(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2018 (15.03.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/048731 A1

(51) International Patent Classification:
*H04W 64/00* (2009.01)

(21) International Application Number:
PCT/US2017/049799

(22) International Filing Date:
01 September 2017 (01.09.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/260,314 08 September 2016 (08.09.2016) US

(71) Applicant: **MICROSOFT TECHNOLOGY LICENSING, LLC** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

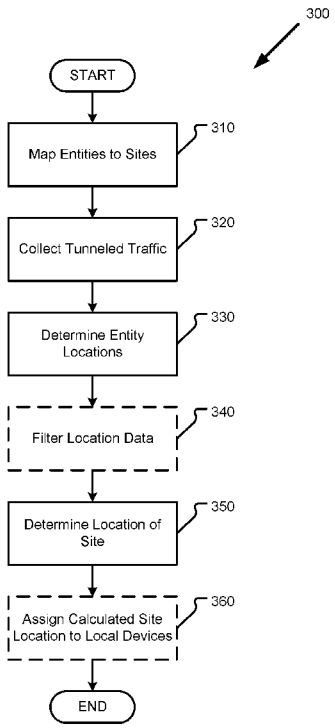
(72) Inventors: **JURGENSON, Tom**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **BE'ERY, Tal Arieh**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **PLOTNIK, Idan**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **DUBINSKY, Michael**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **KRIGSMAN, Sivan**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US). **DAVID, Gil**; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(74) Agent: **MINHAS, Sandip S.** et al.; MICROSOFT TECHNOLOGY LICENSING, LLC, One Microsoft Way, Redmond, Washington 98052-6399 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,

(54) Title: PHYSICAL LOCATION DETERMINATION OF INTERNAL NETWORK COMPONENTS




(57) Abstract: The present disclosure provides for improved computational efficiency and security in a network by determining the physical location of network connected components, without requiring the components to self-locate. The locations of devices remotely connected to a site within the network are geolocated so that the physical location of that site may be inferred from a centralized point to the remote devices' locations. This calculate site location may be compared against a known site location to improve a generalized algorithm for determining the calculated location of a site with an unknown location, and may be applied to devices that are locally connected to the network, which may be otherwise incapable of being geolocated.

WO 2018/048731 A1

[Continued on next page]

TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Declarations under Rule 4.17:**

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

**Published:**

— *with international search report (Art. 21(3))*

# PHYSICAL LOCATION DETERMINATION OF INTERNAL NETWORK COMPONENTS

## BACKGROUND

**[0001]** Knowing the physical location of a device connected to an internal network can allow the network administrators to improve the security of the network and to improve the efficiency of the network and the devices connected to that network. To obtain this information, however, network administrators often rely on the device self-reporting its location (e.g., via global positioning system (GPS) coordinates) or hand-reporting of a device's location. Self-reporting requires the device to send its coordinate data to the network, consuming additional bandwidth, and can be spoofed by malicious parties; providing the network administrators with incorrect coordinates. Hand-reporting of a device's location requires the manual entry of a location each time a device is moved, which is time consuming, prone to inaccuracies, and inoperable in the event of theft or poor checkout procedures.

## SUMMARY

**[0002]** This summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description section. This summary is not intended to identify all key or essential features of the claimed subject matter, nor is it intended as an aid in determining the scope of the claimed subject matter.

**[0003]** Systems and methods for determining the physical location of a networked entity without relying on a device to provide real world location data to the network are described in the present disclosure. Example use cases of these systems and methods are discussed in relation to efficient datacenter positioning, although one of ordinary skill in the art will appreciate other use cases. Examples are implemented as a computer process, a computing system, or as an article of manufacture such as a device, computer program product, or computer readable medium. According to an aspect, the computer program product is a computer storage medium readable by a computer system and encoding a computer program comprising instructions for executing a computer process.

**[0004]** As will be understood, a network can be divided into various sites, which correspond to physical locations in the real world where the servers reside, so that remote users can connect to the site that is closest to them to access the services and data stored in the network. For example, a cloud-based service may have sites located in New York and Tokyo, where residents of New York will connect to the New York site and residents of

Tokyo will connect to the Tokyo site to receive the lowest latency connection. Sites may be connected to by user accounts from devices that are remote from the site or local to the site.

**[0005]** Each site is enabled to learn the location of the remote devices connected to the network by monitoring and logging the VPN (or other network tunnel) traffic used to connect the device to the network. As users connect to a given site in the network, the site will use the Internet Protocol (IP) or other address associated with the devices to perform geolocation for the connected devices. Each site aggregates the geolocation information for selected accounts connected to that site over a period of time to estimate a calculated location for its own physical location. User accounts that access the site via local devices (i.e., not via a VPN or network tunnel) and use an internal IP address can be assigned a location equal to the site's location (calculated or physical), but may be excluded from the aggregation of geolocation information.

**[0006]** By determining the calculated location for a site, the network administrators may determine new physical locations to set up sites that will be closer to their users' remote locations to provide remote users with lower latency connections. Network administrators may determine multiple calculated locations for a site based on dividing the user accounts housed on a given site into clusters to provide the administrators with potential locations to set up additional sites when expanding the network or splitting a given site. Network administrators may also combined the location information for the user accounts housed on multiple sites to determine a central location for the user base when combining sites or otherwise shrinking the network's physical footprint.

**[0007]** By employing the present disclosure, the functionality of the devices may be improved by reducing the amount of data that need to be transmitted to the network to implement location based administration, and thereby gain the benefits in speed and security associated with location based administration of the network among other benefits. The efficiency, security, and reliability of the network itself may also be improved by improving the reliability of the location data received by the network and reducing the amount of data that the network receives to determine the location of a given device.

**[0008]** The details of one or more aspects are set forth in the accompanying drawings and description below. Other features and advantages will be apparent from a reading of the following detailed description and a review of the associated drawings. It is to be understood that the following detailed description is explanatory only and is not restrictive of the claims.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0009]** The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate various aspects. In the drawings:

**FIGURE 1** illustrates an example environment in which the present disclosure may be practiced;

**FIGURES 2A** and **2B** illustrate example maps against which the locations of remote logins and sites are plotted;

**FIGURE 3** is a flow chart showing general stages involved in an example method for determining the physical location of network components;

**FIGURE 4** is a block diagram illustrating example physical components of a computing device; and

**FIGURES 5A** and **5B** are block diagrams of a mobile computing device.

## DETAILED DESCRIPTION

**[0010]** The following detailed description refers to the accompanying drawings. Wherever possible, the same reference numbers are used in the drawings and the following description refers to the same or similar elements. While examples may be described, modifications, adaptations, and other implementations are possible. For example, substitutions, additions, or modifications may be made to the elements illustrated in the drawings, and the methods described herein may be modified by substituting, reordering, or adding stages to the disclosed methods. Accordingly, the following detailed description is not limiting, but instead, the proper scope is defined by the appended claims. Examples may take the form of a hardware implementation, or an entirely software implementation, or an implementation combining software and hardware aspects. The following detailed description is, therefore, not to be taken in a limiting sense.

**[0011]** By using the network address information of devices that remotely log into a system (e.g., Internet Protocol (IP) addresses), the physical locations of those devices may be determined through geolocation without requiring those devices to self-locate. The aggregated geolocations for the devices connecting to a node of the system are then used to infer a location of that node, which may then be assigned to devices that are locally connected to that node, which may otherwise be un-locatable via geolocation.

**[0012]** **FIGURE 1** illustrates an example environment **100** in which the present disclosure may be practiced. As illustrated, an enterprise network **110** is divided into multiple sites **120**. A given site **120** may be accessed remotely by a remote device **130**, which is located externally to the enterprise network **110** or remotely from the sites **120**, or

may be accessed locally by a local device **140**, which is located internally to the enterprise network **110** or locally to the sites **120**. The enterprise network **110** is in communication with a geolocation service **150** to provide locational data for the remote devices **130**. Although two sites **120**, one remote device **130**, and one local device **140** are illustrated, the number of sites **120**, remote devices **130**, and local devices **140** may be greater than or less than what is illustrated in the example environment **100**.

**[0013]** The enterprise network **110** provides a single operating environment over which computing devices may interact despite being spread across multiple sites **120** and domains (e.g., for a company, a governmental agency, an educational institution spread over a large geographical area). Each site **120** of the enterprise network **110** includes: a gateway **122**, operable to accept communications from devices connecting to the site **120**; a domain controller **124**, which is in communication with the gateway **122** and operable to authenticate entities seeking to access the enterprise network **110**; and a monitor **126**, in communication with the domain controller **124**, and operable to aggregate connection information from the remote devices **130** to manage entity location data. Gateways **122** and domain controllers **124** will be understood by one of skill in the art to include hardware devices and software running on those devices to provide the functionalities thereof. In various aspects, the monitor **126** may be run on dedicated hardware or may be provided via software on a computing device used for several purposes, such as, for example, on the same hardware as the domain controller **124**. In additional aspects, the enterprise network **110** may make use of fewer monitors **126** than sites **120**; some or all of the sites **120** may share a monitor **126**.

