Signalling Storms and Taylor's Law

Erol Gelenbe
Inst. of Theoretical & App. Informatics
Polish Acad. of Sciences (IITIS-PAN)
44100 Gliwice, PL
& CNRS I3S, Université Côte d'Azur, 06103 Nice, FR
ORCID:0000-0001-9688-2201

Omer H. Abdelrahman
Virgin Media O2
3 Sheldon Square, London W26HY, UK
ORCID:0000-0001-9582-3250

***Abstract*—Signalling storms have occurred in several generations of mobile networks due to malevolent end users, as well as a consequence of service disruptions and system failures. Due to the massive increase in the volume of traffic and the diversity of end users and applications in $6G$, including the massive access of the Internet of Things, signalling storms and other cyberattacks will require attention with research on adequate detection and mitigation schemes, as we move towards the next generation of mobile networks. Thus, in the present paper, we conduct discrete event simulations of a signalling storm, measure its effects in a simulated environment, and observe that it results in deviations from the well-known and naturally observed statistical property known as "Taylor's Law". We then discuss a mathematical model of storms, linking the fraction of malevolent or malfunctioning users to the rate of call establishment requests, and show that the mathematical model also exhibits a violation of Taylor's Law. Since the detection of cyberattacks from network behaviour parameters is a challenging problem, we suggest that the violation of Taylor's Law may be a useful tool for designing detectors for signalling attacks, or other network attacks or malfunctions.**

***Index Terms*—Attack Detection and Mitigation, 6G, Signalling Attacks, Taylor's Law**

I. Introduction

While the number of Internet users worldwide reaches approximately 6 billion, it is expected that in 2025 over 61.5% of Internet traffic will originate with mobile devices, and each smartphone will use some 24 GB of data per month [1]. As shown in Figure I, the amount of traffic per smartphone user is expected to grow even further in the coming years, and over-and-above this traffic that is driven by human users, Machine-to-Machine and Internet of Things (IoT) traffic increasingly shares the common backbone network [2] and uses the same wireless networks. Furthermore, the number of IoT-connected devices worldwide has doubled between 2019 and 2023 to reach 15.70 billion, and then grown further to 17.70 billion in 2024, and is expected to reach 31 billion by 2030 [3].

However, this expansion is accompanied by huge cybersecurity risks, both for human end users and for the IoT, including examples such as cyberattacks that purposely misdirect incoming road traffic in smart cities [4]. For instance, the 2024 statistics reveal an increase in IoT malware attacks by 37% in the first half of the year, resulting in 77.9 million attacks in that period, up from the 57 million in the corresponding period of 2022 [5], [6].

Erol Gelenbe's work was partially supported by the EU Horizon 2020 Project DOSS, Grant Agreement No. Grant Agreement No. 101120270.

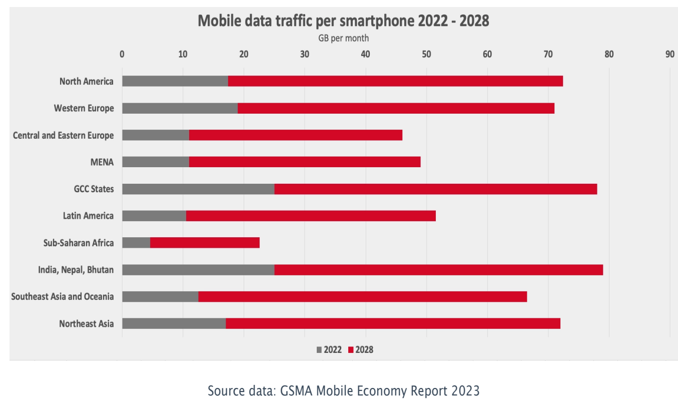


Fig. 1. The expected growth of data volumes per smartphone in the 2022 – 2028 period, from the GSMA Mobile Economy Report 2023.

A. Cyberattacks and Cybersecurity Risks

Data gathered by approximately 120 million IoT devices across 2.6 million smart homes worldwide in a cybersecurity report from 2023 [7], showed that U.S. households boasted an average of 46 connected devices, while European homes maintained an average of 25, and that in a 24-hour timeframe, home networks witnessed an average of 8 attacks targeting connected devices, including port scanning, brute-force attacks, and credential stuffing. Indeed, an industry survey showed that 63% of respondents were concerned about the lack of cybersecurity expertise [8], and threats to the IoT included malware infiltration, data interception, and Denial of Service (DoS) attacks [9]. For instance, at the device layer, IoT endpoints can be compromised to become unwitting participants in a DoS attack [10]. To improve our understanding of cyberattacks, early research was conducted to identify and block attacks by tracing them back to their sources [11], while recent studies regarding Botnets have invented algorithms to identify the actual "clique of Bots" which form during an attack to spread and intensify the attack over time [12]. Attackers can also exploit vulnerabilities in a sensor's firmware to flood the network with forged/attack requests, overwhelming system resources and impeding the regular operation of critical devices [13]. Thus, recent work has developed algorithms that detect the vulnerability of software and firmware on network-connected systems [14]–[16].

Network vulnerabilities facilitate malware infiltration, compromise the integrity of IoT networks [17], disrupt the normal functioning of connected devices and facilitate unauthorized access to user data [18]. Such breaches can compromise the confidentiality of data and allow malicious actors to exploit the intercepted information [19]. Thus, fast attack detection is an important element in overall system security [20]. Industry has long been concerned with the potential effects of mobile network attacks and malfunctions [21], [22], which result in reputation damage, loss of market share and performance crashes during peak usage hours, leading to loss of income, increased energy consumption and increases in operating expenditures for Mobile Network Operators (MNOs). Thus, many authors have studied the sources of such attacks [23], [24] and the means to detect and mitigate them [25].

