

(51) International Patent Classification:
H04L 29/08 (2006.01) *B60L 11/18* (2006.01)(21) International Application Number:
PCT/US2012/043415(22) International Filing Date:
20 June 2012 (20.06.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/499,562 21 June 2011 (21.06.2011) US
13/527,486 19 June 2012 (19.06.2012) US(71) Applicant (for all designated States except US): **QUALCOMM ATHEROS, INC.** [US/US]; 1700 Technology Drive, San Jose, CA 95110 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **KATAR, Srinivas** [IN/US]; c/o Qualcomm Atheros, Inc., 1700 Technology Drive, San Jose, California 95110 (US). **YONGE III, Lawrence, W.** [US/US]; c/o Qualcomm Atheros, Inc., 1700 Technology Drive, San Jose, California 95110 (US).**NEWMAN, Richard, E.** [US/US]; c/o Qualcomm Atheros, Inc., 1700 Technology Drive, San Jose, California 95110 (US).(74) Agents: **LEWIN, Mario, J.** et al.; 15201 Mason Road, Suite 1000-312, Cypress, TX 77433 (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, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, 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,

[Continued on next page]

(54) Title: SECURE CLIENT AUTHENTICATION AND NETWORK SERVICE AUTHORIZATION

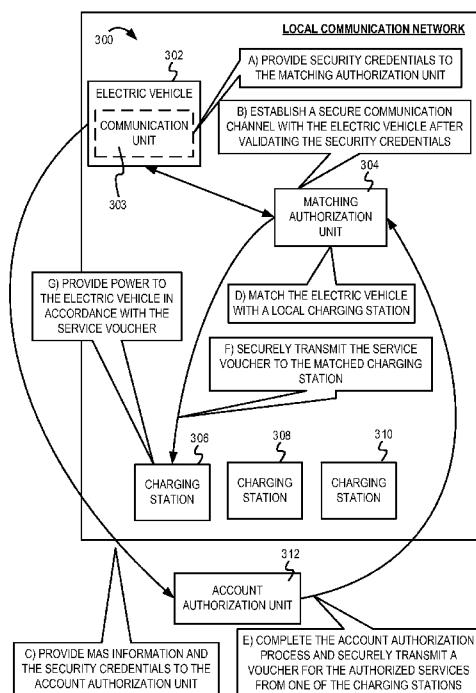


FIG. 3

(57) Abstract: Functionality for secure client authentication and service authorization in a shared communication network are disclosed. A managing network device of a communication network causes a securely connected client network device to perform an account authorization process with an accounting network device in parallel with a service matching process with the managing network device and one or more service providers of the communication network. The managing network device executes the service matching process and securely matches the client network device with one of the service providers. The accounting network device executes the account authorizing process with the client network device and provides a service voucher to the managing network device authorizing one or more of the service providers to service the client network device. The managing network device transmits the service voucher to the matched service provider to prompt the matched service provider to service the client network device.

WO 2012/177812 A1



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, **Published:**
ML, MR, NE, SN, TD, TG).

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

SECURE CLIENT AUTHENTICATION AND NETWORK SERVICE AUTHORIZATION

RELATED APPLICATIONS

[0001] This application claims the priority benefit of United States Provisional Application No. 61/499,562 filed June 21, 2011 and to United States Application 13/527,486 filed June 19, 2012.

BACKGROUND

[0002] Embodiments of the inventive subject matter generally relate to the field of communication networks and, more particularly, to secure client authentication and service authorization in a shared communication network.

[0003] Electric vehicles typically charge from conventional power outlets or dedicated charging stations. Prior to receiving power from the charging stations, the charging station can ensure that the user of the electric vehicle has a valid account and proper authorization to receive the electric power and to pay for the received electric power.

SUMMARY

[0004] In some embodiments, a method comprises: establishing a secure communication channel between a client network device and a managing network device of a communication network based, at least in part, on a client identifier of the client network device; causing the client network device to perform an account authorization process with an accounting network device in parallel with a service matching process with the managing network device and one or more of a plurality of service providers of the communication network; securely matching the client network device with a first of the plurality of service providers; securely receiving a service voucher at the managing network device from the accounting network device authorizing one or more of the service providers of the communication network to service the client network device in response to the accounting network device executing the account authorizing process with the client network device; and securely transmitting the service voucher from the managing

network device to the matching service provider to allow the client network device to be serviced by the matching service provider.

[0005] In some embodiments, said securely matching the client network device with the first of the plurality of service providers further comprises generating, at the managing network device, a client key that is unique to the client network device based, at least in part, on the client identifier and on a master key known to the managing network device and the plurality of service providers of the communication network; providing the client key from the managing network device to the client network device via the secure communication channel to allow the client network device to securely communicate with the plurality of service providers of the communication network; receiving, from each of the plurality of service providers, a message that indicates a signal level detected at the service provider in response to a service matching message from the client network device; and selecting the first of the plurality of service providers that detected the highest signal level as the matching service provider for the client network device.

[0006] In some embodiments, the method further comprises transmitting, from the managing network device to the client network device, a number of service matching messages that should be transmitted from the client network device to the plurality of service providers.

[0007] In some embodiments, the client key is a temporary key and is generated based, at least in part, on the master key, the client identifier, and one or more of a sequence number, a random number, a start/end timestamp, a lifetime duration, a message counter, and/or a location identifier.

[0008] In some embodiments, the client key is a public encryption key.

[0009] In some embodiments, the client identifier is authenticated by the managing network device and by the accounting network device, and the service voucher is bound to the client identifier.

[0010] In some embodiments, the managing network device is one of the plurality of service providers.

[0011] In some embodiments, the method further comprises determining, at the managing network device, a message counter value from a message received from the client network device; comparing the received message counter value with a previously received message counter value from the client network device; discarding the received message if the received message counter value is less than or equal to the previously received message counter value; and processing the received message if the received message counter value is greater than the previously received message counter value.

[0012] In some embodiments, the client network device comprises a plug-in electric vehicle, the plurality of service providers comprise a plurality of electric charging stations, the managing network device comprises a managing system associated with the plurality of electric charging stations, and the accounting network device comprises a remote account authorization server for one or more client accounts.

[0013] In some embodiments, the method further comprises determining, at the managing network device, a first value of the client identifier associated with the client network device, wherein the first value of the client identifier was used for executing the service matching process; determining a second value of the client identifier associated with the client network device, wherein the second value was used for executing the account authorization process; determining whether the first value of the client identifier matches the second value of the client identifier; in response to determining that the first value of the client identifier matches the second value of the client identifier, said securely transmitting the service voucher from the managing network device to the matching service provider to allow the client network device to be serviced by the matching service provider; and in response to determining that the first value of the client identifier does not match the second value of the client identifier, preventing the matching service provider from servicing the client network device.

[0014] In some embodiments, a method comprises: establishing, at a client network device, a secure communication channel with a managing network device of a communication network based, at least in part, on a client identifier of the client network device; receiving, from the managing network device, identification information associated with the managing network device via the secure communication channel; providing the client identifier and the identification information associated with the managing network device to an accounting network device to cause the accounting network device to execute an account authorization

process with the client network device; in parallel with the account authorization process, executing a service matching process with the managing network device and one or more of a plurality of service providers of the communication network; detecting receipt of service from a first of the plurality of service providers of the communication network after completion of the account authorization process and the service matching process; and transmitting an acknowledgement message to one of the managing network device and the first of the plurality of service providers in response to said detecting receipt of service from the first of the plurality of service providers of the communication network.

[0015] In some embodiments, the identification information associated with the managing network device comprises a device identifier of the managing network device and a location of the managing network device.

[0016] In some embodiments, said receiving, from the managing network device, identification information associated with the managing network device further comprises receiving, from the managing network device, one or more service matching parameters to cause the client network device to initiate the service matching process with the managing network device and the plurality of service providers of the communication network.

[0017] In some embodiments, the method further comprises receiving, from the managing network device, a client key that is unique to the client network device, via the secure communication channel, wherein the client key enables the client network device to securely communicate with the plurality of service providers of the communication network; receiving client key generation parameters based on which the client key was determined, wherein the client key generation parameters comprise one or more of a sequence number, a random number, a start/end timestamp, a lifetime duration, a message counter, and a location identifier; wherein said executing the service matching process with the managing network device and one or more of a plurality of service providers of the communication network comprises signing one or more service matching messages using the client key; and transmitting the one or more service matching messages and the client key generation parameters to the plurality of service providers.

[0018] In some embodiments, said transmitting the one or more service matching messages and the client key generation parameters to the plurality of service providers comprises determining whether a length of the service matching message scheduled to be transmitted to the

plurality of service providers is greater than a predetermined threshold message length; in response to determining that the length of the service matching message is greater than the predetermined threshold message length, transmitting an initialization message includes the client key generation parameters to the plurality of service providers, and transmitting the client identifier and the sequence number in the one or more service matching messages; and in response to determining that the length of the service matching message is less than the predetermined threshold message length, transmitting the client key generation parameters as part of the one or more service matching messages.

[0019] In some embodiments, a managing network device comprises: a network interface; and a matching authorization unit coupled with the network interface, the matching authorization unit operable to establish a secure communication channel between a client network device and the managing network device of a communication network based, at least in part, on a client identifier of the client network device; cause the client network device to perform an account authorization process with an accounting network device in parallel with a service matching process with the managing network device and one or more of a plurality of service providers of the communication network; securely match the client network device with a first of the plurality of service providers; securely receive a service voucher from the accounting network device authorizing one or more of the service providers of the communication network to service the client network device in response to the accounting network device executing the account authorizing process with the client network device; and securely transmit the service voucher to the matching service provider to allow the client network device to be serviced by the matching service provider.

[0020] In some embodiments, the matching authorization unit operable to securely match the client network device with the first of the plurality of service providers further comprises the matching authorization unit operable to generate a client key that is unique to the client network device based, at least in part, on the client identifier and on a master key known to the managing network device and the plurality of service providers of the communication network; provide the client key to the client network device via the secure communication channel to allow the client network device to securely communicate with the plurality of service providers of the communication network; receive, from each of the plurality of service providers, a message that indicates a signal level detected at the service provider in response to a service matching

message from the client network device; and select the first of the plurality of service providers that detected the highest signal level as the matching service provider for the client network device.

[0021] In some embodiments, the matching authorization unit is further operable to transmit, to the client network device, a number of service matching messages that should be transmitted from the client network device to the plurality of service providers.

[0022] In some embodiments, the client key is a temporary key and is generated based, at least in part, on the master key, the client identifier, and one or more of a sequence number, a random number, a start/end timestamp, a lifetime duration, a message counter, and/or a location identifier.

[0023] In some embodiments, the matching authorization unit is further operable to determine a first value of the client identifier associated with the client network device, wherein the first value of the client identifier was used for executing the service matching process; determine a second value of the client identifier associated with the client network device, wherein the second value was used for executing the account authorization process; determine whether the first value of the client identifier matches the second value of the client identifier; in response to the matching authorization unit determining that the first value of the client identifier matches the second value of the client identifier, the matching authorization unit is operable to securely transmit the service voucher to the matching service provider to allow the client network device to be serviced by the matching service provider; and in response to the matching authorization unit determining that the first value of the client identifier does not match the second value of the client identifier, the matching authorization unit is operable to prevent the matching service provider from servicing the client network device.

[0024] In some embodiments, a network device comprises: a network interface; and a communication unit coupled with the network interface, the communication unit operable to establish a secure communication channel with a managing network device of a communication network based, at least in part, on a client identifier of the network device; receive, from the managing network device, identification information associated with the managing network device via the secure communication channel; provide the client identifier and the identification information associated with the managing network device to an accounting network device to

cause the accounting network device to execute an account authorization process with the network device; in parallel with the account authorization process, execute a service matching process with the managing network device and one or more of a plurality of service providers of the communication network; detect receipt of service from a first of the plurality of service providers of the communication network after completion of the account authorization process and the service matching process; and transmit an acknowledgement message to one of the managing network device and the first of the plurality of service providers in response to the communication unit detecting receipt of service from the first of the plurality of service providers of the communication network.

[0025] In some embodiments, the communication unit operable to receive, from the managing network device, identification information associated with the managing network device further comprises the communication unit operable to receive, from the managing network device, one or more service matching parameters to cause the network device to initiate the service matching process with the managing network device and the plurality of service providers of the communication network.

[0026] In some embodiments, the communication unit is further operable to receive, from the managing network device, a client key that is unique to the network device, via the secure communication channel, wherein the client key enables the network device to securely communicate with the plurality of service providers of the communication network; receive client key generation parameters based on which the client key was determined, wherein the client key generation parameters comprise one or more of a sequence number, a random number, a start/end timestamp, a lifetime duration, a message counter, and a location identifier; wherein the communication unit operable to execute the service matching process with the managing network device and one or more of a plurality of service providers of the communication network comprises the communication unit operable to sign one or more service matching messages using the client key; and transmit the one or more service matching messages and the client key generation parameters to the plurality of service providers.

[0027] In some embodiments, the communication unit operable to transmit the one or more service matching messages and the client key generation parameters to the plurality of service providers comprises the communication unit operable to determine whether a length of the service matching message scheduled to be transmitted to the plurality of service providers is

greater than a predetermined threshold message length; in response to the communication unit determining that the length of the service matching message is greater than the predetermined threshold message length, transmit an initialization message includes the client key generation parameters to the plurality of service providers, and transmit the client identifier and the sequence number in the one or more service matching messages; and in response to the communication unit determining that the length of the service matching message is less than the predetermined threshold message length, transmit the client key generation parameters as part of the one or more service matching messages.

[0028] In some embodiments, a method comprises: establishing a secure communication channel between a plug-in electric vehicle and a managing network device of a communication network based, at least in part, on a client identifier of the plug-in electric vehicle; causing the plug-in electric vehicle to perform an account authorization process with an accounting network device in parallel with a service matching process with the managing network device and one or more of a plurality of electric charging stations of the communication network; securely matching the plug-in electric vehicle with a first of the plurality of electric charging stations; securely receiving a service voucher at the managing network device from the accounting network device authorizing one or more of the electric charging stations of the communication network to provide electric power to the plug-in electric vehicle in response to the accounting network device executing the account authorizing process with the plug-in electric vehicle; and securely transmitting the service voucher from the managing network device to the matching electric charging station to allow the plug-in electric vehicle to receive electric power from the matching electric charging station.

