This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings

Characterizing Data Services in a 3G Network: Usage, Mobility and Access Issues

Zhichao Zhu*, Guohong Cao*, Ram Keralapura† and Antonio Nucci†
*Department of Computer Science and Engineering, The Pennsylvania State University, University Park, PA
†Narus Inc, Mountain View, CA
*{zzhu,gcao}@cse.psu.edu † {rkeralapura, anucci}@narus.com

***Abstract*—Although 3G networks have been largely deployed to cope with the increasing demand of wireless data services, little is known on how these networks are used from the network perspective. In this paper, we present analysis of data services based on a nation-wide 3G network trace collected from one of the largest cellular network service providers in North America. Our work differentiates from previous studies by examining data service usage and mobility patterns from various dimensions including application breakdown, user roles, device types and diurnal characteristics. We also look into various access issues such as termination failures and frequent registrations to better understand how the network performs. Our results are important for cellular network operators and protocol designers to improve data service performance and user satisfaction.**

I. Introduction

Cellular networks are becoming more and more important in our daily life. In addition to traditional voice services, cellular networks provide a wide variety of broadband data services such as Web browsing, Multimedia Messaging Service (MMS) and voice over IP (VoIP). Although 3G networks have been broadly deployed to cope with the increasing demand of wireless data services, little is known about how they are used from a network perspective. For example, what kinds of services are more popular among the users? What is the diurnal characteristic and mobility pattern of the users and what is the relationship between them? How reliable is the network and what is the failure rate? To answer these questions, a comprehensive analysis of the usage of data services in real 3G networks is necessary. Moreover, mobile devices are rapidly evolved from ordinary phones to smartphones such as iPhone or Google Nexus One, and even laptops with aircards, which are expected to exhibit different usage patterns and mobility patterns [9]. Therefore, characterizing the user behaviors, mobility patterns and network performance of different services and devices is critical for network providers who develop and manage the network systems and resources, and is also helpful for protocol designers who develop network standards and better protocols.

In this paper, we address these problems based on a 3G network traffic trace collected from one of the largest cellular network service providers in North America. This trace was collected for one entire week beginning on April 16th 2009, and includes all the data service activities within the 3G network. To the best of our knowledge, this is the first work to study data service usage patterns, user access behaviors and network performance issues based on measurements from such a large cellular carrier. This paper differentiates from previous work on the scale of the trace and the detailed multi-dimension analysis. It can be viewed as a significant extension of previous large-scale trace-driven measurement work on SMS analysis [5] and phone call analysis [7] [8] in cellular networks and low-layer performance analysis [4] in 3G data networks.

More specifically, our work examines different 3G data services diurnal patterns on a daily basis, and shows totally different usage patterns between HTTP, MMS and SIP services, local users and roaming users, laptop users and mobile phone users. Moreover, we study various network termination failures and how these failures affect local and roaming users differently. We also discuss frequent registration failure and its correlation with malware issue [10] to better understand how the network performs. Our results either verify some of the speculations in previous observations, or reveal novel domains for further research, and are important for cellular network operators and protocol designers to improve network performance and user satisfaction.

The remainder of this paper is organized as follows. Section II describes our data trace collection methodology. Section III presents the usage characteristics of data services from multi-dimension. Section IV studies the user mobility pattern and commuting phenomena. Section V investigates the network termination failure and frequent registration issue. Section VI concludes the paper and lists recommendations for developers and designers of 3G data networks.

II. Data Trace

To address the 3G data network characterization problem, we collect a nation-wide network traffic trace from one of the largest cellular service providers in North America. The trace provides a session-level information for traffic (bytes and packets) exchanged between two endpoints per application over a one-week period from April 16th to 22nd, 2009. The endpoints present in the trace were anonymized while preserving the uniqueness of the identifiers of IP addresses and phone numbers involved. This trace involves 2 million users across 65000 base station cells all over the US and contains all the transactions of HTTP [2] sessions, MMS [1] session, SIP [3] based VoIP sessions exchanged between users and SIP based Push-To-Talk. Note that our data collectors do not monitor the cellular service provider's voice network. All the traffic captured for this paper came from the 3G network, not the 2G GPRS/Edge network.