II. Signalling Storms

In particular, numerous attacks known as "Signalling Storms" [26] exploit weaknesses in the Radio Access Network (RAN) [27], and have impaired mobile networks ranging from $3G$ to the current $5G$ [28]. Many high-profile network service outages worldwide in the last decade can be attributed to signalling storms, resulting in substantial financial losses and the overall wastage of millions of subscriber hours [29], [30]. For IoT networks, where the number of devices that need to communicate is in the tens of thousands or more, signalling storms cause major disruptions, and can even be life-threatening when dealing with remote patient monitoring devices or fire detection and alarm systems in smart buildings. Storms can also be caused by network malfunctions and misconfiguration, such as an IoT-specific outage that occurred in Japan in 2021, after a malfunction resulting from a MNO's upgrade which caused an automatic software rollback to the previous server software, and then triggered a massive number of registration requests from the IoT devices, causing congestion in the location management server that spread to the core network.

Next generation 6G communication networks will offer full connectivity and coverage of User Equipment (UE), from traditional two-dimensional coverage to three-dimensional full-service, including Base Stations (BSs) and aerial nodes such as Unmanned Aerial Vehicles, High-Altitude Platforms, Stratospheric Platforms and Low Earth Orbit satellites. Thus, their signalling traffic will rapidly build with network slices and the 30 billion IoT devices that are predicted for 2030, causing serious congestion whenever service disruptions require new accesses to the control plane [31]. Service in such systems can be disrupted by malware or other forms of attacks, high-altitude electromagnetic effects (such as solar storms), low-altitude interference such as sandstorms, particle pollution and clutter, which can cause signalling storms when disrupted connections attempt to re-establish connectivity [32].

It has also been suggested [33] that the use of 6G for immersive real-time interactions in large digital models such as digital twins, with large data sets and connected devices, can also result in signalling storms. Other recent work regarding 6G [34] has suggested that Open RAN's inherent overheads can also increase the effects of high data rate congestion and signalling storms, and that mitigation could be sought using adaptive controls. Thus, the purpose of the present paper is to:

- Simulate a signalling storm and measure its effects in a simulated environment, including deviations from the well-known "Taylor's Law" [35] that we observe in measurements from simulations.
- Discuss a mathematical model of storms, linking the fraction α of malevolent or malfunctioning users to the rate γ of call establishment requests, and its effect on Taylor's Law.

This work also suggests that future research could use Taylor's Law to construct attack or anomaly detectors for signalling storms, which can constitute a significant issue for $6G$ networks.

III. Simulating the Mobile Network in the Presence of Signalling Attacks

To illustrate the effect of the attacks on a signalling server, we have run several three-hour-long simulations which represent a part of a mobile network with 500 active users, with the discrete event simulator described in [36], where "time" here refers to the "real-time" of the network. In these simulations, the system operates normally for approximately a real-time equivalent of 80 minutes, and then a signalling attack is launched by some malicious app which is activated on M of the mobile devices simultaneously.

The six distinct simulation outputs of Figure 2 show the initial phase where there is no attack, and the subsequent period when M mobile devices have been compromised and are behaving as we described earlier, making bandwidth requests, then not utilising the bandwidth and being stopped via a time-out, followed by yet another bandwidth request and so on.

The request queue length at the signalling server is measured over subsequent real-time one-minute intervals and the mean and variance of all measurements over the one-minute "bin" are calculated and plotted, as shown on Figure 2. As expected, each curve shows that before the attack begins, the queue length is very small. After the attack starts, the queue length increases substantially. Also, the queue length is larger (as expected) when more devices are attacked. The curve on the top left hand corner corresponds to the case where there is *no attack throughout the three hours of the simulation*, while the curve on the bottom right hand corner shows the case when starting at around 80 minutes midway through the simulation, an attack is activated on the same 250 mobile devices. From top left to bottom right, the number of attacking mobile devices is $M = 0,\ 50,\ 100,\ 150,\ 200, 250$. The successive curves

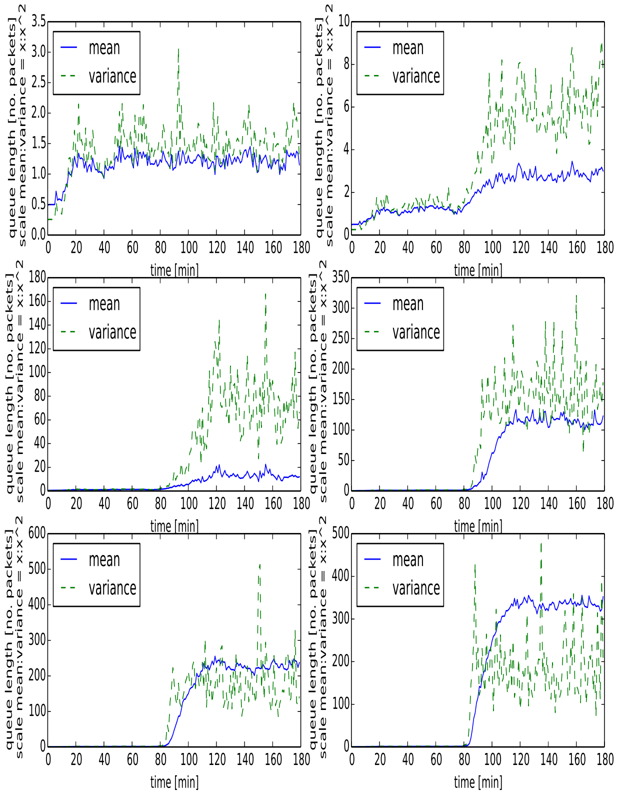


Fig. 2. In each diagram, the mean and variance of the signalling server's request queue length (y-axis) is plotted against time (x-axis) for different numbers of comprised mobile devices, in six distinct simulations with a total of 500 mobile devices. In the six successive simulations the number of compromised mobiles are set to 0, 50, 100, 150, 200, 250, as shown in the successive figures from left to right, and top to bottom.

of Figure 2 clearly show the increasing queue length as the number M of attackers increases.