[0029] In some embodiments, said securely matching the plug-in electric vehicle with the first of the plurality of electric charging stations further comprises generating, at the managing network device, a client key that is unique to the plug-in electric vehicle based, at least in part, on the client identifier and on a master key known to the managing network device and the plurality of electric charging stations of the communication network; providing the client key from the managing network device to the plug-in electric vehicle via the secure communication channel to allow the plug-in electric vehicle to securely communicate with the plurality of electric charging stations of the communication network; receiving, from each of the plurality of electric charging stations, a message that indicates a signal level detected at the electric charging

station in response to a service matching message from the plug-in electric vehicle; and selecting the first of the plurality of electric charging stations that detected the highest signal level as the matching electric charging station for the plug-in electric vehicle.

[0030] In some embodiments, the client key is a temporary key and is generated based, at least in part, on the master key, the client identifier, and one or more of a sequence number, a random number, a start/end timestamp, a lifetime duration, a message counter, and/or a location identifier.

[0031] In some embodiments, one or more machine-readable storage media having instructions stored therein, which when executed by one or more processors causes the one or more processors to perform operations that comprise: establishing a secure communication channel between a client network device and a managing network device of a communication network based, at least in part, on a client identifier of the client network device; causing the client network device to perform an account authorization process with an accounting network device in parallel with a service matching process with the managing network device and one or more of a plurality of service providers of the communication network; securely matching the client network device with a first of the plurality of service providers; securely receiving a service voucher at the managing network device from the accounting network device authorizing one or more of the service providers of the communication network to service the client network device in response to the accounting network device executing the account authorizing process with the client network device; and securely transmitting the service voucher from the managing network device to the matching service provider to allow the client network device to be serviced by the matching service provider.

[0032] In some embodiments, said operation of securely matching the client network device with the first of the plurality of service providers further comprises generating a client key that is unique to the client network device based, at least in part, on the client identifier and on a master key known to the managing network device and the plurality of service providers of the communication network; providing the client key to the client network device via the secure communication channel to allow the client network device to securely communicate with the plurality of service providers of the communication network; receiving, from each of the plurality of service providers, a message that indicates a signal level detected at the service provider in response to a service matching message from the client network device; and selecting

the first of the plurality of service providers that detected the highest signal level as the matching service provider for the client network device.

[0033] In some embodiments, the operations further comprise determining a first value of the client identifier associated with the client network device, wherein the first value of the client identifier was used for executing the service matching process; determining a second value of the client identifier associated with the client network device, wherein the second value was used for executing the account authorization process; determining whether the first value of the client identifier matches the second value of the client identifier; in response to determining that the first value of the client identifier matches the second value of the client identifier, said securely transmitting the service voucher from the managing network device to the matching service provider to allow the client network device to be serviced by the matching service provider; and in response to determining that the first value of the client identifier does not match the second value of the client identifier, preventing the matching service provider from servicing the client network device.

[0034] One or more machine-readable storage media having instructions stored therein, which when executed by one or more processors causes the one or more processors to perform operations that comprise: establishing a secure communication channel with a managing network device of a communication network based, at least in part, on a client identifier of a client network device; receiving, from the managing network device, identification information associated with the managing network device via the secure communication channel; providing the client identifier and the identification information associated with the managing network device to an accounting network device to cause the accounting network device to execute an account authorization process with the client network device; in parallel with the account authorization process, executing a service matching process with the managing network device and one or more of a plurality of service providers of the communication network; detecting receipt of service from a first of the plurality of service providers of the communication network after completion of the account authorization process and the service matching process; and transmitting an acknowledgement message to one of the managing network device and the first of the plurality of service providers in response to said detecting receipt of service from the first of the plurality of service providers of the communication network.

[0035] In some embodiments, the operations further comprise receiving, from the managing network device, a client key that is unique to the client network device, via the secure communication channel, wherein the client key enables the client network device to securely communicate with the plurality of service providers of the communication network; receiving client key generation parameters based on which the client key was determined, wherein the client key generation parameters comprise one or more of a sequence number, a random number, a start/end timestamp, a lifetime duration, a message counter, and a location identifier; wherein said executing the service matching process with the managing network device and one or more of a plurality of service providers of the communication network comprises signing one or more service matching messages using the client key; and transmitting the one or more service matching messages and the client key generation parameters to the plurality of service providers.

[0036] In some embodiments, said operation of transmitting the one or more service matching messages and the client key generation parameters to the plurality of service providers comprises determining whether a length of the service matching message scheduled to be transmitted to the plurality of service providers is greater than a predetermined threshold message length; in response to determining that the length of the service matching message is greater than the predetermined threshold message length, transmitting an initialization message includes the client key generation parameters to the plurality of service providers, and transmitting the client identifier and the sequence number in the one or more service matching messages; and in response to determining that the length of the service matching message is less than the predetermined threshold message length, transmitting the client key generation parameters as part of the one or more service matching messages.

BRIEF DESCRIPTION OF THE DRAWINGS

[0037] The present embodiments may be better understood, and numerous objects, features, and advantages made apparent to those skilled in the art by referencing the accompanying drawings.

[0038] **Figure 1** is an example conceptual diagram of a broadcast authentication mechanism in a communication network;

[0039] **Figure 2** is a flow diagram illustrating example operations of a key distribution unit executing the broadcast authentication mechanism;

[0040] **Figure 3** is an example conceptual diagram of a distributed authentication mechanism in a communication network;

[0041] **Figure 4** is a flow diagram illustrating example operations of a matching authorization unit in a distributed client authentication and service authorization environment;

[0042] **Figure 5** is a flow diagram illustrating example operations of a customer device in a distributed client authentication and service authorization environment; and

[0043] **Figure 6** is a block diagram of one embodiment of an electronic device including a broadcast authentication and service matching mechanism in a communication network.

DESCRIPTION OF EMBODIMENT(S)

[0044] The description that follows includes exemplary systems, methods, techniques, instruction sequences, and computer program products that embody techniques of the present inventive subject matter. However, it is understood that the described embodiments may be practiced without these specific details. For instance, although examples refer to executing operations (e.g., exchanging messages) for simultaneous client authentication and account authorization in a powerline communication (PLC) network, embodiments are not so limited. In other embodiments, the operations described herein for simultaneous client authentication and account authorization can be executed in other suitable shared communication networks (e.g., Ethernet over Coax (EoC), wireless local area networks (WLAN), such as IEEE 802.11 networks, etc.). In other instances, well-known instruction instances, protocols, structures, and techniques have not been shown in detail in order not to obfuscate the description.

[0045] When an electric vehicle connects to a charging facility that comprises multiple charging stations, an association between the electric vehicle and one of the charging stations may be established to enable the electric vehicle to receive power from the charging station. Because messages between the electric vehicle and the charging station may be exchanged (e.g., for authenticating the electric vehicle, etc.) via a shared communication medium, it may be possible for malicious users to intercept legitimate communications, transmit counterfeit

messages, cause confusion at the charging station, and steal power intended for the electric vehicle. Traditional methods for authenticating broadcast messages transmitted by the electric vehicle rely on either the electric vehicle using a public key signature to sign each message or a key distributor providing a unique electric vehicle verification key to each of the charging stations over a secure connection. However, using a public key signature typically can require each charging station to perform expensive public key encryption/decryption operations to verify the authenticity of each received message. Also, distributing the electric vehicle verification key to each charging station can be costly in terms of the number of messages transmitted. Furthermore, the electric vehicle verification key may be transmitted to all the charging stations even though only a small subset of the charging stations may actually use the electric vehicle verification key to verify the messages from the electric vehicle.

[0046] In some embodiments, a broadcast authorization mechanism can be implemented in the charging facility to validate the electric vehicle and to ensure that the electric vehicle that transmitted a message is the same as the electric vehicle that is connected in the charging facility. In this embodiment, a key distributor and the charging stations of the charging facility can have a priori knowledge of a master key. The key distributor can determine a unique vehicle verification key for the electric vehicle based on a vehicle identifier (ID) and one or more other parameters (e.g., sequence number, timestamp, location, random number, etc.). The electric vehicle can sign messages (transmitted from the electric vehicle) using the vehicle verification key and can also provide the vehicle ID and the one or more other parameters (in the transmitted message). Based on the charging station's knowledge of the master key, the received vehicle ID, and the other received parameters, the charging station can derive the vehicle verification key and authenticate the received message. Such a broadcast authentication mechanism can enable secure communications between the electric vehicle and the charging stations, and can enable the charging stations to authenticate transmissions from the electric vehicle without expensive computations and without exchanging a large number of messages.

[0047] Additionally, whether an electric vehicle receives power at a charging facility may be contingent on two factors – 1) identification of the charging station that should provide power to the electric vehicle (“service matching”) and 2) authorization of a payment account (“account authorization”) associated with the electric vehicle (e.g., determining whether the electric vehicle can pay for the received power). Identifying the charging station may be a local decision.

However, authorizing the payment account may involve communicating with a remote account authorization unit (e.g., via the Internet) and this can incur communication latencies. Traditional authorization mechanisms are sequential where the charging station that should provide power to the electric vehicle is not identified until the payment account associated with the electric vehicle is authorized. Communication latencies and network latencies can result in the user of the electric vehicle having to wait for a significant amount of time between connecting the electric vehicle to the charging facility and the electric vehicle receiving power.

[0048] In some embodiments, a distributed authorization architecture can be implemented to minimize latency between the time instant when the electric vehicle connects to the charging facility and the time instant when the electric vehicle receives power. In accordance with the distributed authorization architecture, the service matching process and the account authorization process may be executed in parallel. In some embodiments, when the electric vehicle plugs into the charging facility, a local matching authorization unit can initiate the service matching process for the electric vehicle and can prompt a remote account authorization unit to initiate the account authorization process for the electric vehicle. The matching authorization unit can match the electric vehicle to one of the charging stations (“matched charging station”). Once the account authorization process is completed, the matching authorization unit can receive a service voucher (e.g., indicating whether the account was authorized, the type and amount of power that can be provided to the electric vehicle, etc.) from the account authorization unit. The matching authorization unit can provide the service voucher to the matched charging station and can cause the matched charging station to provide power to the electric vehicle in accordance with the service voucher. Such a distributed authorization architecture where the service matching process executes in parallel with the account authorization process can reduce the latency between the electric vehicle connecting to the charging facility and receiving electric power.

[0049] **Figure 1** is an example conceptual diagram of a broadcast authentication mechanism in a communication network 100. In Figure 1, the communication network 100 comprises an electric vehicle 102, a key distribution unit 104, and charging stations 110, 112, and 114. The electric vehicle 102 comprises a communication unit 103. The communication unit 103 can implement protocols and functionality to enable the electric vehicle 102 to communicate with the key distribution unit 104 and one or more of the charging stations 110, 112, and 114 in the communication network 100. The key distribution unit 104 comprises a key generation unit 106

and a transceiver unit 108. In some embodiments, the communication network 100 can be a shared communication network (e.g., a powerline communication (PLC) network). In other embodiments, the communication network 100 can be other suitable types of networks (e.g., Ethernet over Coax (EoC), wireless local area networks (WLAN), such as IEEE 802.11 networks, etc.). All the charging stations 110, 112, and 114 and the key distribution unit 104 may be trusted entities with respect to each other. The key distribution unit 104 and the charging stations 110, 112, and 114 can be communicatively coupled using wireless communication protocols (e.g., WLAN, Bluetooth, etc.) or using wired communication protocols (e.g., PLC, Ethernet, etc.).

[0050] At stage A, the electric vehicle 102 connects to the communication network 100 and provides security credentials to the key distribution unit 104. In some embodiments, the electric vehicle 102 (e.g., the communication unit 103) may transmit a vehicle identifier (ID). In other embodiments, the electric vehicle 102 may also provide other suitable security credentials (e.g. an X.509v3 certificate with public keys bound to the vehicle ID) to the key distribution unit 104. In some embodiments, as depicted in Figure 1, the key distribution unit 104 may be another network device (e.g., a managing network device or a coordinator device) that is distinct from the charging stations 110, 112, and 114. In another embodiment, one of the charging stations in the communication network 100 can be designated as the key distribution unit 104. As will be further described below, the key distribution unit 104 can use the vehicle ID and other suitable information to generate a signing key that can be used by the electric vehicle 102 for transmitting messages and by the charging stations for verifying the authenticity of messages received from the electric vehicle 102.

[0051] At stage B, the key distribution unit 104 establishes a secure communication link with the electric vehicle 102 after validating the security credentials received from the electric vehicle 102, as will be further described in blocks 204 – 208 of Figure 2.

[0052] At stage C, the key generation unit 106 generates a temporary sender signing key based, at least in part, on the received security credentials and a master key associated with the key distribution unit. For example, the key generation unit 106 can generate the temporary sender signing key based, at least in part, on the vehicle ID received at stage A and the master key. The master key may be known to the key generation unit 106 and to all the charging stations 110, 112, and 114 in the communication network 100. In one embodiment, the key

generation unit 106 can generate the master key and can distribute the master key to all the charging stations 110, 112, and 114 in the communication network 100. In another embodiment, one of the charging stations 110 can generate the master key and can distribute the master key to the key generation unit 106 and to the other charging stations 112 and 114. In another embodiment, a subset of the charging stations (which may or may not include the key generation unit 106) may generate the master key. In another embodiment, the master key may be predetermined and provided (e.g., input by a network administrator during an installation process, hardcoded during a manufacturing process, etc.) to the key generation unit 106 and to the charging stations 110, 112, and 114.

[0053] In some embodiments, the key generation unit 106 can use a keyed one-way hash function (H) to generate the temporary sender signing key. The key generation unit 106 can use the master key as a key for the hash function. The input to the hash function can be the security credentials associated with the electric vehicle 102 (e.g., vehicle ID). In some embodiments, the input to the hash function can be a concatenation (or another combination) of the vehicle ID and one or more other parameters (e.g., a sequence number, a timestamp, a random value, a location identifier, etc.). The key generation unit 106 may increment the sequence number each time the key generation unit 106 distributes a new temporary sender signing key to the electric vehicle 102. The timestamp may include a start time and an end time for which the temporary sender signing key is valid. Combining the vehicle ID with one or more other parameters (e.g., the sequence number, the timestamp, the random value, the location identifier, etc.) can prevent spoofing attacks. It should be noted that the temporary sender signing key is unique to the electric vehicle, so that the charging stations 110, 112, and 114 can uniquely associate the messages sent by a particular electric vehicle with that electric vehicle.

