Visual Analytics for enhancing supervised attack attribution in mobile networks*

Stavros Papadopoulos, Vasilios Mavroudis, Anastasios Drosou, and Dimitrios Tzovaras

Abstract Researchers have recently uncovered numerous anomalies that affect 3G/4G networks, caused either by hardware failures, or by Denial of Service (DoS) attacks against core network components. Detection and attribution of these anomalies are of major importance for the mobile operators. In this respect, this paper presents a lightweight application, which aims at analyzing signalling activity in the mobile network. The proposed approach combines the advantages of anomaly detection and visualization, in order to efficiently enable the analyst to detect and to attribute anomalies. Specifically, an outlier based anomaly detection technique is applied onto hourly statistics of multiple traffic variables, collected from one HLR (Home Location Register). The calculated anomaly scores are afterwards visualized utilizing stacked graphs, in order to allow the analyst to have an overview of the signaling activity and detect time windows of significant change in their behavior. Afterwards, the analyst can perform root cause analysis of suspicious time periods, utilizing graph representations, which illustrate the high level topology of the mobile network and the cumulative signaling activity of each network component. Experimental demonstration on synthetically generated anomalies illustrates the efficiency of the proposed approach.

1 Introduction

Mobile networks and devices are becoming the targets of cyber-criminals aiming to exploit the infrastructure and the provided services for their purposes.As a countermeasure, mobile network operators employ authentication-based techniques to prevent illegitimate users from attaching to the network. Malicious individuals, however, can still infiltrate the network by utilizing compromised mobile devices of legitimate subscribers, and launching attacks agianst the infrastructure or the subscribers. The main focus of this paper is the detection and attribution of signaling-oriented Denial of Service (SDoS) attacks [1][2], which target mobile network components in the core network. The effect of a SDoS attack can be amplified when a botnet (i.e. network of compromised devices) is utilized to launch attacks from multiple nodes, which target to overload a specific component of the network.

1.1 Related Work

Anomaly detection techniques for the detection of signaling attacks in 3G/4G networks have been proposed in the literature. Specifically, Lee et al. [1] [3] proposed a cumulative sum (CUSUM) based method for the detection of signaling attacks that

Stavros Papadopoulos
Imperial College London, e-mail: {s.papadopoulos}@imperial.ac.uk

Vasilios Mavroudis, Anastasios Drosou, Dimitrios Tzovaras
CERTH, ITI e-mail: {mavroudis, drosou, tzovaras}@iti.gr

* This work has been partially supported by the European Commission through project FP7-ICT-317888-NEMESYS funded by the 7th framework program. The opinions expressed in this paper are those of the authors and do not necessarily reflect the views of the European Commission.

the traditional detection systems cannot detect. The authors designed their method so that is it hard for the attackers to evade detection. They also evaluated their approach against a novel SDoS attack that affects the RNC and the Node-B in 3G and potentially WiMax networks. Alconzo et al. [4] propose statistical techniques applied on time-series of unidirectional feature distributions. Coluccia et al. [5] present two distribution-based anomaly detection methods and propose enhancements on the method introduced in [4].

Apart from the analytical methods for anomaly detection, visualization based methods have also been proposed in the literature. Specifically, visualizations based on graph representations of the network topology, have been successfully used in network security. Lad et al. [6] proposes a graph representation of the BGP(Border Gateway Protocol) network topology, which illustrates the routing behavior over a specific time period. The volume of the BGP routing changes computed on the graph has been proposed as a descriptive feature that allows for the detection of anomalous time periods. Shi et la. [7] proposed a system called SAVE, which utilizes graph representations to illustrate the packet delivery paths in sensor networks. Each node represents a sensor which produces a time series of data, which is visualized using GrowthRingMaps [8].

1.2 Motivation

To the best of the authors' knowledge, no previous work has addressed security threads in the control plane of mobile networks by combining both information visualization and anomaly detection techniques. Thus, the main motivation of the proposed system is to bridge this gap and provide a system for the visual analysis and detection of signalling related anomalies.

This paper proposes a novel system for providing an overview of the mobile network signaling activity in suspicious time instances, and for preforming root cause analysis. The main advantage of the proposed system is that it is very lightweight in computational resources. The reason for this is that it operates directly on the statistical data collected from the network with out the need for feature extraction and preprocessing. Additionally, the graph layout is static since it represents the mobile network topology, a fact which eliminates the need for heavy layout computations in the case of structural changes.

