**European Patent Specification**

**Date of publication and mention of the grant of the patent:**
27.03.2019 Bulletin 2019/13

**Application number:** 06759192.5

**Date of filing:** 05.05.2006

**Date of publication of application:**
05.03.2008 Bulletin 2008/10

**Int Cl.:**
- H04L 29/06 (2006.01)
- H04L 12/24 (2006.01)
- H04W 12/06 (2009.01)
- H04W 88/06 (2009.01)
- H04W 84/18 (2009.01)

**Proprietor:** Microsoft Technology Licensing, LLC
Redmond, WA 98052 (US)

**Inventors:**
- ABEL, Miller T.
  Redmond, Washington 98052-6399 (US)
- GUDAY, Shai
  Redmond, Washington 98052-6399 (US)

**Representative:** Goddar, Heinz J. et al
Boehmert & Boehmert
Anwaltspartnerschaft mbB
Pettenkoferstrasse 22
80336 München (DE)

**Designated Contracting States:**
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR

**Priority:** 23.06.2005 US 1596005

**References cited:**
  "Near Field Communication White Paper (Ecma)"
  ECMA/TC32-TG-TG/2004/1 2004, XP002403609

**Note:** Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention.)
BACKGROUND

[0001] Computer products and other networking equipment have emerged as one of the largest and fastest growing industries. With the rapid improvements made within the industry, electronic manufacturers continuously strive to satisfy the on-going demand for products providing functionality without restrictions such as, for example, size, power consumption, compatibility, ergonomics, software capability, lifetime, range, productivity, usability, interface, security, speed, portability, etc.

[0002] One restriction the electronic industries have vastly improved upon is providing a range or degree of freedom associated with employment of wireless networks and/or devices. Wireless networks and/or devices such as, but not limited to, wireless local area networks (WLAN), Bluetooth, local area network (LAN), sub-networks (e.g., wireless mouse and personal computer), portable digital assistants (PDA's), mice, keyboards, speakers, monitors, routers, phones, cellular communication devices, wireless devices, access points, hubs, ... facilitate functionality with mitigation of wires and accompanied restrictions. In addition to providing degree(s) of freedom, wireless devices and/or networks are advantageous to hard-wired networks and/or devices for numerous reasons. Wireless systems are pleasing to the eye since the clutter of unwanted hard-wires is eliminated. For instance, plasma flat-screen televisions involve mounting on a wall similar to that of a painting mounted to a wall. By utilizing a wireless method and/or system, the wires for the television would not be seen hanging from the wall, and the result is a more pleasant looking, wall-mounted television. Furthermore, a hard-wire is a physical restriction by limiting the range of the device and/or network with the actual length of the wire. For example, a hard-wired Ethernet connection for a laptop can only be utilized within physical constraints of length of the Ethernet cable. Additionally, hard-wires have to be connected, which can involve matching an endless amount of plugs and connectors.

[0003] Not only are wireless networks and/or devices employed within the personal computer realm (e.g., wireless keyboards, mice, speakers, ...), but common householdholds are increasing use of wireless home networks and/or devices. For example, broad-band connections are becoming more affordable for home users in which multiple personal computers anticipate connectivity. Dependant upon location of the personal computers, a network can be employed in order to distribute and utilize the broad-band connection. However, common problems of using hard-wires for the network can arise (e.g., cost, degree of freedom, eye-pleasing, ...). Thus, wireless networks and/or devices can be utilized in order to cure the foregoing problems.

[0004] Although benefits are apparent for wireless networks and/or devices, many problems arise involving installation of such products. With the increasing number of wireless networks, a difficulty arises to install a wireless device with a particular network entity (e.g., wireless mouse with a personal computer, wireless speakers with a receiver, wireless access point with a router, ...). Additionally, the network entity does not know when to install a wireless device and/or what wireless device to install. Moreover, a wireless device usually needs to be within range of the network entity in order to be detected and installed.

[0005] Another complex problem involving wireless networks and/or devices involves security and authentication. Although wireless networks and/or devices provide a vast amount of benefits, a hard-wire network and/or device is typically more secure based at least upon the physical connection assumed to be authenticated. On the contrary, wireless networks and/or devices are prone to "sniffing" (e.g., the act of eavesdropping on messages such as, but not limited to, confidential business data or passwords in transit) and other hacking techniques (e.g., port scanning, transfer communication protocol (TCP) spoofing, user datagram protocol (UDP) spoofing, TCP session spoofing, ...) which are utilized in order to intrude and exploit the network security.

[0006] EP 1 633 104 A1 discloses a method of establishing a wireless communication between apparatuses. The method first establishes a near field communication between two communication apparatuses to securely exchange communication information necessary to a Bluetooth communication including, for example, Bluetooth Device address, and next switches the near field communication to a Bluetooth communication based on the communication information just exchanged.

SUMMARY

[0007] The following presents a simplified summary of the innovation in order to provide a basic understanding of some aspects described herein. This summary is not an extensive overview of the claimed subject matter. It is intended to neither identify key or critical elements of the claimed subject matter nor delineate the scope of the subject innovation. Its sole purpose is to present some concepts of the claimed subject matter in a simplified form as a prelude to the more detailed description that is presented later.

[0008] In a first aspect of the invention, independent claim 1 defines a system that facilitates connecting a wireless device to a network. In a second aspect of the invention, independent claim 15 defines a corresponding computer-implemented method that facilitates connecting a wireless device to a network. In a third aspect of the invention, independent claim 18 defines a corresponding computer-implemented system that facilitates connecting a wireless device to a network. Further embodiments of the invention are defined by the dependent claims.

[0009] An installation component can employ provi-
sioning data related to a particular device that is to be connected securely to a specific network and/or verified device. The installation component can invoke such provisioning data through a near field communication (NFC) link, wherein the NFC link is a secure, short proximity, and encrypted link capable of being a trusted medium. It is to be appreciated that the encryption utilized can be a handshake (e.g., 4 way handshake) to establish a secure link on top of an "open" NFC channel. After the provisioning data is exchanged with the network, the device can establish a wireless connection (e.g., wireless local area network, Bluetooth, wireless fidelity, ultra wideband, ...) therewith. The device can be any device capable of wireless connectivity and NFC capability. Moreover, the verified device can be any device that has been previously securely connected to a network that contains at least one wireless connection. In one aspect described herein, a verified master device can be utilized for any and/or all provisioning of wireless devices to a wireless connection on a particular network.

[0010] The installation component can utilize a PONG component. The PONG component can provide a generic data transfer technique that allows provisioning data to be transferred to the network such that a device can be installed and/or authenticated on such network. The plug and go (PONG) technique is generic as to allow any device to be provisioned with any suitable wireless connection such as, but not limited to, a wireless local area network (WLAN), Bluetooth, wireless fidelity (Wi-Fi), ultra-wideband (UWB), etc. The PONG component can utilize, for example, a PONG manager, a PONG handler, a PONG driver, and PONG data (e.g., PONG request, PONG response, ...).

[0011] The installation component can further include a security component. The security component can provide an additional layer of security in relation to determining whether the near field communications link is to be utilized to transfer provisioning data. Although the NFC link is a secure and encrypted channel, the security component can provide an additional layer of security to verify implantation of the NFC link authentication technique. For instance, the security component can utilize various security techniques such as, but not limited to, a user name and password, personal identification number (PIN), a login, time-based proximity, biometric indicia (e.g., fingerprint, inductance, retina), human interactive proofs (HIPs), voice recognition, etc.

[0012] The installation component can include a manager component that manages various aspects associated with the devices, connections, links, etc. of the claimed subject matter. The manager component can also determine whether a device should be associated with a wireless connection based at least in part upon an analysis of other available wireless connections within the network.

[0013] The following description and the annexed drawings set forth in detail certain illustrative aspects of the claimed subject matter. These aspects are indicative, however, of but a few of the various ways in which the principles of the innovation may be employed and the claimed subject matter is intended to include all such aspects. Other advantages and novel features of the claimed subject matter will become apparent from the following detailed description of the innovation when considered in conjunction with the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] Fig. 1 illustrates a block diagram of an exemplary system that facilitates provisioning a wireless device utilizing a near field communications link as a trusted medium.

Fig. 2 illustrates a block diagram of an exemplary system that facilitates securely installing a device to a network by invoking near field communication link and a pong channel.

Fig. 3 illustrates a block diagram of an exemplary system that facilitates connecting a wireless device to a secure network by employing near field communications link to exchange provisioning data.

Fig. 4 illustrates a block diagram of an exemplary system that facilitates connecting a plurality of wireless devices to a network utilizing a near field communication link as a trusted medium.