[0054] At stage D, the electric vehicle 102 uses the temporary sender signing key to sign messages scheduled to be transmitted to the charging stations 110, 112, 114. The messages transmitted to the charging stations 110, 112, and 114 can include the vehicle ID and the one or more other parameters that were used by the key generation unit 106 to generate the temporary sender signing key (e.g., the sequence number, the timestamp, the random value, the location identifier, etc.). The electric vehicle 102 may not transmit the temporary sender signing key to the charging stations 110, 112, and 114. The electric vehicle 102 (e.g., the communication unit 103) can sign the message using the temporary sender signing key to enable the charging stations

110, 112, and 114 to identify and validate the electric vehicle 102. For example, each message can comprise a message authentication code (MAC) that is based on the temporary sender signing key and the content of the message. It should be noted that in some embodiments, the electric vehicle 102 (e.g., the communication unit 103) can broadcast the messages to all the charging stations 110, 112, and 114, as depicted in Figure 1. In other embodiments, the electric vehicle 102 can broadcast the messages to one (or a subset) of the charging stations 110, 112, and 114.

[0055] At stage E, the charging station 110 can validate the message received from the electric vehicle 102 based, at least in part, on information in the received message and the master key. For example, the charging station 110 (and also the charging stations 112 and 114) can verify the message authentication code in the received message by performing the same operations as the key generation unit 106 (described in stage C) using the information provided by the electric vehicle 102 in the message (e.g., the vehicle ID, sequence number, the timestamp, the random value, the location identifier, etc.) and the master key known to the charging station 110. This can enable the charging station 110 to verify the signature in the received message without obtaining additional information from the key distribution unit 104.

[0056] **Figure 2** is a flow diagram (“flow”) 200 illustrating example operations of a key distribution unit executing the broadcast authentication mechanism. The flow begins at block 202.

[0057] At block 202, a key distribution unit of a communication network receives security credentials associated with a network device (“sender device”) that connects to the communication network. In one embodiment, the sender device can be a plug-in electric vehicle (PEV). With reference to the example of Figure 1, the electric vehicle 102 can connect to the communication network 100 that comprises one or more charging stations 110, 112, and 114 to receive electric power from one of the charging stations. The electric vehicle 102 can then provide its security credentials (e.g., a sender ID) to the key distribution unit 104. The key distribution unit 104 may be one of the charging stations or may be distinct from the charging stations. The flow continues at block 204.

[0058] At block 204, it is determined whether the security credentials received from the sender device are valid. For example, the key distribution unit 104 can determine whether the

security credentials received from the electric vehicle 102 are valid and whether the electric vehicle 102 can be authenticated. If the key distribution unit 104 determines that security credentials associated with the electric vehicle are valid, the flow continues at block 208. Otherwise, the flow continues at block 206.

[0059] At block 206, a communication channel is not established with the sender device if the security credentials associated with the electric vehicle are determined not to be valid. The flow 200 moves from block 204 to block 206 if the key distribution unit 104 is unable to authenticate the security credentials associated with the electric vehicle 102. In this instance, the key distribution unit 104 can determine not to establish a communication channel with the electric vehicle 102. If the key distribution unit 104 does not establish the communication channel with the electric vehicle 102, this can indicate that the electric vehicle 102 will not be permitted to receive power from any of the charging stations 110, 112, and 114 in the communication network 100. The key distribution unit 104 may also present a notification (e.g., audio, visual, and/or text notification) to the electric vehicle 102 indicating the inability to establish the communication channel with the electric vehicle 102. From block 206, the flow ends.

[0060] At block 208, a secure communication channel is established with the sender device if the security credentials associated with the electric vehicle are determined to be valid. The flow 200 moves from block 204 to block 208 after the key distribution unit 104 authenticates the security credentials associated with the electric vehicle 102. For example, the key distribution unit 104 can exchange one or more security handshake messages to establish the secure communication channel with the electric vehicle 102. As will be further described below, the key distribution unit 104 can exchange one or more messages with the electric vehicle 102 via the secure communication channel to generate a sender signing key that is unique to the electric vehicle 102. The electric vehicle 102 can then use the sender signing key to communicate with the charging stations 110, 112, and 114 in the communication network 100. The flow continues at block 210.

[0061] At block 210, a temporary sender signing key is generated based, at least in part, on the security credentials associated with the sender device and a master key associated with the key distribution unit. For example, the key generation unit 106 (of the key distribution unit 104) can generate the temporary sender signing key based, at least in part, on the sender ID received

at block 202 and the master key. As described above, the key generation unit 106 and the charging stations 110, 112, and 114 may have a priori knowledge of the master key. As described above at stage C of Figure 1, various embodiments can use employed to determine/provide the master key to the key generation unit 106 and the charging stations 110, 112, and 114. In some embodiments, the key generation unit 106 can use a keyed one-way hash function on the master key, the security credentials (sender ID) associated with the electric vehicle 102, and one or more other parameters (e.g., a sequence number, a timestamp, a random value, a location identifier, etc.) to generate the temporary sender signing key. Because the temporary sender signing key is unique to the electric vehicle 102, charging stations can uniquely associate the messages sent by a particular electric vehicle with that electric vehicle 102. The flow continues at block 212.

[0062] At block 212, the temporary sender signing key is transmitted to the sender device via the secure communication channel. For example, the key distribution unit 104 can transmit (e.g., via the transceiver unit 108) the temporary sender signing key to the electric vehicle 102 via the secure communication channel. In some embodiments, the key distribution unit 104 can also transmit the sequence number, the timestamp, the random value, the location identifier, and other parameters that were used to generate the temporary sender signing key. However, the key distribution unit 104 may not transmit the master key to the electric vehicle 102. As described above with reference to Figure 1, the electric vehicle 102 can use the temporary sender signing key to sign all messages that it broadcasts to the charging stations 110, 112, and 114 so that the charging station (that receives the messages) can easily verify the authenticity of the received messages. From block 212, the flow ends.

[0063] Although Figures 1 and 2 describe the key distribution unit 104 transmitting the temporary sender signing key to the sender device (e.g., the electric vehicle 102) via an insecure medium over which a secure communication channel has been established, embodiments are not so limited. In other embodiments, the key distribution unit 104 can use an alternate secure communication channel, or a secure, out-of-band means of transmitting the temporary sender signing key to the sender device 102 to minimize the possibility of interception. The key distribution unit 104 may transmit the temporary sender signing key to the sender device 102 via a different communication medium, a separate waveguide, or a different communication band that is less susceptible to interception. In other embodiments, the key distribution unit 104 can

use public key encryption techniques (or other suitable encryption techniques) to securely transmit the temporary sender signing key to the sender device 102.

[0064] Although stage D in Figure 1 describes the sender device (e.g., the electric vehicle 102) transmitting the message including the sender ID and the other parameters used to generate the temporary sender signing key (e.g., the sequence number, the timestamp, the random number, the location, etc.), embodiments are not so limited. In some embodiments, the size of the message transmitted by the sender device 102 may not be large enough to accommodate all the parameters that were used to generate the temporary sender signing key. In this embodiment, the sender device 102 can transmit the parameters that were used to generate the temporary sender signing key (e.g., the sender ID, the sequence number, the timestamp, the random number, the location, etc.) in one or more separate initialization messages. The sender device 102 may only include the sender ID and sequence number in subsequent messages (along with the message content). The receiver device (e.g., the charging station 110) can derive the temporary sender signing key unique to the sender device 102 from the information provided in the initialization messages. For each sender device 102, the receiver device 110 can store the derived temporary sender signing key, the sender ID, and the sequence number. The receiver device 110 can look up the previously derived temporary sender signing key based on the sender ID and sequence number received in subsequent messages. The inclusion of the sequence number in the subsequent messages can ensure that the temporary sender signing key associated with the sender device 102 is current (e.g., since the sequence number is incremented each time the sender device 102 receives a new temporary sender signing key).

[0065] In some embodiments, the sender device (e.g., the electric vehicle 102) can also transmit a message counter in each message to minimize the possibility of replay attacks. The sender device 102 can also use the message counter to compute the message authentication code associated with the message. The receiver device (e.g., the charging station 110) can receive messages from the sender device 102 and can store the most recently received message counter value. The receiver device 110 can discard any received messages with a message counter value that is less than or equal to the largest message counter value received in a verified message from the sender device 102. In some embodiments, if the message from the sender device 102 includes a timestamp value and an expiration time, then the receiver device 110 can discard

information about the temporary signing key (including the message counter, the sequence number, location, etc.) after the expiration time is reached.

[0066] In one example, the sender device 102 may be a plug-in electric vehicle (PEV) that connects to one of the charging stations (also known as an electric vehicle supply equipment or EVSE) in a charging facility. The PEV may connect to the charging station via a charging cable. The charging stations, the PEV, and the key distribution unit may be coupled via a powerline communication channel (or another suitable shared communication medium). Accordingly, multiple charging stations may receive the PEV's transmissions and may try to determine the identity of the PEV transmitting each message. In this example, the charging cable that connects the PEV and the charging station may have a control pilot line. The PEV and the charging station can exchange low-speed, secure communications via the control pilot line of the charging cable. In some embodiments, the key distribution unit 104 can provide the electric vehicle 102 with the temporary sender signing key via the control pilot line. Other communications can be conducted over the same control pilot line but in a different communication band, or over different lines (e.g., the power lines).

[0067] Although Figures 1 and 2 describe the key distribution unit 104 generating a temporary sender signing key based on a hash value of the sender ID and/or one or more other parameters (e.g., a sequence number, a location, a random number, a timestamp, etc.), embodiments are not so limited. In other embodiments, other suitable mechanisms can be used to generate the sender signing key. For example, the public key encryption methods can be used and the sender signing key may be a public encryption key. Furthermore, in some embodiments, the sender signing key may not be temporary. Instead, the sender signing key may be any suitable sender-specific key that is assigned to the sender device 102 when the sender device 102 connects to the communication network 100. The sender device 102 can then sign messages (prior to transmitting the messages) with the sender-specific key.

[0068] **Figure 3** is an example conceptual diagram of a distributed authentication mechanism in a communication network. In Figure 3, a local communication network 300 comprises an electric vehicle 302, a matching authorization unit 304, and charging stations 306, 308, and 310. The local communication network 300 is also coupled to an account authorization unit 312 which may be at a remote location (e.g., on another communication network). The electric vehicle 302 comprises a communication unit 303. The communication unit 303 can implement

protocols and functionality to enable the electric vehicle 302 to communicate with the matching authorization unit 304, the account authorization unit 312, and one or more of the charging stations 306, 308, and 310. In some embodiments, the local communication network 300 can be a shared communication network (e.g., a powerline communication network). All the charging stations 306, 308, and 310 and the matching authorization unit 304 may be trusted entities with respect to each other. The charging stations 306, 308, and 310 and the matching authorization unit 304 can be communicatively coupled using wireless communication protocols (e.g., WLAN, Bluetooth, etc.) or using wired communication protocols (e.g., PLC, Ethernet, etc.). The matching authorization unit 304 can perform three types of functions – 1) authenticating the electric vehicle 302 and providing the electric vehicle 302 with a signing key for secure communication, 2) executing a service matching process for determining which charging station should provide power to the electric vehicle 302, and 3) accepting authorization information from the account authorization unit 312 on behalf of the electric vehicle 302 and forwarding this authorization to the charging station that was matched with the electric vehicle 302. Furthermore, it is noted that in some embodiments, as depicted in Figure 3, the matching authorization unit 304 may be another network device (e.g., a managing network device or a coordinator device) that is distinct from the charging stations 306, 308, and 310. In another embodiment, one of the charging stations in the local communication network 300 can be designated as the matching authorization unit 304.

[0069] In some embodiments, after the electric vehicle 302 (e.g., a plug-in electric vehicle (PEV)) plugs into a charging facility (e.g., connects to a charging station or EVSE 306), a control pilot line transmission (CPLT) line associated with the electric vehicle 302 can be activated. The electric vehicle 302 (e.g., a PEV-EVSE matching protocol layer) can determine (e.g., via the CPLT line) that the CPLT line associated with the electric vehicle 302 is active. Additionally, the charging station 306 also can determine that an unmatched electric vehicle 302 is connected to the charging station 306 by detecting that the CPLT line associated with the electric vehicle 302 is activated. In some embodiments, the charging station 306 can transmit a notification to the matching authorization unit 304 indicating that an unmatched electric vehicle 302 is connected to the charging station 306. In some embodiments, the charging station 306 and the electric vehicle 302 can also exchange information needed for electric vehicle 302 to join the charging station's network. For example, the electric vehicle 302 could provide a vehicle identifier, information about supported communication protocols, etc. to the charging station

306. In one example, the charging station 306 can be associated with a powerline communication (PLC) network and can provide a charging station identifier, network information, supported PLC protocols (e.g., Green PHY, HomePlug AV, etc.), and other suitable information to enable the electric vehicle 302 to join the charging station's PLC network. After the electric vehicle 302 joins the charging station's network, the electric vehicle (e.g., upper protocol layers of the electric vehicle) can use dynamic host control protocol (DHCP) to determine IP addresses, router interfaces, domain name server (DNS) information, and other suitable information for communicating with the matching authorization unit 304 and the account authorization unit 312. As will be further described below in stages A – F, the electric vehicle 302 can communicate with the matching authorization unit 304 and the account authorization unit 312 in parallel to enable simultaneous service matching and account authorization.

[0070] At stage A, the electric vehicle 302 (e.g., the communication unit 303) provides security credentials to the matching authorization unit 304. In some embodiments, the electric vehicle 302 may transmit a customer ID. In other embodiments, the electric vehicle 302 may also provide other suitable security credentials bound to the customer ID (e.g. an X.509v3 certificate with public keys bound to the customer ID) to the matching authorization unit 304. In some embodiments, after the electric vehicle 302 connects to the network associated with the charging station 306, a PEV-EVSE matching protocol layer can prompt the upper protocol layers of the electric vehicle to communicate with the matching authorization unit 304. In one example, the electric vehicle 302 (e.g., PEV upper protocol layers) can use a known URL that references the matching authorization unit 304. In some embodiments, the URL used by the electric vehicle 302 to access the matching authorization unit 304 may be intercepted and locally redirected (to the matching authorization unit 304) by a network address translator or a local domain name server.

