Crime Scene Investigation: SMS Spam Data Analysis

Ilona Murynets
AT&T Security Research Center
New York, NY
ilonaa@att.com

Roger Piqueras Jover
AT&T Security Research Center
New York, NY
roger.jover@att.com

ABSTRACT
The Short Messaging Service (SMS), one of the most successful cellular services, generates millions of dollars in revenue for mobile operators. Estimates indicate that billions of text messages are traveling the airwaves daily. Nevertheless, text messaging is becoming a source of customer dissatisfaction due to the rapid surge of messaging abuse activities. Although spam is a well-tackled problem in the email world, SMS spam experiences a yearly growth larger than 500%. In this paper, we present, to the best of our knowledge, the first analysis of SMS spam traffic from a tier-1 cellular operator. Communication patterns of spammers are compared to those of legitimate cell-phone users and Machine to Machine (M2M) connected appliances. The results indicate that M2M systems exhibit communication profiles similar to spammers, which could mislead spam filters. Beyond the expected results, such as a large load of text messages sent out to a wide target list, other interesting findings are made. For example, the results indicate that the great majority of the spammers connect to the network with just a handful of different hardware models. We find the main geographical sources of messaging abuse in the US. We also find evidence of spammer mobility, voice and data traffic resembling the behavior of legitimate customers.

Categories and Subject Descriptors
K.6.5 [Security and Protection]: K.4.1 [Computers and Society]: Public Policy Issues—Abuse and crime involving computers; C.2.3 [Computer Communications Networks]: Network Operations—Network Monitoring

General Terms
Experimentation, Measurement

Keywords
SMS, abuse, spam, traffic analysis, cellular networks

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

IMC’12, November 14–16, 2012, Boston, Massachusetts, USA.
Copyright 2012 ACM 978-1-4503-1705-4/12/11 ...$15.00.

1. INTRODUCTION
For the past three decades, the Short Messaging Service (SMS) has gained tremendous popularity throughout the world. Reports estimate billions of text messages handled daily by cellular providers’ messaging infrastructures [19], generating millions of dollars of yearly revenue [7].

Being unquestionably successful, text messaging is steadily becoming an annoyance due to the surge of SMS fraudulent activities [16]. Spam is the commonly adopted name to refer to unwanted messages that are massively sent to a large number of recipients.

Spam is a well known and tackled problem in the context of e-mail. Multiple solutions detect and block spam e-mails daily resulting in a small amount of spam reaching customer’s inboxes. This is considered a great achievement given the estimates indicating that 90% of the daily electronic mail traversing the Internet is spam [3].

In the case of text messaging abuse, the trend has been rapidly increasing with the introduction of unlimited messaging plans. Current studies estimate mobile SMS spam to be experiencing a steady yearly growth larger than 500% [8]. Effective anti-abuse messaging filters are deployed, sparing networks from spam text messages injected into cellular networks from the Internet. However, content-based algorithms used to detect e-mail spam, are less efficient in the case of SMS spam [11]. The length of an SMS is limited to only 160 characters [23] and customers often use acronyms, pruned spellings and emoticons which mislead detection algorithms. Thus, mobile originated SMS spam still remains a problem for cellular networks.

The criminals - spammers - connect aircards and cell-phones to personal computers (PCs). These are used to send thousands of daily spam text messages, mostly using pre-paid SIM (Subscriber Identity Module) cards with unlimited messaging plans. The defense against such illegitimate activities often involves SIM shutdowns and account cancelations. This does not stop most spammers, though, who purchase multiple cards and swap them to limit the daily per-SIM volume [8].

Millions of illegitimate text messages are transmitted via cellular networks daily [16]. These messages consume network resources that could be allocated to legitimate services otherwise. SMS spam results also in a major inconvenience for cellular customers because, without an unlimited plan, the end user is paying at a per received message basis. Therefore, SMS spam potentially generates unwanted bill charges for some users leading to negative messaging experience and customer dissatisfaction. Spam also exposes smart-
phone users to viruses. Often multiple fraudulent messaging activities such as phishing, identity theft and fraud [25] are related to SMS spam. SMS is also known as an entry vector for malware propagation [15].