Fig. 5 illustrates a block diagram of an exemplary system that facilitates connecting a near field communication link to provision a wireless device to a secured wireless network.

Fig. 6 illustrates a block diagram of an exemplary system that facilitates provisioning a wireless device to a secure network utilizing near field communications.

Fig. 7 illustrates a conventional prior art wireless configuration comprising of a plurality of wireless devices.

Fig. 8 illustrates an exemplary methodology that facilitates provisioning a wireless device to a secure network by employing a near field communication link to exchange provisioning data.

Fig. 9 illustrates a methodology 900 for securely installing a device to a secure network by utilizing a near field communications link.

Fig. 10 illustrates an exemplary networking environment, wherein the novel aspects of the claimed subject matter can be employed.

Fig. 11 illustrates an exemplary operating environment that can be employed in accordance with the claimed subject matter.

DETAILED DESCRIPTION

[0015] As utilized herein, terms "component," "system," "interface," and the like are intended to refer to a computer-related entity, either hardware, software (e.g.,
The installation component 102 can facilitate establishing an ad-hoc network between two devices for the purpose of connectivity there between. It is to be appreciated that the installation component 102 can be a stand-alone component, incorporated into the verified device 108 and/or device 104, and/or any combination thereof.

For example, a wireless keyboard (e.g., the device 104) can utilize the near field communication link 106, wherein the installation component 102 can invoke provisioning data to a PC (e.g., the verified device 108). By utilizing the installation component 102 and exchanging the provisioning data via the NFC link 106 the wireless connection 110 to such network can be established without compromising security constraints associated with the wireless connection 110 and/or network. Once the wireless keyboard is provisioned with the network and/or the verified device 108, the keyboard itself can be considered a verified device 108 from which other devices can be provisioned. It is to be appreciated that the NFC link 106 can be considered a trusted medium for which the installation component 102 can transfer (utilizing the NFC link 106) any suitable provisioning data to allow the device 104 to connect to the network. Moreover, it is to be appreciated and understood that the wireless connection 110 can be any suitable wireless connection associated with the device 104 and/or the verified device 108 where the network can be, but is not limited to being, a wireless local area network (WLAN), Bluetooth, wireless fidelity (Wi-Fi), and ultra-wideband (UWB).

It is to be appreciated that the device 104 and the verified device 108 utilize the short proximity NFC link 106 to securely exchange provisioning data to establish the wireless connection 110 which has a greater communication range when compared to the NFC link 106. The NFC link 106 can be understood and recognized as a short range wireless technology usable for the provisioning of network connectivity without requiring additional hardware and/or battery power. Moreover, the NFC link 106 can establish a secure and/or encrypted link over short distances (e.g., 1 to 2 centimeters, ...) between the device 104 and the verified device 108. It is to be appreciated that the encryption utilized can be a handshake (e.g., 4 way handshake) to establish a secure link on top of an “open” NFC channel associated with the NFC link 106.

In another example, a wireless mouse can be substantially similar to a device 104 that can establish a secure link via NFC link 106 to a wireless keyboard that can be considered a verified device 108 part of a secured network with security constraints. NFC link 106 can be a trusted medium that securely exchanges any provisioning data related to the wireless mouse to the verified device 108 (in this example, the wireless keyboard). It is to be noted that the exchange of provisioning data allows the secure installation and/or connection of the wireless mouse to the secured network that contains the wireless keyboard.

In yet another example, a wireless adapter can
communicate with a wireless router to provide a broadband connection via, for example, a digital subscriber line (DSL). The wireless adapter can be connected to the wireless router via NFC link 106 for a secure/encrypted link over a short distance. The short distance connection can provide provisioning data (e.g., installation protocol, authentication protocol, ...) necessary via the installation component 102 for the wireless adapter and the wireless router to utilize the wireless connection 110. Upon completion of the installation and/or authentication (e.g., transfer of the provisioning data by utilizing the NFC link 106 and/or the installation component 102), the wireless adapter can be disengaged (e.g., placed out of NFC range and/or proximity) from the wireless router. Once disengaged, the wireless adapter and the wireless router can utilize the wireless connection 110 based at least in part upon being authenticated, verified, and/or secured without compromising security constraints. By utilizing NFC link 106, the wireless router is aware of the wireless adapter being installed; the wireless adapter is aware of the wireless router upon which it is being installed; and the security of authentication and installation is heightened.

Moreover, the system 100 can include any suitable and/or necessary interface component (not shown), which provides various adapters, connectors, channels, communication paths, etc. To integrate the installation component 102 into virtually any operating and/or database system(s). In addition, the interface component can provide various adapters, connectors, channels, communication paths, etc., that provide for interaction with the installation component 102, the verified device 108, NFC link 106, and the device 104.

Fig. 2 illustrates a system 200 that facilitates securely installing a device to a network by invoking a near field communications link and a pong channel. An installation component 202 can invoke provisioning data to be exchanged over a NFC link 206 to connect a device 204 to a network (not shown) and/or a verified device 208. The exchange of provisioning data over the NFC link 206 can ensure a secure link based at least in part upon the NFC link 206 in an encrypted link over short distances with a relatively high bandwidth. The provisioning data can ensure the authentication and/or installation of any device that is to be installed on a secure network, wherein the verified device is associated with such secure network. Once the device 204 is provisioned with the network through the NFC link 206, the device 204 can utilize a wireless connection associated with the verified device 208 and/or the network, wherein the wireless connection can be, but is not limited to, a wireless local area network (WLAN), Bluetooth, wireless fidelity (Wi-Fi), ultra-wideband (UWB), etc. It is to be appreciated that the device 204 can utilize the NFC link 206 as a trusted medium to exchange provisioning data with any device and/or network entity that has NFC capabilities and is associated with the network. Moreover, it is to be appreciated and understood that the verified device 208 need not be connected directly to the NFC link 206, yet the verified device 208 can be previously configured to the particular network in order to provision the device 204.

The NFC link 206 can be a trusted medium for provisioning data exchange to establish a secure and/or authenticated wireless connection for any device onto a particular network by utilizing a PONG component 210. The PONG component 210 can implement a plug and go (PONG) architecture to relate a device with a host system (e.g., verified device, network entity, ...). The PONG architecture can include a handler, a driver and a PONG manager, wherein each component can be loaded in a single service process. Each component is described with more detail below. It is to be appreciated that the PONG component 210 is one example of transferring information over the NFC link 206 as a trusted medium, and that various other techniques can be considered under the scope of the claimed subject matter. Yet, the implementation of the PONG component 210 allows for a generic technique, wherein the use of NFC link 206 as a trusted medium can be naturally extended to any other suitable wireless media types such as, but not limited to, Bluetooth and UWB.

The PONG manager can be the central component that facilitates passing data to the correct parties. Based on driver registration, the PONG manager can load the driver files (e.g., .dll file) into the manager's process. When the PONG manager receives a PONG request block from a driver, it looks at the request block header and loads the appropriate PONG handler for that request type. The request block can then be given to the handler for processing. Once the handler is finished, a PONG response block is returned to the driver through the PONG manager.

The PONG driver is responsible for interfacing with either some form of hardware or another software component. The PONG driver is responsible for channeling requests from the PONG manager to the PONG device (e.g., a device that sends PONG request data to the PONG host and receives PONG response(s)) over the trusted medium (e.g., NFC link 206). The driver can detect when a new PONG request should be issued and it either retrieves or generates the request. This request is passed to the PONG manager who can return a PONG response to the driver. It is to be appreciated that multiple PONG handlers can utilize the same PONG driver (e.g., multiple target medium can utilize the same trusted medium). The PONG driver can simply utilize the header for any details on a PONG request clock or PONG response block.

The PONG handler can interface with the service that implements device installation. The PONG handler can be directly related to the target medium (e.g., NFC link 206) and can be the component that has explicit knowledge of the PONG request block for that specific target medium. When the PONG handler receives the PONG request block from the PONG manager, it can parse the contents to determine an appropriate action.
Furthermore, the PONG data can include PONG requests and PONG responses that are organized in a parse-able stream. The stream can consists of a series of PONG attributes, wherein each attribute has a defined type and associated data. This technique, rather than opposed flat structure with pre-defined offsets, provides for easy expansion. It is to be appreciated that a PONG attribute is a single item within a PONG request and/or a PONG response.