The rest of the paper is organized as follows: Section 2 presents the details of the proposed anomaly detection approach. The evaluation takes place at Section 3, while the paper concludes at Section 4.

2 System Overview

This Section presents an overview of the proposed system. It is comprised of two parts, the anomaly detection module and the visualization module. Initially, signaling traffic statistics are collected from the monitoring points in the control plane of the 3G/4G mobile network (section 3.1). Afterwards, these signaling data are fed into the anomaly detection module, which utilizes an outlier based detection method in order to compute anomaly scores for each time period under investigation. The scores are computed by calculating the distance between the examined network traffic instance and the normal traffic instances observed in the past. Thereafter, the visualization module utilizes the anomaly scores, so as to enable the analyst to have an overview of the signalling activity over time, and detect anomalous time periods. Additionally, a graph based representation of the mobile network, facilitates the task of visualizing the actual signaling behaviour of each network component for the selected time period, thus enabling the root cause analysis of the anomalies under investigation.

2.1 Anomaly Detection module: Identification of outliers in the control plane

2.1.1 Problem Definition

Anomaly detection refers to the identification of network traffic instances that do not conform with normal network behaviour [12]. For the definition of the anomaly detection problem, two matrices are used. The first matrix is matrix D, which serves as ground truth and contains only normal traffic instances and the second matrix is E, which is the input for the anomaly detection method: $D = \{d_{i,j} | where\ i \in [1,K], j \in [1,Y]\}$, and $E = \{e_{k,l} | where\ k \in [1,K], l \in [1,Z]\}$. K is the number of traffic variables and Y is the number of observations of normal network traffic and Z is the number of observations that need to be evaluated with regards to their normality. Furthermore, each element of the matrix D is denoted as d_{ij}, the observation sequence of a traffic variable as $D_{row}(i) = \{d_{ij}, \forall j \in [1,Y]\}$, where $i \in [1,K]$ and a traffic instance as $D_{col}(j) = \{d_{ij}, \forall i \in [1..K]\}$, where $j \in [1,Y]$. In both matrices D and E, each row corresponds to a *traffic variable* and each column to an observed *traffic instance*. Based on these definitions, the anomaly detection problems refers to the detection of the traffic instance $E_{col}(j)$, which deviate from the normal behaviour. It should be underlined that the time intervals between consecutive instances remain the same.

2.1.2 Local Outlier Factor Method

Based on the traffic model outlined in the previous section, each traffic instance is modelled as a point in the K-dimensional space. Subsequently, the local outlier factor (LOF) [13] method is applied, so as to detect any anomalous traffic instances found in E. LOF operates by comparing the spatial density around a given point with the density around its k nearest points and then provide a score which indicates if the examined point resides in a low-density area or not. More formally, $\forall e_{(i,n)} \in E$, the outlier score is computed using equation (1), as defined in [13]. The $lrd(e_{col}(n))$ function defines the local reachability density of $e_{col}(n)$[13].

$$LOF(e_{col}(n)) = \frac{\sum_{d_{col}(m) \in R_{(e_{col}(n))}} lrd(d_{col}(m)) / lrd(e_{col}(n))}{| R(e_{col}(n)) |} \quad (1)$$

where $R_{(e_{col}(n))}$ contains the k-nearest neighbours of $e_{(i,n)}$ from D. More details on the LOF method can be found in [13]. In cases of normal traffic instances the LOF score is ~ 1, whereas abnormal instances would exhibit significant deviations from this base [13].

It should be noted that the part of the algorithm which detects the k nearest neighbours is the most computationally demanding. More specifically, for a dataset with stable dimensionality this part has complexity of $O(N^2)$. Hence, in our case the runtime of the LOF algorithm was found to be sufficiently fast for computing outliers in real-time with computation time < 5 seconds on each iteration (i.e. for each hour). This can be attributed to the fact that the size and the dimensionality of the ground-truth dataset D do not change.