[0071] At stage B, the matching authorization unit 304 establishes a secure communication channel with the customer device (e.g., electric vehicle) 302 after validating the security credentials received from the electric vehicle 302. The matching authorization unit 304 can authenticate the electric vehicle 302 and establish a communication channel for securely communicating with the electric vehicle 302 based on the customer ID and other security

credentials associated with the electric vehicle 302 (e.g., a public encryption key, a X.509v3 certificate with public keys bound to the customer ID).

[0072] At stage C, the electric vehicle 302 (e.g., the communication unit 303) receives the information associated with the matching authorization unit 304 (“MAS information”) and provides the MAS information and the security credentials bound to the customer ID to the account authorization unit 312. In some embodiments, the MAS information provided by the matching authorization unit 304 can include MAS identity information, MAS location information, etc. The MAS identity information can be an identifier that is mapped to an IP address of the matching authorization unit 304. In some embodiments, the matching authorization unit 304 can also generate a temporary signing key that is unique to the electric vehicle 302 based, at least in part, on a secure hash of the customer ID, a master key, and one or more other parameters (e.g., a sequence number, a random number, a timestamp, etc.), as described above with reference to Figures 1 – 2. In addition to providing the MAS information to the electric vehicle 302, the matching authorization unit 304 may also provide the temporary signing key and the one or more parameters (except the master key) used for generating the temporary signing key to the electric vehicle 302, as described above in Figures 1 – 2. In this embodiment, the matching authorization unit 304 may comprise the key distribution unit 104 of Figure 1 for generating the temporary signing key as described above in Figures 1 – 2. Alternately, the matching authorization unit 304 may itself execute the functionality described above in Figures 1 – 2 for generating the temporary signing key associated with the electric vehicle 302. Alternately, the matching authorization unit 304 may access a distinct key distribution unit 104 and can request the key distribution unit 104 to generate the temporary signing key for the electric vehicle 302. The matching authorization unit 304 can then provide this temporary signing key to the electric vehicle 302. In other embodiments, the matching authorization unit 304 may not generate the temporary signing key but may instead use a public encryption key for secure communication with the electric vehicle 302.

[0073] In response to receiving the MAS information, the electric vehicle 302 (e.g., the communication unit 303) can initiate the account authorization process with the account authorization unit 312 by using a known URL that references the account authorization unit. In some embodiments, the electric vehicle (or “customer device”) 302 and the account authorization unit 312 can establish a secure communication channel using an X.509v3

certificate associated with the customer device 302. Additionally, the electric vehicle 302 can provide the customer ID and the MAS information to the account authorization unit 312 via the established secure communication channel. While the account authorization unit 312 is executing the account authorization process with the electric vehicle 302, the electric vehicle 302 can execute the service matching process with the matching authorization unit 304. In other words, as will be further discussed below, the account authorization process (e.g., for determining whether the payment account associated with the electric vehicle 302 has sufficient funds to pay for the electric power) can be performed in parallel with the service matching process (e.g., to identify the charging station that is best suited for providing the electric power to the electric vehicle 302). Since account authorization may not depend on which of the charging stations will provide electric power to the electric vehicle 302, the account authorization process can be executed in parallel with the service matching process. This can reduce latency between the electric vehicle 302 joining the local communication network 300 and receiving the electric power from the charging station.

[0074] At stage D, the matching authorization unit 304 executes the service matching process and matches the electric vehicle 302 with a charging station 306 in the local communication network 300. As described above, the account authorization unit 312 may be remote and communication between the account authorization unit 312 and the matching authorization unit 304 may incur long latencies. The service matching process may be executed locally, and therefore the matching authorization unit 304 may initiate the service matching process without account authorization (e.g., before the account authorization unit 312 determines whether the payment account has sufficient funds to pay for the services). Initiating the service matching process before account authorization process is completed can reduce latency between the electric vehicle 302 connecting to the network and receiving the electric power.

[0075] In some embodiments, as part of the service matching process, the matching authorization unit 304 may cause the electric vehicle 302 (e.g., the communication unit 303) to execute a signal level attenuation characteristics (SLAC) protocol with the local charging stations 306, 308, and 310. To enable the electric vehicle 302 to execute the SLAC protocol, the matching authorization unit 304 can transmit one or more SLAC parameters to the electric vehicle 302 (e.g., along with the MAS information at stage C). The SLAC parameters can indicate a number of service matching messages (e.g., sound tones) that should be transmitted to

the local charging stations 306, 308, and 310, and a timeout interval for executing the SLAC protocol. The number of service matching messages may be determined based on a number of cables associated with the charging stations, a number of cable harnesses, a maximum number of switch states associated with the charging stations, the type of charging stations, the type of electric vehicle, local noise, and other such factors. In some embodiments, the number of service matching messages (as indicated by the matching authorization unit 304) can also take into consideration that some service matching messages may not be detected or missed. In some embodiments, the timeout interval for executing the SLAC protocol can be determined based, at least in part, on a number of electric vehicles in the local communication network 300, noise levels detected at the charging stations, cable configurations of the charging stations, etc. The matching authorization unit 304 can start a timer based on the timeout interval for SLAC protocol. In some embodiments, when the electric vehicle 302 receives the SLAC parameters from the matching authorization unit 304, the electric vehicle 302 can initiate operations for executing the SLAC protocol (i.e., without waiting for account authorization from the account authorization unit 312). The electric vehicle 302 can transmit one or more initialization messages (e.g., using multi-network broadcast communications (MNBC)) to indicate that operations for the SLAC protocol will begin. These initialization messages can also include the timeout interval and the number of service matching messages that will be transmitted in accordance with the SLAC protocol. The electric vehicle 302 can transmit the service matching messages using multi-network broadcast communications. In some embodiments, if the matching authorization unit 304 generated a unique signing key for the electric vehicle 302 (in accordance with the operations of Figures 1 – 2), the service matching messages can include a message authentication code that is generated based on a one-way hash of the message content, the signing key, a sequence number, and a message counter. The value of the message counter may be decremented as each service matching message is transmitted. Each service matching message can also include the customer ID, the sequence number, the message counter, and other parameters that were used to generate the signing key. It should be noted that, in other embodiments, the service matching messages may be signed using a key based on a public certificate, or another suitable vehicle-specific key. In some embodiments, after the electric vehicle 302 transmits a first service matching message, the electric vehicle 302 may wait for a predetermined time interval before transmitting a second service matching message.

[0076] Each charging station 306 that receives the service matching message can determine signal level information (or attenuation information) based on the received service matching message and a time instant at which the service matching message was received (e.g., a receive timestamp). In some embodiments, only the charging stations 306 that are not currently matched with another electric vehicle may process the received service matching messages. The charging station 306 can use the information received in the service matching message in conjunction with the master key to derive the signing key associated with the electric vehicle 302. The charging station 306 can then use the signing key to authenticate the received service matching messages. After the last service matching message is received (or after the timeout interval expires), the charging station 306 can provide SLAC results for each authenticated service matching message (e.g., the signal level information, the attenuation information, the receive timestamp, etc.) to the matching authorization unit 304. After the matching authorization unit 304 receives the SLAC results from all the charging stations (or after the timeout interval elapses), the matching authorization unit 304 selects one of the charging stations with the best performance to provide electric power to the customer device 302. For example, the matching authorization unit 304 may analyze the SLAC results and may determine that the charging station 306 that received the service matching message with the highest signal level should provide electric power to the electric vehicle 302. As another example, the matching authorization unit 304 may determine that the charging station 306 that received the service matching message with the smallest latency should provide electric power to the electric vehicle 302. However, in some implementations, the matching authorization unit 304 may not notify the charging station 306 of the results of the service matching process until the account authorization process is completed and the payment account associated with the electric vehicle 302 has been authorized.

[0077] At stage E, the account authorization unit 312 completes the account authorization process and securely transmits a service voucher for the authorized services from one of the charging stations. The account authorization process can comprise operations for authenticating a customer account (e.g., a payment account) associated with the electric vehicle 302 (e.g., for which a user of the electric vehicle 302 has appropriate access permissions). The account authorization unit 312 can verify the account associated with the electric vehicle 302 based on the customer ID and other security credentials associated with the electric vehicle (e.g., an X.509v3 certificate with public keys bound to the customer ID). As part of the account authorization process, it may also be determined whether the payment account associated with

the electric vehicle 302 has sufficient funds to provide compensation for the electric power that will be provided by one of the charging stations. After completing the account authorization process, the account authorization unit 312 can transmit (to the matching authorization unit 304) a service voucher including the results of the account authorization process.

[0078] The service voucher generated by the account authorization unit 312 can indicate whether the electric vehicle 302 has the appropriate authorization to receive the electric power, according the account characteristics and the permissions. The service voucher can also indicate limitations on the service (e.g., how much electric power, etc.) that can be provided by the charging station based on characteristics and state of the account, characteristics of the charging station, characteristics of the electric vehicle 302, and the permissions associated with the account. The service voucher may also comprise the customer ID associated with the electric vehicle 302. In some embodiments, the service voucher can indicate a deadline by which the service matching process should be completed. The service voucher may expire (and the electric vehicle 302 may no longer be able to receive power/services) after this deadline elapses. In some embodiments, the service voucher may also include an authorized maximum amount of time, money, energy. For example, the service voucher may indicate that 100kWh of power should be provided to the electric vehicle 302, that an amount of electric power equivalent to \$10 should be provided to the electric vehicle 302, etc.

[0079] At stage F, the matching authorization unit 304 securely transmits the service voucher to the matched charging station 306. The matching authorization unit 304 can securely transmit the service voucher (or another suitable indication of electric vehicle authorization) to the matched charging station 306 when the matching authorization unit 304 has the service voucher for the electric vehicle 302 (received at stage E after the account authorization process is completed) and knowledge of the matched charging station 306 (after completing the service matching process at stage D). Additionally, the matching authorization unit 304 may also transmit a notification to the electric vehicle 302 identifying the matched charging station 306 that will provide the electric power.

[0080] At stage G, the matched charging station 306 provides the authorized amount of electric power to the electric vehicle 302 in accordance with the service voucher. For example, the matched charging station 306 can close one or more power relays and provide the authorized amount of power to the electric vehicle 302. In some embodiments, the matched charging

station 306 can also provide a notification to the matching authorization unit 304 to indicate that power is being provided to the electric vehicle 302. In some embodiments, after the electric vehicle 302 detects receipt of power from the matched charging station 306, the electric vehicle 302 can transmit an acknowledgement message to the matched charging station 306. In some embodiments, if the matched charging station 306 does not receive an acknowledgement within a predetermined acknowledgment time interval, the matched charging station 306 can suspend power transfer to the electric vehicle 302 and can notify the matching authorization unit 304 of a potential error. After receiving the acknowledgement, the matched charging station 306 and/or the electric vehicle 302 may present one or more audio/visual notifications (e.g., a charging light, a beeping sound, etc.) to notify the user that the service is being provided to the electric vehicle 302 (e.g., that electric vehicle 302 is being charged). The charging station 306 can enforce the limitations (if any) specified in the service voucher and can provide power to the electric vehicle 302 in accordance with the service voucher. The received service voucher can indicate, to the matched charging station 306, that the owner of the electric vehicle 302 will provide compensation for authorized services (indicated in the service voucher) provided by the charging station 306.

[0081] In some embodiments, as described above, if the matched charging station 306 does not receive an acknowledgement from the electric vehicle 302 within a predetermined time interval (after the matched charging station 306 starts providing power), the matched charging station 306 can stop providing power to the electric vehicle 302. In other embodiments, the matched charging station 306 can stop providing power to the electric vehicle 302 if the matched charging station 306 detects that the electric vehicle 302 was unplugged. In another embodiment, the matched charging station 306 can stop providing power to the electric vehicle 302 if the matched charging station 306 detects that an authorized limit (specified in the service voucher) was reached. In another embodiment, the matched charging station 306 can stop providing power to the electric vehicle 302 in response to the electric vehicle 302 requesting power termination.

[0082] It should be understood that although Figure 3 describes the matching authorization unit 304 as a single entity that authenticates the electric vehicle 302, determines a charging station 306 should provide the electric vehicle 302 with power, and forwards authorization information received from account authorization unit 312 to the matched charging station 306,

embodiments are not so limited. In other embodiments, the matching authorization unit 304 can be implemented in a distributed format. For example, the matching authorization unit 304 can include three (or more) distinct sub-units each of which execute one function of the matching authorization unit 304. For example, the first sub-unit can authenticate the electric vehicle 302 and provide the electric vehicle 302 with the MAS information and/or a signing key. The second sub-unit can determine, during the service matching process, which charging station 306 should provide power to the electric vehicle 302. The third sub-unit can accept authorization information from the account authorization unit 312 on behalf of the electric vehicle 302 and forward this authorization to the charging station 306 that was matched with the electric vehicle 302.

[0083] In some embodiments, as described in Figure 3, the matching authorization unit 304 can determine which charging station should be matched with the electric vehicle 302. However, in other embodiments, some/all of the charging stations can determine (in a distributed manner) which charging station should be matched with the electric vehicle 302. For example, in response to receiving the service matching messages from the electric vehicle 302, the charging stations 306, 308, and 310 can determine the signal/attenuation level and communicate this information to a designated charging station 310. The designated charging station 310 can determine which of the charging stations 306, 308, or 310 should be matched with the electric vehicle 302.

[0084] In some embodiments, as described with reference to Figure 3, the service voucher indicating account authorization can be provided to the matching authorization unit 304. Providing the service voucher to the matching authorization unit 304 (instead of waiting until the appropriate charging station is identified) can minimize delay and can ensure that the electric vehicle 302 receives the service (if authorized) as soon as possible. In other embodiments, however, the service voucher indicating account authorization can be provided to another suitable designated device (e.g., a predetermined charging station). In other embodiments, the service voucher indicating account authorization can be provided directly to the electric vehicle 302. In this embodiment, the matching authorization unit 304 may also provide a notification of the matched charging station to the electric vehicle 302. The electric vehicle 302 may then transmit the service voucher to the matched charging station.

