Technical Disclosure Commons

Defensive Publications Series

April 20, 2016

A METHOD FOR CONTROLLING ACCESS TO WIRELESS ELECTRICITY

Maxwell Sills

Ian Wetherbee

A METHOD FOR CONTROLLING ACCESS TO WIRELESS ELECTRICITY

ABSTRACT

A wireless electricity access control system provides a way to authenticate access to a power network. The system provides a method for a user of a wireless energy receiver to perform an authentication action at the receiver. Upon successful authentication, the system presents an advertisement or other media file to the user. After the consumption of the media file, the energy receiver receives a shared secret and a timestamp. The energy receiver uses this information to synchronize clocks at the energy receiver and an energy transmitter such as the power network. The energy receiver then selects a frequency using the synchronized clocks, shared secret, and timestamp information for receiving wireless electricity from the energy transmitter.

PROBLEM STATEMENT

Wireless power transfer or wireless energy transmission is the transmission of electrical power from a power source or power network to a wireless energy receiver or device without using any discrete conductors. The scope for wireless electricity is huge; however in order to make it monetizable and more secure, authenticating access to a power network would be helpful. Presently, most of the power networks do not require an explicit authentication and it is very easy to connect a device to a power source or network. Many companies having huge power networks want their networks either to be solely accessed by their customers or would want to

charge customers who are not directly engaged with the company. Thus there are numerous opportunities to have systems that authenticate access to a power network.

DETAILED DESCRIPTION

The systems and techniques described in this disclosure relate to a wireless electricity access control system. The system can be implemented on a power source or an energy transmitter device and/or implemented across a power consuming or energy receiver device. The power source can be a power network, a coil, a laser beam, mains power lines, etc. The energy receiver device can be any electrical power consuming device such as a mobile phone, a smartphone, a tablet computing device, a laptop computer, a coupling device, an electric or hybrid electric vehicle, an electric or hybrid electric automobile or car, a drone, a wireless electronic toy or game, a satellite, etc.

Fig. 1 illustrates an example method 100 that provides a way to authenticate access to a power network using the wireless electricity access control system.

The system performs 110 an authentication action at a wireless energy receiver. A user interacting with the wireless energy receiver can be asked to perform an authentication action in order to authenticate the wireless energy receiver. The authentication action can entail the system asking the user to enter a password. For example, if the user is using a mobile device (which would be the wireless energy receiver), the user can enter a password with alphanumeric characters or can authenticate the device using a fingerprint sensor present on the device or any other biometric authentication. This authentication action helps the energy receiver authenticate itself to an energy transmitter or a power network.

After the system has authenticated the wireless energy receiver, the system presents 120 an advertisement or other media file at a display and/or loudspeaker associated with the energy receiver. The system can be connected to an advertisement server which is coupled with the energy transmitter or the power network. The system can either fetch a media file from the server or the server can push the media file to a communication unit associated with the energy receiver which includes a data receiver and a data transmitter. For example, the advertisement server can transfer a predetermined or predefined media file on the display of the mobile device when the mobile device is authenticated. This media file can be related to the company which owns or operates the energy transmitter or the power network or can be related to any of the products or services that might be offered by the company. Alternatively, other companies can also advertise their products or services for a premium price. The presentation of an advertisement provides a way for the power network company to monetize their service of wireless energy transfer. Non-advertising media files may include educational videos, public service announcements, weather information, or news clips.

After the media file is presented on a display associated with the data receiver and the energy receiver, the energy receiver can receive 130 a shared secret and a timestamp. The shared secret can be any number of a series of numbers having a one-time password (OTP) type of a mechanism i.e., it can be valid for only one session or transaction on the wireless energy receiver. The shared secret can be shared by the energy transmitter or the power network after the authentication for the receiver is complete. The energy transmitter also shares a timestamp with the energy receiver along with the shared secret. This timestamp can be a sequence of characters or encoded information identifying when the authentication of the energy receiver is

received by the energy transmitter and when the energy transmitter transmits the shared secret. Alternatively, or additionally, the timestamp can also include the clock information of the energy transmitter.

The wireless energy receiver synchronizes 140 clocks at the energy receiver and the energy transmitter. The energy receiver uses the timestamp information, more particularly the clock information from the energy transmitter to synchronize the two clocks. The energy receiver performs this synchronization each time the receiver receives wireless electricity transfer from the energy transmitter.