Our data collectors are located in a central location and collect detailed information of a packet data session from the time the user is authenticated by RADIUS server to the time

978-1-61284-231-8/11/$26.00 ©2011 IEEE

the user logs off. Each data session is captured and recorded in real time with the following relevant information: local timestamp, anonymized user identifier (phone number or email address), anonymized ip-address assigned to the user, correlation identifier, and the base station that was associated with the user's current service. Note that the ip-address allocation for a user can change several times in a day due to mobility, reconnection, etc. We correlate together a user's entire data activity profile by associating between a user identifier (phone number of email address) and his currently assigned ip-address. We also identify each data service accessed by a user by grouping different type of data sessions (HTTP or MMS) that occur after a RADIUS session and have the same assigned ip-address.

The trace was collected in real time for seven days long. We would like to see the network traffic patterns at different time periods. According to our analysis, the network traffic presents very similar diurnal patterns for different days in a week. Therefore, all the results in this paper are presented for an entire day period with 10 minutes as the time interval. There are four time zones that we are monitoring, and the default timestamp in our trace is the time when the collector sees the authentication/data session. However, given that our goal is not only to analyze user behavior at a given point in time, but over the course of a day, we convert all the timestamps to the local time stamps of the users. This will help in comparing the activities of users across time zones and acts as a time normalizer. After this step all the timestamps in our trace are between 0 and 24 hours.

III. Dissecting the 3G Data Network

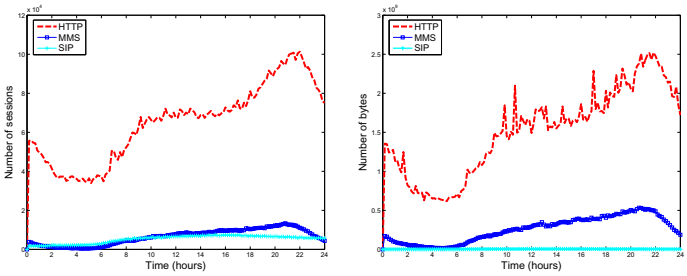
Due to the large amount of data we have collected, we can only present a subset of the most impressive results in this paper. In this section, we look at various services extracted from the trace on a daily basis from different metrics: diurnal, user role and device type.

A. Application Breakdown

Various service types can be observed from the trace. These services are used by different users with different patterns at different time periods. We choose three most popular data services HTTP, MMS and SIP (mainly Push-To-Talk and VoIP) in our trace for further exploration.

HTTP is the most popular application. We breakdown the applications into three subsets: HTTP, MMS, and SIP. We look at the number of users and the number of sessions exchanged over time during an entire day. The time metric in all figures is already shifted to users' local time. Figure 1 displays the number of sessions and bytes respectively over time for each application. These figures show an obvious diurnal pattern with a down valley after midnight and increasing usage during business hours, and also a peak at around 9pm. We can see that HTTP is the most popular data service compared to other services. Figure 1(b) has similar pattern with figure 1(a) except that there are many spikes for HTTP traffic, showing that a number of data sessions carry much more bytes than others and thus consume most of the network bandwidth. Note that SIP traffic in figure 1(b) appears relatively stable due to its small volume.

All the three data services present reasonable strong diurnal patterns as expected. Several differences are also observed due to the unique characteristic of each service type. For example, HTTP sessions behave more active during night than MMS sessions as part of users prefer to leave their mobile devices on for some applications which require frequent updating and downloading. Also, the peaks of HTTP and MMS sessions appear after 8pm at night while the peak of SIP sessions appears at around 2pm in the afternoon with a more stable usage during business hours. From our statistical results, SIP based VoIP and Push-To-Talk services are more associated with business behaviors, therefore are mainly used during business hours; while HTTP and MMS services are more related with personal interests and therefore are mainly used after work.



(a) Sessions over time (b) Bytes over time

Fig. 1. Number of data sessions and bytes over time for each application type

B. Local User vs Roaming User

There are about 2 million users in our network trace, who are categorized as local users and roaming users. As different user roles are experiencing different traffic control and resource allocation policies from the network operator, we expect to see diversity of data service usage patterns from local users and roaming users.