In this paper we analyze the characteristics and communication patterns of SMS spammers. The analysis is based on mining SMS, Voice and IP network traffic from a tier-1 network operator in the United States. The behavior of over 9000 positively identified and known spammers is analyzed and compared to legitimate cell-phone users and embedded Machine to Machine (M2M) appliances. As will be shown throughout the paper, some M2M communication systems exhibit a behavior that resembles in some aspects that of an SMS spammer. The results of this investigation are being used to develop an advanced SMS spam detection engine, the details of which are out of the scope of this paper.

Beyond the expected results, such as the large load of messages sent by spammers to a widely geographically distributed target list, very interesting discoveries are presented in this paper. For example, the vast majority of spammers utilize just five different models of hardware to send the messages. Some of these devices are very popular feature phones that are reflashed to be used as cellular modem. In terms of traffic, spammers make a large number of phone calls, of very short duration, perhaps to mislead detection schemes that might discard accounts with a near-human voice communication profile. We also find the main geographical hot-spots (sources) of messaging abuse activities in the US and that spammers launch very geographically targeted campaigns.

To the best of our knowledge, this paper is the first to

(a) analyze characteristics of fraudulent SMS spam traffic over a major cellular network

(b) analyze voice and IP communication patterns and device and location characteristics of accounts cancelled due to fraudulent SMS activities

(c) compare communication patterns of spammers, legitimate cell-phone users and M2M systems.

The rest of the paper is organized as follows. Section 2 describes the three data sets under analysis (SMS spammers, legitimate users and M2M systems) and how they are labeled. Section 3 presents the data analysis. In Section 4 we give some introductory comments on an SMS spam detection engine that has been designed based on the data analysis in this paper. Section 5 discusses the related work. Finally, the study is concluded with the closing remarks in Section 6.

2. EVIDENCE OF THE CRIME: DATA SET

The analysis presented in this paper is based on traffic data provided by a tier-1 cellular operator in the United States. The data sample contains Call Detail Records (CDR) of 9000 spammer accounts and almost 17000 legitimate accounts. This last set includes about 7000 Machine to Machine devices and 10000 post-paid family plans, from the one year period between March 2011 and February 2012. CDRs are records logging each phone call, text message and data exchange in the network. If two communicating ends belong to the same provider, a duple of records is stored. The Mobile Originated (MO) record logs data of the transmitting party, while the Mobile Terminated (MT) one stores information of the receiver. Note that the MO and the MT records for the same transaction contain duplicated data, such as the originating number and the terminating number. IP (Internet Protocol) data traffic generates only MO logs.

Table 1 summarizes the CDR fields used in our analysis. The originating and terminating phone numbers are fully anonymized and only the first 8 digits of the International Mobile Equipment Identity (IMEI) are parsed, discarding individual serial numbers. This first portion of the device identifier, known as the Type Allocation Code (TAC), determines the manufacturer and model of the wireless device. In the case of a phone, the TAC indicates the manufacturer and model of the phone itself (e.g. Nokia Lumia 900) and, in the case of an M2M connected device, the TAC identifies the embedded cellular modem (e.g. Sierra Wireless Q2687).

The spammer data set is obtained as follows. A list of positively identified spamming accounts and their cancelation dates were provided by the Fraud Department of the cellular operator. The Fraud Department maintains a constantly updated white-list of known legitimate sources of large loads of text messages (i.e. Twitter, American Idol alerts, etc) so they are never confused with spam. Therefore, this data set contains exclusively spammer accounts that were identified and disconnected from the network.

The legitimate account data set is obtained in two steps. First legitimate user accounts are selected and then legitimate M2M appliances are catalogued and included to the set. Our analysis of spammer accounts revealed that 99.64%
of spammers have prepaid plans. Therefore, the set of legitimate customers is drawn from a random and geographically uniform sample of post-paid family plan accounts, which are highly unlikely to be used by a spammer. This way we minimize the probability of having an unknown spammer mislabeled as legitimate. In parallel, M2M connected appliances are identified by the TAC and extracted from the operator’s list of M2M approved devices. This is a database of the M2M devices that have been selected, tested and approved to operate on the provider’s cellular network. These devices include connected appliances running all kinds of services. Some applications found in our data set are asset tracking, remote medical monitoring, security monitoring, Automatic Teller Machines and smart grid power meters. We discard, though, approved M2M systems with a Universal Serial Bus (USB) port because these could be used to send illegitimate messages if plugged to a spammer’s computer.

