November 22, 2017

Detection of lost status of mobile devices

Sandro Feuz

Victor Carbune

Detection of lost status of mobile devices

ABSTRACT

Users often forget or misplace mobile devices, e.g., smartphones. To find or recover such devices, users can utilize find my device features, if available on the device, cause the device to emit a sound, etc. However, no mechanisms exist for a device to automatically detect that it is lost or about to be lost. Per techniques described herein, an on-device predictor determines that a device is lost (separated from the owner) or is about to be lost. The prediction is based on various factors, including device sensor data, recent use of apps, recent user context, etc. for which the user has provided access. If it is determined that the device is lost, various mitigating actions as permitted by the user are performed. For example, such actions include sending notifications to other devices of the same user, initiating communicating with the user or a trusted contact, locking the device, encrypting user data, disabling notifications, etc.

KEYWORDS

- Lost phone
- Phone recovery
- Find my device
- Unauthorized access
- Device security

BACKGROUND

Users sometimes forget or lose mobile devices, e.g., smartphones, tablets, etc. In such situations, users employ various methods to try to locate the misplaced device. For example, users attempt to call a lost phone from another device. Some devices have built-in “find my device” features that users can employ to locate the misplaced device, or to disable access to the

device. There are also mobile apps that enable device recovery. However, these approaches require users to initiate action. These approaches do not work, e.g., if the device is on mute, lacks internet connectivity, has location sensors turned off, etc.

DESCRIPTION

Techniques described use on-device machine learning models to determine whether a device is likely to be lost, or has been lost. Based on the determination, the device is configured to perform actions to notify the device owner of the lost device location. The models determine various mechanisms to reach the owner. For example, the actions to notify the device owner include notifying a nearby different device, e.g., another device of the user, a trusted friend's nearby device, etc. of the location and status of the lost device; automatically ringing the lost device; and displaying notifications on the device lock screen, e.g., that include contact information of the device owner, a nearby lost and found office, etc. to facilitate identification of the owner and return of the device to the owner.

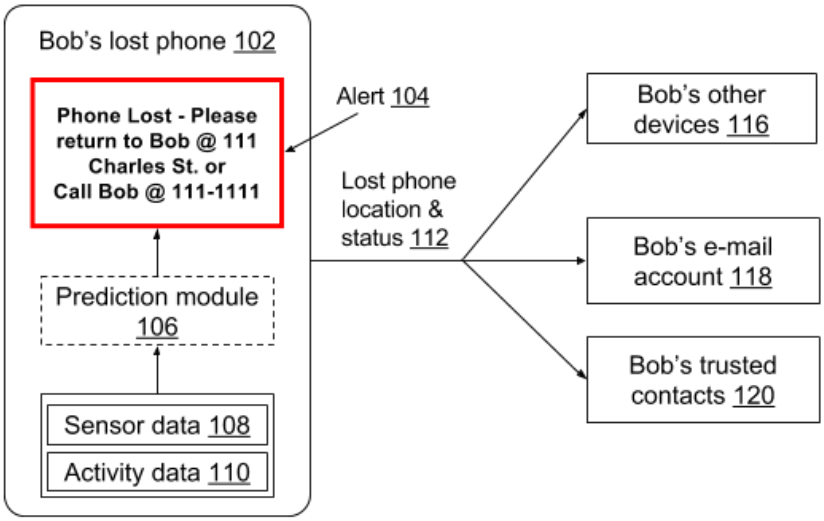

Fig. 1

Notification and alerts are provided based on evaluation of contextual factors, upon permission for the user to access and use such factors. The user can select specific factors that

can be used for lost device prediction and can choose to deny permission or disable lost device prediction. Fig. 1 illustrates a scenario where a phone belonging to a user Bob (102) observes sensor data (108) and user activity data (110), as permitted by the user, to determine via a prediction module (106) whether it is lost.

In this scenario, the prediction module utilizes an on-device machine learning model. Alternatively, or in addition, rule-based heuristics can also be used for such prediction. The model is run periodically to determine whether a device has been lost, or is likely to be lost. When the prediction module determines a lost phone condition, it updates or instructs the phone operating system to update the phone settings to lock the phone and display an alert (104). For example, the alert can include an address to which the phone can be returned and/or an alternate contact number for the user. Further, the lost phone is also configured to transmit its location and status (112) to the user's other devices (116), e.g., as notifications, to the user's email account (118), and to the user's trusted contacts (120).

The device can also be configured to take actions to automatically secure user data upon determination that the device is likely lost. Such actions ensure that private data is not subject to unauthorized access. For example, if the lost device is in an unfamiliar location or a public location (e.g., on a train, in a taxi, etc.), such actions can include automatically locking the device and encrypting user data. In this situation, the user data is made accessible only with second-factor authentication. Further, personal notifications are removed and the device lock-screen is configured to omit private and confidential content.

Alternatively, based on predetermined context information, it may be inferred that the device was intentionally left at a location. The model takes as inputs contextual data permitted by the user, e.g., sensor values from various on-device sensors, app status, recent user actions, e.g.,

screen state and touch events, and information about nearby devices that belong to the same user. Such data is accessed only with prior user permission and express consent, and to conserve the battery, is obtained periodically.

The model can be implemented as multiple blocks of neural networks, e.g., one for each input signal. The model provides a confidence score as the output. For example, a high confidence score is an indication that the device is lost. A medium score indicates that the device is lost, but in a familiar or secure location such as the user's home, office, personal vehicle, etc. Other traditional, non-neural network models can also be used for prediction.

A high confidence score triggers an alert the device owner of the lost device status and its current location. The techniques determine one or more paths to alert the owner of the lost device location. The paths can be identified based on available data such as other devices of the owner located nearby, trusted contacts of the owner or devices of trusted contacts, and nature of the device location, e.g., familiar/secure location and unfamiliar/public location.

For example, a lost device automatically notifies other nearby devices owned by the user of the lost device status and location. Also, this information is communicated to the user's preferred messaging or email account. The user can reply to a message with a known emergency code, and the device can respond with its current location. Such actions can be extended, with user permission and express consent, to respective devices and/or email/messaging accounts of the user's trusted contacts. For example, such communication can be limited to trusted contacts travelling or residing with the user (identified based on the context). For example, a phone forgotten on a train can send a message to the phone or to the email account of the owner's trusted friend traveling on the same train stating that the owner has forgotten the phone and include in that message the location of the lost phone. When the model determines, based on the

context, that the device is likely to be lost, the device is caused to ring. For example, such activation can occur when the owner is about to exit a train, taxi, etc.

The present techniques enable a device to determine a lost condition and automatically activate various mechanisms to contact the user and/or take other actions. The techniques can be implemented as part of device operating systems and/or applications. The techniques are suitable for portable devices, including mobile phones, tablets, PCs, and other internet-connected devices.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. 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. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

An on-device predictor determines that a device is lost (separated from the owner) or is about to be lost. The prediction is based on various factors, including device sensor data, recent use of apps, recent user context, etc. for which the user has provided access. An on device trained machine learning model is deployed to generate a confidence score based on the factors. Based on the confidence score, if it is determined that the device is lost, various mitigating

actions as permitted by the user are performed. For example, such actions include sending notifications to other devices of the same user, initiating communicating with the user or a trusted contact, locking the device, encrypting user data, disabling notifications, etc.