- Local users: subscribe to our network carrier and also access to our network's data services. 74% of users in our trace are local users.
- Roaming users: subscribe to other network carriers but access to our network's data services. 26% of users were

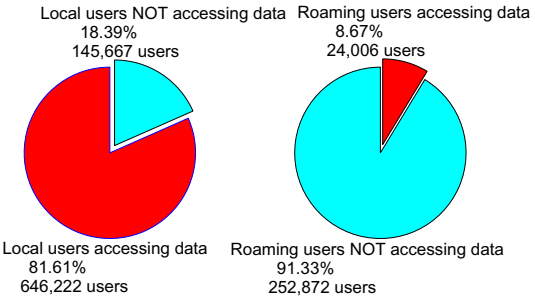
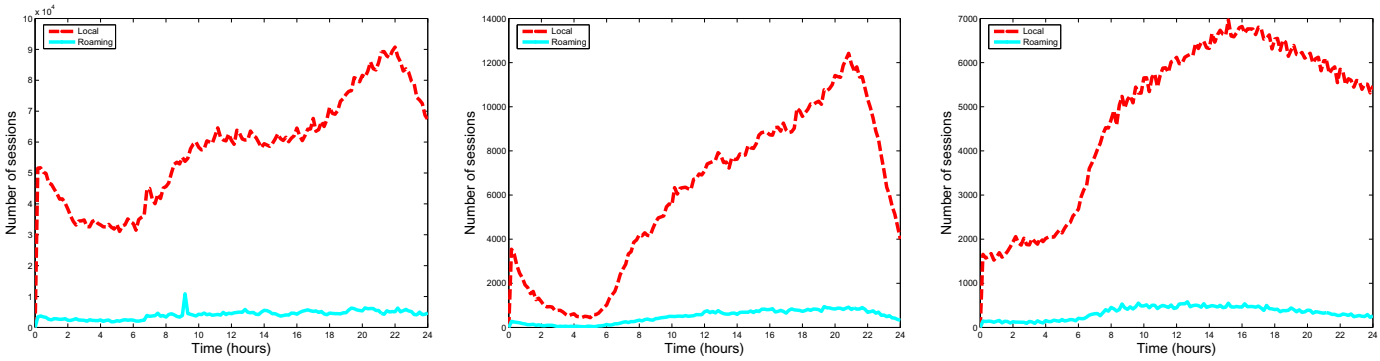


Fig. 2. Users breakdown by data access for local and roaming users

Local users are more active than roaming users in data usage. Our results show different behaviors between local



(a) HTTP sessions (b) MMS sessions (c) SIP sessions

Fig. 3. Number of HTTP, MMS and SIP sessions over time for each roaming type users

users and roaming users. Figure 2 shows the data service usage between local and roaming users for the one million users observed from our trace during one day. 82% of the local users access data services at least once a day, while the other 18% just register with the network without using any data service. On the other hand, for roaming users, 9% of them use data services at least once during a day while 91% of them have never accessed any data service during the same time. Thus, when mobile users are roaming, most of them would rather not access any data service. From our conversations with specific service provider, the main reason of such behavior is due to the high-cost of using data services during roaming.

From our trace, we can also see that local users are more active than roaming users. Figure 3 shows the numbers of HTTP, MMS and SIP sessions for local and roaming users. As can be seen, local users always contribute to most of the data sessions for all three service types. Although there are 74% of local users, they contribute to 97% of the data sessions, whereas 26% roaming users count for 3% of the data sessions. We also observe clear diversity of the three diurnal curves from local users. As mentioned before, the peaks of HTTP and MMS appear at 8pm while the peak of SIP appears at around 2pm. SIP traffic does not drop as much as MMS during the night, mainly because SIP clients have to update and exchange information with SIP proxy servers periodically under the VoIP and PTT scenario even when there is no usage.

C. Mobile Device Types

Mobile devices are rapidly evolving from traditional phones to smartphones, and even laptops with aircards plugged in. These distinct device types are expected to present different usage patterns. As the HTTP sessions initiated from mobile devices carry either the exact model of the end-device or the screen resolution of the device, we can map an end-device to a specific type, i.e., small phones, PDA phones, laptops and blackberrys, and look at network usage patterns by different device types.

By further looking into HTTP data service for different types of devices, we see ***totally different application usage profiles for each device type***. Each bar in figure 4 shows the percentage of users of each device type has been using a certain application. Note that this plot just shows the popularity of different applications for each device type and there unavoidably are overlaps between these users, since most users use more than one applications. Almost all of the small phone users mainly use ringtones, gaming and MMS, while more than 95% of blackberry users focus on mail application. On the other hand, both PDA users and laptop users are involved in large range of usage types like searching, news and social networking but with some minor difference. Streaming video is widely used by laptop users but less popular within PDA users with a coverage lower than 20%. The unique feature of each device type decides its usage profile: laptops and PDA phones are more powerful thus are able to be used for various applications, especially those involving large data traffic; small phones are only equipped with simple functions thus their usages are limited to some basic applications such as ringtones, gaming and MMS; blackberry phones are well known for their push mail functions thus users are interested in choosing blackberry phones for their mail services. Therefore, the choice of different device types drives users to present different browsing behaviors.