Message abusing accounts stay alive for a short period of time (see Section 3.1), therefore we collected CDR records for spammer accounts for one week prior to cancelation. For each legitimate account we collected data for a random week between March 2011 and February 2012.

From the CDR data fields we extract multiple features that characterize customer communication patterns. For example, based on the time stamp of each MO SMS (and MO call) we calculate the intervals between two consecutive outgoing messages (and phone calls) and the number of outgoing messages (calls) per day. Based on the time stamps of MT SMSs (MT calls) we calculate the average number of MT messages (calls) per day. The response ratio is computed combining the average number of MO and MT messages (calls) per day. The terminating number field for SMS and voice traffic, also anonymized, is used to calculate the number of individual recipients and the number of different terminating area codes per day. From uplink and downlink byte counts we compute aggregated data usage per week.

Finally, geo-location data is extracted from the CDR records. The coordinates of the serving base station are recorded each time an SMS is transmitted. MO records contain the coordinates of the tower receiving the message in the uplink, whereas the MT record lists the base station delivering the SMS in the downlink. Based on this data fields, the location of a device can be estimated with an accuracy equivalent to the size of a cell or sector. If two communicating devices are connected to the same operator, we know approximate locations of both the sender and the receiver.

3. INVESTIGATION

This section describes the analysis of confirmed SMS spammer accounts that were canceled due to messaging abuse activities. The study compares communication pat-
terns of spammers to those of legitimate customers, both cell-phone users and M2M devices.

In all the figures throughout the paper, legitimate cell-phone users, M2M systems and spammers are represented in green, blue and red, respectively.

This section is organized in five subsections. We start with Subsection 3.1, which briefly describes the characteristics of the accounts of message abusers. Subsection 3.2 investigates the SMS spam traffic in general and Subsection 3.3 studies the location information of both spammers and their targets. Finally, Subsection 3.4 discusses tools used in messaging abuse and voice and data traffic are described in Subsection 3.5.

### 3.1 Spammer sketch: Account information

Detailed analysis of Call Detail Records indicates that the great majority of spammers (99.64%) are using pre-paid accounts. As the GSMA Messaging Anti-Abuse Working Group investigated [8], spammers purchase bulk SIM cards with unlimited messaging plans. These SIM cards are constantly switched to circumvent detection schemes and reduce the number of messages sent per day. Also they discard them once an account is canceled and continue spamming with a new one.

The average age of an illegitimate account is 7 to 11 days. This indicates that message abuse accounts are canceled rapidly on average. The account age of a legitimate user is often several months to a couple years.

### 3.2 The Crime: Messaging Abuse

Figures 1a and 1b compare the empirical histograms for the number of text messages sent and received by legitimate accounts, M2M and spammers. Intuitively, spammers generate a large load of messages. The number of spam SMSs is two orders of magnitude higher than that of legitimate user text messages and one order of magnitude above the number of messages from networked appliances.

Spammers not only send but also receive two orders of magnitude more messages than legitimate customers do. Although this behavior is, at first, unexpected, it can be explained by the nature of SMS spam messages. Upon reception of an unrequested text message, users sometimes attempt to reply to opt-out from the advertised service. Furthermore, actual spam messages often attempt to trick the recipient into replying to the message (Figure 2). Despite a small percentage of users will reply, the large amount of accounts targeted in a spam campaign results in many responses.

Figure 1c, which plots the distribution of the number of destinations, shows that legitimate accounts have a small set of recipients. Cell-phone users text on average to 7 contacts per day, while spammers hit a couple of thousand victims each day.

The ratio of the number of recipients to the number of messages, shown in Figure 1d, provides an additional insight. On average, spammers send one message to each victim. Legitimate users send multiple messages to a small set of destinations. For this specific feature, M2M appliances display a mixed distribution. Some devices send many messages to a small set of destinations while others transmit one single message to each destination. It is important to note that such M2M systems could be miss-labeled as message abusers by simple spam filters.