The PONG request can be a series of PONG attributes. The first attribute can be an association type that can be utilized to identify which PONG handler the request is to be directed to. The value can be a GUID that is defined by the PONG handler. For instance, to associate with a Bluetooth device, there can be a Bluetooth specific GUID, and a PONG handler that has specified that it handles that particular GUID. The second attribute in the PONG request can be the length. This is the total length of all the attributes in this request including the association type and length field itself. This can be utilized to aide in parsing, such that if a component is not interested in a specific association type, it can skip over the whole thing as opposed to having to parse each attribute with it.

The attribute(s) that follow the length can be defined such that simple devices can implement basic association with minimal processing. Independent hardware vendors (IHVs) may want to make silicon-only solutions without firmware, so being able to simply jump to a pre-defined offset in a structure in order to extract desired data as necessary. So the attributes immediately following the length can contain the minimal amount of data needed to carry out basic association. The attributes can also be laid out in a pre-defined order. In fact, it may be desirable to have a vast majority of this data contained within a single attribute. Note that any variable length fields can be at the end of these basic attributes; otherwise the offset in the PONG request can change. Any number of attributes may follow in order to provide extended functionality.

The PONG Response can be a series of PONG attributes. The first attribute can be the association type. This is used to echo the association type of the PONG request that resulted in this response. The second attribute in the PONG response can be the length. This is the total length of all of the attributes in this request including the association type and length field itself. This is used to aide in parsing, so that if a component is not interested in a specific association type, it can skip over the whole response as opposed to having to parse each attribute within it.

The third attribute of the PONG response can be the association status. This is to notify the PONG device as to the result of the PONG request. If the Association process was successful, then this value will be 0x0000, meaning that the device can continue to read the attributes in the response. If the value is 0x0001, then the PONG host could not find a PONG handler that can handle the specified association type. In this case, the device may not make any assumptions about further attributes in the PONG response.

The attribute(s) following the association status can be defined very carefully. There is a goal to allow simple devices to be able to implement basic association with minimal processing. In fact, IHVs want to be able to make silicon-only solutions with no firmware. In order to achieve this, being able to simply jump to a pre-defined offset in a structure in order to extract desired data is necessary. So these attributes can contain the minimal amount of data needed to carry out basic association. The attributes should also be laid out in a pre-defined order and can be present. In fact, it may be desirable to have all of this required data contained within a single attribute. Note that any variable length fields can be at the end of these basic attributes otherwise the offset in the PONG request can change. Any number of attributes may follow in order to provide extended functionality.

The PONG component 210 can implement the PONG technique described above to transfer provisioning data across the NFC link 206, wherein the NFC link 206 is a trusted medium that allows the safe and secure installation and/or authentication of a device to the network and/or verified device such that the device can utilize the wireless connection associated therewith. Although the PONG technique is described as the technique to transfer such data across the NFC link 206, it is to be appreciated and understood that the provisioning data can be transferred by any suitable and/or efficient technique over the NFC link 206 to allow for the connectivity of devices with a wireless connection (e.g., a wireless local area network (WLAN), Bluetooth, wireless fidelity (Wi-Fi), ultra-wideband (UWB), ...). Moreover, the claimed subject matter is not so limited to using the PONG techniques as described above.

Fig. 3 illustrates a system 300 that facilitates connecting a wireless device to a secure network by employing a near field communications link to exchange provisioning data. A device 304 can utilize an installation component 302 to invoke the provisioning of the device 304 wireless connectivity to a verified device 308 associated with a network (not shown). A NFC link 306 can be utilized to exchange any data (e.g., provisioning data 316) related to the authentication and/or installation of the device 304 onto the network to which the verified device is associated with. Thus, the NFC link 306 enacts as a trusted medium, wherein configuration data (e.g., provisioning data 316) can be exchanged to allow an unverified device, such as device 304, to become connected to the verified device 308 and/or network by a wireless connection 310, wherein the wireless connection can be any suitable wireless connection, such as a wireless local area network (WLAN), Bluetooth, Wi-Fi, ultra-wideband (UWB), etc. It is to be appreciated that the verified device 308 can be any suitable network entity securely associated with the network. Moreover, the device 304, the installation component 302, the NFC link
In one example, the verified device 308 can be work in order to provision the device 304. Furthermore, it is to be appreciated and understood that the verified device 308 need not be connected directly to the NFC link 306, yet the verified device 308 can be previously configured to the particular network in order to provision the device 304.

[0037] In one example, the verified device 308 can be a personal computer that utilizes a Bluetooth connection for wireless devices, wherein a wireless speaker is unverified and uninstalled to the personal computer. A user can place the wireless speaker close to the personal computer, wherein NFC link 306 can be utilized to allow the installation component 302 to install installation and/or authentication data (e.g., provisioning data). The NFC link 306 can be utilized as a trusted medium based at least in part upon the connection being secure and encrypted over such short distances. Upon completion of the transfer over the NFC link 306, the wireless speaker can be utilized by the personal computer over the Bluetooth connection based at least in part upon the authentication and/or verification over the NFC link 306.

[0039] The installation component 302 can include a security component 312 that can ensure security related to the initiation of a NFC link 306 between a device 304 and a verified device 308. For example, although the implementation of NFC link 306 can provide a trusted medium for data exchange, not all close proximity interactions are intended to exchange information for provisioning devices. Thus, the security component 312 can provide an additional security layer such that various security techniques can be employed to ensure the intended, authenticated, and/or verified utilization of NFC link 306 to exchange data related to provisioning a device 304. The security techniques can be employed such as, but not limited to, smart cards, certificates, knowledge of cryptographic keys, user name and password, personal identification number (PIN), time-based proximity, biometric indicia (e.g., fingerprint, inductance, retina, ...), human interactive proofs (HIPs), voice recognition, etc. to deter malicious attacks and/or unauthorized provisioning of devices to the network.

[0039] The installation component 302 can further include a manager component 314 that can manage any devices, connections, and/or configurations associated with the system 300. For example, the manager component 314 can manage the connectivity of devices (e.g., number, type, location, ...), manage proximity settings associated with the NFC link 306 (e.g., time length, distance, range, ...), manage the association of the wireless connection, etc. For instance, the manager component 314 can manage which wireless connection 310 to a particular device (provisioned by NFC link as a trusted medium) is established upon. Thus, a device 304 can be provisioned utilizing the NFC link 306 as a trusted medium to exchange authentication and/or installation data (e.g., provisioning data 316), wherein the manager component 314 can efficiently associate the device 304 with a network and/or wireless connection 310. In other words, a device can be provisioned via NFC link 306, and the manager component 314 can determine whether a WLAN connection, a Bluetooth, a wireless fidelity (Wi-Fi), a WUWB, etc. is most efficient and/or provides the strongest signal to the device 304. In one example, the manager component 314 can deny connectivity based at least upon a threshold of signal strength not being met.

[0040] The installation component 302 can utilize a data store (not shown), wherein the data store can store various data related to the system 300. The data store can provide storage for any provisioning data 316, wherein the data store can be associated with a network, a particular device, installation protocols, authentication protocols, etc. The data store can be, for example, either volatile memory or nonvolatile memory, or can include both volatile and nonvolatile memory. By way of illustration, and not limitation, nonvolatile memory can include read only memory (ROM), programmable ROM (PROM), electrically programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), or flash memory. Volatile memory can include random access memory (RAM), which acts as external cache memory. By way of illustration and not limitation, RAM is available in many forms such as static RAM (SRAM), dynamic RAM (DRAM), synchronous DRAM (SDRAM), enhanced SDRAM (ES-DRAM), Synchlink DRAM (SLDRAM), Rambus direct RAM (RDRAM), direct Rambus dynamic RAM (DRDRAM), and Rambus dynamic RAM (RDRAM). The data store of the subject systems and methods is intended to comprise, without being limited to, these and any other suitable types of memory. In addition, it is to be appreciated that the data store can be a server, a database, a hard drive, and the like.

[0041] Fig. 4 illustrates a system 400 that facilitates connecting a plurality of wireless devices to a network utilizing a near field communication link as a trusted medium. In general, once a wireless device has been connected to a network entity 404 via a NFC link 408 in which an installation component 406 establishes a wireless connection utilizing provisioning data, the wireless device can be utilized as a verified device, and in particular a verified master device 402 from which a plurality of wireless devices 410 (having a wireless device 1 to wireless device N, where N is an integer greater than or equal to 1) can connect to the network entity 404. It is to be appreciated that the installation component 406, NFC link 408 and the wireless connection can be substantially similar to previously described elements. Furthermore, it is to be appreciated and understood that the verified master device 402 need not be connected directly to the NFC link 408, yet the verified master device 402 can be provisioned utilizing the NFC link 306 as a trusted medium to exchange authentication and/or installation data (e.g., provisioning data 316), wherein the manager component 314 can efficiently associate the device 304 with a network and/or wireless connection 310. In other words, a device can be provisioned via NFC link 306, and the manager component 314 can determine whether a WLAN connection, a Bluetooth, a wireless fidelity (Wi-Fi), a WUWB, etc. is most efficient and/or provides a strongest signal to the device 304. In one example, the manager component 314 can deny connectivity based at least upon a threshold of signal strength not being met.