2.2 Visualization module: Root cause analysis of signaling anomalies

2.2.1 An efficient approach for multiple visualizations over extended periods of time

In order to draw the attention of the analyst in interesting parts of the data, temporal visualizations of anomaly scores are utilized. This way, the analyst can has an

overview of the signalling activity over time, and can detect anomalous time periods and perform a more detailed analysis. The proposed temporal visualizations provide an information rich overview of the data and enable the efficient understanding and exploration of the datasets, following the information seeking mantra suggested by Shneiderman: *"Analyze first, show the important, zoom, filter and analyze further, details on demand"*[14].

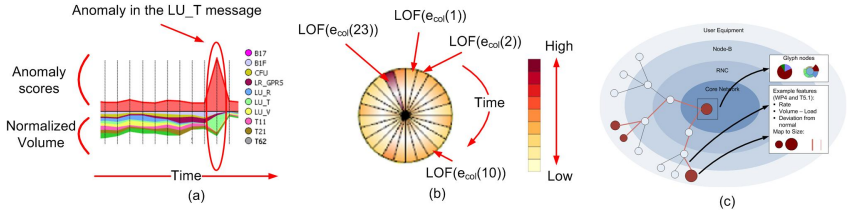


Fig. 1 (a) Stacked graphs visualization of the anomaly scores and signalling volume. (b) Glyph representation of the anomaly scores for one network component. (c) A scheme of the proposed layered layout of the Mobile Network Graph.

The temporal visualization utilized by the proposed approach are depicted in figures 1(a) and (b). The first overview is provided by the stacked graph representation. This representation provides an overview of the anomaly scores for one network component, computed for each time period, while it also provides information regarding the normalized volume of each traffic variable for the same period, utilizing the z-score normalization. Each traffic variable is represented using a different color. The glyph representation also provides an overview of the anomaly scores of each time period, for one network component. Color is utilized to represent the actual value of the score at each time period, while the circular layout of the scores represents the time parameter, resembling a clock metaphor. Both these methods are used in combination, in order to provide an information rich visualizations and allow the analyst detect anomalous time periods to focus on, and perform root cause analysis utilizing the Mobile Network Graph presented in the next section.

2.2.2 Visualization of the network topology and signalling activity

The section presents the Mobile Network Graph visualization approach that is utilized for root cause analysis. The proposed approach utilizes a graph representations, to illustrate the actual topology of the mobile network. Each node represents a network component, while edges illustrate connections between them. The positioning of the nodes of the graph is calculated in consecutive layers. This layout enables the easier perception of the topology of anomalous events, since one additional visual element, i.e. the position, is utilized to encode additional topological information. Specifically, four layers, comprised of multiple network components are defined, as shown in figure 1(c):

1. UE (User Equipment): Contains actual mobile devices.
2. NodeB: Contains NodeBs, which are the network component that provides the mobile devices with wireless connectivity. Each NodeB serves multiple mobile devices, i.e. all the devices in range.
3. RNC: Contains RNCs (Radio Network Controller)which are responsible for controlling the NodeBs that are connected to them.
4. Core Network: Core network is the central part of a telecommunication network that is responsible for providing all the network services to the customers, e.g. SMS/Call routing. This layer is comprised of all the nodes that belong to the Core Network, e.g. the most important are SGSN (Serving GPRS Support Node), GGSN (Gateway GPRS Support Node), HLR (Home Location Register), MSC (Mobile Switching Centre), and VLR (Visitor Location Register).

It should be noted that the proposed layered graph layout is computed only once, and is thereafter static. The main computational bottleneck of the proposed system is the anomaly detection through the LOF calculation ($O(N^2)$). But as mentioned in Section 2.1.2, the LOF implementation is very fast, capable of operatizing in real-time. These facts render the system very lightweight in computational recourses and enable the real-time analysis of signaling anomalies. Screenshots of the developed system are shown in figures 2 and 3.

