February 22, 2017

Smart data saver based on predicted information needs

Matthew Sharifi

Jakob Foerster

Smart data saver based on predicted information needs

ABSTRACT

This disclosure describes techniques to manage consumption of network bandwidth, e.g., by a mobile device. Dynamic classification of mobile device applications is performed based on permissions and levels of background data usable by an application. Background data requests from an application are selectively permitted or denied access to the network, based on device state such as content displayed on screen, text input state, application usage information, etc. Such selective permission or denial of network access results in savings in network bandwidth consumption while allowing the mobile device to access the network for important tasks, e.g., to receive updates.

KEYWORDS

- Background data
- Data saver
- Network access request
- Bandwidth optimization

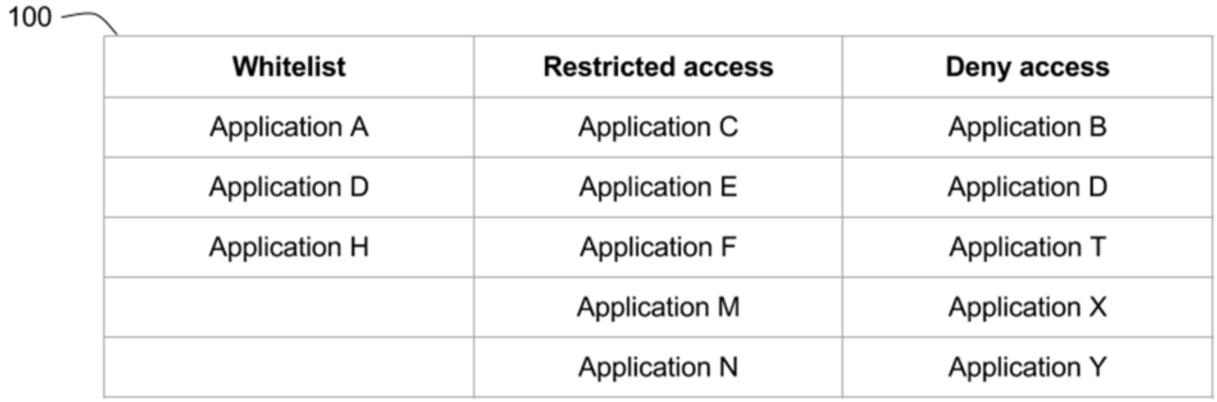
BACKGROUND

Cellular data plans offer a limited amount of data (e.g., 1 GB/$40 per month, 4-6 GB/$60 per month, etc.). Smartphones are often configured with many software applications ("apps") that access the cellular network and consume data. Applications can access the cellular network when they are in the foreground (e.g., in active use) or in the background (e.g., not in active use). For example, an email application actively sends and receives data when in use, and also accesses the network for periodic updates e.g., to refresh the inbox every 15 minutes. Similarly, a chat application delivers responses quickly when actively used, but can be a lower priority application when not in use.

Some mobile operating systems allow users to switch on a data-saving mode to optimize network usage. For example, when the user enables such a data-saving mode, the operating system blocks all background data usage and signals apps to use less data in the foreground whenever possible. However, even as the device is in a data-saving mode, it is often useful to enable some flow of background data for various apps, e.g., such that important updates or messages are received. On the other hand, blanket whitelisting of certain apps, as implemented in some current mobile devices, permits excessive data use by whitelisted apps while the device is in data-saving mode, even when data access by such whitelisted apps is not of immediate importance.

It is useful for a mobile device to be configured such that intelligent decisions are made regarding when to allow an app to use the cellular data network while the app is in the background. Such configuration permits apps to receive important information without delay and ensures that the app deliver quality user experience, yet enables a reduction in overall data usage over a metered network, e.g., the cellular network.