The energy receiver then selects 150 a frequency hopping sequence for receiving wireless electricity. As well known, in a frequency hopping system, a transmitter changes the carrier frequency according to certain “hopping” pattern. The energy receiver uses the synchronized clock information, shared secret, and timestamp information to generate a time based sequence of numbers i.e., a certain “hopping” pattern. A processing module present within the energy receiver can be used to generate these numbers. The processing module can include a microprocessor, a microcontroller, or any other processor with the necessary means for performing this generation of numbers. A smoothing function generator also present within the energy receiver then performs a smoothing function operation on the time based number to create a number which will be an acceptable frequency for both the energy transmitter and the energy receiver to tune to. Additionally, the energy transmitter and the energy receiver keep re-tuning their frequencies.

The energy receiver then receives 160 wireless electricity at the selected frequency hopping sequence from the energy transmitter. After the frequency sequence is coordinated

between the energy receiver and the energy transmitter, the energy transmitter can transfer wireless electricity in the form of electromotive force (EMF) to the energy receiver. For example, after the selection of frequency has been made by the mobile device, a power network can transfer wireless electricity to the mobile device for charging the mobile device wirelessly. In an alternative embodiment, after the energy receiver has authenticated itself to the energy transmitter, the transmitter can use phased arrays or similar technology to beam electromotive force directly to charging coils present within the receiver.

FIG. 2 is a block diagram of an exemplary environment that shows components of a system for implementing the techniques described in this disclosure. The environment includes a wireless charging apparatus according to an embodiment of the present disclosure. The wireless charging apparatus includes a wireless energy receiver 200a and an energy transmitter or a power source 200b. In accordance with an embodiment, the wireless energy receiver 200a can include a power receiving unit 250, a battery unit 240, a controller 230, a communication unit 210, and a display 220. The power receiving unit 250 can receive supply power through a coil 211 as the transmitter 200b transmits at the same frequency sequence as that of the wireless energy receiver 200a. Additionally, the the power receiving unit 250 can supply the received power to the battery unit 240. The battery unit 240 can charge a rechargeable battery using the power received by the power receiving unit 250, and when the charging is completed, the battery unit 240 notifies the controller 230. In accordance with an embodiment, the transmitter 200b can be a power source or a power network and can include a power supplying unit 260, a power supply controller 270, and a communication unit 280.

The subject matter described herein can be implemented in software and/or hardware (for example, computers, circuits, or processors). The subject matter can be implemented on a single device or across multiple devices (for example, a client device and a server device). Devices implementing the subject matter can be connected through a wired and/or wireless network. Such devices can receive inputs from a user (for example, from a mouse, keyboard, or touchscreen) and produce an output to a user (for example, through a display and/or a speaker). Specific examples disclosed are provided for illustrative purposes and do not limit the scope of the disclosure.