[0085] **Figure 4** is a flow diagram 400 illustrating example operations of a matching authorization unit in a distributed client authentication and service authorization environment. The flow begins at block 402.

[0086] At block 402, a matching authorization unit of a local communication network receives security credentials associated with a customer device that connects to the local communication network. With reference to the example of Figure 3, the customer device can be an electric vehicle 302 (e.g., a plug-in electric vehicle (PEV)). The customer device 302 can connect to the local communication network 300 that comprises one or more local service providers (e.g., the charging stations 306, 308, and 310) to receive power from one of the charging stations. The customer device 302 can then provide its security credentials (e.g., a customer ID) to the matching authorization unit 304. In some embodiments, one of the local service providers 310 in the local communication network 300 can be designated as the matching authorization unit 304. In another embodiment, the matching authorization unit 304 may be another network device that is distinct from the local service providers 306, 308, and 310. The flow continues at block 404.

[0087] At block 404, it is determined whether the security credentials received from the customer device are valid. For example, the matching authorization unit 304 can determine whether the security credentials received from the electric vehicle 302 are valid and whether the electric vehicle 302 can be authenticated. If the matching authorization unit 304 determines that security credentials associated with the customer device are valid, the flow continues at block 408. Otherwise, the flow continues at block 406.

[0088] At block 406, a communication channel is not established with the customer device if the security credentials received from the customer device are determined not to be valid. For example, the flow 400 moves from block 404 to block 406 if the matching authorization unit 304 is unable to authenticate the security credentials associated with the electric vehicle 302. As described above with reference to block 206 of Figure 2, the matching authorization unit 304 can determine not to establish a communication link with the electric vehicle 302 and can prevent the electric vehicle 302 from receiving power from any of the charging stations 306, 308, and 310. From block 406, the flow ends.

[0089] At block 408, a secure communication channel is established with the customer device if the security credentials received from the customer device are determined to be valid. The flow 400 moves from block 404 to block 408 after the matching authorization unit 304 authenticates the security credentials associated with the customer device. For example, as described above with reference to block 208 of Figure 2, the matching authorization unit 304 can establish a secure communication channel with the electric vehicle 302. The flow continues at block 410.

[0090] At block 410, information associated with the matching authorization unit (“MAS information”) is provided to the customer device. For example, the matching authorization unit 304 can transmit the MAS information (e.g., identity, location, etc.) to the customer device 302. In some embodiments, the matching authorization unit 304 may execute operations that are similar to the key distribution unit 104 of Figures 1 – 2 to determine the signing key unique to the customer device 302. For example, the matching authorization unit 304 and the local service providers (e.g., the charging stations) may have a priori knowledge of a secret master key. In this embodiment, the matching authorization unit 304 can generate a temporary signing key based on the master key, the customer ID and one or more suitable parameters (e.g., a sequence number, a timestamp, a random number, a location, etc.). Any messages transmitted by the customer device 302 can be signed using this temporary signing key for identification of the customer device 302. In another embodiment, the matching authorization unit 304, the customer device 302, and the local service providers 306, 308, 310 can use public key encryption to exchange messages during the local service matching process. For example, the customer device 302 can connect to the local communication network 300 and provide its public certificate to all the local service providers 306, 308, 310 and to the matching authorization unit 304. The customer device 302 can use a key based on the public certificate to sign all messages transmitted by the customer device 302. The matching authorization unit 304 (and the local service providers 306, 308, 310) can validate the received message based on this key. The flow continues at block 412.

[0091] At block 412, the matching authorization unit initiates a service matching process with the customer device. As described above with reference to stage D of Figure 3, the matching authorization unit 304 can execute the service matching process in conjunction with

the customer device 302 and the local service providers 306, 308, and 310. The flow continues at block 414.

[0092] At block 414, the customer device is matched to one of the local service providers. In other words, after the service matching process is completed, the matching authorization unit 304 identifies one of the local service providers 306 that should provide services to the customer device 302. The matching authorization unit 304 may identify the matched local service provider based on availability of local service providers, proximity of the local service providers to the customer device, compatibility of the local service providers with the customer device, etc. In one example, after the matching process is completed, the matching authorization unit 304 identifies one of the charging stations 306 that is matched to the electric vehicle 302 and that will provide power to the electric vehicle 302. The flow continues at block 416.

[0093] At block 416, a service voucher that indicates authentication of a payment account associated with the customer device is received from an account authorization unit. For example, after the account authorization unit 312 of Figure 3 completes the account authorization process (using the MAS information and the security credentials associated with the customer device 302), the account authorization unit 312 can securely transmit the service voucher to the matching authorization unit 304. The service voucher can indicate an account balance available to the customer device 302 and authorized services that can be provided by the charging stations. In some embodiments, the service voucher may be a notification from the account authorization unit 312 that indicates that the payment account associated with the customer device 302 comprises sufficient funds to pay for the service. The flow continues at block 418.

[0094] At block 418, the service voucher is provided to the matched local service provider to cause the matched local service provider to provide a service to the customer device. The matching authorization unit 304 can securely transmit the service voucher to the matched local service provider 306 when the matching authorization unit 304 has the service voucher for the customer device 302 (received at block 416 after the account authorization process is completed) and knowledge of the matched local service provider 306 (after completing the service matching process at block 414). The service voucher can also indicate limitations on the service that can be provided, based on characteristics and state of the payment account, characteristics of the local service provider, characteristics of the customer device, and permissions the customer has

for the account. As described above with reference to Figure 3, after the matched local service provider 306 receives the service voucher, the matched local service provider 306 can provide the service (e.g., an authorized amount of power) to the customer device 302 in accordance with the received service voucher. From block 418, the flow ends.

[0095] In some embodiments, in addition to providing the service voucher to the matched charging station 306, the matching authorization unit 304 can also cause the matched charging station 306 to close its power relays on an appropriate power cable and to provide power to the electric vehicle 302. The matching authorization unit 304 can receive an acknowledgement message from the electric vehicle 302 after the matched charging station 306 begins providing power to the electric vehicle 302. The matching authorization unit 304 can forward the acknowledgement message received from the electric vehicle 302 to the matched charging station 306. Furthermore, it is noted that if the account authorization unit 312 indicates to the matching authorization unit 304 that the account associated with the electric vehicle 302 is not valid (e.g., that the account does not have sufficient funds), the matching authorization unit 304 can notify the matched charging station 306 to not provide power to the electric vehicle 302. The matching authorization unit 304 may also prompt the electric vehicle 302 to disconnect from the local communication network 300. In some embodiments, if the matching authorization unit 304 receives a notification from the charging station 306 that the electric vehicle 302 is no longer in the local communication network 300, the matching authorization unit 304 can forward this notification to the account authorization unit 312.

[0096] **Figure 5** is a flow diagram 500 illustrating example operations of a customer device in a distributed client authentication and service authorization environment. The flow 500 begins at block 502.

[0097] At block 502, a customer device connects to a communication network and transmits security credentials to a matching authorization unit of the communication network. In one embodiment, the customer device can be an electric vehicle. As described above in Figure 3, the electric vehicle 302 can detect activity on a pilot line after connecting to a charging station of a charging facility (e.g., the local communication network 300). In some embodiments, after detecting that the pilot line is activated, the electric vehicle 302 (e.g., a communication unit 303 of the electric vehicle 302) can transmit “join request” messages on the communication network. The electric vehicle 302 can receive a “join confirmation” message from one of the charging

stations in the communication network. In response to receiving the “join confirmation” message from a charging station, the electric vehicle can join a network associated with that charging station. In some embodiments, the customer device 302 can then transmit identification information (e.g., a customer ID), an X.509v3 certificate with public keys bound to the customer ID, etc. to the matching authorization unit 304 of the local communication network 300. The flow continues at block 504.

[0098] At block 504, a secure communication channel is established with the matching authorization unit. For example, after the customer device 302 transmits its security credentials to the matching authorization unit 304, the matching authorization unit 304 can authenticate the customer device 302 and can establish the secure communication channel with the customer device 302. In some embodiments, the secure communication link can be established using an X.509v3 certificate that includes an identifier of the customer device 302. The flow continues at block 506.

[0099] At block 506, information for conducting the matching service process and the account authorization process in parallel are received from the matching authorization unit. For example, in one embodiment, the customer device 302 (e.g., the communication unit) can receive a unique signing key (generated by the matching authorization unit 304 as described above in Figures 1 – 4) and other parameters that were used for generating the signing key. Additionally, the electric vehicle may also receive MAS information (e.g., an identifier or location of the matching authorization unit 304). The customer device 302 may also receive one or more SLAC parameters (e.g., a number of service matching messages that should be transmitted to each local service provider, a maximum time interval for conducting the service matching process, etc.) to enable the customer device 302 to execute the service matching process in conjunction with the matching authorization unit 304. The flow continues at block 508.

[00100] At block 508, a secure communication channel is established with the account authorization unit and account authorization is requested. For example, the customer device 302 (e.g., the communication unit) can transmit its customer ID and the MAS information to the account authorization unit 312. As described above in Figure 3, the account authorization unit 312 can authenticate the customer device 302 and can establish the secure communication channel with the customer device 302. In some embodiments, the secure communication

channel can be established using an X.509v3 certificate that includes an identifier of the customer device 302. The customer device 302 can also request that the account associated with the customer device 302 be authorized and that the authorization results be provided to the matching authorization unit 304. The flow continues at block 510.

[00101] At block 510, while the account authorization process is ongoing, the matching service process is conducted with the local service providers and the matching authorization unit. As described above in Figure 3, the customer device 302 (e.g., the communication unit 303) can transmit one or more service matching messages to each of the local service providers 306, 308, and 310 in the local communication network 300. In some embodiments, the customer device 302 can sign each service matching message with the signing key (or another suitable key) received at block 506 and can also provide one or more parameters (if necessary) that were used to generate the signing key. As described above with reference to Figures 3 – 4, the matching authorization unit 304 can analyze signal/attenuation information received from the local service providers (based on the service matching messages) and can identify one of the local service providers that should provide service to the customer device. The flow continues at block 512.

[00102] At block 512, it is detected that service is provided by a local service provider. For example, the electric vehicle 302 (e.g., the communication unit) can detect that power is being provided by one of the charging stations 306. The flow continues at block 514.

[00103] At block 514, an acknowledgement for the received service is transmitted. For example, the electric vehicle 302 (e.g., the communication unit 303) can transmit the acknowledgement for the received power (e.g., to the local service provider 306 and/or to the matching authorization unit 304). From block 514, the flow ends.

[00104] It should be understood that Figures 1 – 5 are examples meant to aid in understanding embodiments and should not be used to limit embodiments or limit scope of the claims. Embodiments may comprise additional circuit components, different circuit components, and/or may perform additional operations, fewer operations, operations in a different order, operations in parallel, and some operations differently. In some embodiments, in order for the account authorization process to execute in parallel with the service matching process, it may be required that the customer device 302 identified in the service matching process be inextricably bound to the customer device 302 identified in the account authorization process. In this embodiment, a

unique customer ID that is bound to a public key in a public key certificate (e.g., X.509v3), signed by a trusted certificate authority (CA) can be used for customer identity binding. The customer ID in a certificate used by the customer device 302 in the service matching process (e.g., to obtain the signing key, the MAS information, etc.) can be compared against the customer ID used by the customer device to obtain account authorization from the account authorization unit 312, to ensure that they are identical.

[00105] It is also noted that although examples refer to simultaneous client authentication and account authorization in an electric vehicle charging environment, embodiments are not so limited. In other embodiments, the operations described herein for simultaneous client authentication and account authorization can be extended to other suitable operating environments (e.g., gaming environments).

[00106] As will be appreciated by one skilled in the art, aspects of the present inventive subject matter may be embodied as a system, method, or computer program product. Accordingly, aspects of the present inventive subject matter may take the form of an entirely hardware embodiment, a software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a “circuit,” “module” or “system.” Furthermore, aspects of the present inventive subject matter may take the form of a computer program product embodied in one or more computer readable medium(s) having computer readable program code embodied thereon.

[00107] Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage

medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

[00108] A computer readable signal medium may include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal may take any of a variety of forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A computer readable signal medium may be any computer readable medium that is not a computer readable storage medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device.

[00109] Program code embodied on a computer readable medium may be transmitted using any appropriate medium, including but not limited to wireless, wireline, optical fiber cable, RF, etc., or any suitable combination of the foregoing.

[00110] Computer program code for carrying out operations for aspects of the present inventive subject matter may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

[00111] Aspects of the present inventive subject matter are described with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the inventive subject matter. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data

processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[00112] These computer program instructions may also be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

[00113] The computer program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[00114] **Figure 6** is a block diagram of one embodiment of an electronic device 600 including a broadcast authentication and service matching mechanism in a communication network. In some implementations, the communication network may be a public charging facility and the electronic device 600 may be a charging station or another suitable coordinator unit in the charging facility. In other implementations, the electronic device 600 may be a desktop computer, a workstation, a server computer, or other electronic systems with wired communication capabilities (e.g., powerline communication capabilities) and/or wireless communication capabilities (e.g., WLAN communication capabilities). The electronic device 600 includes a processor unit 602 (possibly including multiple processors, multiple cores, multiple nodes, and/or implementing multi-threading, etc.). The electronic device 600 includes a memory unit 606. The memory unit 606 may be system memory (e.g., one or more of cache, SRAM, DRAM, zero capacitor RAM, Twin Transistor RAM, eDRAM, EDO RAM, DDR RAM, EEPROM, NRAM, RRAM, SONOS, PRAM, etc.) or any one or more of the above already described possible realizations of machine-readable media. The electronic device 600 also includes a bus 610 (e.g., PCI, ISA, PCI-Express, HyperTransport®, InfiniBand®, NuBus, AHB, AXI, etc.), and network interfaces 604 that include at least one of a wireless network interface (e.g., a Bluetooth interface, a WLAN 802.11 interface, a WiMAX interface, a ZigBee®

interface, a Wireless USB interface, etc.) and a wired network interface (e.g., an Ethernet interface, a powerline communication interface, etc.).