#### 3.2.1 Response ratio

In subsection we investigate the ratio between the number of received and transmitted messages (response ratio). Although spammers receive a lot of messages, the response ratio is very different to that of a legitimate user. Figure 3 plots an example for a randomly selected spammer and legitimate user (with a post-paid family plan). The number of messages is equally normalized in both cases.

In the case of legitimate users, generally messages are sent in response to a previous message in a sequential way. Therefore, the response ratio close to 1. For spammers the amount of MT SMSs is proportionally very small to the number of transmitted messages. Therefore, the response ratio is close to 0.

#### 3.2.2 Message timing and time series

This sub-section investigates timing characteristics of spam text messages. Due to the large load of SMSs spammers send, the intervals between two consecutive messages are short. On the other hand, both legitimate customers and M2M systems send messages less frequently. This can be observed in Figure 4a, which shows the distribution of the intervals between two sequential messages.

Figure 4b plots the distribution of the inter-message time entropy. Usually, spammers send messages at a constant rate using a computer. Legitimate users are less predictable. One cannot accurately estimate when the next text message will be sent given the time of the previous one. Inter-SMS intervals for spammers are less random resulting in low entropy values. On the other hand, intervals between two legitimate messages are random, with higher entropy.

Messaging activities of certain M2M devices are prescheduled. For example, smart grid meters report measurements periodically. Other applications, such as parking meters and ATMs, have communications initiated by humans. A message is sent each time a parking receipt is issued. Therefore, we observe a large number of M2M connected devices with a low value of the entropy, overlapping with spammers, and some with a higher value of the entropy, overlapping with legitimate users.

Beyond the large messaging load at a high frequency, we investigate what strategy spammers follow to transmit text messages over time. Figure 5 plots a typical example of the
number of messages per minute sent over the span of one day. The results indicate that spammers focus the illegitimate activity during the day time. This might be to minimize the annoyance caused to recipients and lower the chances to be reported to spam detections services such as the 7726 service [1].

3.2.3 Message content

The analysis of the content of spam messages is out of the scope of this paper. However, we offer a brief glimpse of some of our findings. Querying the Cloudmark 7726 data-base of user reported spam messages [1], we access the content of the messages sent by positively identified spammers. Based on this data we determine that spammers based in far apart locations sometimes flood messages with exactly the same content. This could be an indication of either collaboration or a set of common sources both for revenue and content.

3.3 The Scene of the Crime

The next step of our analysis is to determine the geographical distribution of messaging abuse. We aim to find out where spammers base their activities and where the targets of such SMS traffic are located. Finally, we attempt to determine whether spammers are mobile or not.

3.3.1 Location of spammers and their targets

Figure 6 shows the locations of accounts identified for messaging abuse activities during the one year period under analysis. Data indicates that spammers are mainly located in California, specifically in the counties of Sacramento and Orange and in the surroundings of Los Angeles. Other notable sources of spam are observed in the New York/New Jersey/Long Island areas and in Miami Beach. Smaller sources of messaging abuse are found in Illinois, Michigan, North Carolina and Texas. Note that this does not im-
Figure 5: The number of messages sent per minute by a typical randomly selected spammer

Figure 6: Location of SMS spammers.

Assume that spam will always come from only these areas, but gives an indication of the non-uniform origin of SMS spam messages. Messaging abuse in the SMS world appears to originate from a few locations over the US.

Figures 7a and 7b show the recipients of SMS messages sent out in one day by a randomly selected spammer and legitimate customer respectively. Each map plots the source (spammer or legitimate user) with a pin and individual recipients with a diamond. Note that we only have location information for customers (recipients) subscribed to the cellular operator under analysis. The legitimate customer communicates only with a small number of contacts. Most of the recipients for the given user belong to the local area (i.e. the area around the subscriber’s home) as well as several other locations (e.g. areas where the subscriber works, used to live or where friends and relatives reside). In contrast, the recipients of spam text messages appear to be distributed...
uniformly over the US population (the spammer sends messages to most area codes).

Figure 8a plots the distribution of the number of unique area codes contacted in one day by spammers, legitimate customers and M2M systems. Spammers are characterized by messaging a large number of area codes, always greater than those of cell-phone users and M2M. We observe, though, a small amount of spammers contacting a reduced number of area codes. Most M2M devices contact numbers just within one area code.