[0042] A user can employ a daisy chain scheme (e.g., a hardware configuration in which devices are connected in series in which signals can be received by each device)
utilizing a previously established secure and/or trusted device (referred to as the verified master device 402). A user can place a wireless device not connected to the network and/or network entity 404 within a close proximity of the verified master device 402 such that NFC link 408 can be utilized as a trusted medium to exchange installation and/or provisioning data. Once the NFC link 408 is implemented, the installation component 406 can invoke provisioning data to allow the secure installation and/or connection configuration for such wireless device. Thus, any one and/or all of the plurality of wireless devices 410 can establish a wireless connection 414 that is secure based at least in part upon the exchange of provisioning data between the verified master device 402 and the plurality of wireless devices via NFC link 408. In other words, the verified master device 402 can utilize NFC link 408 to allow any one of the plurality of wireless devices 410 to be provisioned with the network entity 404 based at least in part upon the secured and/or authenticated wireless connection 412 (authenticated and/or verified with or without the use of the trusted medium NFC link 406).

[0043] For example, a computer can be a network entity for a plurality of wireless devices such as, but not limited to, wireless mouse, wireless keyboard, wireless monitor, wireless adapter, wireless speakers, wireless headset, wireless microphone, etc. By utilizing the system 400, a user can employ the daisy chain scheme to install the plurality of wireless devices. Once a first device is secured and/or authenticated, such device can be utilized as a verified master device 402, wherein a trusted wireless connection is established therewith. The future wireless devices can be verified by implementing NFC link 408 between a newly introduced wireless device (one of and/or all of the plurality of wireless devices 410) and the verified master device 402. Thus, after a wireless mouse is installed and/or authenticated, the wireless keyboard can be placed in close proximity to allow NFC link 408 to be utilized to exchange provisioning data. Once the NFC link 408 is established, the installation component 406 can invoke the installation and/or authentication of the wireless keyboard utilizing such provisioning data. After the exchange is complete, the computer can have two wireless devices connected via two separate and distinct wireless connections (wireless connection 412 and newly established wireless connection 414).

[0044] Fig. 5 illustrates a system 500 that facilitates utilizing a near field communications link to provision a wireless device to a secured wireless network. The system 500 can include a verified device 502 (e.g., established a secure connection to a network) and a wireless device 506 that is not verified. The wireless device 506 and the verified device can exchange provisioning data during a NFC link connection between the sensor 504 and sensor 508 in order to establish a wireless connection 512. It is to be appreciated that the NFC link connection between the wireless device 506 and the verified device 502 can be initiated based at least in part upon a proximity 510, wherein if the distance of the wireless device 506 and the verified device 502 is less than such proximity 510, the NFC link connection can be established.

[0045] The installation component (not shown) can invoke the provisioning data during the NFC link connection provided by the sensors 504 and 508. It is to be appreciated that the installation component can be incorporated into the sensor 508 for the wireless device 506 or within the verified device 502. In other words, the installation component can be incorporated into either the wireless device 506 or within the network (not shown) such that upon the NFC link connection between the sensors 508 and 504, the installation component can invoke the installation and/or authentication of the wireless device utilizing the provisioning data. The sensors 508 and 504 facilitate the complications involved with installing and/or authenticating the wireless device 506 to the verified device 502 by employing the NFC link connection as a trusted medium between such devices. The sensors 508 and 504 can be any suitable sensors associated with a near field communication link that can receive and/or send communications wirelessly within short ranges.

[0046] Fig. 6 illustrates a system 600 that employs intelligence to facilitate provisioning a wireless device to a secure network utilizing a near field communications link. The system 600 can include an installation component 602, a device 604, a NFC link 606, and a verified device 608 that can all be substantially similar to respective components described in previous figures. Furthermore, it is to be appreciated and understood that the verified device 608 need not be connected directly to the NFC link 606, yet the verified device 608 can be previously configured to the particular network in order to provision the device 604. The system 600 further includes an intelligent component 610. The intelligent component 610 can be utilized by the installation component 602 to facilitate provisioning a wireless device to a network and/or a verified device associated with the network. For example, the intelligent component 610 can infer the installation of a particular device to a particular network; whether a close proximity is a valid attempt to exchange provisioning data; association of provisioning data to devices and/or networks, etc.

[0047] It is to be understood that the intelligent component 610 can provide for reasoning about or infer states of the system, environment, and/or user from a set of observations as captured via events and/or data. Inference can be employed to identify a specific context or action, or can generate a probability distribution over states, for example. The inference can be probabilistic - that is, the computation of a probability distribution over states of interest based on a consideration of data and events. Inference can also refer to techniques employed for composing higher-level events from a set of events and/or data. Such inference results in the construction of new events or actions from a set of observed events and/or stored event data, whether or not the events are
correlated in close temporal proximity, and whether the events and data come from one or several event and data sources. Various classification (explicitly and/or implicitly trained) schemes and/or systems (e.g., support vector machines, neural networks, expert systems, Bayesian belief networks, fuzzy logic, data fusion engines...) can be employed in connection with performing automatic and/or inferred action in connection with the claimed subject matter.

[0048] A classifier is a function that maps an input attribute vector, \( x = (x_1, x_2, x_3, x_4, xn) \), to a confidence that the input belongs to a class, that is, \( f(x) = \text{confidence}(\text{class}) \). Such classification can employ a probabilistic and/or statistical-based analysis (e.g., factoring into the analysis utilities and costs) to prognose or infer an action that a user desires to be automatically performed. A support vector machine (SVM) is an example of a classifier that can be employed. The SVM operates by finding a hypersurface in the space of possible inputs, which hypersurface attempts to split the triggering criteria from the non-triggering events. Intuitively, this makes the classification correct for testing data that is near, but not identical to training data. Other directed and undirected model classification approaches include, e.g., naïve Bayes, Bayesian networks, decision trees, neural networks, fuzzy logic models, and probabilistic classification models providing different patterns of independence can be employed. Classification as used herein also is inclusive of statistical regression that is utilized to develop models of priority.

[0049] Fig. 7 illustrates a conventional prior art wireless configuration 700 comprising of a plurality of wireless devices 7021, 7022, 7023, 7024, and 702N (collectively referred to as the wireless devices 702) which are connected wirelessly to a network entity 704 to mitigate the use of hard wiring. It is to be appreciated the number of wireless devices connected to a network entity can be 1 to N, where N is an integer greater than or equal to 1. Conventionally, a user would install each wireless device 702 individually finding a network entity 704 to connect in order to establish a wireless connection 7061, 7062, 7063, 7064, and 706N (collectively the wireless connections 706, in which each wireless connection relates to a wireless device and where N is an integer as defined above). Once the user selects the intended network entity 704 for installation, authentication of the wireless connection 706 for the wireless device 702 and the network entity 704 can be invoked. Thus, installation is initiated with the network entity 704 detecting a particular wireless device 702 and the network entity 704 for the wireless device 702 and the network entity 704 to establish a wireless connection 706. Second, if the network entity 704 finds wireless devices 702, determination of which wireless devices 702 to install is not known. Third, a wireless device 702 must be within range of the wireless connection 706 for installation and/or authentication. Lastly, authentication and security issues arise with the use of a wireless connection 706 such as, but not limited to, PIN limitations, "sniffing," password limitations, etc.

[0050] For example, a typical security measure invoked is the use of PINs which regulate wireless adapters that are authenticated to connect to the wireless router. In the present example, a user can provide a universal PIN which provides the wireless adapter to connect to the wireless router. However, the PIN is limited by what the user can remember and the character values that are compatible to each side (e.g., the wireless device side and the network entity side). For example, some PIN limitations can be requirements on the length, containing numbers, being different than user name, not incorporating user name, certain characters (e.g., "", ..., _), capital and lower case letters, ... Moreover, the PIN is vulnerable to "sniffing" from hackers who attempt to steal PINs to connect to the wireless router.