**[0014]** The remote device **130** and local device **140** are illustrative of a multitude of computing systems including, without limitation, desktop computer systems, wired and wireless computing systems, mobile computing systems (e.g., mobile telephones, netbooks, tablet or slate type computers, notebook computers, and laptop computers), hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, minicomputers, printers, and mainframe computers. The hardware of these computing systems is discussed in greater detail in regard to **FIGURES 4**, **5A**, and **5B**.

**[0015]** Remote devices **130** and local device **140** are operated by users, who may be humans or automated systems (e.g., "bots") that request connections to one or more sites **120** of the enterprise network **110**. For example, an instance of the SIRI®, GOOGLE NOW™ or CORTANA® electronic assistant (available from Apple, Inc. of Cupertino, CA; Alphabet, Inc. of Mountain View, CA; and Microsoft, Corp. of Redmond, WA,

respectively) may request a connection in response to or in anticipation of queries from a human user.

**[0016]** The remote device **130** and local devices **140** access the enterprise network **110** by being authenticated by a domain controller **124** of a site **120**. Remote devices **130** may connect to a given site **120** via a Virtual Private Network (VPN) connection or other tunnel to initiate a session, whereas local devices **140** connect to the site **120** at which they are located. Whether a given device is a remote device **130** or a local device **140** depends on how it connects to the enterprise network **110**, and a given device may be both a remote device **130** and a local device **140**. For example, a user may use a local device **140** while in the office to connect locally to the enterprise network **110** and take that device home and log into the enterprise network **110**, making the device a remote device **130** for the remote session.

**[0017]** In various aspects, the user may specify a particular site **120** to log into, or the site **120** that is connected to may be automatically selected by a login agent running on the user's device based on a determination of the site **120** that is physically closest to the user, the site **120** that responds fastest to the user's communications (e.g., to avoid network congestion, to connect to a site **120** that has a better ping despite being located further away), etc.

**[0018]** Entities (devices or user accounts) that frequently connect to a given site **120** may be noted and mapped by either the domain controller **124** or the monitor **126** as using the given site **120** as their "home" site **120**, whereas entities that infrequently connect to the given site **120** may be noted as connecting to a "guest" site **120**. In one aspect, entities are mapped to the one site **120** on which they are most active (locally, remotely, or locally and remotely), while in other aspects a given entity may have "home" status on more than one site **120** or on no sites **120** based on a minimum number of connections to a given site **120**. For example, a user based out of Office A and whose account is associated with a first site **120** as a "home," may be transferred to Office B and begin using a second site **120** associated with Office B more frequently. The example user's account may be remapped to the second site **120** as a "home" over the course of several days/weeks/months as the user connects to Office B more frequently than Office A's site **120**. Contrarily, if the example user used (and left) a first device at Office A and the user were assigned a new device at Office B, the fist device may remain associated with the first site **120** as its "home." In another example, a salesperson who frequently travels and logs on remotely to a first site **120** and a second site **120** may have each site **120** consider itself the "home" of the user's account due to the

frequency at which the salesperson connects to each site **120** and the salesperson exceeding a minimum number of connections to each site **120** during a time period. When the monitor **126** determines the calculated location of the site **120**, it may exclude the location information from "guest" entities, provide greater emphasis on the location information from "home" entities, or treat the location information equivalently, regardless of home/guest status. The monitor **126** may also periodically reevaluate whether a given entity has home or guest status on a given site **120**.

**[0019]** The monitor **126** will observe the network address information from remote devices **130** connecting to the associated site **120** and will decide whether to store those addresses for use when inferring a calculated location of the site **120**. Each time a user account successfully logs into the site **120** and establishes a session on the enterprise network **110**, the monitor **126** may store the address information associated with the login request, or the monitor **126** may filter or restrict the number of logins from a given user account for a given time period for which to store the address information. For example, a user of a remote device **130** with an intermittent Wi-Fi signal may repeatedly gain and lose connection to the site **120**, and may be forced to constantly re-authenticate with the domain controller **124**, which the monitor **126** may choose to treat as multiple successful login attempts or as a single login attempt if the attempts fall within a given time range of one another (e.g., an hour, a day, a week). Alternatively, the monitor **126** may collect all of the address information and later filter it when determining the calculated location of a given site **120**.

**[0020]** Local devices **140** may also have their connection attempts to the domain controller **124** and activity session logged by the monitor **126** for security purposes. As will be appreciated, local devices **140** are associated with IP addresses internal to the enterprise network **110**, which may be masked for use within the enterprise network **110**, and therefore may produce spurious results if provided to the geolocation service **150**. The monitor **126** will note the entities associated with the login and session (e.g., the user account and devices), and will assign the location (calculated or physical) of the site **120** to the entity at the time of login. For example, a user account for a user entity or Media Access Control (MAC) address, serial number, etc., for a device entity may be tracked to determine whether a second login using the same entity identifiers occurring at a second time violates one or more security rules for the user account.

**[0021]** In various aspects, the monitor **126** may store and use, store and filter, or exclude from storage connection attempts that were rejected by the domain controller **124**

(e.g., an incorrect username or password were provided). Similarly, the monitor **126** may store and filter (or block from storage) connection attempts received from a list of addresses that are associated with blocked parties, unreliable geolocation, or whose duration or number of connections meet an unreliability threshold (e.g., multiple short connections may indicate an unstable connection, and may be filtered out or ignored). For example, a user making use of a VPN connection from a smartphone may have a signal routed through a cell-provider's network to reach the site **120**, and the address of the cell-provider's network is provided to the monitor **126** instead of the remote device's **120** address internal to the cell-provider's network, making the address unreliable for geolocation, which may be flagged for the monitor **126** or noted over time by the monitor **126** as being unreliable based on the Internet Service Provider (ISP) frequently providing IP addresses unreliable for geolocation. Additionally, the monitor **126** may filter out data from connection attempts that are beyond a preset distance from a site **120** or that specify a specific site **120**, as their inclusion may affect the calculation of the location of the site **120**.

**[0022]** When the monitor **126** uses the address to determine the calculated location of the site **120**, the stored addresses that are to be used are transmitted to the geolocation service **150**, which returns a geographic location associated with the address. Examples of geolocation services **150** include, but are not limited to MaxMind of Waltham, MA and NeuStar of Sterling, VA, which provide geographic coordinates correlated to IP (or MAC) addresses back to the monitor **126**. The geographic coordinates may be provided in terms of latitude/longitude coordinates, cities, regions, and countries. Geographic coordinates may be requested in real-time (as entities connect) or held in batches for periodic (e.g., daily, weekly, monthly) or on-demand processing by the geolocation services **150**.

**[0023]** **FIGURE 2A** illustrates a first example map **201** against which the positions of located remote logins **210** are plotted. Also plotted are the calculated site location **220** and the physical site location **230**. Each located remote login **210** is associated with the geolocation provided by the geolocation service **150** and the time at which it was made to the enterprise network **110**. Using these data, the monitor **126** is operable to infer a centralized location to the remote connections to use as the calculated site location **220**. As more located remote logins **210** are used, the inference of the calculated site location **220** can be made more accurately, and the monitor **126** may apply additional filtering to which geographic data and login data are used in the calculations.

**[0024]** As will be appreciated, various algorithms and methods may be used to determine the centralized location for use as the calculated site location **220**. In one aspect,

arithmetic mean values are calculated for the latitude and longitude from the latitudes and longitudes of the geolocation values of the located remote logins **210**. In another aspect, when the geolocation values are not provided as latitude/longitude coordinates, but as the name of a city, region, or country, the monitor may use the mode of the geolocation values from the located remote logins **210** or may convert the non-coordinate geolocation values into a latitude/longitude pair of coordinate for a central location of the city, region, or country.

**[0025]** In various aspects, different weights may be applied to the geolocation values based on the frequency of use of a given identifier, a physical or temporal proximity of one login attempt to another login attempt, a physical proximity to the centralized location (which may be calculated recursively), a given time range at which the located remote login **210** was made (e.g., during business hours, on a weekday), and whether the identifiers are unique during the period being calculated. The monitor **126** may also account for geographic and geopolitical data when calculating the centralized location, such as, for example, to avoid placing the centralized location in a body of water, across a national/provincial border, on a road, in a use-restricted space (e.g., a park, a facility known to be used by another entity, an area zoned for residential use when a commercially zoned area is required), an area with high crime/taxes/rents, etc., or to specifically place the centralized location in a given nation/province/city/neighborhood.

**[0026]** In aspects where the coordinates of the physical site location **230** are known to the monitor **126**, the monitor **126** may apply machine learning techniques to vary the weights or hyperparameters of the learning algorithm to match the calculated site location **220** to the physical site location **230** and apply the adjusted weights and hyperparameters in subsequent calculations for sites **120** that do not have a known physical site location **230** or to identify hypothetical locations for sites **120** when expanding, contracting, or otherwise modifying the physical footprint of the enterprise network **110**.

**[0027]** The calculated site location **220** may be provided as a recommendation to network administrators for new locations for a given site **120**, used for network load balancing, or may be assigned as a location for local devices **140** (which may still be mobile devices that can be present at several sites) for security purposes.