Independent of the number of unique area codes, it is interesting to know how often these area codes are contacted. Figure 8b plots the entropy of these area codes. In this context, entropy stands for the randomness of the connections in one day. A low value of the entropy implies that this specific user contacts repeatedly the same area codes. On the other hand, a high value of the entropy indicates a user that sends messages to a more random set of area codes.

Network enabled appliances report to specific servers and data collectors or, in the case of user applications (i.e. home monitoring), to a predefined set of cell-phones. Therefore, the entropy is the lowest. Spammers show a much more random set of SMS abuse targets with a high entropy. Further analysis of the spam data identifies a messaging strategy that consists of messaging numbers in ascendent order. Thus, sending bulk SMSs to each area code sequentially.

The aforementioned results are summarized in Figure 8c, which plots the correlation between the number of sent messages and the number of recipients. The linear relation in the case of SMS spammers is obvious. Both M2M systems and cell-phone users cluster around the bottom-left area of the graph. One can notice in the figure some M2M appliances sending up to 20000 messages to 1 single destination. This is a common situation in, for example, security or monitoring M2M applications in which reports are timely sent to a controlling server.

The relation between the ratio (number of message recipients)/(number of messages sent) and the average number of area codes reached by day is plotted in Figure 8d. Cell-phone users congregate at the bottom left of the Figure, with low destinations-to-messages ratio and a small set of contacted area codes. A great majority of spammers exhibit the opposite behavior, clustering on the top-right corner of the figure. Nevertheless, a substantial number of spammers with a different behavior is identified.

The spammers aggregated on the bottom-right corner of Figure 8d are message abusers that target very specific geographical regions. These accounts still send thousands of messages per day with a ratio close to one destination per message. However, the number of targeted area codes is in the range of the number of recipients from legitimate cell-phone users.

3.3.2 Do spammers move? Yes, they do!

In terms of mobility, one expects spammers to not move. Therefore, all messages should be handled by one single base station. Figure 9 plots the distribution of the number of base stations (Location Area Code - Cell ID, LACCI) a device is connected to in one day. Legitimate customers display a highly mobile behavior, with most of the users visiting at most 30 cells sectors. This number depends on many factors, such as the length of the daily commute. The distribution exhibits a long tail with a minority of highly mobile cell-phone users.

Spammers, as expected, are much less mobile. They still appear to traverse an average of about 4 cells or sectors. This might be due to the following reasons. On one hand, spammers might mount their equipment on a vehicle and drive around the area in an attempt to misguide detection schemes looking at device mobility. On the other hand, especially in the case of aircards, the hardware often connects to the network by means of a Third Generation (3G) technology. 3G wireless networks in the operator under study are based on Wideband Code Multiple Division Access (WCDMA). In such technology, the receiver can be physically connected to up to 6 sectors at the same time, combining the signal at the RAKE receiver [22]. Depending on the channel conditions and fading, the serving base station might fluctuate throughout this list of 6 LACCIIs. This would result in CDR records from the same static device appearing to come from up to 6 different sectors.

Note that, though, based on the IMEI, we are able to determine the actual hardware used by the spammer to send messages. In the case of GSM devices, a cell-phone or cellular modem is at all time connected to, at most, one cell tower [6]. Camping on base stations miles away from each other definitively indicates movement.

The distribution of recipients’ area codes for M2M is mixed. The majority of appliances are quasi-static, with most of their messaging load being handled by a couple of sectors. This corresponds to non-mobility M2M applications...
such as alarms and smart grid readers. Another large set of devices are highly mobile, with an average of 28 sectors visited per day. In this case, these are mobile applications such as fleet control/monitoring and asset tracking.

The final answer to the question is found in Figure 10, which plots the observed locations of a randomly chosen spammer on the map of an undisclosed area. The legend indicates the length on the map that corresponds to 1 mile and 2km. Based on this information, it seems that certain spammers move while sending illegitimate SMSs. In the case of the example, this spammer is observed in the vicinity of cell sites as far as 4 miles apart. Computing the longest distance between the cell sites every spammer camps on indicates a maximum displacement of 15 miles.