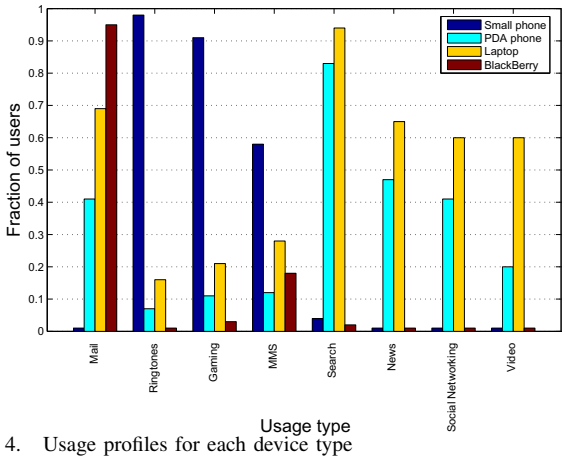


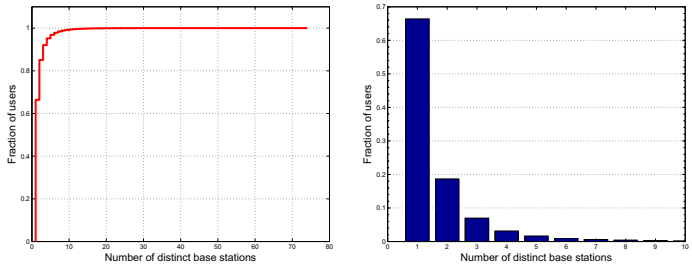
Fig. 4. Usage profiles for each device type

IV. User Mobility Pattern

Here we explore users' mobility patterns when they are active in data service usage. We first look at the number of distinct base stations seen by each user, which we use to represent the moving range of the user during his data service usage. In the trace, we have a total of 65000 base stations across a nation-wide map. The area (cell) served by a base

station in the network varies from hundreds of square meters (area with dense population) to several square miles (area with sparse population). On average each cell serves a 4-square kilometer area. In the remainder of the paper, when we refer to the number of base stations seen or crossed by a user, we use statistically averaged cell size as the coverage of each base station. While our trace does not provide GPS-level location information, we will show that location information at base station-level is enough for extracting generic user mobility properties during data service usage.

Figure 5(a) shows the CDF of number of distinct base stations seen by each user during a day. The mobility is comparably low for most users as over 95% of the users travel across less than 5 base stations in a day. On the other hand, a few highly mobile users cross up to 74 distinct base stations in a day. These users contribute more to the network's mobility activities, for example, handoff activity. If we zoom in those users who have seen 1 to 10 base stations by figure 5(b), we can observe clearly that about 66% of users are stationary as they see only 1 base station. The number of users decreases exponentially as the number of base stations increases. 27% of users see 2 to 5 base stations while 6% of users see 6 to 10 base stations in a day. Here, we categorize users into three classes: static users who see only 1 base station in a day, short-range users (commuters) who see 2-5 base stations in a day and long-range users (commuters) who see more than 5 base stations in a day. we examine the mobility behaviors of these different user users in detail.



(a) CDF of distinct base stations (b) zoom-in view

Fig. 5. CDF and zoom-in view of number of distinct base stations seen by users

Short-range users vs long-range users To identify how short-range users and long-range users behave differently, we need to see when and how frequent do users typically move. Figure 6 gives us a picture of number of base station crossed at different time of a day for short-range commuters and long-range commuters respectively. An obvious diurnal pattern can be seen from the figure that highly mobile activities happen during the business time with the peak appearing at 8am and 6pm. Therefore, we identify the commuting time as 8am in the morning and 6pm in the evening. Moreover, long-range commuters show this characteristic more vivid, so that typical commuting range should be larger than 5 base stations.