3 Demonstration on suspicious incidents

3.1 Datasets

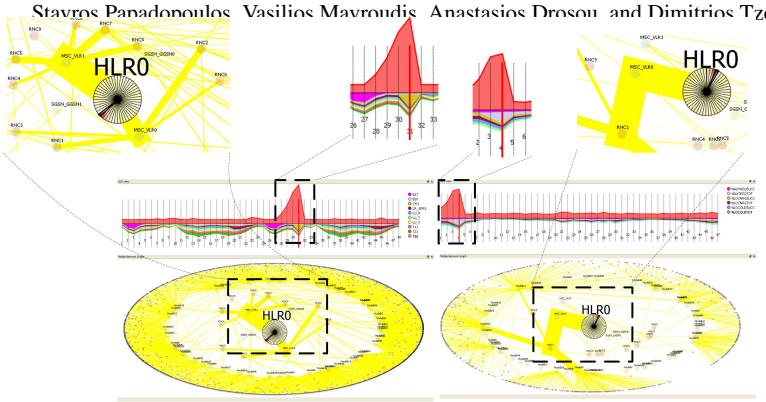
In order to demonstrate the effectiveness of the proposed system four synthetic datasets were generated using two raw datasets containing traces collected from the 3G/4G mobile networks of two major European telecommunications providers. These raw datasets contain statistical data collected from one HLR of the network. Additionally, they reportedly include no abnormal network incidents, so it is assumed that all the traffic instances included in each dataset exhibit normal network activity. The first raw dataset contains data for 10 signaling messages (e.g. location update etc) with granularity of one hour. The second raw dataset contains data for three types of signaling requests. However, none of these datasets provide information about the activity of individual subscribers and their position in the network topology (e.g. NodeB that the subscriber is attached to) and thus do not provide enough information for performing root cause analysis of any detected anomalies. To address this, a data generator was designed and implemented. The generation process is defined as follows: 1) Initially the raw data containing the HLR signaling traffic statistics are fed into the generator, 2) the raw data are analyzed and the corresponding Gaussian distribution for each time of the day is computed, 3) then based on the overall traffic for the HLR the traffic distribution for a normal user is computed (Normal User traffic profile), and 4) using the aforementioned profiles a synthetic dataset which contains statistical data for the HLR and for each subscriber is generated. As a final step, abnormal instances were manually inserted based on the related literature [15] [16] [17] [18] [19].

3.2 Demonstration Scenarios

Based on network incidents that have been studied in the literature [15] [16] [17] [18] [19], different scenarios were designed and implemented so as to evaluate the proposed approach. These scenarios cover incidents that vary from network component malfunctioning (i.e. section 3.2.3) to malicious attacks (i.e. section 3.2.2). The performance of the proposed approach is demonstrated in the sections that follow.

3.2.1 Call forwarding DDoS

This scenario simulates a DDoS attack that has been proposed by Traynor et. al in [16] and can effectively overload the HLR/HSS component, so as to degrade the QoS for the network subscribers. More specifically, a large number of mobile devices are compromised by malware and launch a DDoS attack by exploiting call forwarding signaling requests. Although, these requests on a per packet basis are legitimate, such a coordinated attack can significantly increase the load in the HLR/HSS and render it unresponsive. In this scenario, the attack has a high growth rate and reaches its peak (i.e. maximum throughput from infected devices) very fast. As seen in figure 2(a), our proposed approach is able to detect and highlight the incident from an early stage and visually inform the human operator before the network stability is affected. As shown in the stacked graph representations, at the time of the anomaly,



(a) DDoS (b) Authentication attack

Fig. 2 The network visualization during two abnormal network events, a DDos attack and an Authentication attack.

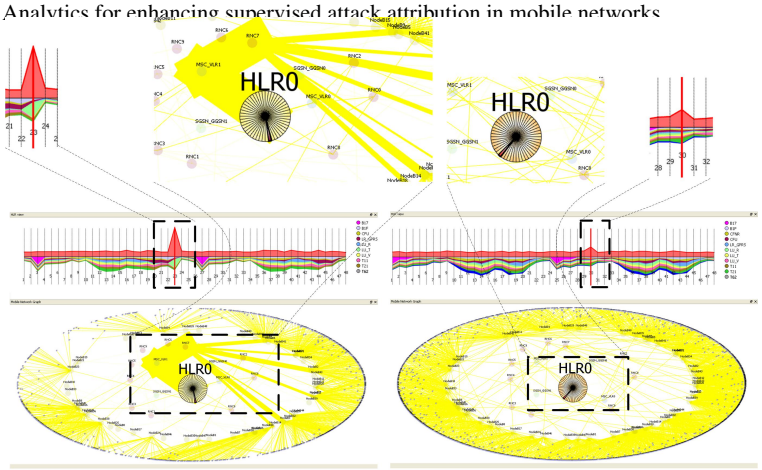
the CFU (Call Forwarding Unconditional) signalling message has increased volume. Upon the detection, the operator is able to clearly identify the distributed nature of the attack, since the excessive signalling does not originates from a specific region of the network, but instead it is uniformly distributed. The operator also is able to identify the exploited signaling messages and the misbehaving subscribers, and design countermeasures (e.g. rejection rules for the control plane firewall).