DESCRIPTION



Whitelist	Restricted access	Deny access
Application A	Application C	Application B
Application D	Application E	Application D
Application H	Application F	Application T
	Application M	Application X
	Application N	Application Y

Fig. 1: Classification table for applications that request network access

Fig. 1 shows an example of a table (100) that classifies applications according to their network access privileges. When a user consents (e.g., enables a smart data saver feature and provides permission to access user data), the table is determined based user preferences and/or patterns of application usage.

Applications in the column “whitelist” can access the network at all times. One example of a whitelisted app is business or work email.

Applications in the column “restricted access” are configured with one or more criteria that need to be met in order to gain access. An example of such criteria is “permit immediate access if the requesting application is in the foreground and active.” When such an application is not in the foreground or not active, network access and updates are suppressed until the application is in the foreground and active. Examples of applications on the restricted access list can include messaging software, stock market apps, weather, etc. Another example of such criteria is “permit immediate access if the requesting application is a messaging application and an incoming message is classified as important.”

Applications in the column “deny access” are configured to not have network access, or are permitted to access the network only when the network access is free (e.g., not metered, or unlimited), e.g., over a home wireless network. An example of such an application is a game. While the examples here refer to business email, messaging software, games, etc. being configured in specific columns, different devices can have alternate configurations based on respective user preferences or patterns of application usage. The smart data saver accesses the classification table when an app makes a network access request and determines whether the request is to be permitted or denied. Per techniques of this disclosure, an app is dynamically moved across the columns of the classification table, e.g., based on recent and historic usage patterns, data activity in relation to user interest in the app, current device context, app context, etc. when a user permits the smart data saver to access such data for their device.