Another way to explore the user mobility level is by looking at the number of crossings between base stations by each user. While the number of distinct base stations shows the total moving range of each user, the number of crossings indicates how frequently this user moves across between different base

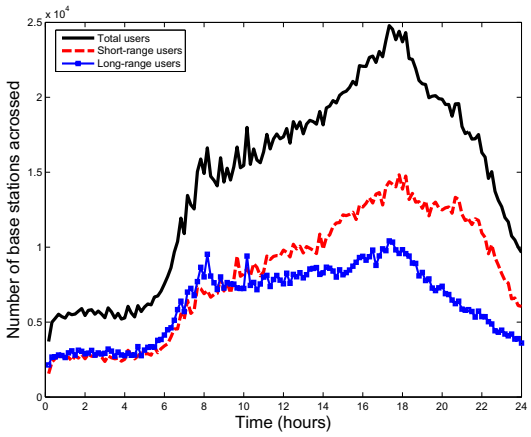


Fig. 6. Number of crossings between base stations over time for short and long commuters

stations. When we compare the number of distinct base stations seen by each user and the number of base station crossings by the same user, we found the two are not necessarily correlated since some users who only see small number of distinct base stations have experienced over 100 base station crossings in a day. In fact, a few users keep moving between two or three neighboring base stations repeatedly during a day. Most of these users are observed staying around the boundary area between two base stations and thus experience frequent handoffs. Generally, users associated with more distinct base stations tend to cross more base stations.

V. Network Access Issues

In this section, we study several network access issues such as termination failures and frequent registration.

A. Network-induced Termination Failures

When users complete their data sessions, they close the connection and log off from the network. This is considered as a successful connection termination. However, sometimes connections are terminated unexpectedly for various reasons and users are forced to deregister from the network. These unexpected terminations are considered as network issues. Table I lists various termination causes with the number (percentage) of cases observed from our trace. These causes are clarified into two types: user-induced terminations and network-induced terminations. We can see that around 77% of terminations are caused by user requests. In other words, the percentage of network-induced terminations which are unexpected by users is as high as 23%, although part of them may not be felt by users. The most notable network-induced terminations include **NAS Request** and **Session Timeout**. NAS (Network Access Server) works with RADIUS accounting server to deliver accounting information and provide services to mobile users. NAS request failure occurs when NAS ends a session for a non-error and unexpected reason induced by the network. More details about NAS request can be referred to [6].

The network-induced terminations which are unexpected by users are considered as termination failures, and will be studied in more detail. First we examine individual users who

experience termination failures by looking at their distributions on the number of termination failures. There is a large diversity among individual users if we spread the termination failures across users. Some users do not experience any termination failure, while others experience a very large number of failures (up to 800 times of the average). More specifically, we can see from figure 7 that about 96% of the users experience less than 10 termination failures. Nearly half of the users experience only one failure. Several individual users even experience more than 3000 failures.

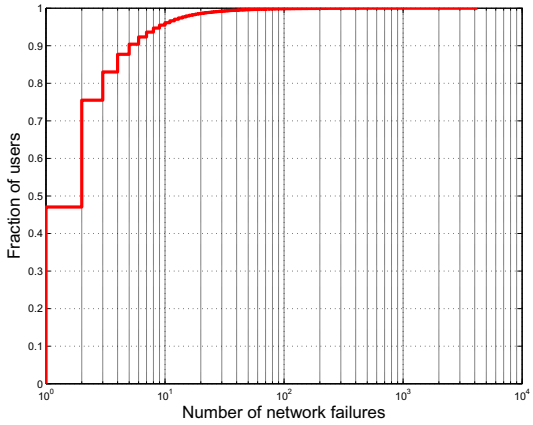


Fig. 7. CDF of number of network-induced termination failures

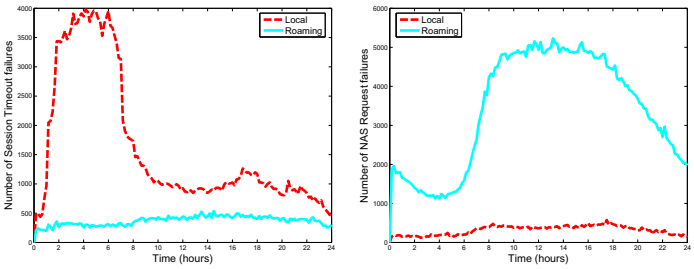
This small part of problematic users who experience extremely high failure rate deserve more attention from the network operator's perspective. We sample the top ten users who experience the most number of failures during a day, and list them in Table II. Surprisingly, most of them are roaming users. More specifically, local users are mainly suffering from Port Suspended failures while roaming users mainly experience NAS Request failures. These users keep crossing between base stations up to 4000 times in a day and keep registering with the network accordingly. They always move between the same base stations and acquire the same IP address for their registrations. Frequent handoff is the reason behind the the high failure rate, especially for the roaming users. There is one stationary user who does not move but registers frequently. It turns out the device error should be responsible for the high termination failure rate.