A. *Detection of Signalling Storms and Taylor's Law*

The rapid real-time detection of any type of cyberattack requires the use of robust statistical detectors, and in many cases the lack of adequate statistical tools has resulted in the use of alternatives based on machine learning (ML) [37], [38]. However, in the case of signalling storms, we have observed from these simulation results that Taylor's Law [35] could be a useful detection tool.

Taylor's Law is an empirical relationship observed in natural environments, such as the number of birds of some species that are counted in a field at some given time [39]. Successive samples of this number n counted at different times will have an average value $E = E[n]$ and a variance $V = E[n^2] - E^2$. If the measurement is repeated in different fields where birds rest between flights and feed on seeds or insects, and F is the set of fields where the observations are made, we will have a set of sample averages and variances E_i, V_i where $i \in F$.

Taylor's Law, that was initially noticed in observations from biological settings, indicates that we may observe an empirical linear relationship of the form:

$$E_i = aV_i^b, \ \ or \ \ \log E_i = \log a + b \log V_i, \qquad (1)$$

where (1) is obviously linear on a $log - log$ scale.

Simulation experiments were conducted to examine the relation of the mean to the variance of the queue length in signalling server in a mobile network under signalling attacks. The basic parameters of the simulations include the following. The number of UEs was 500, and the duration of each network simulation covered three hours of network operation. During this time, we simulated a mix of traffic types, including web browsing, SMS and voice chat traffic. The number of attacked UEs was varied with six distinct values as before, and the attacks started during the first 10 minutes of the simulation.

Assuming that the attacker is very "smart", so that she knows the value of the inactivity timer of the network, the attacker establishes a call, then immediately becomes inactive and waits for the inactivity timer to activate. As soon as the inactivity timer cancels the call, the attacker relaunches the call request after a time τ of average value $\hat{\tau}$.

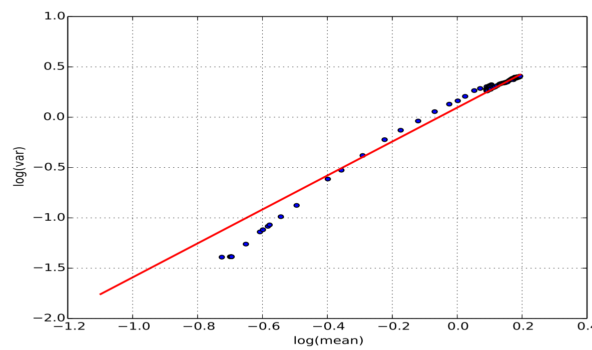


Fig. 3. Number of attackers: 0, Period considered [0,3h]

During each simulation, we measure the length of the job queue at the signalling server over the two hours of simulation time. We calculate the overall mean and variance of the queue length from the set of samples taken over successive one-minute intervals. The following figures show the logarithm of the variance against the logarithm of the mean queue length, where the standard least squares linear regression is used to estimate the linear approximation of the logarithm of variance against the logarithm of mean of queue length from the data. The results of Figures 3 through 8 clearly illustrate the increasing deviation from Taylor's Law as the number of attacking mobiles M increases.

IV. A Mathematical Model of Traffic and Congestion During a Signalling Storm

Signalling attacks substantially increase the workload of the signalling servers, creating congestion [24], [37] that may be so severe as to stop normal properly functioning mobile

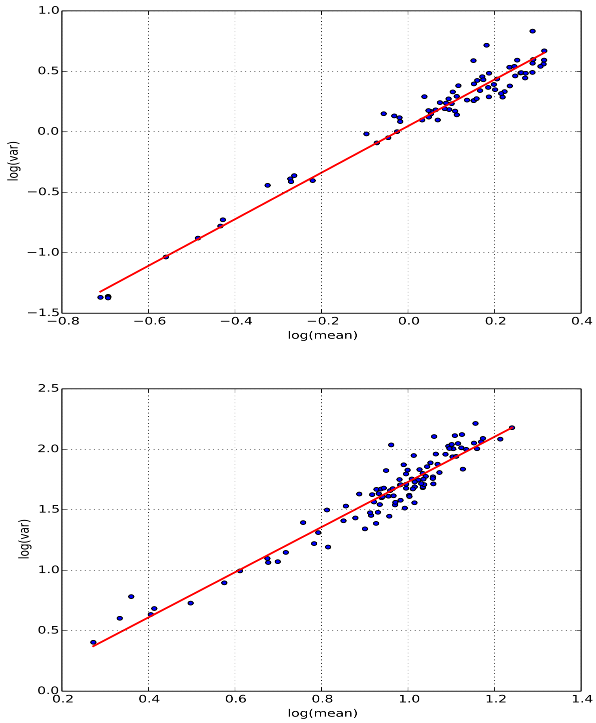


Fig. 4. Number of attackers: 50, a) Above, Period Considered: [0,80min], b) Below, Period Considered: [80min,3h]