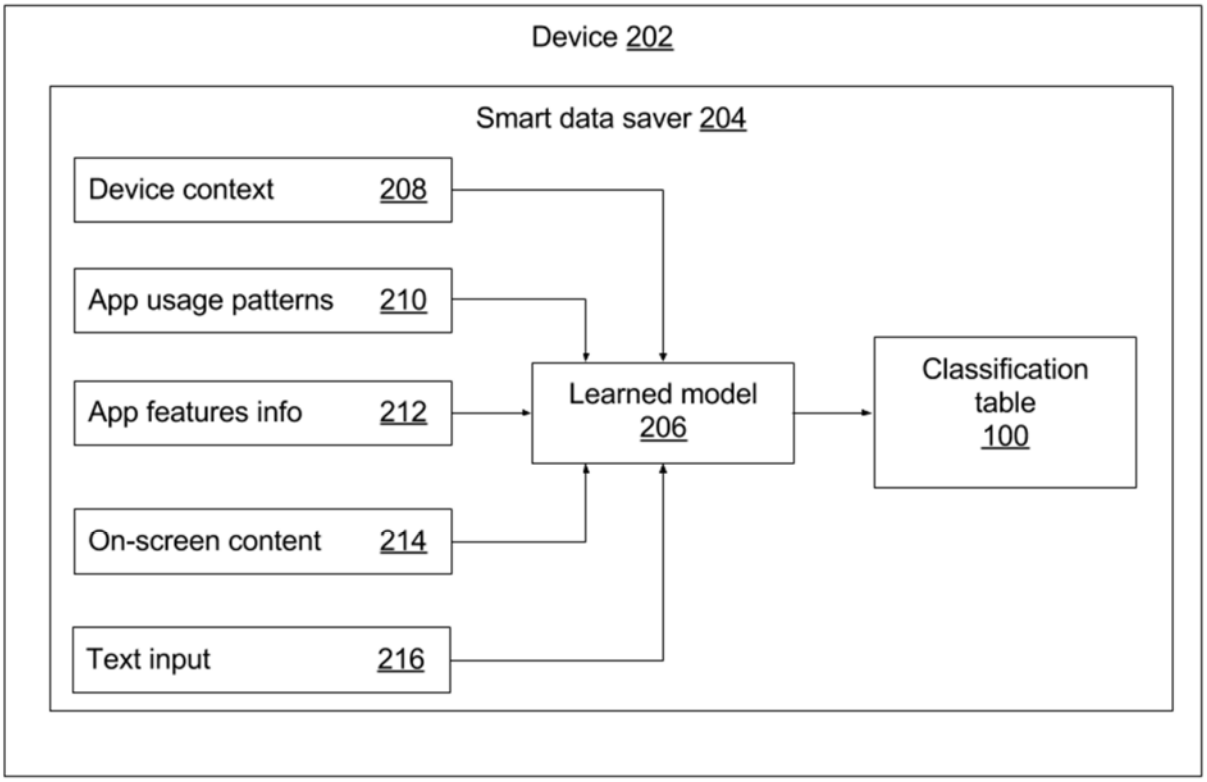


Fig. 2: Creation and updating of the classification table using a learned model

Fig. 2 illustrates the creation and updating of the classification table (e.g., as shown in Fig. 1) using a learned model. A device (202), e.g., a user smartphone, etc. includes a smart data saver module (204). The smart data saver is implemented and activated upon specific user consent. For example, the smart data saver is implemented with settings that do not require access to user data when the user does not provide consent for access to such data. Users are permitted to configure the smart data saver, e.g., enable or disable, permit or deny access to certain user data, etc.

The smart data saver includes learned model (206), that generates classification table 100 based on data such as the current device context (208), usage patterns of various applications (210), information about features of various applications (212), current on-screen content (214), and recent text input by the user (216). The user can enable the smart data saver to access such data selectively, e.g., permit current device context to be accessed, deny on-screen content, etc. If additional information about a network request made by the app is available, e.g., based on application programming interfaces (APIs) that are used by the app, these are also provided as an input to the learned model if permitted by the user. The learned model can be a neural network, a support vector machine, or any other machine learned model. The neural network may be trained, e.g., for logistic regression. Application usage patterns include, e.g., speed of user response to a notification from the app, usage frequency, times-of-day during periods of activity over the last *n,* e.g., 30 days. The learned model updates the classification table, such that applications are dynamically configured as “whitelist,” “restricted access,” or “deny access” per columns of the classification table.

When an application requests network access, the smart data saver looks up the classification table to determine whether to grant, deny, or provide restricted network access. The decision to grant or deny network access to an app is made at a more fine-grained level when compared with coarse decision making, e.g., based solely on app identity. For example, for a messenger application that is configured in the "restricted access" column of the classification table, messages that are classified as important, or originate from a priority contact, are allowed, while other messages are denied. The decision made by the smart data saver to allow, deny, or provide restricted network access is based not just on the app making the network access request but also on the context of the request, while incorporating any interesting information from the app, based on user permission for use of such context data. The context of the network access request, or additional information from the app, is provided to the smart data saver only upon explicit permission by the user.

Training data for the learned model is obtained during times when all background network requests are permitted, e.g., when the device accesses a network, e.g., Wi-Fi, that has zero or minimal data charges. While the device is connected to such a network, if the smart data saver determines that the user interacts with an app shortly after it makes a background network access request, then that network access request is considered as useful, and therefore a positive training example for the model. Similarly, if no interaction is forthcoming from a user, or a negative interaction, e.g., marking a certain message as spam, is observed by the smart data saver, then the corresponding network access request by the app is considered as a negative training example for the model. Such observations of user behavior, and inferences therefrom, occur only when explicitly permitted by the user.

With further user permission, learned models that have been trained based on data from distinct users are anonymized and aggregated, e.g., to determine average user behavior. Such a model that captures large-scale user behavior is used to initialize the learned model for a new user of the smart data saver. The model is adapted via further training to reflect a user's actual behavior, the apps installed in the device, etc. if permitted by the user.