**[0028]** **FIGURE 2B** illustrates a second example map **202** against which the positions of located remote logins **210** are plotted. As plotted, the entities are divided into subgroups **240** (illustrated as a dotted line surrounding multiple located remote logins **210** of the plurality) to produce a calculated site location **220** for each subgroup **240**.

Additionally, the subgroups **240** may be created based off of an individual entity's use patterns to determine the point about which the entity's remote logins are centered. Subgroups **240** may be set according to criteria specified by the network administrators (e.g., entities connecting at least X times per month, entities at least X km away from a given point, entities within X km of a given point, a specified entity or entities) or may be identified automatically by the monitor **126** according to a clustering or distribution algorithm (e.g., k-means, DBSCAN).

**[0029]** The monitor **126** is operative to use the calculated site locations **220** for subgroups **240** as the located remote login **210** to recursively find centralized locations, or may provide the calculated site locations **220** for the subgroups **240** as suggestions for new locations for a site **120**. In another example, the monitor **126** may use the located remote logins **210** associated with multiple sites **120** to determine a single centralized location, which may be provided as a recommendation to the network administrators as a site to condense sites **120** into, or a shared calculated location to use for local devices **140** that may connect to one or more sites located throughout a campus.

**[0030]** **FIGURE 3** is a flow chart showing general stages involved in an example method **300** for determining the physical location of network components. Method **300** operates passively on each site **120**; that is without requiring remote devices **130** to transmit their own location data, which may be unreliable, and without requiring administrators to keep track of the location of network components, thus improving the security of the enterprise network **110** and the computational efficiency of the components therein.

**[0031]** Method **300** begins at OPERATION **310**, where entities are mapped to sites **120**. A given entity may be mapped to the one site **120** that the entity is most active on, or an entity may be mapped to sites **120** to which the entity connected to a set number of times within a given time period. The site **120** to which the entity is mapped is considered the "home" site **120** for that entity and other sites **120**, which the entity may connect to are considered "guest" sites **120** for the entity. For example, if a user account is noted as connecting to a first site **120** twice within the last month and to a second site **120** once in the last month, the user account may have home status on the first site **120** and guest status on the second site **120**. Alternatively, if the network administrators set a threshold for home status of three connections within a month, the example user account may have guest status on both the first site **120** and the second site **120**. In yet another alternative, if the user account connected to both the first site **120** and the second site **120** an equal number of times within a given time period, the home status for the entity may be given for both sites **120**,

the site **120** that the entity connected to first or last may be considered the "home" site **120**, or the site **120** with the fewest entities with home status may be mapped for the entity.

**[0032]** Method **300** proceeds to OPERATION **320**, where tunneled traffic is collected at a site **120** of the enterprise network **110**. Tunneled traffic is received from remote devices **130** connecting to the site **120**, and may include only requests that have been authorized by the domain controller **124** of the site **120** and from entities that are mapped to the given site **120** or may include requests from entities that are guests to the site **120** and/or were rejected by the domain controller **124** (which may be later filtered out at OPTIONAL OPERATION **340**). Activities from the remote devices **130** are associated with timestamps in the site **120**, and the monitor **126** for the site may filter the tunneled traffic of determine which aspects of the tunneled traffic are to be recorded (e.g., only a login request and a latest activity) for analysis. The monitor **126** may collect tunneled traffic during a training period to assure that a sufficient amount of tunneled traffic (where "significant" may be defined by a network administrator) is collected to accurately infer the calculated site location **220**.

**[0033]** In different aspects, traffic of individual entities may be collected separately by the monitor **126** or in conjunction with other entities. For example, a device may have its tunneled traffic collected independently of the traffic associated with a user account logged into that device, or the traffic associated with the device/account pair may be collected in as a single set of traffic data.

**[0034]** At OPERATION **330** the entity locations are determined. In various aspects, entity locations may be determined when a login request is received, after a set duration of connection to the site **120**, on a schedule set on the site **120**, or whenever the address used by the remote device **130** changes during a connectivity session with the site **120** (e.g., via a wireless handoff), and combinations thereof. For example, an entity may have its location determined from an initial login time and every five minutes thereafter or an entity may have its location determined from an initial login time and at every five minute interval of the hour (e.g., at 8:55, 9:00, 9:05, 9:10, 9:15, etc.) thereafter. In another example, a remote device **130** may be used while an employee is commuting into work (e.g., via train, bus, carpool) and the address may be updated as the remote device **130** is handed off to new connectivity providers (e.g., Wi-Fi hotspots, cell towers), and the monitor **126** may be interested in the geolocation of each of the addresses used by the remote device **130** along the commute.

**[0035]** To determine the location of the entity remotely connected to the site **120**, the monitor **126** will query a geolocation service **150** to provide geographic coordinates

based on an IP address (or other identifier) sent in the login request or subsequent communication from the remote device **130**. In some aspects, the communications from the remote device **130** may be flagged as using a separate tunneling service or an ISP that has proven unreliable in providing addresses to devices that can be reliably geolocated, in which case the monitor **126** may not determine the location for the entity. In other aspects, connection attempts that are made by a given entity in rapid succession that are indicative of connectivity problems may be aggregated into a single connection attempt for determining the location of the entity.

**[0036]** OPTIONAL OPERATION **340** allows for the monitor **126** to filter the IP addresses or geographic information received at the previous operations to remove spurious results, to give greater or lesser weight to various data, to split the entities into subgroups, or combine location data from multiple sites. In various aspects, optional operation 340 may be run recursively, such that filtered data are further filtered by the monitor **126**.

**[0037]** At OPERATION **350** the monitor determines or infers the physical location of the site **120** from the geolocation data from the remote devices **130** that have connected to the site **120** over a designated time period (e.g., a learning period, the last X days of operation). The geolocations of the entities remotely connected to the enterprise network **110** may be averaged as mean values for the calculated site location **220**, or the monitor **126** may apply various weights or adjustments for the geolocation values of located remote logins **210**, including additional or recursive filtering per OPTIONAL OPERATION **340**. For example, the monitor **126** may compare an initial calculated site location **220** against a definition file of forbidden locations to locate the site **120** (e.g., in bodies of water, parks, restricted spaces) and adjust the calculation accordingly. When the physical site location **230** of one site **120** is known, the parameters used to filter and adjust the calculation to determine the associated calculated site location **220** may be adjusted until the calculated site location **220** and the physical site location **230** match, and the parameters may then be applied to the calculations for sites **120** whose physical site location **230** are not known, which may include hypothetical sites **120** to which the enterprise network **110** may be reorganized when its physical footprint is grown, shrunk, or adjusted.

**[0038]** At OPTIONAL OPERATION **360** the monitor **126** assigns the calculated site location **220** to local devices **140** that connect to the given site **120**. These locations may be transmitted back to the "home" site **120** to which the entities are mapped for implementation of one or more security protections.

**[0039]** Method **300** may then conclude.

**[0040]** While implementations have been described in the general context of program modules that execute in conjunction with an application program that runs on an operating system on a computer, those skilled in the art will recognize that aspects may also be implemented in combination with other program modules. Generally, program modules include routines, programs, components, data structures, and other types of structures that perform particular tasks or implement particular abstract data types.

**[0041]** The aspects and functionalities described herein may operate via a multitude of computing systems including, without limitation, desktop computer systems, wired and wireless computing systems, mobile computing systems (e.g., mobile telephones, netbooks, tablet or slate type computers, notebook computers, and laptop computers), hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, minicomputers, and mainframe computers.

**[0042]** In addition, according to an aspect, the aspects and functionalities described herein operate over distributed systems (e.g., cloud-based computing systems), where application functionality, memory, data storage and retrieval and various processing functions are operated remotely from each other over a distributed computing network, such as the Internet or an intranet. According to an aspect, user interfaces and information of various types are displayed via on-board computing device displays or via remote display units associated with one or more computing devices. For example, user interfaces and information of various types are displayed and interacted with on a wall surface onto which user interfaces and information of various types are projected. Interaction with the multitude of computing systems with which implementations are practiced include, keystroke entry, touch screen entry, voice or other audio entry, gesture entry where an associated computing device is equipped with detection (e.g., camera) functionality for capturing and interpreting user gestures for controlling the functionality of the computing device, and the like.

**[0043]** **FIGURES 4-5B** and the associated descriptions provide a discussion of a variety of operating environments in which examples are practiced. However, the devices and systems illustrated and discussed with respect to **FIGURES 4-5B** are for purposes of example and illustration and are not limiting of a vast number of computing device configurations that are used for practicing aspects, described herein.