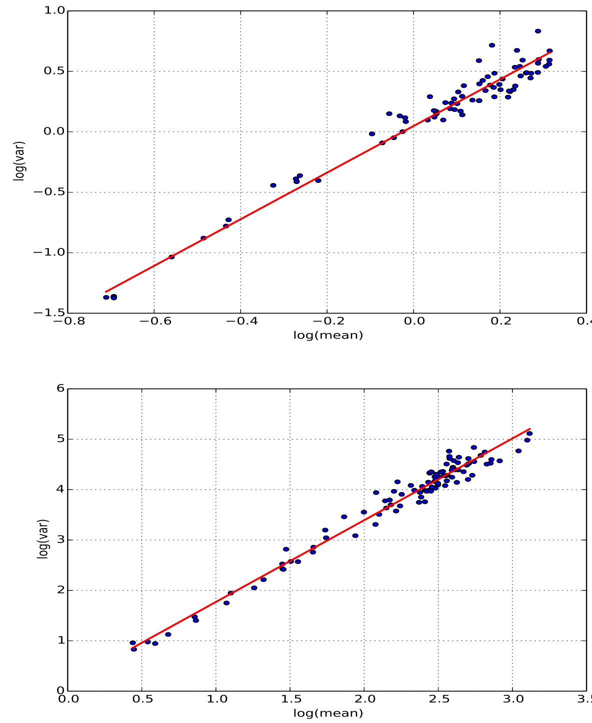


Fig. 5. Number of attackers: 100, a) Above, Period Considered: [0,80min], b) Below, Period Considered: [80min,3h]

users from obtaining the service that they request, including the establishment of ordinary phone calls and web accesses, which require a server's authorization to allocate wireless bandwidth to the end user. Such signalling attacks can be implemented through apps that are installed within the mobile device, or that act through a website that a mobile device may be connected to. Similar attacks can also be simply the result of malfunctioning apps, without any malicious intent.

A signalling attack mimics a user that requests a connection, and hence requests bandwidth from the base station, which assigns it for the user. Then, once the bandwidth is obtained, the "malignant user or app" holds on to the bandwidth, but does not make use of it. As a result, a "time-out" at the base station eventually disconnects the malignant user and informs the signalling server, but the malicious or malfunctioning app will then immediately make a further request, and so on. The effect will be to overload the base station, the signalling server and the backbone network. It will also result in the useless bandwidth occupancy. In addition, such attacks can also deplete the energy that is stored in the batteries of mobile devices [40].

Thus, in this section, we first review the mathematical model developed in [41], [42], and extend it to evaluate the congestion at the mobile network signalling server. The model considers a simplified radio resource control (RRC) state machine in which a user equipment (UE) can be either detached from or attached to the network. While a UE is attached to the network, it moves between low and high bandwidth modes, where state promotions (i.e., transitions from low to high states) occur when the mobile sends or receives traffic, while state demotions are triggered by an inactivity timer. This timer is set by the operator for all the mobile devices so that they will not remain in high power and bandwidth states if they are not actually making use of it, and in practice, it is of the order of a few seconds. There are two types of calls in the system: calls which generate "normal" user traffic, and calls which misbehave by repeatedly establishing and tearing down data connections without making use of the requested bandwidth. With these assumptions, the state of the mobile network at time t is represented by a random variable $s(t) = (b, B, C, A_1, a_1, \ \dots \ , A_i, a_i, \ \dots; t)$ 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 communicate in high bandwidth mode.
- a_i is the number of attacking mobiles which have entered low bandwidth mode from high bandwidth mode after i time-outs.
- A_i is the number of attacking mobiles which are in high bandwidth mode and have undergone a time-out for $i-1$ times.

All times in the model are independent and exponentially distributed random variables, and the rate parameters that we introduce during the discussion are the inverses of the

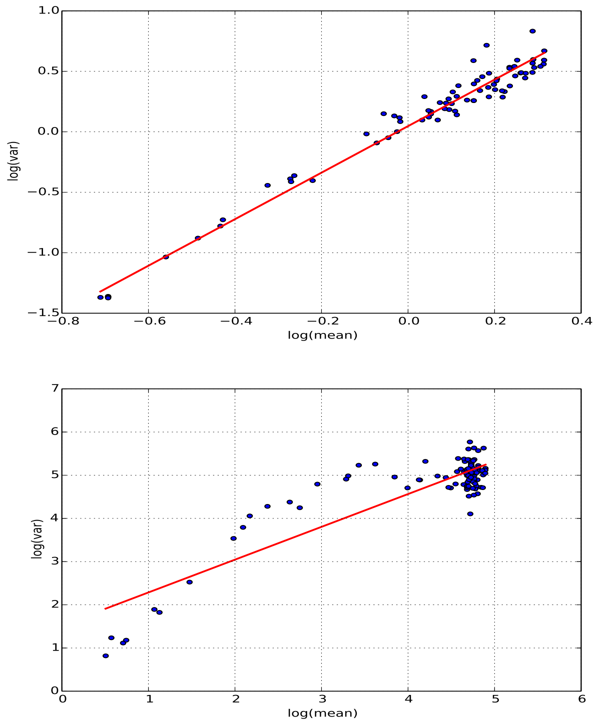


Fig. 6. Number of attackers: 150, a) Above, Period Considered: [0,80min], b) Below, Period Considered: [80min,3h]