DRAWINGS

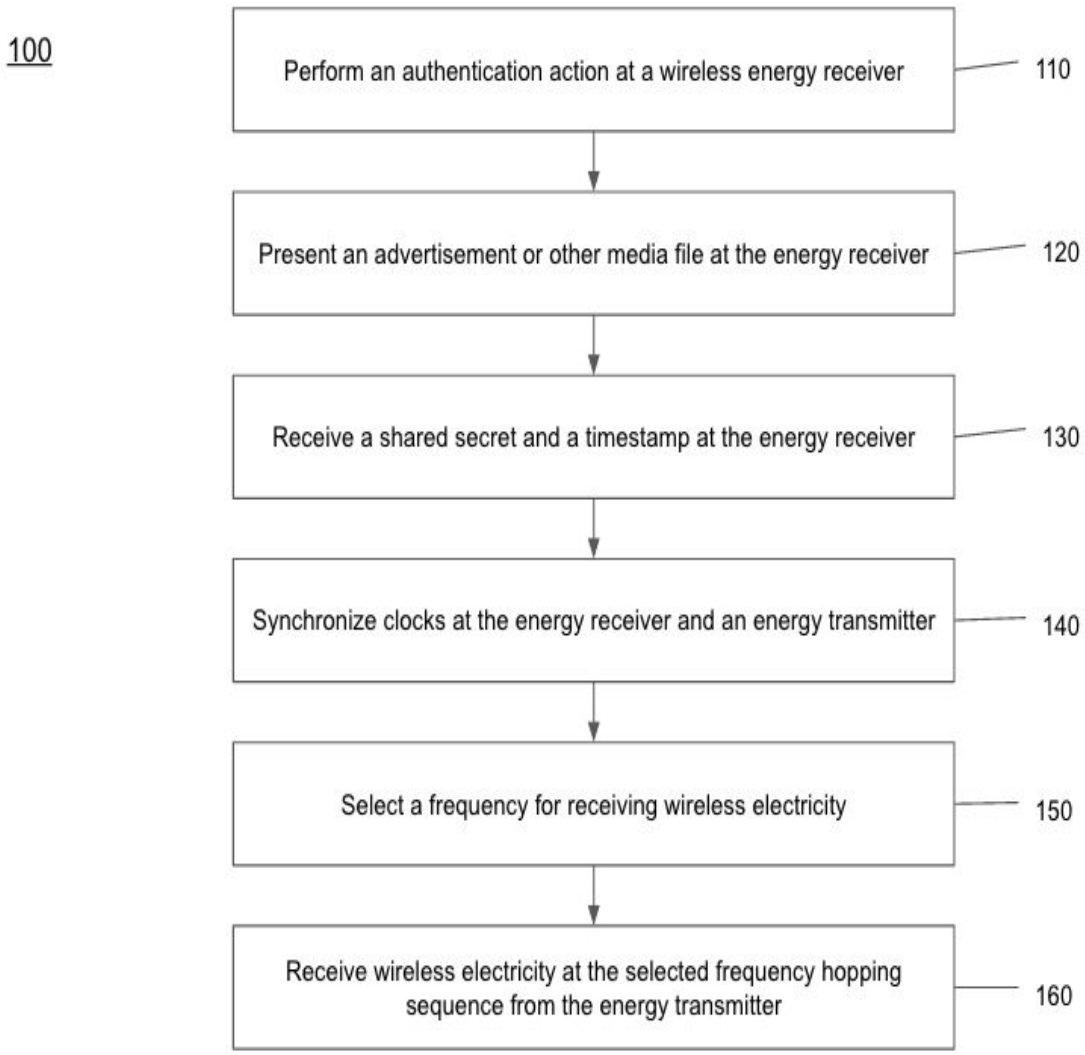

Fig. 1

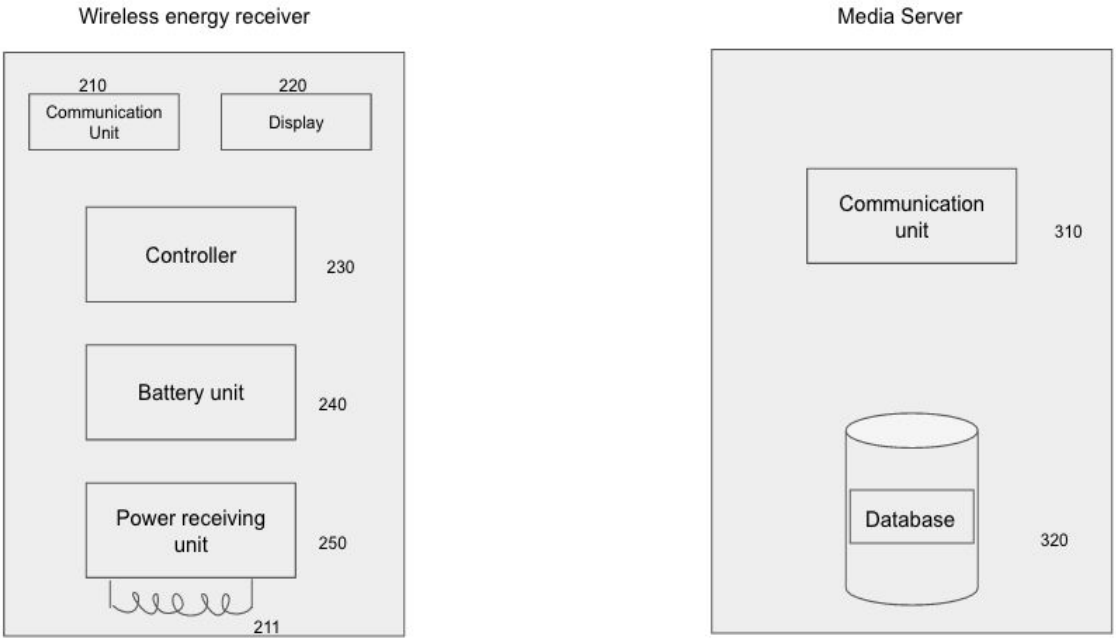
Wireless energy receiver
210
Communication Unit
220
Display
Controller
230
Battery unit
240
Power receiving unit
250
211
200a
Media Server
Communication unit
310
Database
320
200c
Transmitter/Power source
212
Power supplying unit
260
Power supply controller
270
Communication unit
280
200b

Fig. 2