Local users are affected most by the network failure of Session Timeout, while roaming users are affected most by the network failure of NAS Request. Figure 8 shows the number of two network failures over time for local users and roaming users. As can be seen, session timeout failures affect local users most, but have less effect on roaming users. On the other hand, NAS Request failures mostly affect roaming users, but have little effect on local users.

Moreover, local users experience peak session timeout failures during midnight from 2am to 6am, while roaming users experience peak NAS Request failures during business hours from 8am to 6pm. As far as we know, cellular providers perform various timeout checking mechanism around midnight and mandatorily close the connections which are not in use to conserve resources. This explains why timeout failures mainly

TABLE I
CONNECTION TERMINATION CAUSES

Name	Number	Type	%	Net_%
Unknown	5848	Unknown	0.08	-
User Request	5432184	User	73.95	-
Lost Service	560	Network	0.008	0.03
Idle Timeout	235491	User	3.2	-
Session Timeout	335826	Network	4.57	20.75
Admin Reset	191020	Network	2.6	11.80
Port Error	493	Network	0.00067	0.03
NAS Request	1036467	Network	14.11	64.04
Port Preempted	1042	Network	0.0014	0.06
Port Suspended	53108	Network	0.72	3.28
User Error	41955	User	0.57	-



(a) Session Timeout failures (b) NAS Request failures

Fig. 8. Number of Session Timeout failures and NAS Request failures over time

appear during midnight. The NAS Request failures present strong diurnal pattern with a peak during business hours. This is due to network congestions which usually happen during business hours. From the results, our network applies provision mechanism which treats local users and roaming users differently, where roaming users have less priority for getting the network resources and then are more vulnerable to NAS Request failures.

B. Frequent Registrations

To use any kind of data services, the user needs to first register with the cellular network to obtain a dynamic IP address, which is allocated by DHCP. Then the user accesses zero or more data services before logging off.

Figure 9 shows the number of registrations for each user during a day. The number of data sessions for each user is also shown in the same figure for comparison. The data is sorted based on the number of data sessions for each user. We can see that a number of users make more than 1000 registrations but do not have any data session. There are two cases responsible for this situation: there is something wrong with their mobile devices which keep registering to the network automatically without users' awareness, or they are under week signal environment (e.g. driving through a tunnel) that their mobile devices keep scanning and registering with the network. Another reason might be that these users suffer from some specific termination failures, which are described in previous subsection.

When we look into the small number of users who make large number of registrations, we find that users experiencing largest number of registrations are usually the ones with largest number of malware/spyware accesses. Of the 75000 hosts that users have accessed during their HTTP sessions,

TABLE II
NETWORK FAILURES ANALYSIS FOR TOP 10 USERS

ID	User role	# of failures	Major causes	# of IP	# of REGs	# of BS	# of BS crossings
1	local	4214	Port Suspended(4214)	1	4233	4	4057
2	roaming	2436	NAS Request(2436)	8	3217	27	2321
3	roaming	1676	NAS Request(1675)	7	3448	9	1737
4	roaming	1408	NAS Request(1342)	7	2105	2	1374
5	roaming	1399	NAS Request(1321)	5	2118	10	1374
6	roaming	1148	NAS Request(1078)	6	1765	1	0
7	roaming	1118	NAS Request(1059)	3	1682	4	867
8	roaming	959	NAS Request(917)	5	1478	4	960
9	local	943	Port Suspended(943)	6	948	2	896
10	roaming	793	NAS Request(793)	3	1575	26	789