**[0044]** **FIGURE 4** is a block diagram illustrating physical components (i.e., hardware) of a computing device **400** with which examples of the present disclosure may be practiced. In a basic configuration, the computing device **400** includes at least one processing unit **402** and a system memory **404**. According to an aspect, depending on the

configuration and type of computing device, the system memory **404** comprises, but is not limited to, volatile storage (e.g., random access memory), non-volatile storage (e.g., read-only memory), flash memory, or any combination of such memories. According to an aspect, the system memory **404** includes an operating system **405** and one or more program modules **406** suitable for running software applications **450**. According to an aspect, the application **450** includes a monitor **126**, which is operable to infer the location of a site **120** and track the locations of various devices to improve the efficiency and security of an enterprise network **110**. The operating system **405**, for example, is suitable for controlling the operation of the computing device **400**. Furthermore, aspects are practiced in conjunction with a graphics library, other operating systems, or any other application program, and are not limited to any particular application or system. This basic configuration is illustrated in **FIGURE 4** by those components within a dashed line **408**. According to an aspect, the computing device **400** has additional features or functionality. For example, according to an aspect, the computing device **400** includes additional data storage devices (removable and/or non-removable) such as, for example, magnetic disks, optical disks, or tape. Such additional storage is illustrated in **FIGURE 4** by a removable storage device **409** and a non-removable storage device **410**.

**[0045]** As stated above, according to an aspect, a number of program modules and data files are stored in the system memory **404**. While executing on the processing unit **402**, the program modules **406** (e.g., applications **450**) perform processes including, but not limited to, one or more of the stages of the method **300** illustrated in **FIGURE 3**. According to an aspect, other program modules are used in accordance with examples and include applications such as electronic mail and contacts applications, word processing applications, spreadsheet applications, database applications, slide presentation applications, drawing or computer-aided application programs, etc.

**[0046]** According to an aspect, the computing device **400** has one or more input device(s) **412** such as a keyboard, a mouse, a pen, a sound input device, a touch input device, etc. The output device(s) **414** such as a display, speakers, a printer, etc. are also included according to an aspect. The aforementioned devices are examples and others may be used. According to an aspect, the computing device **400** includes one or more communication connections **416** allowing communications with other computing devices **418**. Examples of suitable communication connections **416** include, but are not limited to, radio frequency (RF) transmitter, receiver, and/or transceiver circuitry; universal serial bus (USB), parallel, and/or serial ports.

**[0047]** The term computer readable media, as used herein, includes computer storage media. Computer storage media include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, or program modules. The system memory **404**, the removable storage device **409**, and the non-removable storage device **410** are all computer storage media examples (i.e., memory storage.) According to an aspect, computer storage media include RAM, ROM, electrically erasable programmable read-only memory (EEPROM), flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other article of manufacture which can be used to store information and which can be accessed by the computing device **400**. According to an aspect, any such computer storage media are part of the computing device **400**. Computer storage media do not include a carrier wave or other propagated data signal.

**[0048]** According to an aspect, communication media are embodied by computer readable instructions, data structures, program modules, or other data in a modulated data signal, such as a carrier wave or other transport mechanism, and include any information delivery media. According to an aspect, the term "modulated data signal" describes a signal that has one or more characteristics set or changed in such a manner as to encode information in the signal. By way of example, and not limitation, communication media include wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, radio frequency (RF), infrared, and other wireless media.

**[0049]** **FIGURES 5A** and **5B** illustrate a mobile computing device **500**, for example, a mobile telephone, a smart phone, a tablet personal computer, a laptop computer, and the like, with which aspects may be practiced. With reference to **FIGURE 5A**, an example of a mobile computing device **500** for implementing the aspects is illustrated. In a basic configuration, the mobile computing device **500** is a handheld computer having both input elements and output elements. The mobile computing device **500** typically includes a display **505** and one or more input buttons **510** that allow the user to enter information into the mobile computing device **500**. According to an aspect, the display **505** of the mobile computing device **500** functions as an input device (e.g., a touch screen display). If included, an optional side input element **515** allows further user input. According to an aspect, the side input element **515** is a rotary switch, a button, or any other type of manual input element. In alternative examples, mobile computing device **500** incorporates more or fewer input elements. For example, the display **505** may not be a touch screen in some examples.

In alternative examples, the mobile computing device **500** is a portable phone system, such as a cellular phone. According to an aspect, the mobile computing device **500** includes an optional keypad **535**. According to an aspect, the optional keypad **535** is a physical keypad. According to another aspect, the optional keypad **535** is a "soft" keypad generated on the touch screen display. In various aspects, the output elements include the display **505** for showing a graphical user interface (GUI), a visual indicator **520** (e.g., a light emitting diode), and/or an audio transducer **525** (e.g., a speaker). In some examples, the mobile computing device **500** incorporates a vibration transducer for providing the user with tactile feedback. In yet another example, the mobile computing device **500** incorporates input and/or output ports, such as an audio input (e.g., a microphone jack), an audio output (e.g., a headphone jack), and a video output (e.g., a HDMI port) for sending signals to or receiving signals from an external device. In yet another example, the mobile computing device **500** incorporates peripheral device port **540**, such as an audio input (e.g., a microphone jack), an audio output (e.g., a headphone jack), and a video output (e.g., a HDMI port) for sending signals to or receiving signals from an external device.

**[0050]** **FIGURE 5B** is a block diagram illustrating the architecture of one example of a mobile computing device. That is, the mobile computing device **500** incorporates a system (i.e., an architecture) **502** to implement some examples. In one example, the system **502** is implemented as a "smart phone" capable of running one or more applications (e.g., browser, e-mail, calendaring, contact managers, messaging clients, games, and media clients/players). In some examples, the system **502** is integrated as a computing device, such as an integrated personal digital assistant (PDA) and wireless phone.

**[0051]** According to an aspect, one or more application programs **550** are loaded into the memory **562** and run on or in association with the operating system **564**. Examples of the application programs include phone dialer programs, e-mail programs, personal information management (PIM) programs, word processing programs, spreadsheet programs, Internet browser programs, messaging programs, and so forth. The system **502** also includes a non-volatile storage area **568** within the memory **562**. The non-volatile storage area **568** is used to store persistent information that should not be lost if the system **502** is powered down. The application programs **550** may use and store information in the non-volatile storage area **568**, such as e-mail or other messages used by an e-mail application, and the like. A synchronization application (not shown) also resides on the system **502** and is programmed to interact with a corresponding synchronization application resident on a host computer to keep the information stored in the non-volatile storage area

**568** synchronized with corresponding information stored at the host computer. As should be appreciated, other applications may be loaded into the memory **562** and run on the mobile computing device **500**.

**[0052]** According to an aspect, the system **502** has a power supply **570**, which is implemented as one or more batteries. According to an aspect, the power supply **570** further includes an external power source, such as an AC adapter or a powered docking cradle that supplements or recharges the batteries.

**[0053]** According to an aspect, the system **502** includes a radio **572** that performs the function of transmitting and receiving radio frequency communications. The radio **572** facilitates wireless connectivity between the system **502** and the "outside world," via a communications carrier or service provider. Transmissions to and from the radio **572** are conducted under control of the operating system **564**. In other words, communications received by the radio **572** may be disseminated to the application programs **550** via the operating system **564**, and vice versa.

**[0054]** According to an aspect, the visual indicator **520** is used to provide visual notifications and/or an audio interface **574** is used for producing audible notifications via the audio transducer **525**. In the illustrated example, the visual indicator **520** is a light emitting diode (LED) and the audio transducer **525** is a speaker. These devices may be directly coupled to the power supply **570** so that when activated, they remain on for a duration dictated by the notification mechanism even though the processor **560** and other components might shut down for conserving battery power. The LED may be programmed to remain on indefinitely until the user takes action to indicate the powered-on status of the device. The audio interface **574** is used to provide audible signals to and receive audible signals from the user. For example, in addition to being coupled to the audio transducer **525**, the audio interface **574** may also be coupled to a microphone to receive audible input, such as to facilitate a telephone conversation. According to an aspect, the system **502** further includes a video interface **576** that enables an operation of an on-board camera **530** to record still images, video stream, and the like.

**[0055]** According to an aspect, a mobile computing device **500** implementing the system **502** has additional features or functionality. For example, the mobile computing device **500** includes additional data storage devices (removable and/or non-removable) such as, magnetic disks, optical disks, or tape. Such additional storage is illustrated in **FIGURE 5B** by the non-volatile storage area **568**.

**[0056]** According to an aspect, data/information generated or captured by the mobile computing device **500** and stored via the system **502** are stored locally on the mobile computing device **500**, as described above. According to another aspect, the data are stored on any number of storage media that are accessible by the device via the radio **572** or via a wired connection between the mobile computing device **500** and a separate computing device associated with the mobile computing device **500**, for example, a server computer in a distributed computing network, such as the Internet. As should be appreciated such data/information are accessible via the mobile computing device **500** via the radio **572** or via a distributed computing network. Similarly, according to an aspect, such data/information are readily transferred between computing devices for storage and use according to well-known data/information transfer and storage means, including electronic mail and collaborative data/information sharing systems.

**[0057]** Implementations, for example, are described above with reference to block diagrams and/or operational illustrations of methods, systems, and computer program products according to aspects. The functions/acts noted in the blocks may occur out of the order as shown in any flowchart. For example, two blocks shown in succession may in fact be executed substantially concurrently or the blocks may sometimes be executed in the reverse order, depending upon the functionality/acts involved.