[00115] The electronic device 600 also includes a coordinator unit 608. The coordinator unit 608 comprises a key distribution unit 612 and a matching authorization unit 614. The key distribution unit 612 can execute operations described above with reference to Figures 1 – 2 to generate a signing key for a sender device (e.g., an electric vehicle) for easier verification of messages transmitted by the sender device. The matching authorization unit 614 can execute operations described above with reference to Figures 3 – 4 to A) authenticate a customer device (e.g., an electric vehicle), B) provide the customer device with information to enable the customer device 302 to execute the service matching process and the account authorization process in parallel, C) execute the service matching process for determining which service provider should service the customer device, D) accept authorization information from a remote account authorization unit on behalf of the customer device, and E) forward this authorization to the local service provider that was matched with the customer device. It is noted that although Figure 6 depicts the coordinator unit 608 as comprising both the key distribution unit 612 and the matching authorization unit 614, embodiments are not so limited. In other embodiments, the coordinator unit 608 may only comprise the key distribution unit 612 that is configured to execute operations described above in Figures 1 – 2 for broadcast authorization of the sender device. In other embodiments, the coordinator unit 608 may comprise the matching authorization unit 614 that is configured to execute functionality described above in Figures 3 – 4. In this embodiment, the matching authorization unit 614 may or may not execute the functionality of the key distribution unit 612.

[00116] Any one of these functionalities may be partially (or entirely) implemented in hardware and/or on the processor unit 602. For example, the functionality may be implemented with an application specific integrated circuit, in logic implemented in the processor unit 602, in a co-processor on a peripheral device or card, etc. Further, realizations may include fewer or additional components not illustrated in Figure 6 (e.g., video cards, audio cards, additional network interfaces, peripheral devices, etc.). The processor unit 602, the memory unit 606, and the network interfaces 604 are coupled to the bus 610. Although illustrated as being coupled to the bus 610, the memory unit 606 may be coupled to the processor unit 602.

[00117] While the embodiments are described with reference to various implementations and exploitations, it will be understood that these embodiments are illustrative and that the scope of the inventive subject matter is not limited to them. In general, a mechanism for secure client authentication and service authorization in a shared communication network as described herein may be implemented with facilities consistent with any hardware system or hardware systems. Many variations, modifications, additions, and improvements are possible.

[00118] Plural instances may be provided for components, operations, or structures described herein as a single instance. Finally, boundaries between various components, operations, and data stores are somewhat arbitrary, and particular operations are illustrated in the context of specific illustrative configurations. Other allocations of functionality are envisioned and may fall within the scope of the inventive subject matter. In general, structures and functionality presented as separate components in the exemplary configurations may be implemented as a combined structure or component. Similarly, structures and functionality presented as a single component may be implemented as separate components. These and other variations, modifications, additions, and improvements may fall within the scope of the inventive subject matter.

CLAIMS

1. A method comprising:
 - establishing a secure communication channel between a client network device and a managing network device of a communication network based, at least in part, on a client identifier of the client network device;
 - causing the client network device to perform an account authorization process with an accounting network device in parallel with a service matching process with the managing network device and one or more of a plurality of service providers of the communication network;
 - securely matching the client network device with a first of the plurality of service providers;
 - securely receiving a service voucher at the managing network device from the accounting network device authorizing one or more of the service providers of the communication network to service the client network device in response to the accounting network device executing the account authorizing process with the client network device; and
 - securely transmitting the service voucher from the managing network device to the matching service provider to allow the client network device to be serviced by the matching service provider.
2. The method of claim 1, wherein said securely matching the client network device with the first of the plurality of service providers further comprises:
 - generating, at the managing network device, a client key that is unique to the client network device based, at least in part, on the client identifier and on a master key known to the managing network device and the plurality of service providers of the communication network;
 - providing the client key from the managing network device to the client network device via the secure communication channel to allow the client network device to securely communicate with the plurality of service providers of the communication network;

- receiving, from each of the plurality of service providers, a message that indicates a signal level detected at the service provider in response to a service matching message from the client network device; and
- selecting the first of the plurality of service providers that detected the highest signal level as the matching service provider for the client network device.
3. The method of claim 2, further comprising:
transmitting, from the managing network device to the client network device, a number of service matching messages that should be transmitted from the client network device to the plurality of service providers.
 4. The method of claim 2, wherein the client key is a temporary key and is generated based, at least in part, on the master key, the client identifier, and one or more of a sequence number, a random number, a start/end timestamp, a lifetime duration, a message counter, and/or a location identifier.
 5. The method of claim 2, wherein the client key is a public encryption key.
 6. The method of claim 1, wherein the client identifier is authenticated by the managing network device and by the accounting network device, and the service voucher is bound to the client identifier.
 7. The method of claim 1, wherein the managing network device is one of the plurality of service providers.
 8. The method of claim 7, further comprising:
determining, at the managing network device, a message counter value from a message received from the client network device;
comparing the received message counter value with a previously received message counter value from the client network device;
discarding the received message if the received message counter value is less than or equal to the previously received message counter value; and
processing the received message if the received message counter value is greater than the previously received message counter value.

9. The method of claim 1, wherein the client network device comprises a plug-in electric vehicle, the plurality of service providers comprise a plurality of electric charging stations, the managing network device comprises a managing system associated with the plurality of electric charging stations, and the accounting network device comprises a remote account authorization server for one or more client accounts.
10. The method of claim 1, further comprising:
determining, at the managing network device, a first value of the client identifier associated with the client network device, wherein the first value of the client identifier was used for executing the service matching process;
determining a second value of the client identifier associated with the client network device, wherein the second value was used for executing the account authorization process;
determining whether the first value of the client identifier matches the second value of the client identifier;
in response to determining that the first value of the client identifier matches the second value of the client identifier, said securely transmitting the service voucher from the managing network device to the matching service provider to allow the client network device to be serviced by the matching service provider;
in response to determining that the first value of the client identifier does not match the second value of the client identifier, preventing the matching service provider from servicing the client network device.
11. A method comprising:
establishing, at a client network device, a secure communication channel with a managing network device of a communication network based, at least in part, on a client identifier of the client network device;
receiving, from the managing network device, identification information associated with the managing network device via the secure communication channel;
providing the client identifier and the identification information associated with the managing network device to an accounting network device to cause the accounting network device to execute an account authorization process with the client network device;

in parallel with the account authorization process, executing a service matching process with the managing network device and one or more of a plurality of service providers of the communication network;
detecting receipt of service from a first of the plurality of service providers of the communication network after completion of the account authorization process and the service matching process; and
transmitting an acknowledgement message to one of the managing network device and the first of the plurality of service providers in response to said detecting receipt of service from the first of the plurality of service providers of the communication network.

12. The method of claim 11, wherein the identification information associated with the managing network device comprises a device identifier of the managing network device and a location of the managing network device.
13. The method of claim 11, wherein said receiving, from the managing network device, identification information associated with the managing network device further comprises:
receiving, from the managing network device, one or more service matching parameters to cause the client network device to initiate the service matching process with the managing network device and the plurality of service providers of the communication network.
14. The method of claim 11, further comprising:
receiving, from the managing network device, a client key that is unique to the client network device, via the secure communication channel, wherein the client key enables the client network device to securely communicate with the plurality of service providers of the communication network;
receiving client key generation parameters based on which the client key was determined, wherein the client key generation parameters comprise one or more of a sequence number, a random number, a start/end timestamp, a lifetime duration, a message counter, and a location identifier;

wherein said executing the service matching process with the managing network device and one or more of a plurality of service providers of the communication network comprises:

signing one or more service matching messages using the client key; and
transmitting the one or more service matching messages and the client key generation parameters to the plurality of service providers.

15. The method of claim 14, wherein said transmitting the one or more service matching messages and the client key generation parameters to the plurality of service providers comprises:

determining whether a length of the service matching message scheduled to be transmitted to the plurality of service providers is greater than a predetermined threshold message length;

in response to determining that the length of the service matching message is greater than the predetermined threshold message length,

transmitting an initialization message including the client key generation parameters to the plurality of service providers; and

transmitting the client identifier and the sequence number in the one or more service matching messages; and

in response to determining that the length of the service matching message is less than the predetermined threshold message length,

transmitting the client key generation parameters as part of the one or more service matching messages.

16. A managing network device comprising:

a network interface; and

a matching authorization unit coupled with the network interface, the matching authorization unit operable to:

establish a secure communication channel between a client network device and the managing network device of a communication network based, at least in part, on a client identifier of the client network device;

cause the client network device to perform an account authorization process with an accounting network device in parallel with a service matching process

- with the managing network device and one or more of a plurality of service providers of the communication network;
- securely match the client network device with a first of the plurality of service providers;
- securely receive a service voucher from the accounting network device authorizing one or more of the service providers of the communication network to service the client network device in response to the accounting network device executing the account authorizing process with the client network device; and
- securely transmit the service voucher to the matching service provider to allow the client network device to be serviced by the matching service provider.
17. The managing network device of claim 16, wherein the matching authorization unit operable to securely match the client network device with the first of the plurality of service providers further comprises the matching authorization unit operable to:
- generate a client key that is unique to the client network device based, at least in part, on the client identifier and on a master key known to the managing network device and the plurality of service providers of the communication network;
- provide the client key to the client network device via the secure communication channel to allow the client network device to securely communicate with the plurality of service providers of the communication network;
- receive, from each of the plurality of service providers, a message that indicates a signal level detected at the service provider in response to a service matching message from the client network device; and
- select the first of the plurality of service providers that detected the highest signal level as the matching service provider for the client network device.
18. The managing network device of claim 17, wherein the matching authorization unit is further operable to:
- transmit, to the client network device, a number of service matching messages that should be transmitted from the client network device to the plurality of service providers.
19. The managing network device of claim 17, wherein the client key is a temporary key and is generated based, at least in part, on the master key, the client identifier, and one or

more of a sequence number, a random number, a start/end timestamp, a lifetime duration, a message counter, and/or a location identifier.

20. The managing network device of claim 16, wherein the matching authorization unit is further operable to:
- determine a first value of the client identifier associated with the client network device, wherein the first value of the client identifier was used for executing the service matching process;
 - determine a second value of the client identifier associated with the client network device, wherein the second value was used for executing the account authorization process;
 - determine whether the first value of the client identifier matches the second value of the client identifier;
 - in response to the matching authorization unit determining that the first value of the client identifier matches the second value of the client identifier, the matching authorization unit is operable to securely transmit the service voucher to the matching service provider to allow the client network device to be serviced by the matching service provider;
 - in response to the matching authorization unit determining that the first value of the client identifier does not match the second value of the client identifier, the matching authorization unit is operable to prevent the matching service provider from servicing the client network device.
21. A network device comprising:
- a network interface; and
 - a communication unit coupled with the network interface, the communication unit operable to:
 - establish a secure communication channel with a managing network device of a communication network based, at least in part, on a client identifier of the network device;
 - receive, from the managing network device, identification information associated with the managing network device via the secure communication channel;

- provide the client identifier and the identification information associated with the managing network device to an accounting network device to cause the accounting network device to execute an account authorization process with the network device;
- in parallel with the account authorization process, execute a service matching process with the managing network device and one or more of a plurality of service providers of the communication network;
- detect receipt of service from a first of the plurality of service providers of the communication network after completion of the account authorization process and the service matching process; and
- transmit an acknowledgement message to one of the managing network device and the first of the plurality of service providers in response to the communication unit detecting receipt of service from the first of the plurality of service providers of the communication network.
22. The network device of claim 21, wherein the communication unit operable to receive, from the managing network device, identification information associated with the managing network device further comprises the communication unit operable to:
- receive, from the managing network device, one or more service matching parameters to cause the network device to initiate the service matching process with the managing network device and the plurality of service providers of the communication network.
23. The network device of claim 21, wherein the communication unit is further operable to:
- receive, from the managing network device, a client key that is unique to the network device, via the secure communication channel, wherein the client key enables the network device to securely communicate with the plurality of service providers of the communication network;
- receive client key generation parameters based on which the client key was determined, wherein the client key generation parameters comprise one or more of a sequence number, a random number, a start/end timestamp, a lifetime duration, a message counter, and a location identifier;

wherein the communication unit operable to execute the service matching process with the managing network device and one or more of a plurality of service providers of the communication network comprises the communication unit operable to:
sign one or more service matching messages using the client key; and
transmit the one or more service matching messages and the client key generation parameters to the plurality of service providers.

24. The network device of claim 23, wherein the communication unit operable to transmit the one or more service matching messages and the client key generation parameters to the plurality of service providers comprises the communication unit operable to:
determine whether a length of the service matching message scheduled to be transmitted to the plurality of service providers is greater than a predetermined threshold message length;
in response to the communication unit determining that the length of the service matching message is greater than the predetermined threshold message length,
transmit an initialization message including the client key generation parameters to the plurality of service providers; and
transmit the client identifier and the sequence number in the one or more service matching messages; and
in response to the communication unit determining that the length of the service matching message is less than the predetermined threshold message length,
transmit the client key generation parameters as part of the one or more service matching messages.
25. A method comprising:
establishing a secure communication channel between a plug-in electric vehicle and a managing network device of a communication network based, at least in part, on a client identifier of the plug-in electric vehicle;
causing the plug-in electric vehicle to perform an account authorization process with an accounting network device in parallel with a service matching process with the managing network device and one or more of a plurality of electric charging stations of the communication network;

- securely matching the plug-in electric vehicle with a first of the plurality of electric charging stations;
- securely receiving a service voucher at the managing network device from the accounting network device authorizing one or more of the electric charging stations of the communication network to provide electric power to the plug-in electric vehicle in response to the accounting network device executing the account authorizing process with the plug-in electric vehicle; and
- securely transmitting the service voucher from the managing network device to the matching electric charging station to allow the plug-in electric vehicle to receive electric power from the matching electric charging station.
26. The method of claim 25, wherein said securely matching the plug-in electric vehicle with the first of the plurality of electric charging stations further comprises:
- generating, at the managing network device, a client key that is unique to the plug-in electric vehicle based, at least in part, on the client identifier and on a master key known to the managing network device and the plurality of electric charging stations of the communication network;
- providing the client key from the managing network device to the plug-in electric vehicle via the secure communication channel to allow the plug-in electric vehicle to securely communicate with the plurality of electric charging stations of the communication network;
- receiving, from each of the plurality of electric charging stations, a message that indicates a signal level detected at the electric charging station in response to a service matching message from the plug-in electric vehicle; and
- selecting the first of the plurality of electric charging stations that detected the highest signal level as the matching electric charging station for the plug-in electric vehicle.
27. The method of claim 26, wherein the client key is a temporary key and is generated based, at least in part, on the master key, the client identifier, and one or more of a sequence number, a random number, a start/end timestamp, a lifetime duration, a message counter, and/or a location identifier.