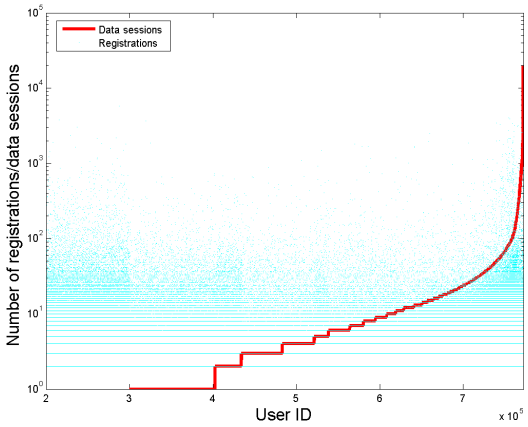


Fig. 9. Number of registrations and data sessions for each user

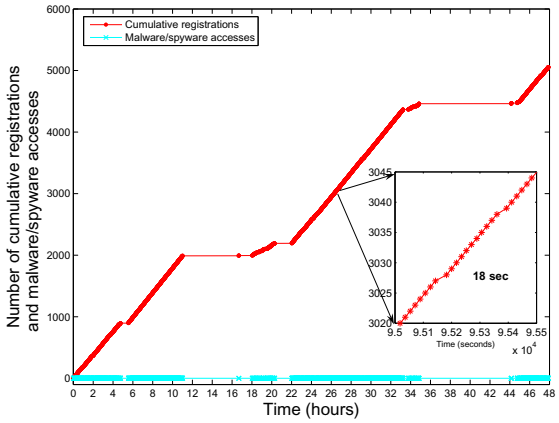


Fig. 10. Number of cumulative registrations and malware/spyware accesses over time

we identify 4.1% of them as malware/spyware hosts, which have the ability to track users' browsing activity and exploit personal information or private data. As a result, 2.5% of users are involved in malware/spyware activity and keep accessing malware/spyware hosts periodically without users' awareness. Figure 10 shows the time of registrations and malware/spyware accesses for the user with largest number of registrations. We can see that registrations and malware/spyware accesses both come in burst that last as long as 11 hours and then suspend for about 10 hours. By zooming into the burst part for 500 seconds, we can see clearly both registrations and malware/spyware accesses happen periodically with a time interval around 18 seconds. The strong correlation between these two suggests that malware/spyware accesses are somehow responsible for the frequent registrations and causing many network failures.

VI. CONCLUSIONS AND RECOMMENDATIONS

This paper characterizes the usage profile, mobility and access issues of data services in a 3G data network based on traces collected from one of the largest cellular service providers in North America. It differentiates from previous works on the scale of the trace and the multi-dimension analysis. Based on our study, HTTP service counts for most of the data services compared to MMS or SIP, all of which exhibit similar diurnal patterns. Different device types have distinct application usage profiles and mobility patterns. Network operators are advised to design appropriate mechanisms in resource provision mobility management based on service types and device types.

A number of users frequently register to the network without using any data service, which may be due to malware/spyware. These users are usually not aware of what is happening to their devices. The network operator is recommended to restrict their registrations. This rule not only reduces resource consumption from the network point of view, but also saves device battery form the user point of view. A small set of users experienced extremely high network failure rate due to their frequent handoffs. Network operators should optimize their mobility management mechanism to avoid unnecessary handoffs.

REFERENCES

[1] Multimedia messaging service: Service aspects; stage 1. 3GPP 3G TS 22.140 1999.
[2] Hypertext transfer protocol — HTTP/1.1. Internet RFC 2616, 1999.
[3] SIP: Session initiation protocol. RFC 2543, 1999.
[4] X. Liu, A. Sridharan, S. Machiraju, M. Seshadri, and H. Zang. Experiences in a 3G network: interplay between the wireless channel and applications. In *ACM MOBICOM*, 2008.
[5] X. Meng, P. Zerfos, V. Samanta, S.H.Y. Wong, and S. Lu. Analysis of the Reliability of a Nationwide Short Message Service. *INFOCOM 2007*.
[6] C. Rigney et al. RADIUS accounting, 2000.
[7] M. Seshadri, S. Machiraju, A. Sridharan, J. Bolot, C. Faloutsos, and J. Leskove. Mobile call graphs: beyond power-law and lognormal distributions. In *ACM SIGKDD*, 2008.
[8] D. Willkomm, S. Machiraju, J. Bolot, and A. Wolisz. Primary users in cellular networks: A large-scale measurement study. *IEEE DySPAN*, 2008.
[9] Z. Zhu and G. Cao. Applaus: A privacy-preserving location proof updating system for location-based services. *IEEE INFOCOM 2011*.
[10] Z. Zhu, G. Cao, S. Zhu, S. Ranjan, and A. Nucci. A social network based patching scheme for worm containment in cellular networks. *IEEE INFOCOM 2009*.