**[0058]** The description and illustration of one or more examples provided in this application are not intended to limit or restrict the scope as claimed in any way. The aspects, examples, and details provided in this application are considered sufficient to convey possession and enable others to make and use the best mode. Implementations should not be construed as being limited to any aspect, example, or detail provided in this application. Regardless of whether shown and described in combination or separately, the various features (both structural and methodological) are intended to be selectively included or omitted to produce an example with a particular set of features. Having been provided with the description and illustration of the present application, one skilled in the art may envision variations, modifications, and alternate examples falling within the spirit of the broader aspects of the general inventive concept embodied in this application that do not depart from the broader scope.

## CLAIMS

1. A method for improving a network, comprising:

collecting tunneled traffic directed to a site of the network, the tunneled traffic including network address information for remote devices;

determining, based on the network address information, geographic coordinates for the remote devices; and

aggregating the geographic coordinates for the remote devices to produce a calculated site location for the site.

2. The method of claim 1, further comprising:

mapping entities to the site, wherein entities mapped to the site access the network most frequently via the site; and

wherein aggregating the geographic coordinates for the remote devices aggregates the geographic coordinates for the remote devices that are associated with entities mapped to the site.

3. The method of claim 2, wherein entities include:

user accounts; and

devices.

4. The method of claim 1, further comprising:

comparing the calculated site location to a definition file comprising forbidden locations; and

in response to the calculated site location matching a forbidden location of the definition file, adjusting the calculated site location so that the adjusted calculated site location does not match the forbidden location.

5. The method of claim 1, wherein determining the geographic coordinates for the remote devices comprises:

querying a geolocation service with IP addresses associated with the remote devices;

in response to querying the geolocation service, receiving the geographic coordinates from the geolocation service.

6. The method of claim 1, wherein the geographic coordinates are provided as a latitude coordinate and a longitude coordinate.

7. The method of claim 1, further comprising:

filtering the geographic coordinates to exclude data from the remote devices that:

are located a preset distance from the calculated site location;

specify a particular site in the network to which to connect; or

are associated with an Internet Service Provider known to provide addresses that are unreliable for geolocation.

8. The method of claim 1, wherein aggregating the geographic coordinates for the remote devices to produce the calculated site location further comprises:

clustering the geographic coordinates to a centralized location for each cluster of the geographic coordinates.

9. The method of claim 1, wherein aggregating the geographic coordinates for the remote devices to produce the calculated site location further comprises:

assigning weights the geographic coordinates, wherein the weights are based on:

a frequency associated with a given entity connecting to the site;

a distance from the geographic coordinates to the calculated site location; and

a temporal proximity of a first login attempt to a subsequent login attempt for the given entity.

10. A system for improving a network comprised of a plurality of sites to which devices may access the system locally or remotely, wherein each site comprises:

a gateway, operable to accept communications from the devices accessing a given site of the network;

a domain controller, in communication with the gateway, operable to authenticate entities seeking to access the network at the given site; and

a monitor, in communication with the domain controller, operable to aggregate connection information from the devices accessing the given site remotely to infer a calculated site location for the given site, wherein to infer the calculated site location, the monitor is operable to:

collect tunneled traffic to the given site from the devices, wherein each of the devices is associated with an IP address that is included in the tunneled traffic;

determine a geolocation for each of the devices based on the IP address associated with each of the devices;

aggregate the geolocation for each device into a centralized location;

assign the centralized location as a calculated site location for the given site.

11. The system of claim 10, wherein the monitor is further operable to observe the tunneled traffic to determine whether the geolocation for a given device corresponds to a forbidden location.

12. The system of claim 11, wherein the monitor is further operable to use the calculated site location as a location for a previous login session when the previous session was made from a local device within the network.

13. The system of claim 11, wherein the wherein the monitor is further operable to use the calculated site location as a location for a current login session when the current login session is made from a local device within the network and a previous session was made from a remote device.

14. The system of claim 10, wherein the monitor is further operable to filter the geographic coordinates to exclude data from:

devices located a preset distance from the calculated site location;

devices that specify a particular site in the network to which to connect; and

the tunneled traffic that originates from an Internet Service Provider known to provide addresses that are unreliable for geolocation.

15. A computer-readable storage medium including instructions to improve a network, which when executed by a processor are operable to:

map entities to sites comprising the network based on an activity level of the entity on a given site within the network;

collect tunneled traffic directed to the given site of the network by the entities mapped to the given site, the tunneled traffic including network address information for remote devices used by the entities and identifiers to identify the entities;

determine, based on the network address information, geographic coordinates for the remote devices; and

produce a calculated site location for the given site by aggregating the geographic coordinates for the remote devices.

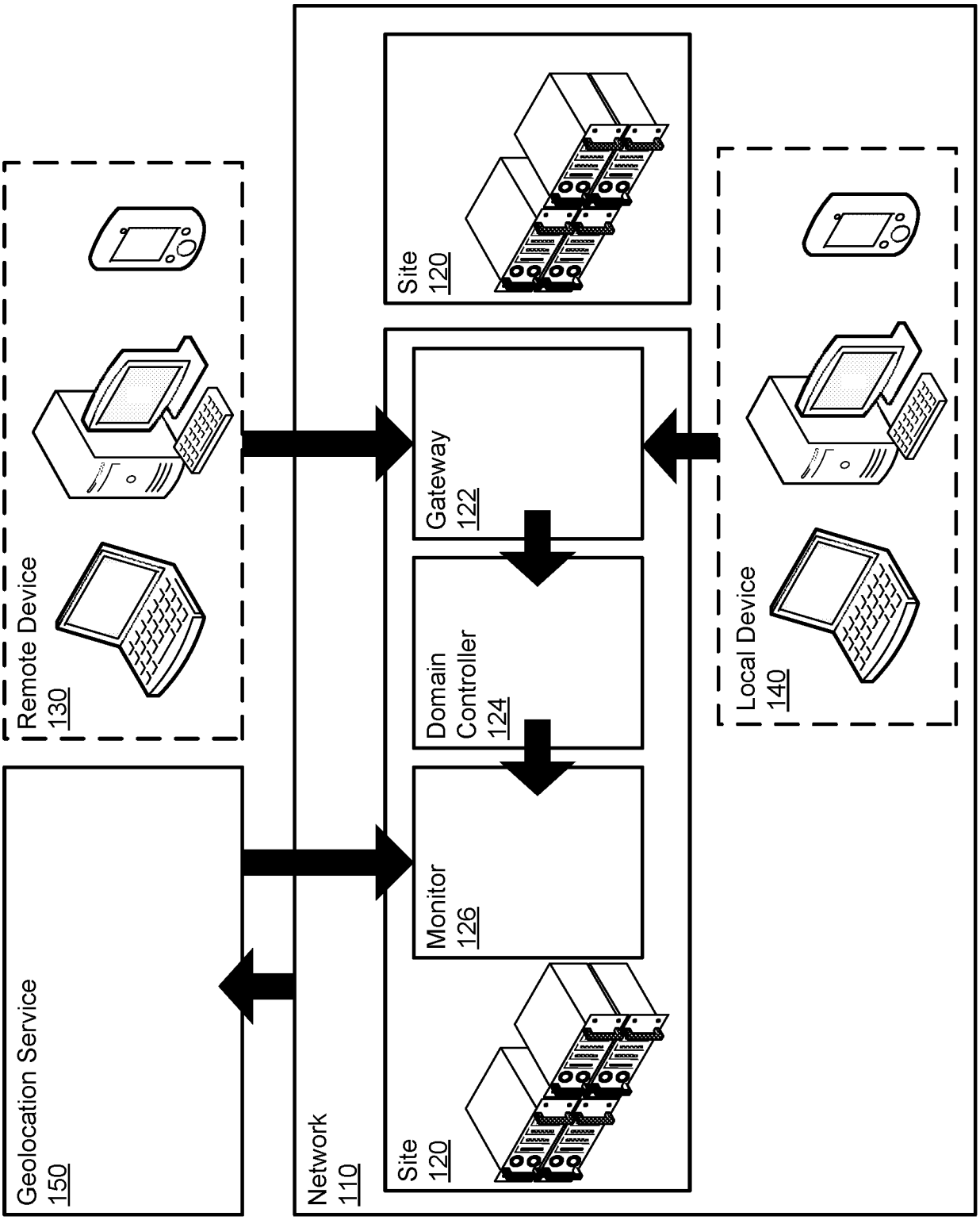

Geolocation Service
150
Network
110
Site
120
Monitor
126
Domain
Controller
124
Gateway
122
Site
120
Remote Device
130
Local Device
140
100