28. One or more machine-readable storage media having instructions stored therein, which when executed by one or more processors causes the one or more processors to perform operations that comprise:
- establishing a secure communication channel between a client network device and a managing network device of a communication network based, at least in part, on a client identifier of the client network device;
 - causing the client network device to perform an account authorization process with an accounting network device in parallel with a service matching process with the managing network device and one or more of a plurality of service providers of the communication network;
 - securely matching the client network device with a first of the plurality of service providers;
 - securely receiving a service voucher at the managing network device from the accounting network device authorizing one or more of the service providers of the communication network to service the client network device in response to the accounting network device executing the account authorizing process with the client network device; and
 - securely transmitting the service voucher from the managing network device to the matching service provider to allow the client network device to be serviced by the matching service provider.
29. The machine-readable storage media of claim 28, wherein said operation of securely matching the client network device with the first of the plurality of service providers further comprises:
- generating a client key that is unique to the client network device based, at least in part, on the client identifier and on a master key known to the managing network device and the plurality of service providers of the communication network;
 - providing the client key to the client network device via the secure communication channel to allow the client network device to securely communicate with the plurality of service providers of the communication network;
 - receiving, from each of the plurality of service providers, a message that indicates a signal level detected at the service provider in response to a service matching message from the client network device; and

selecting the first of the plurality of service providers that detected the highest signal level as the matching service provider for the client network device.

30. The machine-readable storage media of claim 28, wherein the operations further comprise:

determining a first value of the client identifier associated with the client network device, wherein the first value of the client identifier was used for executing the service matching process;

determining a second value of the client identifier associated with the client network device, wherein the second value was used for executing the account authorization process;

determining whether the first value of the client identifier matches the second value of the client identifier;

in response to determining that the first value of the client identifier matches the second value of the client identifier, said securely transmitting the service voucher from the managing network device to the matching service provider to allow the client network device to be serviced by the matching service provider;

in response to determining that the first value of the client identifier does not match the second value of the client identifier, preventing the matching service provider from servicing the client network device.

31. One or more machine-readable storage media having instructions stored therein, which when executed by one or more processors causes the one or more processors to perform operations that comprise:

establishing a secure communication channel with a managing network device of a communication network based, at least in part, on a client identifier of a client network device;

receiving, from the managing network device, identification information associated with the managing network device via the secure communication channel;

providing the client identifier and the identification information associated with the managing network device to an accounting network device to cause the accounting network device to execute an account authorization process with the client network device;

- in parallel with the account authorization process, executing a service matching process with the managing network device and one or more of a plurality of service providers of the communication network;
- detecting receipt of service from a first of the plurality of service providers of the communication network after completion of the account authorization process and the service matching process; and
- transmitting an acknowledgement message to one of the managing network device and the first of the plurality of service providers in response to said detecting receipt of service from the first of the plurality of service providers of the communication network.
32. The machine-readable storage media of claim 31, wherein the operations further comprise:
- receiving, from the managing network device, a client key that is unique to the client network device, via the secure communication channel, wherein the client key enables the client network device to securely communicate with the plurality of service providers of the communication network;
- receiving client key generation parameters based on which the client key was determined, wherein the client key generation parameters comprise one or more of a sequence number, a random number, a start/end timestamp, a lifetime duration, a message counter, and a location identifier;
- wherein said executing the service matching process with the managing network device and one or more of a plurality of service providers of the communication network comprises:
- signing one or more service matching messages using the client key; and
- transmitting the one or more service matching messages and the client key generation parameters to the plurality of service providers.
33. The machine-readable storage media of claim 32, wherein said operation of transmitting the one or more service matching messages and the client key generation parameters to the plurality of service providers comprises:

determining whether a length of the service matching message scheduled to be transmitted to the plurality of service providers is greater than a predetermined threshold message length;

in response to determining that the length of the service matching message is greater than the predetermined threshold message length,

transmitting an initialization message including the client key generation parameters to the plurality of service providers; and

transmitting the client identifier and the sequence number in the one or more service matching messages; and

in response to determining that the length of the service matching message is less than the predetermined threshold message length,

transmitting the client key generation parameters as part of the one or more service matching messages.