Figure 8: Distributions of the average number of destination area codes, their entropy and related scatter-plots for spammers (red), legitimate customers (green) and M2M (blue)

Figure 9: Distribution of the average daily number of base stations (LACCI) visited by spammers (red), legitimate customers (green) and M2M (blue)

3.4 The weapons of choice

Observations of the IMEI from CDR gives us an insight on the kind of device used to connect to the cellular network. Analyzing the TAC data from known and already canceled spamming accounts, we observe that an impressive 83% of the spammers identified in one year is sent from one of the top five identified devices. About 65% of the spammers in the US send messages with the top device.
Devices used by spammers are anonymized and ranked. The top 5 most frequently used devices are listed below.

1. USB Modem/Aircard A1
2. Feature mobile-phone M1
3. Feature mobile-phone M2
4. USB Modem/Aircard A2
5. USB Modem/Aircard A3

Thus spammers often rely on modems and aircards connected to a PC via USB interface. A1, A2 and A3 belong to this category. In parallel, spammers also use common feature phones as cellular modem. This might be done in order to mislead detection schemes by making messages appear to be originated at a legitimate cell-phone. Several resources can be found online with detailed instructions on how to reflash typical feature phones from most manufacturers with custom firmware [2] [5] [4].

Note that these devices are legitimate hardware that spammers use for SMS abuse. All of them are used in legitimate applications, which provides cover for the spam. This is why we anonymize the make and model of these devices.

It is interesting to note that this specific traffic analysis indicates that at least 16% of the SMS traffic originated by all the A1 modems in the network is spam. This shows a clear preference of spammers for this particular cellular modem.

### 3.5 The Alibi: Voice and IP traffic

As observed in the previous sections, SMS spammers attempt to reach as many targets as possible by flooding large amounts of messages. This paper focuses on SMS spam analysis. Nevertheless, we include voice and IP traffic data in our study and the results are rather interesting. Spammers do generate both data and voice traffic, perhaps to increase the chances to go undetected through spam filters that search for non human-like communication traffic or perhaps other forms of fraud.

#### 3.5.1 Voice calls

Figures 11a and 11b plot the empirical histograms of the number of phone calls and their recipients. Figure 11c corresponds to the empirical histogram of the duration of voice
calls. On average, spammers make many more phone calls than legitimate users, however the average number of phone call destinations is much lower (Figures 11a and 11b). This number of phone calls could perhaps indicate that they are trying to mimic legitimate users. In terms of voice traffic duration, phone calls placed by spammers are much shorter than those of legitimate users, as it can be observed on Figure 11c. This is because, despite they seem to attempt to match the calling profile of a legitimate user, these calls cannot be sustained for a long time since the recipient will hang up. The short call duration could also indicate that these calls might be spam as well. Most of the times, the recipient of a spam call will hang up immediately.

Unlike in SMS traffic, spammers do not flood with calls a large number of recipients. They might be communicating with a small set of numbers that they know will pick up the call even though they might hang up quickly.

The results are further detailed in Figure 12. Figure 12a plots the average number of call destinations per day (y-axis) versus the average number of calls (x-axis), in log-log scale. One can see that spammers cluster around a large number of calls to a small set of destinations. In parallel, both cell-phone users and M2M devices make phone calls to a proportional set of destinations.

The difference in behavior of spammers is highly accentuated in Figure 12b, which plots the average number of SMS destinations (x-axis) against the number of voice call destinations (y-axis). Spammers appear to be placing phone calls to a set of recipients that is much smaller than the set of targets for the text message abuse. This figure also hints that legitimate users, on average, tend to communicate to a larger set of contacts by phone than by text message. This could be explained based on the fact that cell-phone users rely on the extremely popular SMS service to communicate with friends and relatives. However, phone calls are made to this same set of users plus other contacts such as restaurant to make a reservation, the doctor’s office to make an appointment, etc. Therefore, the set of call recipients will be larger than for SMSs.

3.5.2 IP traffic

Finally, we examine IP traffic. Figure 13 plots the distribution of the up-link and down-link byte counts related to the three account categories under analysis. Spammers generate a small amount of data, consisting on several small transactions.