FIG. 1

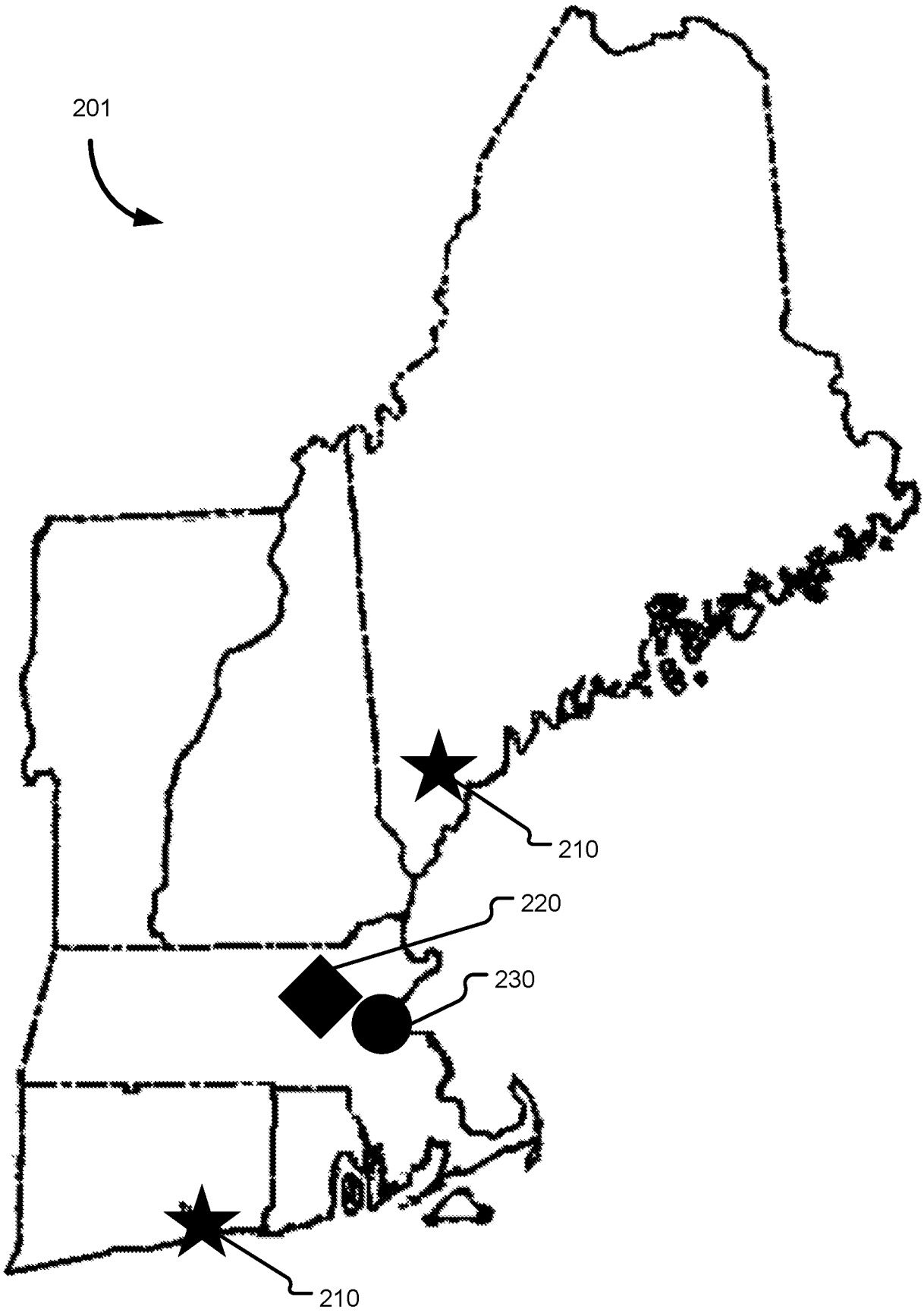



FIG. 2A

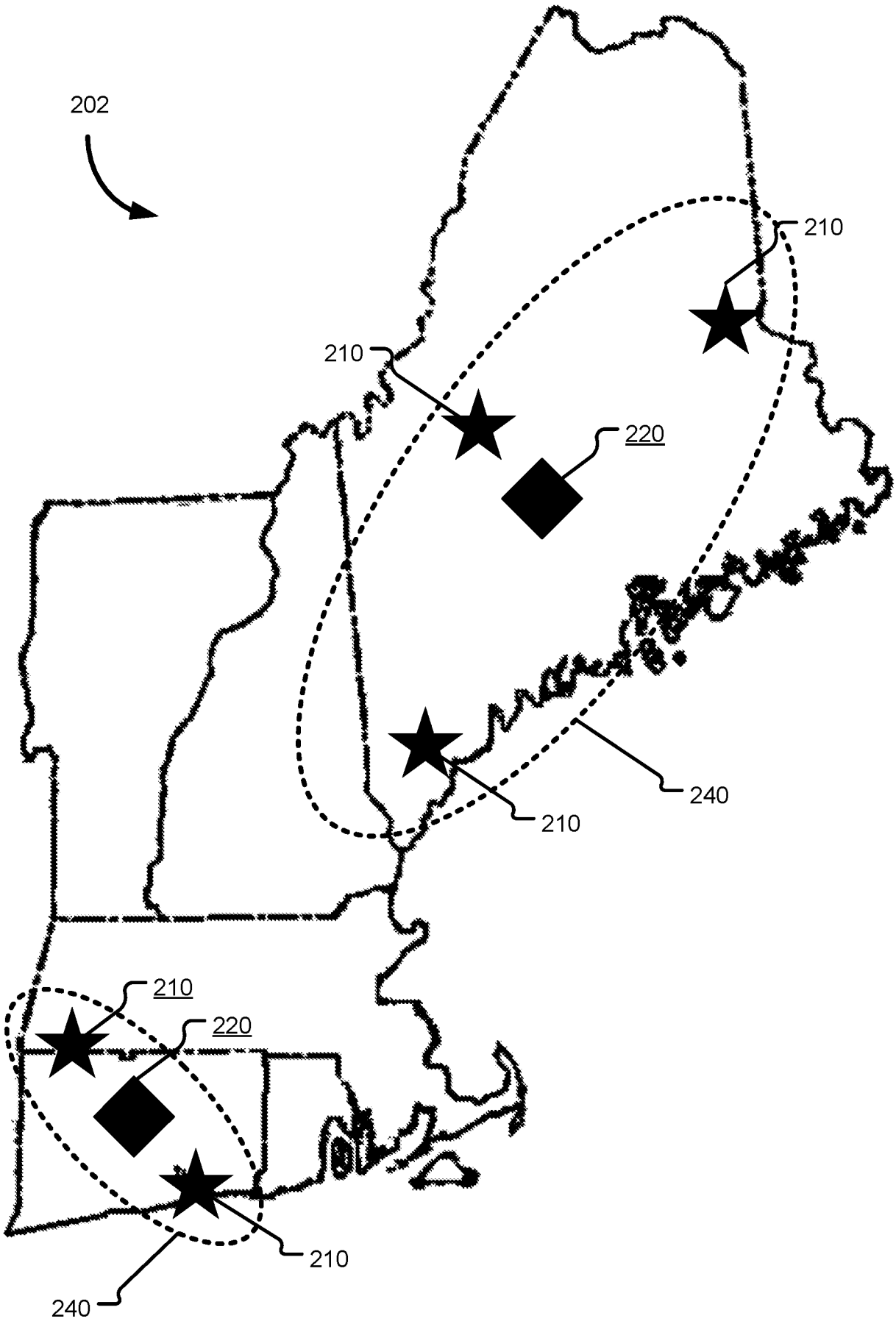



FIG. 2B

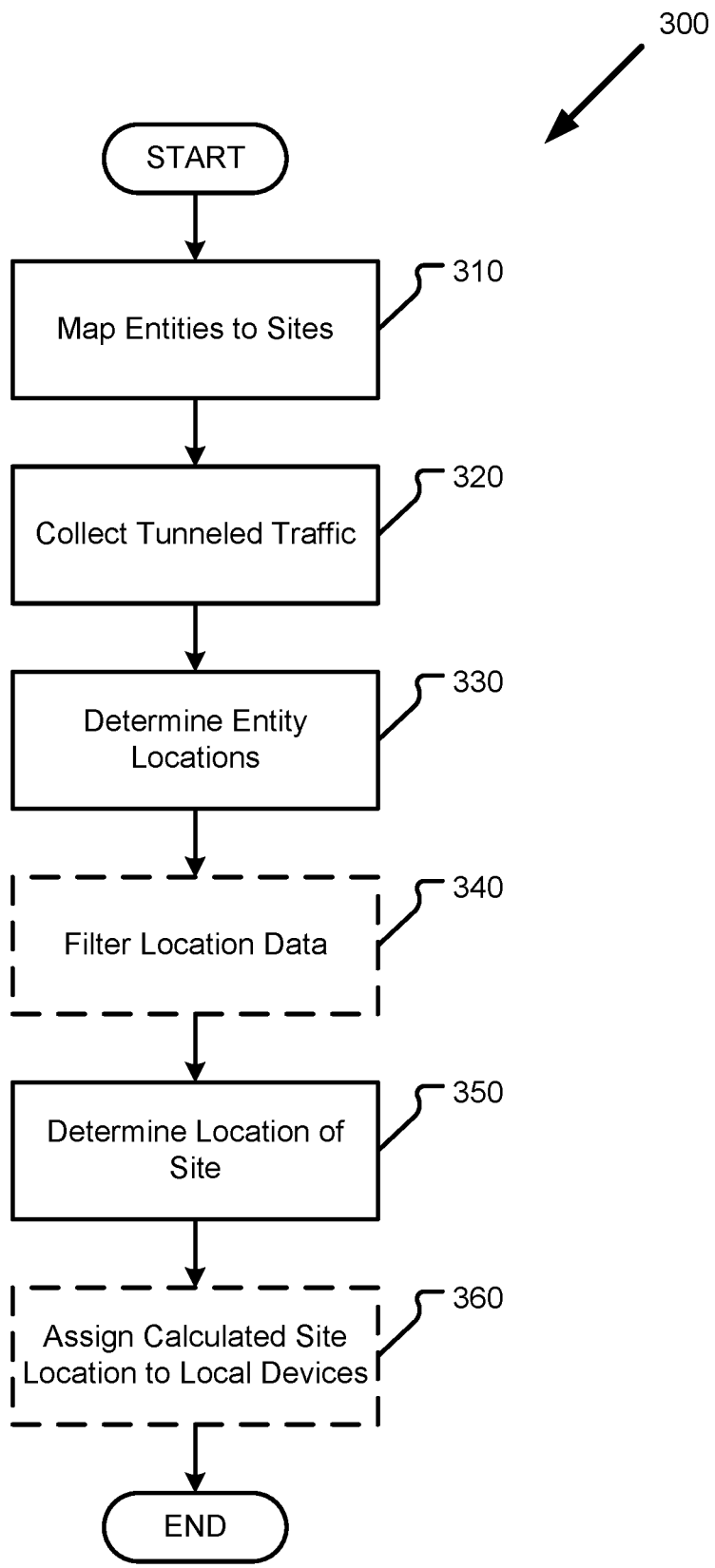

300
START
Map Entities to Sites
310
Collect Tunneled Traffic
320