[0051] In another example involving conventional installation and/or authentication procedures/systems, universal interfaces (UIs) are provided on the network entity 704 and/or the wireless device 702. However, wireless keyboard installation and/or authentication to a computer (e.g., network entity) with a UI can be problematic. By utilizing a UI, a user needs to navigate within the interface in order to install the wireless keyboard. Yet, navigation through a UI can be troublesome without the aid of a keyboard. Since the user is installing a keyboard, one can not be used to navigate through the UI. Additionally, the simultaneous installation of multiple wireless devices 702 can cause immense confusion and complications for the network entity 704. Thus, the subject claimed matter mitigates the complications that arise with conventional installation and/or authentication systems and methods. By utilizing the NFC link as a trusted medium to exchange provisioning date, a secure data exchange can be utilized without compromising security constraints associated with wireless devices, networks, and/or network entities.

[0052] Figs. 8-9 illustrate methodologies in accordance with the claimed subject matter. For simplicity of explanation, the methodologies are depicted and described as a series of acts. It is to be understood and appreciated that the subject innovation is not limited by the acts illustrated and/or by the order of acts, for example acts can occur in various orders and/or concurrently, and with other acts not presented and described herein. Furthermore, not all illustrated acts may be required to implement the methodologies in accordance with the claimed subject matter. In addition, those skilled in the art will understand and appreciate that the methodologies could alternatively be represented as a series of interrelated states via a state diagram or events.

[0053] Fig. 8 illustrates a methodology 800 for provisioning a wireless device to a secure network by employ-
ing a near field communications link to exchange provisioning data. At reference numeral 802, a device can establish a near field communications (NFC) link with a verified device on a network and/or a network entity. The device can be any suitable device capable of a wireless connection and capable of NFC. Moreover, the verified device can be any device that had been previously secured to the network and/or a network entity utilizing a wireless connection and/or a hardwire connection. At reference numeral 804, the device can securely exchange provisioning data with the verified device utilizing the NFC link as a trusted medium. The NFC link can provide a secure and encrypted link over a short proximity and/or distance with a large bandwidth capable of handling the transfer of provisioning data. At reference numeral 808, the device can utilize the wireless connection on the network and/or associated with the network entity and/or verified device. After the secure transfer of provisioning data to the network, the device can be considered provisioned and the wireless connection can be utilized. It is to be appreciated that the wireless connection can be, but is not limited to, a wireless local area network (WLAN), Bluetooth, wireless fidelity (Wi-Fi), ultra-wideband (UWB), etc.

[0054] Fig. 9 illustrates a methodology 900 that facilitates securely installing a device to a secure network by utilizing a near field communications link. At reference numeral 902, a security technique can be implemented to ensure the validity of utilizing the near field communications (NFC) link for a trusted medium to transfer provisioning data related to a device. For instance, the security techniques can be, but are not limited to, a user name and password, personal identification number (PIN), a login, time-based proximity, biometric indicia (e.g., fingerprint, inductance, retina, ...), human interactive proofs (HIPs), voice recognition, etc. Once the security techniques ensure the use of NFC link, the communication channel can be utilized to transfer data securely (e.g., secured in two layers).

[0055] At reference numeral 904, a device can establish the near field communications (NFC) link with a verified device on a network. After the security techniques have been passed and/or initiated, the NFC link can be utilized as a trusted medium for which the device can communicate to the network and/or network entity. At reference numeral 906, a plug and go (PONG) technique can be implemented to transfer provisioning data to the network, network entity and/or verified device. The PONG technique can be considered generic enough to allow the provisioning of any suitable wireless device that employs various wireless connections (e.g., WLAN, Wi-Fi, Bluetooth, UWB, ...).

[0056] At reference numeral 908, the strongest wireless connection from the network can be determined based at least in part upon a statistical analysis. The device can receive a plurality of wireless signals within a particular network. Thus, after the provisioning of the device, a determination can be made as to which wireless connection and/or signal can provide the most efficient and/or strongest connection. Once a determination is made on which wireless connection is most suitable for the device, the device can utilize the wireless connection on the network at reference numeral 910.

[0057] In order to provide additional context for implementing various aspects of the claimed subject matter, Figs. 10-11 and the following discussion is intended to provide a brief, general description of a suitable computing environment in which the various aspects of the subject innovation may be implemented. While the claimed subject matter has been described above in the general context of computer-executable instructions of a computer program that runs on a local computer and/or remote computer, those skilled in the art will recognize that the subject innovation also may be implemented in combination with other program modules. Generally, program modules include routines, programs, components, data structures, etc., that perform particular tasks and/or implement particular abstract data types.

[0058] Moreover, those skilled in the art will appreciate that the inventive methods may be practiced with other computer system configurations, including single-processor or multi-processor computer systems, minicomputers, mainframe computers, as well as personal computers, hand-held computing devices, microprocessor-based and/or programmable consumer electronics, and the like, each of which may operatively communicate with one or more associated devices. The illustrated aspects of the claimed subject matter may also be practiced in distributed computing environments where certain tasks are performed by remote processing devices that are linked through a communications network. However, some, if not all, aspects of the subject innovation may be practiced on stand-alone computers. In a distributed computing environment, program modules may be located in local and/or remote memory storage devices.

[0059] Fig. 10 is a schematic block diagram of a sample computing environment 1000 with which the claimed subject matter can interact. The system 1000 includes one or more client(s) 1010. The client(s) 1010 can be hardware and/or software (e.g., threads, processes, computing devices). The system 1000 also includes one or more server(s) 1020. The server(s) 1020 can be hardware and/or software (e.g., threads, processes, computing devices). The servers 1020 can house threads to perform transformations by employing the subject innovation, for example.

[0060] One possible communication between a client 1010 and a server 1020 can be in the form of a data packet adapted to be transmitted between two or more computer processes. The system 1000 includes a communication framework 1040 that can be employed to facilitate communications between the client(s) 1010 and the server(s) 1020. The client(s) 1010 are operably connected to one or more client data store(s) 1050 that can be employed to store information local to the client(s) 1010. Similarly, the server(s) 1020 are operably connect-
ed to one or more server data store(s) 1030 that can be employed to store information local to the servers 1040. With reference to Fig. 11, an exemplary environment 1100 for implementing various aspects of the claimed subject matter includes a computer 1112. The computer 1112 includes a processing unit 1114, a system memory 1116, and a system bus 1118. The system bus 1118 couples system components including, but not limited to, the system memory 1116 to the processing unit 1114. The processing unit 1114 can be any of various available processors. Dual microprocessors and other multiprocessor architectures also can be employed as the processing unit 1114.

The system bus 1118 can be any of several types of bus structure(s) including the system bus or memory controller, a peripheral bus or external bus, and/or a local bus using any variety of available bus architectures including, but not limited to, Industrial Standard Architecture (ISA), Micro-Channel Architecture (MSA), Extended ISA (EISA), Intelligent Drive Electronics (IDE), VESA Local Bus (VLB), Peripheral Component Interconnect (PCI), Card Bus, Universal Serial Bus (USB), Advanced Graphics Port (AGP), Personal Computer Memory Card International Association bus (PCMCIA), Firewire (IEEE 1394), and Small Computer Systems Interface (SCSI).

The system memory 1116 includes volatile memory 1120 and nonvolatile memory 1122. The basic input/output system (BIOS), containing the basic routines to transfer information between elements within the computer 1112, such as during start-up, is stored in nonvolatile memory 1122. By way of illustration, and not limitation, nonvolatile memory 1122 can include read only memory (ROM), programmable ROM (PROM), electrically programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM), or flash memory. Volatile memory 1120 includes random access memory (RAM), which acts as external cache memory. By way of illustration and not limitation, RAM is available in many forms such as static RAM (SRAM), dynamic RAM (DRAM), synchronous DRAM (SDRAM), double data rate SDRAM (DDR SDRAM), enhanced SDRAM (ES-DRAM), Synchlink DRAM (SLDRAM), Rambus direct RAM (RDRAM), direct Rambus dynamic RAM (DRDRAM), and Rambus dynamic RAM (RDRAM). Computer 1112 also includes removable/non-removable, volatile/nonvolatile computer storage media. Fig. 11 illustrates, for example a disk storage 1124. Disk storage 1124 includes, but is not limited to, devices like a magnetic disk drive, floppy disk drive, tape drive, Jaz drive, Zip drive, LS-100 drive, flash memory card, or memory stick. In addition, disk storage 1124 can include storage media separately or in combination with other storage media including, but not limited to, an optical disk drive such as a compact disk ROM device (CD-ROM), CD recordable drive (CD-R Drive), CD rewritable drive (CD-RW Drive) or a digital versatile disk ROM drive (DVD-ROM). To facilitate connection of the disk storage devices 1124 to the system bus 1118, a removable or non-removable interface is typically used such as interface 1126.