Cell-phone users and M2M systems generate asymmetric IP data traffic. Regular users often consume more bandwidth in the downlink, by browsing videos, media and other kinds of content. Their uplink traffic is generally lower. M2M appliances have the opposite behavior. Used mostly as reporting tools for applications such as remote alarm and fleet control, they often generate a larger load in the uplink.

4. STOPPING THE CRIME

The results presented in this paper have been used to develop an accurate SMS spam detection engine. The description, details and results obtained are out of the scope of this paper, but will be submitted in the near future. In this section, though, we offer a brief overall glimpse.

An advanced SMS spam detection algorithm is proposed based on an ensemble of decision trees. Over 40 specific features are extracted from messaging patterns and processed through a combination of decision trees. Moreover, in order to speed up the spam detection process, the system focuses on features that only require one to a few messages to obtain. This algorithm also leverages the insights on M2M SMS messaging patterns described in this paper.

5. RELATED WORK

SMS spam has not been widely discussed in literature. Nevertheless, there is some work introducing different detection schemes. For example, the authors of [24] propose a detection engine based on analyzing the social network of connections of spammers. Other approaches are based on investigating the content of SMS spam messages [12].

There is plenty of literature on spam messaging analysis on other communication systems. The most widespread type of spam is electronic mail (email) spam. In this context, [17] presents interesting findings on how message abusers harvest large lists of email addresses to use as targets for their spam campaigns. The authors of [18] study the network-level behavior of spammers in the email world. Email messaging abuse is found to originate from a very few regions of the IP address space. This messages are generated from an immense swarm of bots, each one of them sending only a few
6. CONCLUSIONS

In this paper we study characteristics and traffic patterns of SMS spam accounts based on real cellular network from a tier-1 provider in the United States. The results are compared against a sample of real traffic from legitimate cell-phone users and M2M devices.

Confirming the common presumption, we identify that 99.64% of the spammers connect using pre-paid accounts. The simple availability of such SIM cards makes them the perfect tool for SMS abuse. Observations indicate an average age for the pre-paid accounts between 7 and 11 days. We also find indications of the preference spammers have for a very small set of hardware devices. Spam traffic analysis reveals that 84% of the spammers use one of the top 5 spamming tools in the US. In particular, 65% of the spammers choose to connect to the network with the top device.

We confirm common intuitions about spammers, such as the large number of text messages sent per day to a wide target list. Spammers generate two orders of magnitude more messages than cell-phone users and one order of magnitude greater than most M2M systems. These messages are sent mostly to different recipients, with a ratio of recipients to messages sent very close to one. Further investigation of the messaging flow indicates that spammers also receive a large number of messages. Nevertheless, the number of incoming SMS is relatively very low with respect to the number of transmitted spam texts.

The study of geo-location data identifies the areas of Sacramento, Los Angeles-Orange County and Miami Beach as the major spamming hot-spots in the US. From these locations, spammers launch very geographically distributed campaigns targeting all area codes uniformly. Nevertheless, some spammers are engaged in very geographically focused spamming campaigns. In terms of mobility, we conclude that spammers are often mobile around their local area.

Finally, spammers are found to generate a large number of very short phone calls and data transactions with a very small number of end points. This could be perhaps a strategy to mislead spam detection filters by replicating human-like network traffic behavior.

Our traffic analysis indicates that certain networked appliances have messaging behavior close to that of a spammer. A small number of M2M systems transmit a large number of SMSs per day. These are often devices that communicate with a large number of destinations as well. Despite not being very abundant, we identify a substantial number of M2M enabled objects with a ratio destination to number of messages very close to 1. These appliances communicate with a large set of area codes as well. However, these area codes have low entropy in the sense that the recipients of the messages are always the same. Based on the investigation in this paper, we identify Machine to Machine communications as an important player in SMS networks. Such systems should be taken into consideration when designing SMS spam detection and filtering schemes. Systems designed otherwise could incur the risk of blocking or erroneously labeling legitimate text messages as message abuse.

The results presented in this paper are being used to design an advanced SMS spam detection system.
ACKNOWLEDGEMENTS

The authors would like to thank Cheri Kerstetter, Rick Becker, Joel Casey, Jeff Bickford and Alex Bobotek for their help, comments and valuable suggestions.

7. REFERENCES