1/6

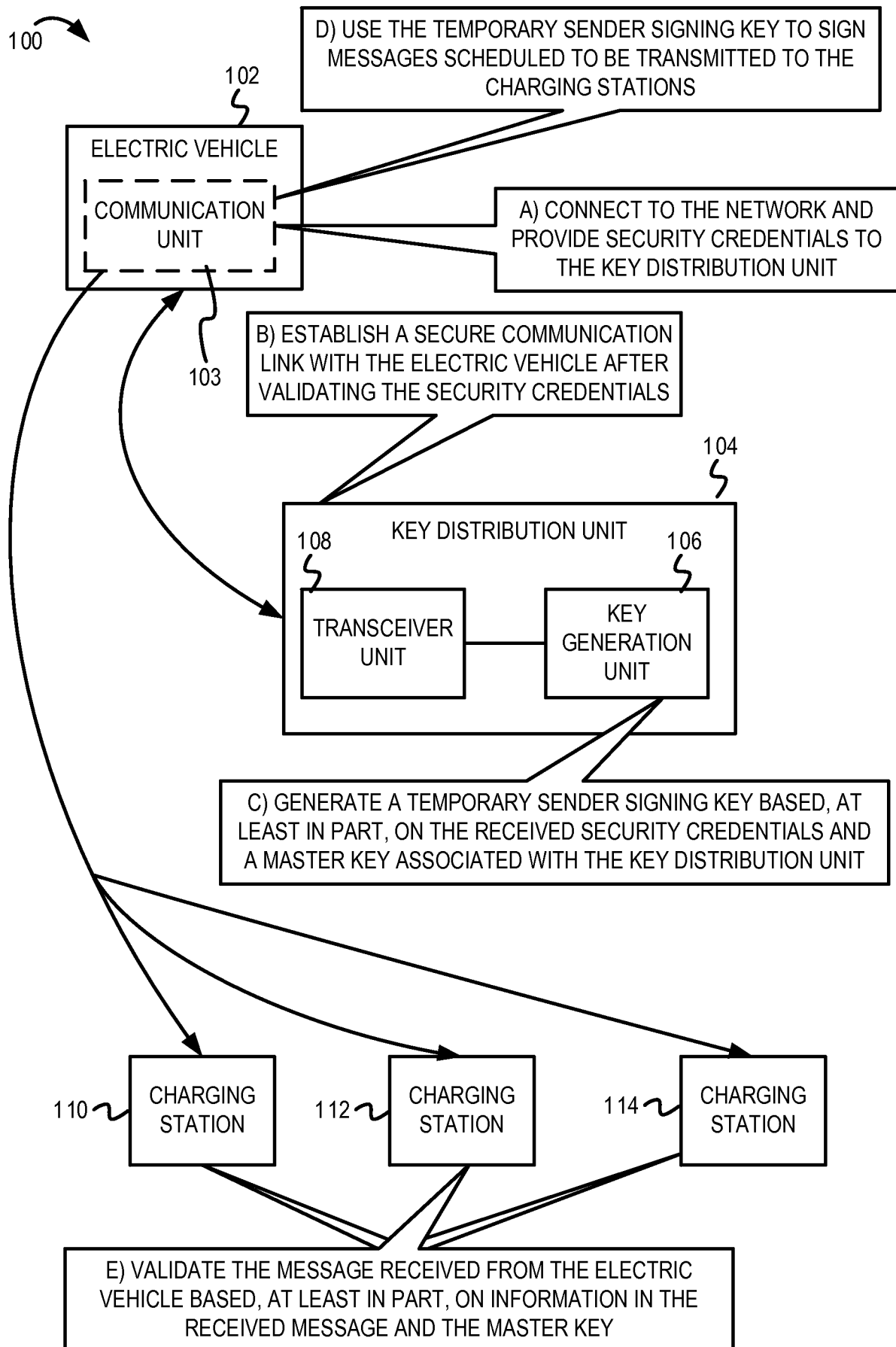


FIG. 1

2/6

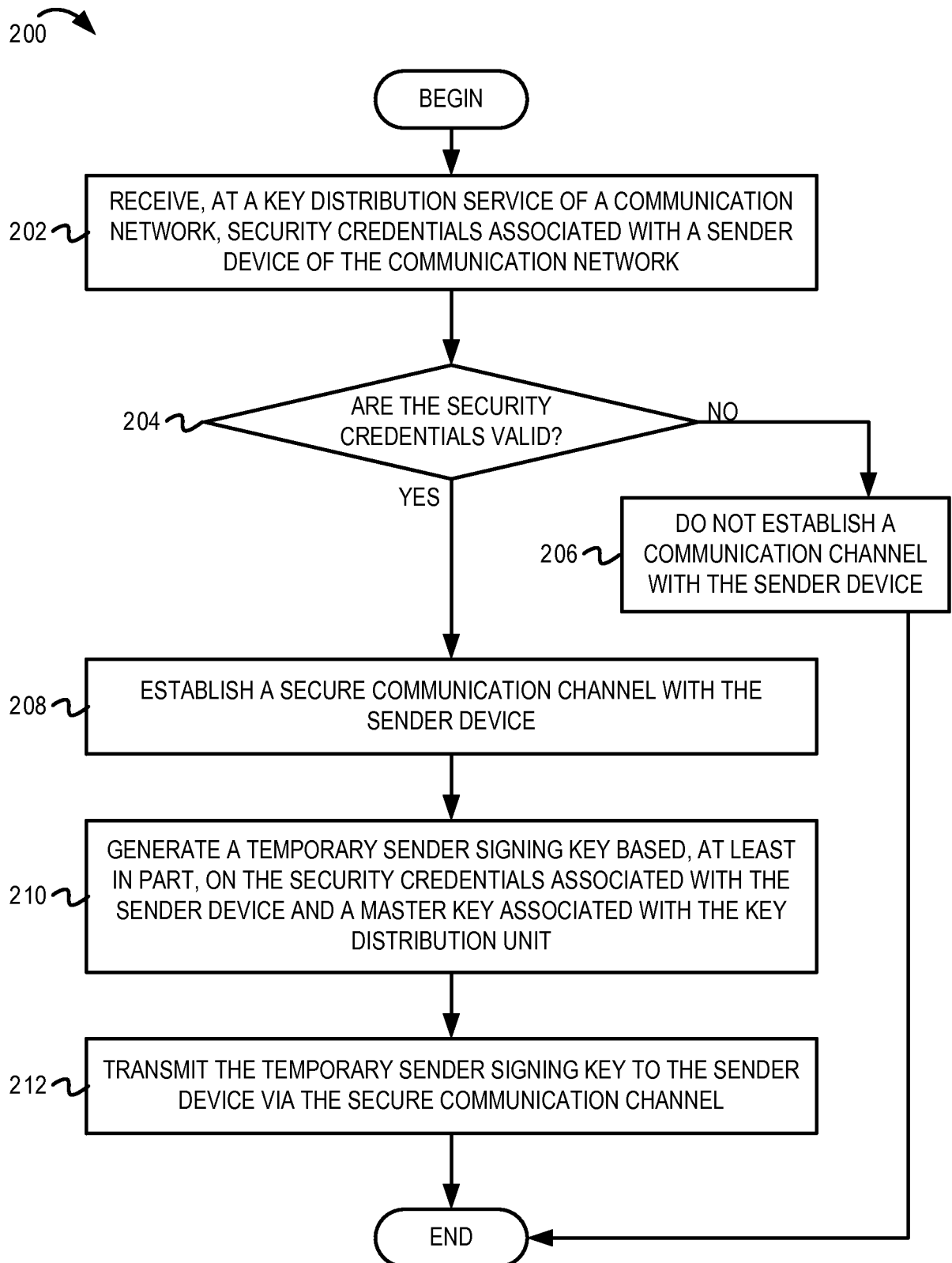


FIG. 2

3/6

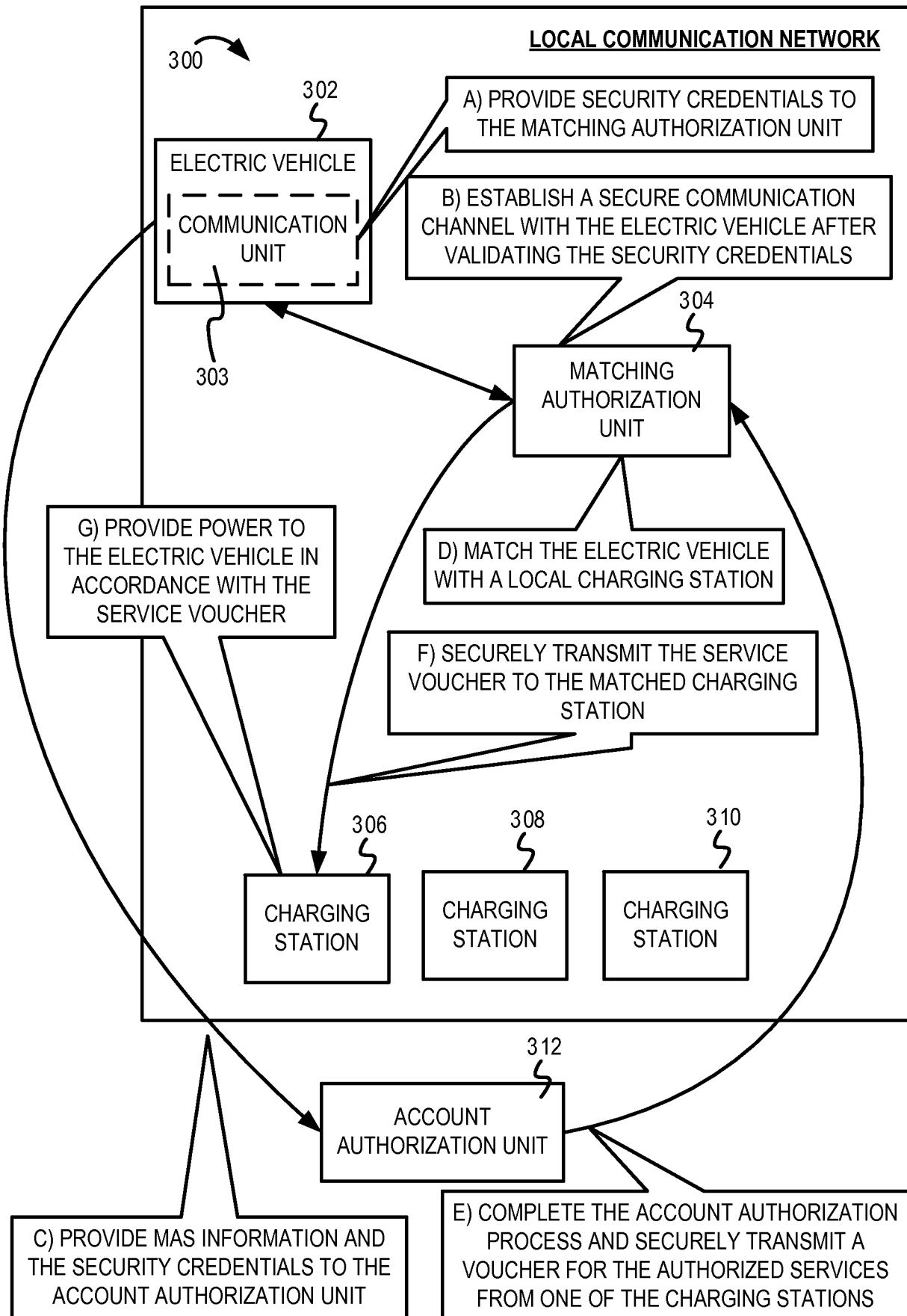


FIG. 3

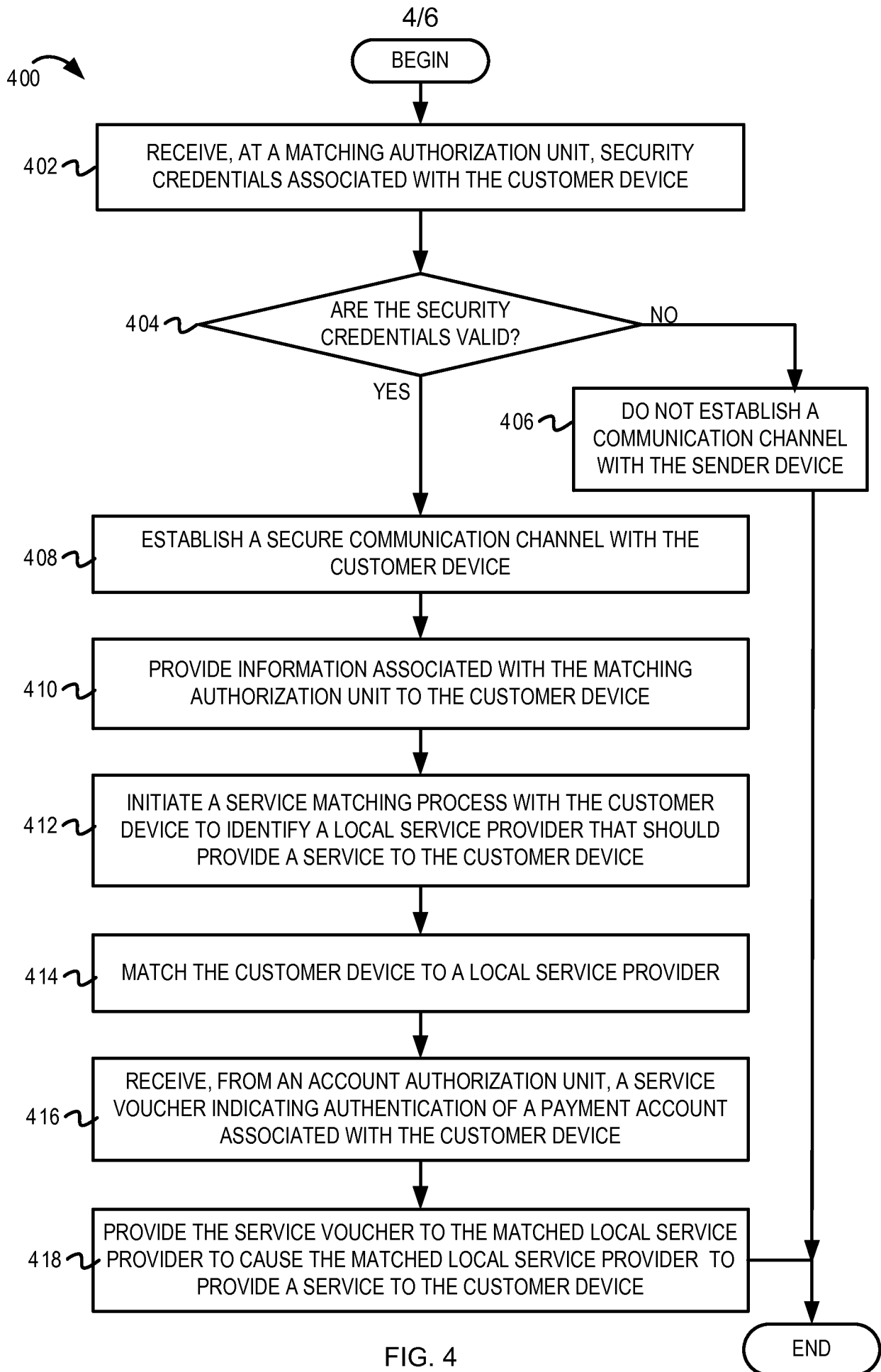


FIG. 4

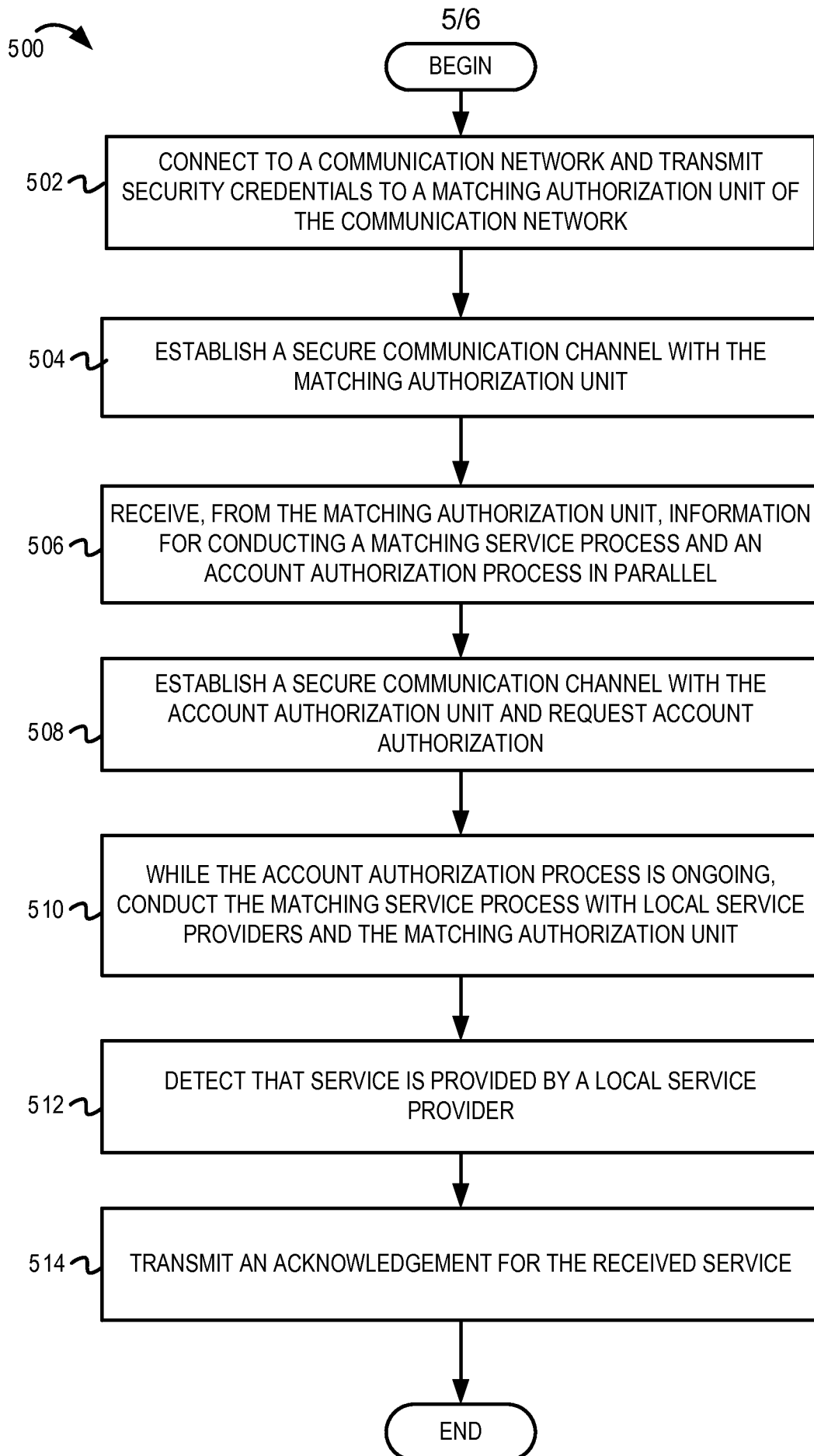


FIG. 5

6/6

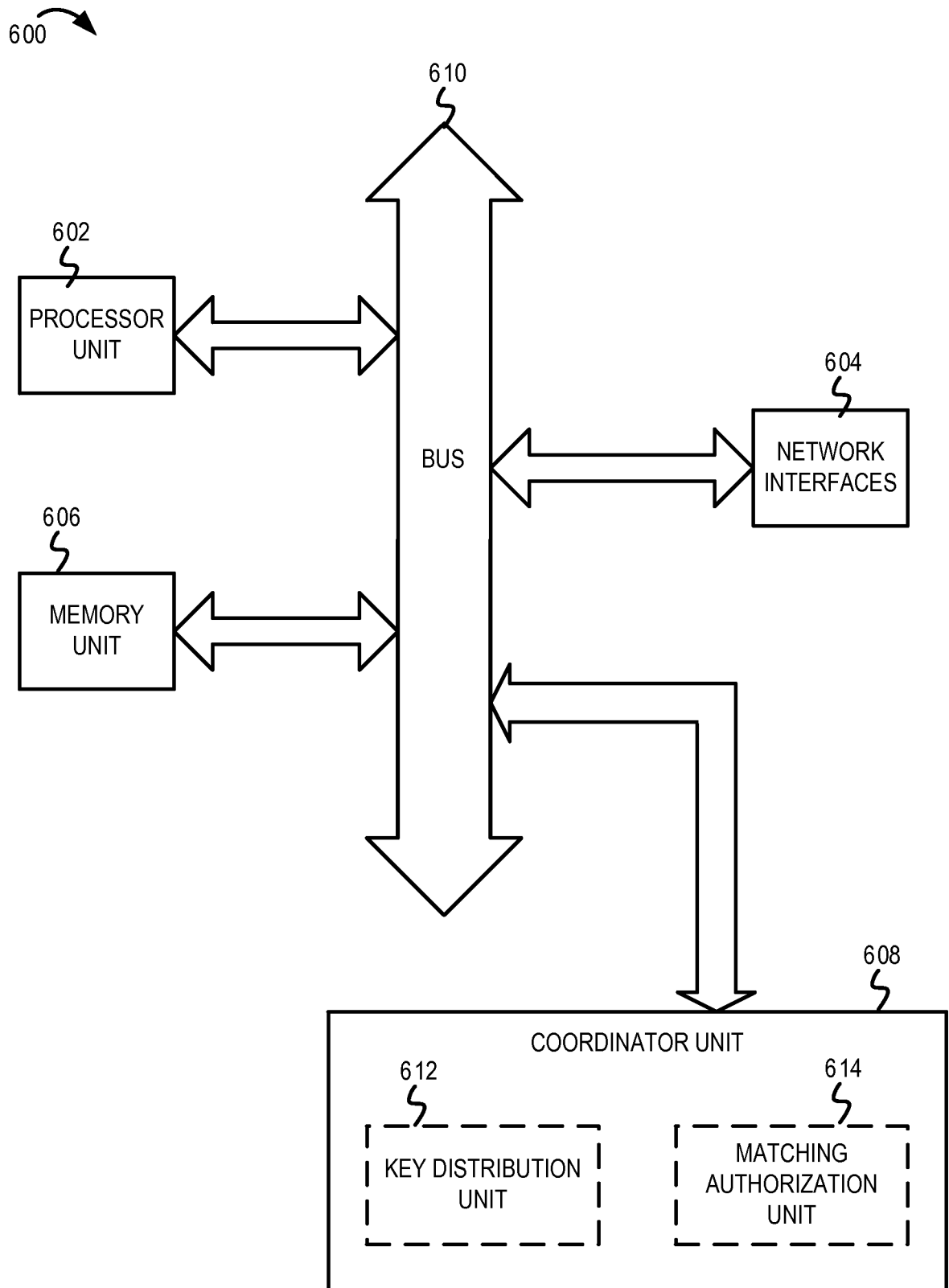


FIG. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/043415

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/08 B60L11/18
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)

H04L H04M H04Q H04W B60L

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)

EP0-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	EP 1 180 886 A1 (SUN MICROSYSTEMS INC [US]) 20 February 2002 (2002-02-20) paragraphs [0006] - [0014]; claim 10 -----	1-33
X	WO 2010/009502 A1 (DIUS COMPUTING PTY LTD [AU]; STAUGAITIS PAUL [AU]; ANDERSON MARK [AU]) 28 January 2010 (2010-01-28) page 2, line 2 - page 3, line 6 -----	1-33



Further documents are listed in the continuation of Box C.



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

3 October 2012

Date of mailing of the international search report

10/10/2012

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Veen, Gerardus

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2012/043415

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
EP 1180886	A1	20-02-2002	DE	60031266 T2		19-04-2007
			EP	1180886 A1		20-02-2002

WO 2010009502	A1	28-01-2010	AU	2009273757 A1		28-01-2010
			CN	102160327 A		17-08-2011
			EP	2308195 A1		13-04-2011
			EP	2364874 A2		14-09-2011
			US	2011213983 A1		01-09-2011
			WO	2010009502 A1		28-01-2010