It is to be appreciated that Fig. 11 describes software that acts as an intermediary between users and the basic computer resources described in the suitable operating environment 1100. Such software includes an operating system 1128. Operating system 1128, which can be stored on disk storage 1124, acts to control and allocate resources of the computer system 1112. System applications 1130 take advantage of the management of resources by operating system 1128 through program modules 1132 and program data 1134 stored either in system memory 1116 or on disk storage 1124. It is to be appreciated that the claimed subject matter can be implemented with various operating systems or combinations of operating systems.

A user enters commands or information into the computer 1112 through input device(s) 1136. Input devices 1136 include, but are not limited to, a pointing device such as a mouse, trackball, stylus, touch pad, keyboard, microphone, joystick, game pad, satellite dish, scanner, TV tuner card, digital camera, digital video camera, web camera, and the like. These and other input devices connect to the processing unit 1114 through the system bus 1118 via interface port(s) 1138. Interface port(s) 1138 include, for example, a serial port, a parallel port, a game port, and a universal serial bus (USB). Output device(s) 1140 use some of the same type of ports as input device(s) 1136. Thus, for example, a USB port may be used to provide input to computer 1112, and to output information from computer 1112 to an output device 1140. Output adapter 1142 is provided to illustrate that there are some output devices 1140 like monitors, speakers, and printers, among other output devices 1140, which require special adapters. The output adapters 1142 include, by way of illustration and not limitation, video and sound cards that provide a means of connection between the output device 1140 and the system bus 1118. It should be noted that other devices and/or systems of devices provide both input and output capabilities such as remote computer(s) 1144.

Computer 1112 can operate in a networked environment using logical connections to one or more remote computers, such as remote computer(s) 1144. The remote computer(s) 1144 can be a personal computer, a server, a router, a network PC, a workstation, a microprocessor based appliance, a peer device or other common network node and the like, and typically includes many or all of the elements described relative to computer 1112. For purposes of brevity, only a memory storage device 1146 is illustrated with remote computer(s) 1144. Remote computer(s) 1144 is logically connected to computer 1112 through a network interface 1148 and then physically connected via communication connection 1150. Network interface 1148 encompasses wire and/or wireless communication networks such as local-area networks (LAN) and wide-area networks (WAN). LAN
Communication connection(s) 1150 refers to networks, and Digital Subscriber Lines (DSL), works (ISDN) and variations thereon, packet switching networks like Integrated Services Digital Network cards. The hardware/software necessary for connection to the network interface 1148 includes, for exemplary purposes only, internal and external technologies such as, modems including regular telephone grade modems, cable modems and DSL modems, ISDN adapters, and Ethernet cards.

What has been described above includes examples of the subject innovation. It is, of course, not possible to describe every conceivable combination of components or methodologies for purposes of describing the claimed subject matter, but one of ordinary skill in the art may recognize that many further combinations and permutations of the subject innovation are possible. Accordingly, the claimed subject matter is intended to embrace all such alterations, modifications, and variations that fall within the scope of the appended claims.

In particular and in regard to the various functions performed by the above described components, devices, circuits, systems and the like, the terms (including a reference to a "means") used to describe such components are intended to correspond, unless otherwise indicated, to any component which performs the specified function of the described component (e.g., a functional equivalent), even though not structurally equivalent to the disclosed structure, which performs the function in the herein illustrated exemplary aspects of the claimed subject matter. In this regard, it will also be recognized that the innovation includes a system as well as a computer-readable medium having computer-executable instructions for performing the acts and/or events of the various methods of the claimed subject matter.

In addition, while a particular feature of the subject innovation may have been disclosed with respect to only one of several implementations, such feature may be combined with one or more other features of the other implementations as may be desired and advantageous for any given or particular application. Furthermore, to the extent that the terms "includes," and "including" and variants thereof are used in either the detailed description or the claims, these terms are intended to be inclusive in a manner similar to the term "comprising."

Claims

1. A system (400) that facilitates connecting a wireless device to a network, comprising:

   a verified master device (402) configured to have a trusted wireless connection (412) with a network entity (404) on the network;
   a wireless device (410) configured to establish a near field communication link (408) with the verified master device on the network;
   an installation component (406) incorporated in the wireless device and/or the verified master device that is configured to invoke transfer of provisioning data, via the near field communication link, to secure a wireless connection for the wireless device to the network,
   characterized in that the wireless device is configured to establish a wireless connection (414) with the network entity (404) utilizing the provisioning data,
   wherein the wireless connection (414) is secure based at least in part upon the exchanging of provisioning data between the verified master device and the wireless device via the near field communication link.

2. The system of claim 1, wherein the installation component (406) utilizes a PONG component (210) that utilizes a plug and go technique to transfer the provisioning data to the network via the near field communication link, the PONG components comprising a PONG manager that associates a PONG handler to a request associated with the provisioning data, and a PONG driver that channels request from the PONG manager to a PONG device over the near field communication link.

3. The system of claim 2, wherein the PONG handler sends a response to a driver through the PONG manager.

4. The system of claim 2, wherein the PONG handler receives a request from the PONG manager and parses the contents to determine an appropriate action.

5. The system of claim 4, wherein the PONG component (210) further comprises the implementation of a PONG request and a PONG response that are in a parse-able stream that includes at least one PONG attribute.

6. The system of claim 1, wherein the wireless device is at least one of the following: a computer; a network; a keyboard; a speaker; a mouse; a monitor; a headset; a pair of headphones; a remote; a router; an access point; a printer; a hard drive; a modem; a phone; a cellular communication device; a portable digital assistant (PDA); and a microphone.
7. The system of claim 1, wherein the wireless connection is at least one of a wireless local area network (WLAN), Bluetooth, wireless fidelity (Wi-Fi), and ultra-wideband (UWB).

8. The system of claim 1, wherein the installation component (406) establishes an ad-hoc network between at least the wireless device and an unverified device to enable connectivity there between.

9. The system of claim 1, further comprising a security component (312) that provides an additional security layer to ensure valid utilization of close proximity data transfer with respect to the near field communication link (408).

10. The system of claim 9, wherein the security layer includes at least one of the following security techniques: a smart card; a certificate; a cryptographic key; a user name and password; a personal identification number (PIN); a login; a time-based proximity; a biometric indicia; a fingerprint; an inductance; a retinal scan; a human interactive proof (HIP); and a voice recognition.

11. The system of claim 1, further comprising a manager component (314) that can manage at least one of the device connectivity to the network, association of one of a plurality of wireless connections associated with the network, and a proximity setting related to the near field communications.

12. The system of claim 10, wherein the manager component utilizes statistical analysis to determine the most efficient wireless connection for the wireless device from a plurality of wireless connections associated with the network.

13. The system of claim 1, wherein the plurality of wireless devices can connect to the network entity utilizing a near field connection link with the verified master device.

14. The system of claim 1, wherein the provisioning data includes at least one of installation protocol, authentication protocol, device configuration data, and device related data.

15. A computer-implemented method that facilitates connecting a wireless device to a network, comprising:

- establishing a near field communication link (408) between a wireless device (410) and a verified master device (402) on the network, the verified master device having a trusted wireless connection (412) with a network entity (404) on the network; and
- securely exchanging provisioning data to secure a wireless connection for the wireless device to the network, via the near field communication link (408),

characterized in that the method further comprises:
- establishing a wireless connection (414) between the wireless device and the network entity utilizing the provisioning data, wherein the wireless connection (414) is secure based at least in part upon the exchanging of provisioning data between the verified master device and the wireless device via the near field communication link.

16. The method of claim 15, further comprising:

- utilizing a PONG component (210) which utilizes a plug and go technique to transfer the provisioning data via the near field communication link;
- channeling requests from a PONG manager to a PONG device over the near field communication link via a PONG driver; and
- allowing the wireless device to utilize the wireless connection (414) associated with the network.

17. The method of claim 15, further comprising:

- implementing a security technique to ensure valid use of the near field communication link; and
- determining an efficient wireless connection (414) for the wireless device to utilize on the network.