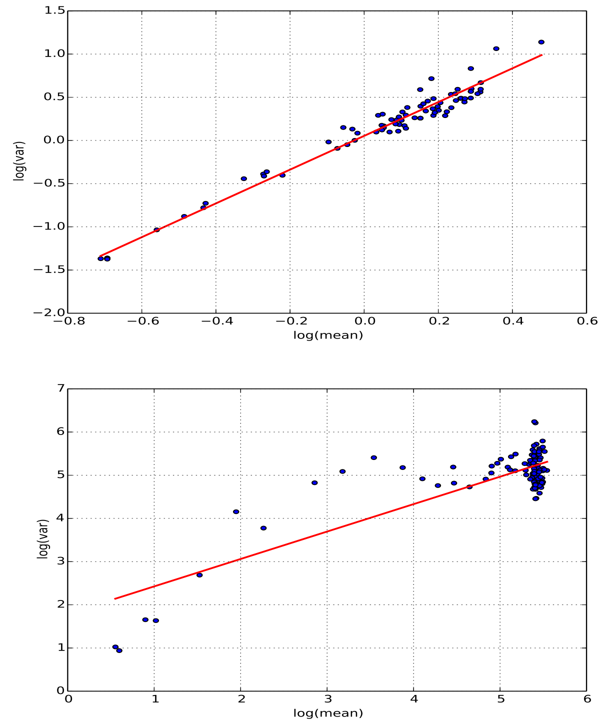


Fig. 7. Number of attackers: 200, a) Above, Period Considered: [0,80min], b) Below, Period Considered: [80min,3h]

corresponding average times.

We assume a Poisson arrival process of rate λ of new mobile activations or calls. A call that is first admitted in state b then requests high bandwidth at rate r. With probability $1-\alpha$ such a call will be of normal type and will enter state B, from which it 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 and will return to state B at rate μ, or it may end at rate δ leaving the system. The parameters κ, μ and δ allow us to represent a wide range of normal mobile usage patterns. For instance, a web browsing session normally lasts for several minutes or even hours (i.e. δ is small), but may include several downloading and reading times of average durations μ^{-1} and κ^{-1}, respectively, where the timer operates only while the user is reading, taking the state from B to b.

Let Λ_j denote the arrival rate of calls into state $j \in \{b, B, C\}$. It satisfies the system of linear equations:

$$\Lambda_b = \lambda + \frac{\tau\Lambda_B}{\tau+\kappa},\ \Lambda_B = (1-\alpha)\Lambda_b + \frac{\mu\Lambda_C}{\mu+\delta},\ \Lambda_C = \frac{\kappa\Lambda_B}{\tau+\kappa} \quad (2)$$

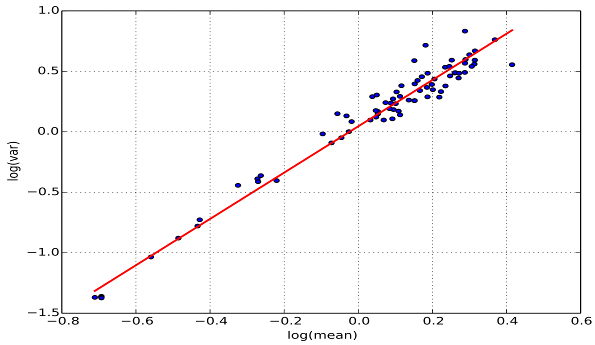
If we write $\phi = \frac{\alpha\tau + \frac{\kappa\delta}{\mu+\delta}}{\tau + \frac{\kappa\delta}{\mu+\delta}}$, then the above equations yield:

$$\Lambda_b = \frac{\lambda}{\phi},\quad \Lambda_B = \frac{\lambda(\tau+\kappa)}{\tau}[\frac{1}{\phi}-1],\quad \Lambda_C = \frac{\lambda\kappa}{\tau}[\frac{1}{\phi}-1] \quad (3)$$

On the other hand, a call in state b can be an attack with probability α, in which case it will request high bandwidth and hence enter state A_1, indicating the first request for bandwidth that is made by a malfunctioning app or malware that can contribute to a storm. Once a call enters state A_1, it will not start a communication and will time out after some time of average value τ^{-1} and enter state a_1. It will again request high bandwidth and enter state A_2 at rate r, and will time out after an average time τ^{-1} and enter state a_2. This behavior will continue until the call reaches states $a_i,\ i \geq n$ (i.e., triggers at least n superfluous transitions), where it will terminate with rate β, due to either the nature of the misbehavior itself or the presence of a counter-based mitigation mechanism [41], [42] at the mobile network or the device. The equations governing the arrival rates of attack calls $\Lambda_j,\ j \in \{a_1, A_1, a_2, A_2, \ldots, a_i, A_i, \ldots\}$ in the system can be expressed as:

$$\Lambda_{a_i} = \Lambda_{A_i} = \begin{cases} \alpha\Lambda_b, & i < n, \\ \Lambda_{a_{i-1}}\frac{r}{r+\beta} = \alpha\Lambda_b\big(\frac{r}{r+\beta}\big)^{i-n}, & i \geq n\ . \end{cases} \quad (4)$$

We model the signalling server as a processor sharing (PS) queue with a total service capacity of ν connection setup requests per second, and only consider the connection requests when computing the signalling load on the server because they trigger significantly more control plane messages [36] than other procedures, such as state demotions. The load on the signalling server γ (in requests per unit time) is then given by the total transition rate from low to high bandwidth modes,



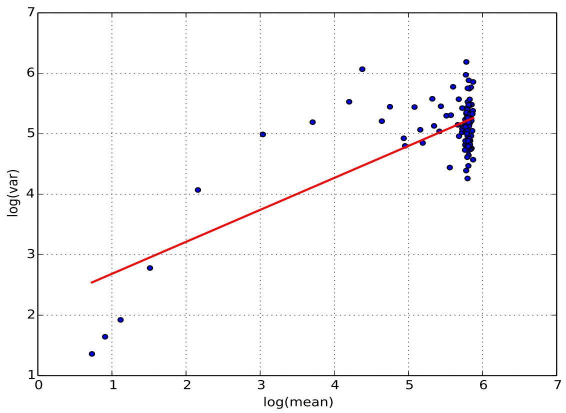


Fig. 8. Number of attackers: 250, a) Above, Period Considered: [0,80min], b) Below, Period Considered: [80min,3h]

which is induced by both normal and malicious calls:

$$\begin{aligned}\gamma = & \quad (1-\alpha)\Lambda_b + \alpha\Lambda_b[n-1+\sum_{i=n}^{\infty}\left(\frac{r}{r+\beta}\right)^{i-n}], \\ = & \quad (1-\alpha+\alpha[n+\frac{r}{\beta}])\Lambda_b = \Lambda_b[1+\alpha(\frac{r}{\beta}+n-1)]. \quad (5)\end{aligned}$$