Determine Entity Locations
330
Filter Location Data
340
Determine Location of Site
350
Assign Calculated Site Location to Local Devices
360
END

FIG. 3

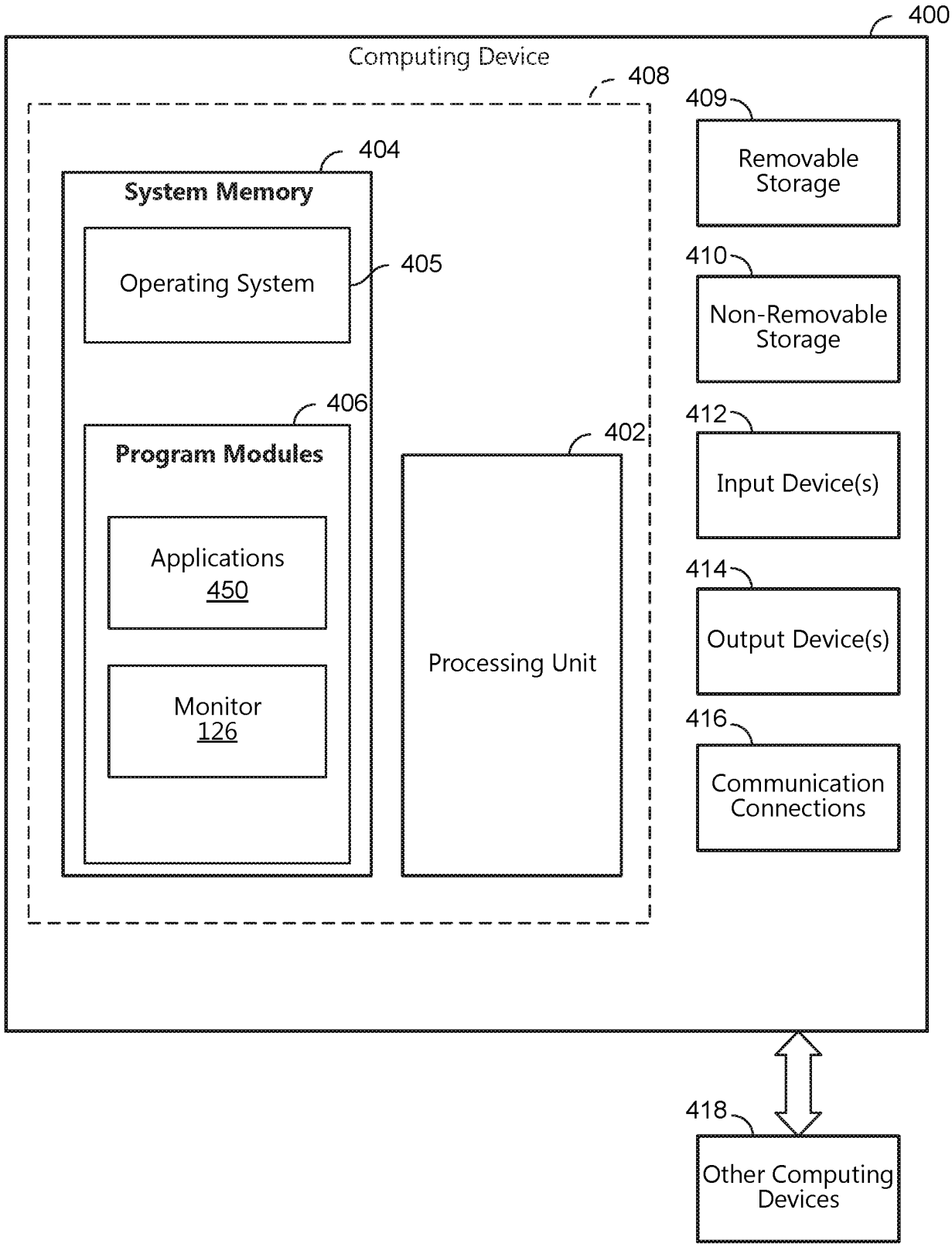
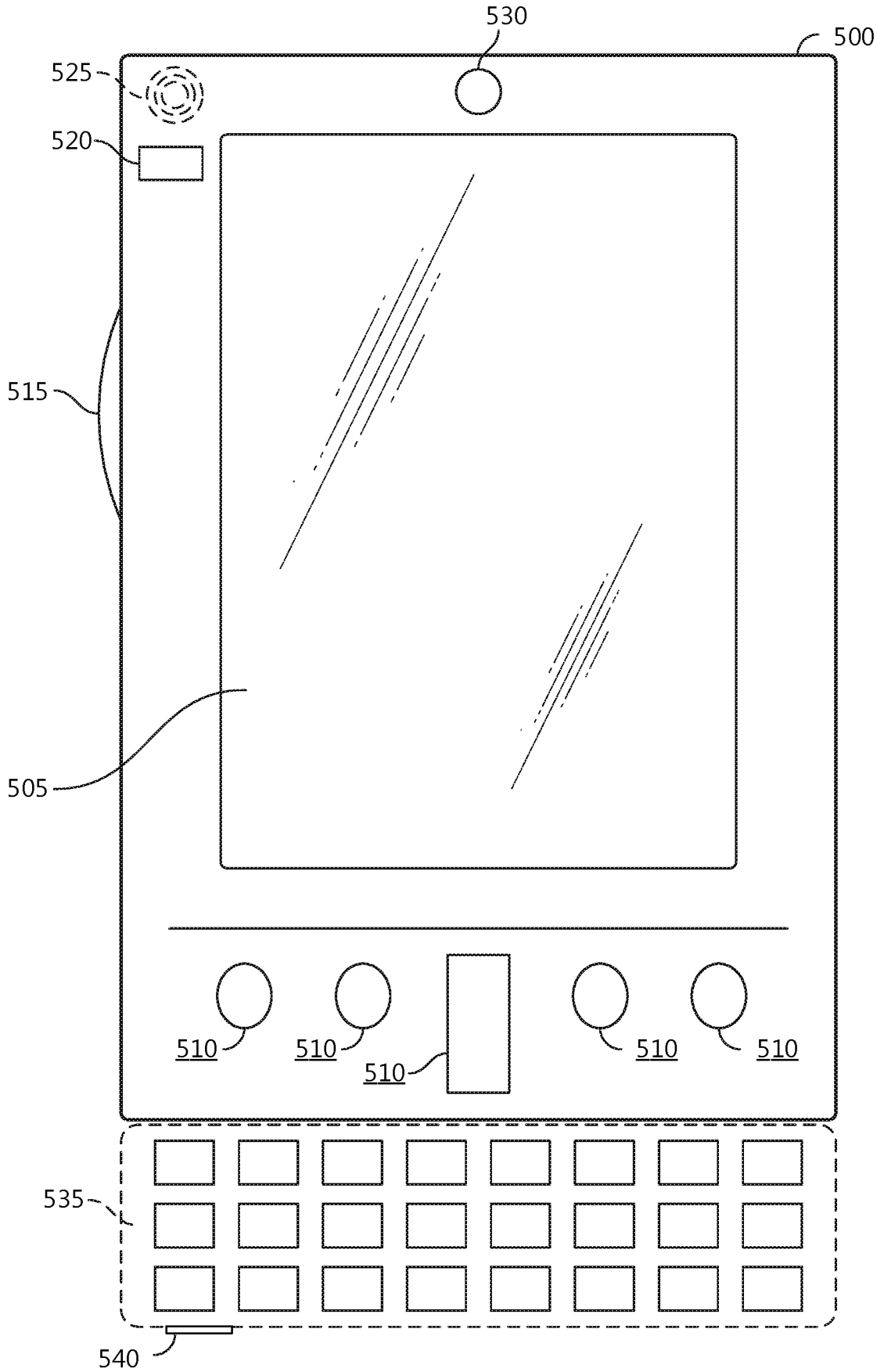