18. A computer-implemented system that facilitates connecting a wireless device to a network, comprising:

- means for establishing a near field communication link (408) between a wireless device (410) and a verified master device (402) on the network, the verified master device having a trusted wireless connection (412) with a network entity (404) on the network; and
- means for invoking the transfer of provisioning data, via the near field communication link, to secure a wireless connection (110) for the wireless device to the network,

characterized in that the system further comprises: means for establishing a wireless connection (414) between the wireless device and the network entity utilizing the provisioning data, wherein the wireless connection (414) is secure based at least in part upon the exchanging of provisioning data between the verified master device and the wireless device via the near field communication link.
Patentansprüche

1. System (400), das das Verbinden einer drahtlosen Vorrichtung mit einem Netzwerk erleichtert, umfassend:
   eine verifizierte Hauptvorrichtung (402), die zum Verfügen über eine vertrauenswürdige drahtlose Verbindung (412) mit einer Netzwerkeinheit (404) im Netzwerk ausgelegt ist;
   eine drahtlose Vorrichtung (410), die zum Errichten einer Nahfeldkommunikationsverbindung (408) mit der verifizierten Hauptvorrichtung im Netzwerk ausgelegt ist;
   eine in die drahtlose Vorrichtung und/oder die verifizierte Hauptvorrichtung integrierte Installationskomponente (406), die zum Aufrufen einer Übertragung von Berechtigungsdaten über die Nahfeldkommunikationsverbindung ausgelegt ist, um eine drahtlose Verbindung der drahtlosen Vorrichtung mit dem Netzwerk zu sichern, dadurch gekennzeichnet, dass die drahtlose Vorrichtung zum Errichten einer drahtlosen Verbindung (414) mit der Netzwerkeinheit (404) unter Nutzung der Berechtigungsdaten ausgelegt ist, wobei die drahtlose Verbindung (414) zumindest teilweise auf der Grundlage des Austausches von Berechtigungsdaten zwischen der verifizierten Hauptvorrichtung und der drahtlosen Vorrichtung über die Nahfeldkommunikationsverbindung gesichert ist.

2. System nach Anspruch 1, wobei die Installationskomponente (406) eine PONG-Komponente (210) nutzt, die zum Übertragen der Berechtigungsdaten an das Netzwerk über die Nahfeldkommunikationsverbindung eine Plug-&-Go-Technik nutzt, wobei die PONG-Komponenten einen PONG-Manager, der einen PONG-Handler mit einer mit den Berechtigungsdaten verknüpften Anforderung verknüpft, und einen PONG-Treiber, der Anforderungen des PONG-Managers über die Nahfeldkommunikationsverbindung an eine PONG-Vorrichtung leitet, umfasst.


5. System nach Anspruch 4, wobei die PONG-Komponente (210) weiterhin die Implementierung einer PONG-Anforderung und einer PONG-Antwort umfasst, die sich in einem parsbaren Strom befinden, der mindestens ein PONG-Attribut enthält.

6. System nach Anspruch 1, wobei die drahtlose Vorrichtung mindestens eine der Folgenden ist: ein Computer; ein Netzwerk; eine Tastatur; ein Lautsprecher; eine Maus; ein Bildschirm; ein Headset; ein Paar Kopfhörer; eine Fernsteuerung; ein Router; ein Zugriffspunkt; ein Drucker; eine Festplatte; ein Modem; ein Telefon; eine zelluläre Kommunikationsvorrichtung; ein persönlicher digitaler Assistent (PDA) und ein Mikrofon.

7. System nach Anspruch 1, wobei die drahtlose Verbindung mindestens eine eines drahtlosen lokalen Netzwerks (WLAN), Bluetooth, Wireless Fidelity (Wi-Fi) und Ultrabreitband (UWB) ist.

8. System nach Anspruch 1, wobei die Installationskomponente (406) ein Ad-hoc-Netzwerk zwischen mindestens der drahtlosen Vorrichtung und einer nicht verifizierten Vorrichtung errichtet, um dazwischen Konnektivität zu ermöglichen.

9. System nach Anspruch 1, weiterhin umfassend eine Sicherheitskomponente (312), die eine zusätzliche Sicherheitsschicht bereitstellt, um eine gültige Nutzung von Datenübertragung aus nächster Nähe in Bezug auf die Nahfeldkommunikationsverbindung (408) zu gewährleisten.

10. System nach Anspruch 9, wobei die Sicherheitsschicht mindestens eine der folgenden Sicherheitstechniken enthält: eine Smartcard; ein Zertifikat; einen kryptografischen Schlüssel; einen Benutzernamen und ein Passwort; eine persönliche Identifizierungsnummer (PIN); ein Login; eine zeitbasierte Näh- he; ein biometrisches Indiz; einen Fingerabdruck; eine Induktivität; einen Retinascan; einen menschlichen interaktiven Beweis (HIP) und eine Spracherkennung.


12. System nach Anspruch 10, wobei die Managerkomponente statistische Analyse zum Bestimmen der effizientesten drahtlosen Verbindung für die drahtlose Vorrichtung aus einer Vielzahl von mit dem Netzwerk verknüpften drahtlosen Verbindungen nutzt.

13. System nach Anspruch 1, wobei die Vielzahl von drahtlosen Vorrichtungen unter Nutzung einer Nah-
feldkommunikationsverbindung mit der verifizierten Hauptvorrichtung mit der Netzwerkeinheit verbinderbar ist.

14. System nach Anspruch 1, wobei die Berechtigungsdaten mindestens eines von einem Installationsprotokoll, einem Authentifizierungsprotokoll, Vorrichtungskonfigurationsdaten und vorrichtungsbezogenen Daten enthalten.

15. Computerimplementiertes Verfahren, das das Verbinden einer drahtlosen Vorrichtung mit einem Netzwerk erleichtert, umfassend:

Errichten einer Nahfeldkommunikationsverbindung (408) zwischen einer drahtlosen Vorrichtung (410) und einer verifizierten Hauptvorrichtung (402) im Netzwerk, wobei die verifizierte Hauptvorrichtung eine vertrauenswürdige drahtlose Verbindung (412) mit einer Netzwerkeinheit (404) im Netzwerk aufweist; und sicheres Austauschen von Berechtigungsdaten, um eine drahtlose Verbindung der drahtlosen Vorrichtung mit dem Netzwerk über die Nahfeldkommunikationsverbindung (408) zu sichern, dadurch gekennzeichnet, dass das Verfahren ferner umfasst:

Errichten einer drahtlosen Verbindung (414) zwischen der drahtlosen Vorrichtung und der Netzwerkeinheit unter Nutzung der Berechtigungsdaten, wobei die drahtlose Verbindung (414) zumindest teilweise auf der Grundlage des Austausches von Berechtigungsdaten zwischen der verifizierten Hauptvorrichtung und der drahtlosen Vorrichtung über die Nahfeldkommunikationsverbindung gesichert ist.

16. Verfahren nach Anspruch 15, weiterhin umfassend:

Nutzung einer PONG-Komponente (210), die zum Übertragen der Berechtigungsdaten über die Nahfeldkommunikationsverbindung eine Plug-&-Go-Technik nutzt; Leiten von Anforderungen eines PONG-Managers über die Nahfeldkommunikationsverbindung via eines PONG-Treibers an die PONG-Vorrichtung; und Zulassen der Nutzung der mit dem Netzwerk verknüpften drahtlosen Verbindung (414) durch die drahtlose Vorrichtung.

17. Verfahren nach Anspruch 15, weiterhin umfassend:

Implementieren einer Sicherheitstechnik zum Gewährleisten einer gültigen Verwendung der Nahfeldkommunikationsverbindung; und Bestimmen einer effizienten drahtlosen Verbindung (414) für die drahtlose Vorrichtung zur Nutzung im Netzwerk.

18. Computerimplementiertes System, das das Verbinden einer drahtlosen Vorrichtung mit einem Netzwerk erleichtert, umfassend:

Mittel zum Errichten einer Nahfeldkommunikationsverbindung (408) zwischen einer drahtlosen Vorrichtung (410) und einer verifizierten Hauptvorrichtung (402) im Netzwerk, wobei die verifizierte Hauptvorrichtung eine vertrauenswürdige drahtlose Verbindung (412) mit einer Netzwerkeinheit (404) im Netzwerk aufweist; und Mittel zum Aufrufen der Übertragung von Berechtigungsdaten über die Nahfeldkommunikationsverbindung, um eine drahtlose Verbindung (110) der drahtlosen Vorrichtung mit dem Netzwerk zu sichern, dadurch gekennzeichnet, dass das System ferner umfasst:

Mittel zum Errichten einer drahtlosen Verbindung (414) zwischen der drahtlosen Vorrichtung und der Netzwerkeinheit unter Nutzung der Berechtigungsdaten, wobei die drahtlose Verbindung (414) zumindest teilweise auf der Grundlage des Austausches von Berechtigungsdaten zwischen der verifizierten Hauptvorrichtung und der drahtlosen Vorrichtung über die Nahfeldkommunikationsverbindung gesichert ist.