Using standard results for an M/M/1-PS system with an equivalent average service time per connection request given by $\frac{1}{\nu}$, the average value of the setup time R, and its variance, denoted respectively by $E(R)$, $Var(R)$, are given by the expressions:

$$E(R) = \frac{1}{\nu-\gamma},\ Var(R) = \frac{1}{(\nu-\gamma)^2}\frac{2+\frac{\gamma}{\nu}}{2-\frac{\gamma}{\nu}}. \quad (6)$$

Remark: Figure 9, obtained from (6), shows that as the attack probability α increases, the relationship between $Var(R)$ and $E(R)$ deviates from Taylor's Law. Similarly, we can study directly the expressions in (6) and notice that:

$$\frac{\gamma}{\nu} = 1 - \frac{1}{\nu E(R)},\ Var(R) = [E(R)]^2\frac{3-\frac{1}{\nu E(R)}}{1+\frac{1}{\nu E(R)}}, \quad (7)$$

so that:

$$\begin{aligned}Var(R) &= [E(R)]^2[1+2\frac{1-\frac{1}{\nu E(R)}}{1+\frac{1}{\nu E(R)}}] \\ &= [E(R)]^2[1+2(\frac{\nu E(R)-1}{\nu E(R)+1})], \quad (8)\end{aligned}$$

which yields:

$$\log Var(R) = 2\log E(R) + \log[1+2(\frac{\nu E(R)-1}{\nu E(R)+1})], \quad (9)$$

where $1 \leq \nu E(R) < +\infty$. Notice that when $\nu E(R) = 1$, which from (6) corresponds to the case where the system has no workload, i.e. $\gamma = 0$, implies that the second term on the right-hand-side of (9) is zero. However, we know from the expression for $Var(R)$ in (6), that $Var(R)$ depends on γ and hence on α which is the probability that an attack occurs.

Now, taking the derivative of the second term on the right-hand-side of (9) with respect to $E(R)$, we have:

$$\begin{aligned}\frac{d\log[1+2(\frac{\nu E(R)-1}{\nu E(R)+1})]}{dE(R)} &= \frac{2\frac{\nu(\nu E(R)+1)-\nu(\nu E(R)-1)}{(\nu E(R)+1)^2}}{1+2(\frac{\nu E(R)-1}{\nu E(R)+1})} \\ &= \frac{\frac{4\nu}{(\nu E(R)+1)^2}}{1+2(\frac{\nu E(R)-1}{\nu E(R)+1})}, \\ &= \frac{4\nu}{3\nu^2E(R)^2+2\nu E(R)-1}, \quad (10)\end{aligned}$$

which shows that the response time variable R does not satisfy Taylor's Law when $\gamma > 0$ which implies that $\nu E(R) > 1$. This confirms the observations that we report in Section III, from the data collected from simulations, and in the numerical results presented Figure 9.

Thus, this analysis suggests that the violation of Taylor's Law by the response time random variable R, may be used as a tool to detect possible signalling storms which will necessarily increase γ, and hence $E(R)$ as well, leading to a possible novel attack detection for storms in $6G$ networks.

V. Conclusions

This paper briefly reviews the growth of mobile and IoT traffic over the last few years and its growth projections in the coming years. The variety and growth of cyberattacks and similar network malfunctions is also briefly reviewed. Then, we focus on signalling storm attacks, which have been very common in successive generations of mobile networks from $3G$ to $5G$, and which are predicted to be likely to occur in $6G$ networks. Signalling storms may also be caused when a network with a large number of connected entities is restarted after a malfunction, failure or attack, and can even be caused by natural transient phenomena in the propagation medium.

We therefore examine data from a discrete event simulation of signalling storms, and also analyze a mathematical model of signalling storms, to observe that when congestion occurs at the signalling system of the mobile network, both the simulation results and the mathematical model, show a significant deviation from a well-known naturally observed

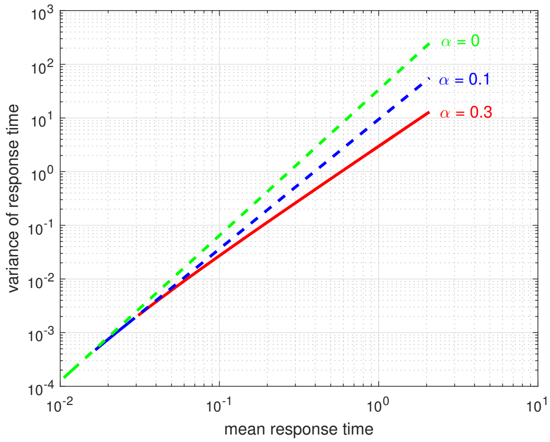


Fig. 9. Theoretical results based on the mathematical model for the log-log plot of Var(R) against $E(R)$ as the normal signalling traffic Λ_b is varied between 3 to 4 activations per second, for different fractions α of attacks. All times in the model are independent and exponentially distributed random variables. The other parameters are: $\kappa^{-1} = 10sec$, $\mu^{-1} = 5\ sec$, $\delta^{-1} = 10\ sec$, $\tau^{-1} = 6\ sec$, $\nu = 128\ requests/sec$, $n = 20$ and we have set $\beta \to \infty$. Dashed lines are linear extrapolations of the corresponding loci, which are plotted with solid lines.

statistical relation known as Taylor's Law. Since it is very challenging to find statistical relations that can help us detect cyberattacks or network malfunctions, we thus suggest that the violation of Taylor's Law may be used to design detectors for signalling storms and signalling attacks.

