traynor, P., Lin, M., Ongtang, M., Rao, V., Jaeger, T., McDaniel, P., La Porta, T.: On cellular botnets: measuring the impact of malicious devices on a cellular network core. In: Proceedings of 16th ACM conference on Computer and Communications Security (CCS), Chicago, pp. 223–234 (2009). doi:10.1145/1653662.1653690
38. Wang, Z., Qian, Z., Xu, Q., Mao, Z., Zhang, M.: An untold story of middleboxes in cellular networks. In: Proceedings of ACM SIGCOMM, Toronto, pp. 374–385 (2011). doi:10.1145/2018436.2018479