The smart data saver, per techniques of this disclosure, can determine whitelist applications dynamically and providing suggestions regarding such applications to the user. If useful background data usage is detected, a data saver whitelist is suggested to the user, e.g., by generating a notification for the user. The whitelist can have a time duration associated with it. This time duration can also be edited by the user. These whitelist suggestions are made for apps which are not permanently set in the data saver whitelist by the user. The whitelist suggestion feature can also suggest to the user that they remove an app from the whitelist. Such a suggestion is made if the app is using a lot of background data with little user interest in the form of usage or interaction with the app user interface or notifications. Suggesting entries to whitelist for addition or deletion provides transparency and enables selective configuration of the smart data saver.

Examples of use

The examples below illustrate selective network access by the smart data saver when the user has provided consent for the smart data saver to use user data. When such consent is not provided, the smart data saver is disabled, or is configured to operate based only such user data for which the user has provided consent.

Example 1

A user ("User 1") is having a chat conversation with another user ("User 2") on a messaging app that has restricted data access. The chat proceeds in the foreground as follows.

User 1: "I will be done with my presentation is a little bit. What about you?"

User 2: "I am wrapping up too."

At this point, both users put this app in the background. Soon thereafter, User 1 sends the following message:

User 1: "Let's meet for lunch in 30 mins!"

Without the smart data saver, the messaging app being in the background can lead to this message not being delivered to a device of User 2, even though User 2 was only recently in conversation, and is likely interested on updates from the chat conversation with User 1. Using the smart data saver, as described herein, an inference is made that User 2 is likely to want network access to be enabled for the messaging app even when the app is in the background, based on observations, such as:

1. User 2 was recently in frequent interaction with the messaging app, and
2. On-screen content and text received from User 1("meet", "lunch", "30 mins") that suggests that User-2 is interested in the conversation.

Example 2

On a particular day, a user checks a flight-status app periodically to monitor flights and receive latest schedule changes. The observation that the user has, within the span of a few hours, checked the app a few times and interacted with an otherwise rarely used app enables an inference by the smart data saver that in the present context, the user is likely interested in updates from this app. The smart data saver selectively enables access to the network even when the flight-status app is in the background based on such an inference, even if the flight-status app is not normally in the whitelist. Further, the smart data saver disables such access, e.g., when the flight-status app is no longer of interest to the user. For example, the flight-status app is configured on the whitelist for a certain time duration, e.g., twenty-four hours

Example 3

A messenger application is in the restricted access list, such that only messages from individuals on a priority contact list, or messages that are marked as important, are allowed. The user receives the message “urgent, reply immediately” from an individual on a priority contact list. Based on the provenance and text of the message, the smart data saver allows the message even though the messenger application is in the background.

In situations in which certain implementations discussed herein may collect or use personal information about users (e.g., user data, information about a user’s social network, user's location and time at the location, user's biometric information, user's activities and demographic information), users are provided with one or more opportunities to control whether information is collected, whether the personal information is stored, whether the personal information is used, and how the information is collected about the user, stored and used. That is, the systems and methods discussed herein collect, store and/or use user personal information specifically upon receiving explicit authorization from the relevant users to do so. For example, a user is provided with control over whether programs or features collect user information about that particular user or other users relevant to the program or feature. Each user for which personal information is to be collected is presented with one or more options to allow control over the information collection relevant to that user, to provide permission or authorization as to whether the information is collected and as to which portions of the information are to be collected. For example, users can be provided with one or more such control options over a communication network. In addition, certain data may be treated in one or more ways before it is stored or used so that personally identifiable information is removed. As one example, a user’s identity may be treated so that no personally identifiable information can be determined.

As another example, a user’s geographic location may be generalized to a larger region so that the user's particular location cannot be determined.

CONCLUSION

Techniques are disclosed that can intelligently decide to receive, transmit or otherwise notify users of important information originating from apps that are not ordinarily in the user’s whitelist for background data activity. In this manner, important updates are delivered to the user while continuing to limit data usage on the device. The smart data saver can generate dynamic data saver whitelists that are active for certain durations of time and also make whitelist suggestions to the user.