In future work we plan to design and test a purely statistical detector of signalling storms based on Taylor's Law, and also to incorporate Taylor's Law in a Machine Learning based [43] Attack Detector of signalling storms for future $6G$ networks.

References

[1] Digital-Silk, "Top 40 mobile traffic statistics you should know," June 2025. [Online]. Available: https://www.digitalsilk.com/digital-trends/top-mobile-traffic-statistics/

[2] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang, "A first look at cellular machine-to-machine traffic: large scale measurement and characterization," *SIGMETRICS Perform. Eval. Rev.*, vol. 40, no. 1, p. 65–76, June 2012. [Online]. Available: https://doi.org/10.1145/2318857.2254767

[3] Statista, "Number of internet of things (iot) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2034," May 2025, accessed: 2025-06-11. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[4] A. Frötscher, et al., "Improve cybersecurity of C-ITS road side infrastructure installations: the seriot-secure and safe IoT approach," in *2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE)*. IEEE, 2019, pp. 1–5.

[5] SonicWall, "The mid-year update to the 2023 sonicwall cyber threat report," Aug 2024, accessed: 2024-12-29. [Online]. Available: https://www.sonicwall.com/2023-mid-year-cyber-threat-report/#:~:text=Volume%20is%20up%2037%25%20globally,SonicWall%20began%20tracking%20these%20threats.

[6] Forescout-Research-Labs, "The enterprise of things security report: Insights into iot security," Sep 2024, accessed: 2024-12-29. [Online]. Available: https://www.forescout.com/the-enterprise-of-things-security-report-state-of-iot-security/

[7] Bitdefender-NETGEAR, "The 2023 IoT security landscape report," April 2023, accessed: 2025-03-11. [Online]. Available: https://www.bitdefender.com/files/News/CaseStudies/study/429/2023-IoT-Security-Landscape-Report.pdf

[8] ISACA, "State of cybersecurity 2023 report," Oct 2023, accessed: 2025-03-11. [Online]. Available: https://www.isaca.org/resources/reports/state-of-cybersecurity-2023

[9] S. A. Ansar, S. Arya, S. Aggrawal, S. Saxena, A. Kushwaha, and P. C. Pathak, "Security in iot layers: Emerging challenges with countermeasures," in *Computer Vision and Robotics: Proceedings of CVR 2022*. Springer, 2023, pp. 551–563.

[10] X. Liang and Y. Kim, "A survey on security attacks and solutions in the iot network," in *2021 IEEE 11th annual computing and communication workshop and conference (CCWC)*. IEEE, 2021, pp. 0853–0859.

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

[12] M. Nakip and E. Gelenbe, "An associated random neural network detects intrusions and estimates attack graphs," in *32nd International Conference on Modelling, Analysis and Simulation of Computer and Telecommunication Systems*. https://www.computer.org/csdl/proceedings-article/mascots/2024/10786521 . . . , 2024, pp. 1–4.

[13] S. M. Almeghlef, A. A.-M. AL-Ghamdi, M. S. Ramzan, and M. Ragab, "Application layer-based denial-of-service attacks detection against iot-coap," *Electronics*, vol. 12, no. 12, p. 2563, 2023.

[14] E. Gelenbe, B. C. Gul, and M. Nakip, "Disfida: Distributed self-supervised federated intrusion detection algorithm with online learning for health internet of things and internet of vehicles," *Internet of Things*, vol. 28, no. 101340, pp. https–doi, 2024.

[15] M. Siavvas, I. Kalouptsoglou, E. Gelenbe, D. Kehagias, and D. Tzovaras, "Transforming the field of vulnerability prediction: Are large language models the key?" in *2024 32nd International Conference on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS)*. IEEE, 2024, pp. 1–6.

[16] E. Gelenbe, M. Nakip, and M. Siavvas, "System wide vulnerability and trust in multi-component communication system software," *IEEE Network*, vol. 39, no. 2, pp. 108–114, 2025.

[17] A. Jahangeer, S. U. Bazai, S. Aslam, S. Marjan, M. Anas, and S. H. Hashemi, "A review on the security of iot networks: From network layer's perspective," *IEEE Access*, vol. 11, pp. 71 073–71 087, 2023.

[18] N. Mishra and S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," *IEEE Access*, vol. 9, pp. 59 353–59 377, 2021.

[19] C. Cilleruelo, J. Junquera-Sánchez, L. de Marcos, N. Logghe, and J.-J. Martinez-Herraiz, "Security and privacy issues of data-over-sound technologies used in iot healthcare devices," in *2021 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2021, pp. 1–6.

[20] G. Baldini, et al., *IoT Network Risk Assessment and Mitigation: The SerIoT Approach*. DOI: 10.1561/9781680836837.ch5. NOW Publishers, 2020.

[21] M. Baltatu, R. D'Alessandro, and R. D'Amico, "Nemesys: First year project experience in Telecom Italia Information Technology," in *Proceedings 28th Int. Symp. on Computer and Information Sciences (ISCIS 2013), Volume 264 of Lecture Notes in Electrical Engineering*. Springer, October 2013, pp. 399–407.

[22] G. Lyberopoulos, H. Theodoropoulou, and K. Filis, "Mobile Network Threat Analysis and MNO positioning," in *Proceedings 28th Int. Symp. on Computer and Information Sciences (ISCIS 2013), Volume 264 of Lecture Notes in Electrical Engineering*. Springer, October 2013, pp. 419–428.