400
Computing Device
408
409
Removable Storage
404
System Memory
Operating System
405
410
Non-Removable Storage
406
Program Modules
Applications 450
Monitor 126
402
Processing Unit
412
Input Device(s)
414
Output Device(s)
416
Communication Connections
418
Other Computing Devices

FIG. 4




MOBILE COMPUTING DEVICE

FIG. 5A

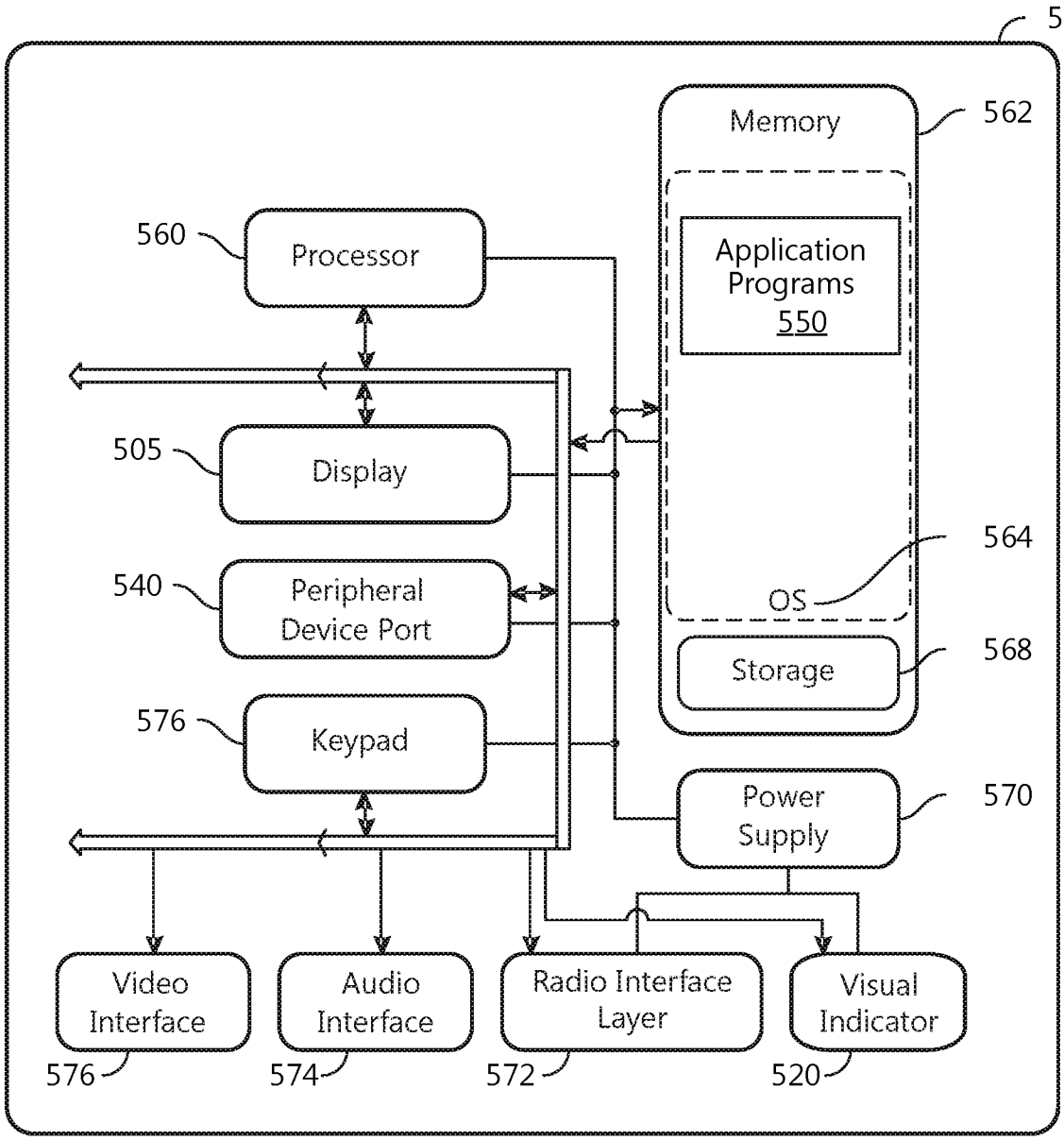

502
Memory
562
Application Programs 550
560
Processor
505
Display
564
OS
540
Peripheral Device Port
568
Storage
576
Keypad
570
Power Supply
Video Interface
Audio Interface
Radio Interface Layer
Visual Indicator
576
574
572
520

FIG. 5B

# INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/049799

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W64/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 2014/274113 A1 (TEED-GILLEN LOIS A [US] ET AL) 18 September 2014 (2014-09-18) paragraphs [0032] - [0036], [0039] - [0040], [0046] - [0057]; figures 1,4-6,9,16,17 | 1-15 |
| X | US 2008/318596 A1 (TENNY NATHAN EDWARD [US]) 25 December 2008 (2008-12-25) paragraphs [0037] - [0043]; figures 1,3a,3b | 1-15 |
| A | US 2014/036768 A1 (GAO WEIHUA [US] ET AL) 6 February 2014 (2014-02-06) paragraphs [0026], [0038] - [0047]; figures 1a,2,3 | 1-15 |

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 8 November 2017 | 16/11/2017 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Bocking, Philip |

# INTERNATIONAL SEARCH REPORT

International application No
PCT/US2017/049799

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 2011/176523 A1 (HUANG RONALD K [US] ET AL) 21 July 2011 (2011-07-21) paragraphs [0031] - [0032]; figure 1 ----- | 1-15 |
| A | US 2015/312722 A1 (MORI KOICHI [US] ET AL) 29 October 2015 (2015-10-29) paragraphs [0110] - [0122] ----- | 1-15 |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2017/049799

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2014274113 A1 | 18-09-2014 | CN 105191359 A | 23-12-2015 |
| | | EP 2974397 A1 | 20-01-2016 |
| | | JP 2016517203 A | 09-06-2016 |
| | | KR 20150129315 A | 19-11-2015 |
| | | US 2014274113 A1 | 18-09-2014 |
| | | US 2015148070 A1 | 28-05-2015 |
| | | US 2015319732 A1 | 05-11-2015 |
| | | US 2015319733 A1 | 05-11-2015 |
| | | US 2015327209 A1 | 12-11-2015 |
| | | US 2016219551 A1 | 28-07-2016 |
| | | WO 2014158566 A1 | 02-10-2014 |
| US 2008318596 A1 | 25-12-2008 | CN 101682907 A | 24-03-2010 |
| | | CN 103533639 A | 22-01-2014 |
| | | EP 2165548 A1 | 24-03-2010 |
| | | JP 6165825 B2 | 19-07-2017 |
| | | JP 2010531583 A | 24-09-2010 |
| | | JP 2013138459 A | 11-07-2013 |
| | | JP 2014225899 A | 04-12-2014 |
| | | JP 2016116211 A | 23-06-2016 |
| | | JP 2016165121 A | 08-09-2016 |
| | | JP 2017169208 A | 21-09-2017 |
| | | KR 20100022117 A | 26-02-2010 |
| | | US 2008318596 A1 | 25-12-2008 |
| | | WO 2008157841 A1 | 24-12-2008 |
| US 2014036768 A1 | 06-02-2014 | CN 104509183 A | 08-04-2015 |
| | | EP 2880931 A1 | 10-06-2015 |
| | | JP 5833281 B2 | 16-12-2015 |
| | | JP 2015529060 A | 01-10-2015 |
| | | US 2014036768 A1 | 06-02-2014 |
| | | US 2015319604 A1 | 05-11-2015 |
| | | WO 2014022069 A1 | 06-02-2014 |
| US 2011176523 A1 | 21-07-2011 | AU 2010341772 A1 | 23-08-2012 |
| | | BR 112012017530 A2 | 28-06-2016 |
| | | CN 102204374 A | 28-09-2011 |
| | | CN 104125638 A | 29-10-2014 |
| | | EP 2524553 A1 | 21-11-2012 |
| | | JP 5395963 B2 | 22-01-2014 |
| | | JP 5722408 B2 | 20-05-2015 |
| | | JP 2013517679 A | 16-05-2013 |
| | | JP 2014060737 A | 03-04-2014 |
| | | KR 20120124446 A | 13-11-2012 |
| | | US 2011176523 A1 | 21-07-2011 |
| | | US 2013231132 A1 | 05-09-2013 |
| | | WO 2011087529 A1 | 21-07-2011 |
| US 2015312722 A1 | 29-10-2015 | CN 106461768 A | 22-02-2017 |
| | | EP 3139196 A1 | 08-03-2017 |
| | | KR 20150124396 A | 05-11-2015 |
| | | US 2015312722 A1 | 29-10-2015 |
| | | US 2017041761 A1 | 09-02-2017 |