3.2.2 Authentication Attack

In this scenario, an authentication attack which uses sim-less devices, as described in [15], is implemented. As in Section 3.2.1, the attacker aims to affect the network stability and degrade the performance of the network. However, in this case the attacker is regionally constrained and thus he launches the attack from a limited number of NodeBs which all belong in the same geographical area. During the attack, the proposed approach initially detects an abnormal increase in the incoming authentication attempts and displays a high anomaly score. The human operator, then uses the stacked graph to compare the volume of authentication attempts with the volume of successful authentication transactions and verifies that the observed behavior is potentially malicious, since the success/attempts ratio is very low. Then he/she utilizes the network graph to identify the root cause of the incident. As seen in figure 2(b), RNC1 exhibits increased traffic load, due to the high volume of signaling messages received from specific NodeBs (i.e. NodeB1, NodeB10, NodeB11). This analysis enables the operator, which know is aware of the nature of the attack, to design effective mitigation countermeasures. For instance, one mitigation approach would be to lower the processing priority of authentication requests originating from the affected NodeBs in order to avoid congestion in the HLR/HSS.

3.2.3 RNC restart

In this scenario, the proposed approach is evaluated during the restart of a malfunctioning RNC [19]. According to [19] the network becomes unstable due to the flood of location update requests towards the HLR/HSS, as the mobile devices switch from 2G to 3G or 4G, when the malfunctioning component becomes available again. More specifically, as seen in figure 3(a), the RNC7 has been restarted and this results in a flood of signaling requests from all subscribers which reside in the NodeBs it controls. Our proposed approach displays an increased anomaly score and informs the human operator of that the volume of location update requests from home subscribers (i.e. LU_T) is higher than normal. Additionally, the network graph provides



(a) RNC restart (b) Spam SMS

Fig. 3 The network visualization during two abnormal network events, an RNC restart and an SMS spam campaign.

enough information for the operator to pin point the root cause of the incident, i.e. RNC7.

3.2.4 Spam SMS campaign

This scenario was designed based on the findings of [18] [17] [20] regarding the modus operandi of the spammers and the impact of their activities on the network. In particular, a spam outburst was implemented as an increase in the number of mobile terminated SMS messages towards the users of the monitored HLR/HSS was inserted in the dataset. In this scenario, the unsolicited spam messages affect 1% of the subscribers [17]. This abnormal increase in the number of incoming messages, is detectable from the HLR/HSS component, as it controls all the communications of the subscribers it serves. The proposed approach, depicted in figure 3(b), initially detects the anomalous incident by examining the incoming traffic of the HLR/HSS and displays a small increase in the anomaly score and the volume of the signaling message that relates with mobile terminated SMS messages (i.e. Send Routing Information T21). In the specific scenario, the spam messages originate from an attacker that resides outside of the MNOs network and thus the network graph does not indicate any significant increase in the network volume of the NodeB, RNC and MSC/SGSN components.

4 Conclusions

A complete system for anomaly detection and root cause analysis in the mobile network has been presented. The proposed system enables supervised attack attribution and root cause analysis of anomalous phenomena in the mobile network. To achieve this efficiently, it combines methods from the fields of anomaly detection and information visualization, in order to enhance the analytical potential and allow the user understand and explore the data. The efficiency of the proposed approach in detecting and attributing unknown anomalies, has been demonstrated based on four network incident scenarios that affect the currently deployed mobile networks and have been analyzed in depth in the literature. The current implementation of the system enables the human operator to analyze anomalies in the control plane of the mobile network. Future work includes the enhancement of the current system in order to visualize both the user plane and the control plane, and further improve

the root cause analysis of events, such as signaling storms. User studies will also be performed in order evaluate the proposed approach on real users, including mobile network analysts.