Revendications

1. Système (400) qui facilite la connexion d’un dispositif sans fil à un réseau, comprenant :

un dispositif maître vérifié (402) configuré de manière à présenter une connexion sans fil fiable (412) avec une entité de réseau (404) sur le réseau ;

un dispositif sans fil (410) configuré de manière à établir une liaison de communication en champ proche (408) avec le dispositif maître vérifié sur le réseau ;

un composant d’installation (406) incorporé dans le dispositif sans fil et/ou dans le dispositif maître vérifié, qui est configuré de manière à invoquer un transfert de données de provisionnement par l’intermédiaire de la liaison de communication en champ proche, à sécuriser une connexion sans fil pour le dispositif sans fil au réseau, caractérisé en ce que le dispositif sans fil est configuré de manière à établir une connexion sans fil (414) avec l’entité de réseau (404) en utilisant les données de provisionnement, dans lequel la connexion sans fil (414) est...
sécurisée sur la base, au moins en partie, de l’échange de données de provisionnement entre le dispositif maître vérifié et le dispositif sans fil par l’intermédiaire de la liaison de communication en champ proche.

2. Système selon la revendication 1, dans lequel le composant d’installation (406) utilise un composant PONG (210) qui fait appel à une technique « prêt à l’emploi » en vue de transférer les données de provisionnement au réseau par l’intermédiaire de la liaison de communication en champ proche, les composants PONG comprenant un gestionnaire PONG qui associe un module de traitement PONG à une demande associée aux données de provisionnement, et un pilote PONG qui achemine la demande, du gestionnaire PONG à un dispositif PONG sur la liaison de communication en champ proche.

3. Système selon la revendication 2, dans lequel le module de traitement PONG envoie une réponse à un pilote par l’intermédiaire du gestionnaire PONG.

4. Système selon la revendication 2, dans lequel le module de traitement PONG reçoit une demande en provenance du gestionnaire PONG et analyse les contenus en vue de déterminer une action appropriée.

5. Système selon la revendication 4, dans lequel le composant PONG (210) comprend en outre la mise en œuvre d’une demande PONG et d’une réponse PONG qui sont dans un flux analysable lequel inclut au moins un attribut PONG.

6. Système selon la revendication 1, dans lequel le dispositif sans fil correspond à au moins l’un des éléments suivants : un ordinateur ; un réseau ; un clavier ; un haut-parleur ; une souris ; un moniteur ; un casque d’écoute ; une paire d’écouteurs ; une télécommande ; un routeur ; un point d’accès ; une imprimante ; un disque dur ; un modem ; un téléphone ; un dispositif de communication cellulaire ; un assistant numérique portable (PDA) et un microphone.

7. Système selon la revendication 1, dans lequel la connexion sans fil correspond à au moins l’une parmi une connexion de réseau local sans fil (WLAN), une connexion Bluetooth, une connexion de technologie Wi-Fi et une connexion ultra-large bande (UWB).

8. Système selon la revendication 1, dans lequel le composant d’installation (406) établit un réseau ad hoc entre au moins le dispositif sans fil et un dispositif non vérifié en vue de permettre une connectivité entre eux.

9. Système selon la revendication 1, comprenant en outre un composant de sécurité (312) qui fournit une couche de sécurité supplémentaire permettant de garantir une utilisation valide d’un transfert de données à proximité immédiate par rapport à la liaison de communication en champ proche (408).

10. Système selon la revendication 9, dans lequel la couche de sécurité inclut au moins l’une des techniques de sécurité ci-après : une carte à puce intelligente, un certificat, une clé cryptographique, un nom d’utilisateur et un mot de passe ; un numéro d’identification personnel (PIN) ; un identifiant ; une proximité temporelle ; un indice biométrique ; une empreinte digitale ; une indiscrétion ; un balayage rétinien ; une preuve d’interaction humaine (HIP) ; et une reconnaissance vocale.

11. Système selon la revendication 1, comprenant en outre un composant de gestionnaire (314) en mesure de gérer au moins l’un des éléments parmi une connectivité de dispositif au réseau, l’association de l’une d’une pluralité de connexions sans fil associées au réseau, et un réglage de proximité connexe aux communications en champ proche.

12. Système selon la revendication 10, dans lequel le composant de gestionnaire fait appel à une analyse statistique en vue de déterminer la connexion sans fil la plus efficace pour le dispositif sans fil parmi une pluralité de connexions sans fil associées au réseau.

13. Système selon la revendication 1, dans lequel la pluralité de dispositifs sans fil peut se connecter à l’entité de réseau en faisant appel à une liaison de connexion en champ proche avec le dispositif maître vérifié.

14. Système selon la revendication 1, dans lequel les données de provisionnement incluent au moins un élément parmi un protocole d’installation, un protocole d’authentification, des données de configuration de dispositif, et des données connexes au dispositif.

15. Procédé, mis en œuvre par ordinateur, qui facilite la connexion d’un dispositif sans fil à un réseau, comprenant les étapes ci-dessous consistant à établir une liaison de communication en champ proche (408) entre un dispositif sans fil (410) et un dispositif maître vérifié (402) sur le réseau, dans lequel le dispositif maître vérifié présente une connexion sans fil fiable (412) avec une entité de réseau (404) sur le réseau ; et échanger, de manière sécurisée, des données de provisionnement pour sécuriser une connexion sans fil pour le dispositif sans fil au ré-
seau, par l'intermédiaire de la liaison de communication en champ proche (408) ;
caractérisé en ce que le procédé comprend en outre l'étape ci-dessous consistant à :
établi une connexion sans fil (414) entre le dispositif sans fil et l'entité de réseau en faisant appel aux données de provisionnement, dans lequel la connexion sans fil (414) est sécurisée sur la base, au moins en partie, de l'échange de données de provisionnement entre le dispositif maître vérifié et le dispositif sans fil, par l'intermédiaire de la liaison de communication en champ proche.

16. Procédé selon la revendication 15, comprenant en outre les étapes ci-dessous consistant à :

- utiliser un composant PONG (210) qui fait appel à une technique « prêt à l'emploi » pour transférer les données de provisionnement par l'intermédiaire de la liaison de communication en champ proche ;
- acheminer des demandes, d'un gestionnaire PONG vers un dispositif PONG, sur la liaison de communication en champ proche, par l'intermédiaire d'un pilote PONG ; et
- permettre au dispositif sans fil d'utiliser la connexion sans fil (414) associée au réseau.

17. Procédé selon la revendication 15, comprenant en outre les étapes ci-dessous consistant à :

- mettre en œuvre une technique de sécurité en vue de garantir l'utilisation valide de la liaison de communication en champ proche ; et
- déterminer une connexion sans fil efficace (414) devant être utilisée par le dispositif sans fil sur le réseau.

18. Système mis en œuvre par ordinateur qui facilite la connexion d'un dispositif sans fil à un réseau, comprenant :

- un moyen pour établir une liaison de communication en champ proche (408) entre un dispositif sans fil (410) et un dispositif maître vérifié (402) sur le réseau, dans lequel le dispositif maître vérifié présente une connexion sans fil fiable (412) avec une entité de réseau (404) sur le réseau ; et
- un moyen pour invoquer le transfert de données de provisionnement par l'intermédiaire de la liaison de communication en champ proche, en vue de sécuriser une connexion sans fil (110) pour le dispositif sans fil au réseau ;
caractérisé en ce que le système comprend en outre :
- un moyen pour établir une connexion sans fil (414) entre le dispositif sans fil et l'entité de réseau en faisant appel aux données de provisionnement, dans lequel la connexion sans fil (414) est sécurisée sur la base, au moins en partie, de l'échange de données de provisionnement entre le dispositif maître vérifié et le dispositif sans fil, par l'intermédiaire de la liaison de communication en champ proche.
FIG. 1
FIG. 2
FIG. 4
FIG. 5
FIG. 7
A DEVICE ESTABLISHES NEAR FIELD COMMUNICATIONS VIA A LINK WITH A VERIFIED DEVICE ON A NETWORK

THE DEVICE SECURELY EXCHANGES PROVISIONING DATA WITH THE VERIFIED DEVICE

THE DEVICE UTILIZES THE WIRELESS CONNECTION ON THE NETWORK

FIG. 8
IMPLEMENT SECURITY TECHNIQUES TO ENSURE VALID USE OF NFC LINK

A DEVICE ESTABLISHES A NEAR FIELD COMMUNICATION WITH A VERIFIED DEVICE ON A NETWORK

UTILIZE PONG TECHNIQUE TO TRANSFER PROVISIONING DATA

DETERMINE THE EFFICIENT WIRELESS CONNECTION FOR THE DEVICE

THE DEVICE UTILIZES THE WIRELESS CONNECTION ON THE NETWORK

FIG. 9
FIG. 10
REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader’s convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

• EP 1633104 A1 [0006]