[23] L. Delosieres and D. Garcia, "Infrastructure for detecting Android malware," in *Proceedings 28th Int. Symp. on Computer and Information Sciences (ISCIS 2013), Volume 264 of Lecture Notes in Electrical Engineering*. Springer, October 2013, pp. 389–398.

[24] S. Liebergeld, L. Matthias, and C. Mulliner, "Nomadic honeypots: A novel concept for smartphone honeypots," in *Proc. Workshop on Mobile Security Technologies (MoST 20113), in conjunction with the 34th IEEE Symp. on Security and Privacy*, 2013.

[25] E. Gelenbe, G. Gorbil, D. Tzovaras, S. Liebergeld, D. Garcia, M. Baltatu, and G. Lyberopoulos, "Nemesys: Enhanced network security for seamless service provisioning in the smart mobile ecosystem," in *Proceedings 28th Int. Symp. on Computer and Information Sciences (ISCIS 2013), Volume 264 of Lecture Notes in Electrical Engineering*. Springer, October 2013, pp. 369–378.

[26] O. H. Abdelrahman and E. Gelenbe, "Signalling storms in 3G mobile networks," in *Proc. IEEE International Conference on Communications (ICC'14)*, Sydney, Australia, Jun. 2014, pp. 1017–1022. [Online]. Available: http://dx.doi.org/10.1109/ICC.2014.6883453

[27] "Machine-type and other mobile data applications communications enhancements (release 12), 3GPP Mobile Competence Centre c/o ETSI, 650 route des Lucioles 06921 Sophia-Antipolis, FRANCE, TR, 23.887," December 2013.

[28] A. Nosir, "Latest cybersecurity attacks on 4g and 5g networks," June 2024. [Online]. Available: https://medium.com/@egycondor/latest-cybersecurity-attacks-on-4g-and-5g-networks-25656d9f8d2c

[29] ESEYE, "Signaling storms and IoT: How to safeguard IoT devices from network disruption," December 2024. [Online]. Available: https://www.eseye.com/

[30] SQUIRE-NETWORKS, "IoT signalling storms, a future risk for MNOs," June 2025. [Online]. Available: https://squire-technologies.co.uk/blog/iot-signalling-storms-a-future-risk-for-mnos

[31] Ö. A. Aslan and R. Samet, "A comprehensive review on malware detection approaches," *IEEE Access*, vol. 8, pp. 6249–6271, 2020.

[32] A. M. Shalaby, N. S. Othman, and M. Shalaby, "Impact of dust and sandstorms on 6g UAV base station performance in arid Saudi Arabian environments," *IEEE Access*, vol. 12, pp. 86 194–86 207, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3412979

[33] R. Yadav, P. Jha, and A. Karandikar, "Signalling as data: How it transforms network architecture for 6g system," in *Proceedings of the CoNEXT on Student Workshop 2024*, ser. CoNEXT-SW '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 23–24. [Online]. Available: https://doi.org/10.1145/3694812.3699923

[34] S. Chatzimiltis, M. Shojafar, M. B. Mashhadi, and R. Tafazolli, "Surviving the storm: The impacts of open ran disaggregation on latency and resilience," 2025. [Online]. Available: https://arxiv.org/abs/2505.00605

[35] L. R. Taylor, "Aggregation, variance and the mean," *Nature*, vol. 189, no. 4766, p. 732–735, 1961.

[36] G. Gorbil, O. H. Abdelrahman, M. Pavloski, and E. Gelenbe, "Modeling and analysis of RRC-based signalling storms in 3G networks," *IEEE Transactions on Emerging Topics in Computing, Special Issue on Emerging Topics in Cyber Security*, vol. 4, no. 1, pp. 113–127, Jan. 2016. [Online]. Available: http://dx.doi.org/10.1109/TETC.2015.2389662

[37] S. Liebergeld and M. Lange, "Android security, pitfalls, lessons learned and BYOD," in *Proceedings 28th Int. Symp. on Computer and Information Sciences (ISCIS 2013), Volume 264 of Lecture Notes in Electrical Engineering*. Springer, October 2013, pp. 409–417.

[38] E. Gelenbe and M. Nasereddin, "Adaptive attack mitigation for IoV flood attacks," *IEEE Internet of Things Journal*, vol. 12, no. 5, pp. 4701–4714, 2025.

[39] T. R. E. Southwood, *Ecological methods, with particular reference to the study of insect populations*. Methuen, 1966.

[40] E. Gelenbe, "Energy packet networks: smart electricity storage to meet surges in demand," in *SIMUTOOLS '12: Proceedings of the 5th International ICST Conference on Simulation Tools and Techniques*. https://web.archive.org/web/20170808152616id_/http://san.ee.ic.ac.uk . . . , 2012, pp. 1–7.

[41] E. Gelenbe and O. H. Abdelrahman, "Countering mobile signaling storms with counters," in *Internet of Things. IoT Infrastructures - Second International Summit, IoT 360° 2015, Rome, Italy, October 27-29, 2015, Revised Selected Papers, Part I*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, B. Mandler, J. Márquez-Barja, M. E. M. Campista, D. Cagánová, H. Chaouchi, S. Zeadally, M. Badra, S. Giordano, M. Fazio, A. Somov, and R. Vieriu, Eds., vol. 169, 2015, pp. 199–209. [Online]. Available: https://doi.org/10.1007/978-3-319-47063-4_18

[42] E. Gelenbe, O. H. Abdelrahman, and G. Gorbil, "Detection and mitigation of signaling storms in mobile networks," in *Proc. IEEE International Conference on Computing, Networking and Communications (ICNC'16)*, Kauai, Hawaii, February 2016, pp. 1–6.

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