References

1. P. P. C. Lee, T. Bu, and T. Woo, "On the detection of signaling DoS attacks on 3G wireless networks," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pp. 1289–1297, IEEE, 2007.
2. G. Kambourakis, C. Kolias, S. Gritzalis, and J. H. Park, "DoS attacks exploiting signaling in UMTS and IMS," *Computer Communications*, vol. 34, no. 3, pp. 226–235, 2011.
3. P. P. C. Lee, T. Bu, and T. Woo, "On the detection of signaling DoS attacks on 3G/WiMax wireless networks," *Computer Networks*, vol. 53, no. 15, pp. 2601–2616, 2009.
4. A. D'Alconzo, A. Coluccia, F. Ricciato, and P. Romirer-Maierhofer, "A distribution-based approach to anomaly detection and application to 3G mobile traffic," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pp. 1–8, IEEE, 2009.
5. A. Coluccia, A. DAlconzo, and F. Ricciato, "Distribution-based anomaly detection in network traffic," in *Data Traffic Monitoring and Analysis*, pp. 202–216, Springer, 2013.
6. M. Lad, D. Massey, and L. Zhang, "Visualizing Internet routing changes.," *IEEE transactions on visualization and computer graphics*, vol. 12, no. 6, pp. 1450–60, 2006.
7. L. Shi, Q. Liao, Y. He, R. Li, A. Striegel, and Z. Su, "SAVE: Sensor anomaly visualization engine," in *Visual Analytics Science and Technology (VAST), 2011 IEEE Conference on*, pp. 201–210, IEEE, 2011.
8. G. Andrienko, N. Andrienko, P. Bak, D. Keim, S. Kisilevich, and S. Wrobel, "A conceptual framework and taxonomy of techniques for analyzing movement," *Journal of Visual Languages & Computing*, vol. 22, no. 3, pp. 213–232, 2011.
9. H. Shiravi, A. Shiravi, and A. A. Ghorbani, "A Survey of Visualization Systems for Network Security.," *IEEE Transactions on Visualization and Computer Graphics*, vol. 1, no. 1, pp. 1–19, 2011.
10. H. Janetzko, F. Stoffel, S. Mittelstädt, and D. A. Keim, "Anomaly detection for visual analytics of power consumption data," *Computers & Graphics*, vol. 38, pp. 27–37, 2014.
11. S. T. Teoh, K. Zhang, S.-M. Tseng, K.-L. Ma, and S. F. Wu, "Combining visual and automated data mining for near-real-time anomaly detection and analysis in BGP," *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security VizSECDMSEC 04*, p. 35, 2004.
12. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys (CSUR)*, vol. 41, no. 3, p. 15, 2009.
13. M. M. Breunig, H.-P. Kriegel, R. T. Ng, and J. Sander, "LOF: identifying density-based local outliers," in *ACM Sigmod Record*, vol. 29, pp. 93–104, ACM, 2000.
14. B. Shneiderman, "The Eyes Have It: A Task by Data Type Taxonomy for Information Visualizations," in *Proceedings of the 1996 IEEE Symposium on Visual Languages*, VL '96, 1996.
15. N. Gobbo, A. Merlo, and M. Migliardi, "A Denial of Service Attack to GSM Networks via Attach Procedure," in *Security Engineering and Intelligence Informatics*, pp. 361–376, Springer, 2013.
16. P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, and T. La Porta, "On cellular botnets: measuring the impact of malicious devices on a cellular network core," in *Proceedings of the 16th ACM conference on Computer and communications security*, pp. 223–234, ACM, 2009.
17. N. Jiang, Y. Jin, A. Skudlark, and Z.-L. Zhang, "Understanding sms spam in a large cellular network: Characteristics, strategies and defenses," in *Research in Attacks, Intrusions, and Defenses*, pp. 328–347, Springer, 2013.
18. T. A. Almeida, J. M. G. Hidalgo, and A. Yamakami, "Contributions to the study of sms spam filtering: new collection and results," in *Proceedings of the 11th ACM symposium on Document engineering*, pp. 259–262, ACM, 2011.
19. 3GPP, "Study on Core Network Overload (CNO) Solutions," TS 23.843, 3rd Generation Partnership Project (3GPP), 12 2013.
20. S. J. Delany, M. Buckley, and D. Greene, "Sms spam filtering: methods and data," *Expert Systems with Applications*, vol. 39, no. 10, pp. 9899–9908, 2012.