US008995981B1

(12) **United States Patent**
Aginsky et al.

(10) **Patent No.: US 8,995,981 B1**
(45) **Date of Patent: Mar. 31, 2015**

(54) **SYSTEMS AND METHODS FOR REMOTE CONTROL ADAPTIVE CONFIGURATION**

(75) Inventors: **Vladislav Aginsky**, Kiryat Yam (IL); **Dani Shaket**, Nesher (IL)

(73) Assignee: **CSR Technology Inc.**, San Jose, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 158 days.

(21) Appl. No.: **13/194,307**

(22) Filed: **Jul. 29, 2011**

Related U.S. Application Data

(60) Provisional application No. 61/482,361, filed on May 4, 2011, provisional application No. 61/422,537, filed on Dec. 13, 2010.

(51) **Int. Cl.**
H04M 3/00 (2006.01)
H04M 1/725 (2006.01)
H04W 4/00 (2009.01)

(52) **U.S. Cl.**
CPC ***H04M 1/72533*** (2013.01); ***H04W 4/008*** (2013.01)
USPC **455/419**

(58) **Field of Classification Search**
USPC 455/418–720, 414.1, 41.2, 41.3, 554.2, 455/556.1
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,623,887 A 11/1986 Welles, II
4,959,810 A 9/1990 Darbee et al.
5,614,906 A 3/1997 Hayes et al.
6,225,938 B1 5/2001 Hayes et al.
6,344,861 B1 2/2002 Naughton et al.
6,407,779 B1 6/2002 Herz
7,155,305 B2 12/2006 Hayes et al.
7,218,243 B2 5/2007 Hayes et al.
7,895,535 B2 * 2/2011 Carlson et al. 715/855
8,006,002 B2 * 8/2011 Kalayjian et al. 710/36
2003/0103088 A1 * 6/2003 Dresti et al. 345/835
2004/0249925 A1 12/2004 Jeon et al.
2006/0148518 A1 7/2006 Ferris
2006/0150120 A1 * 7/2006 Dresti et al. 715/810
2007/0080823 A1 * 4/2007 Fu et al. 340/825.22

(Continued)

OTHER PUBLICATIONS

BD Touch, Copyright 2011 BD Touch, LLC, http://www.bdtouch.com Jun. 3, 2011, pp. 2.

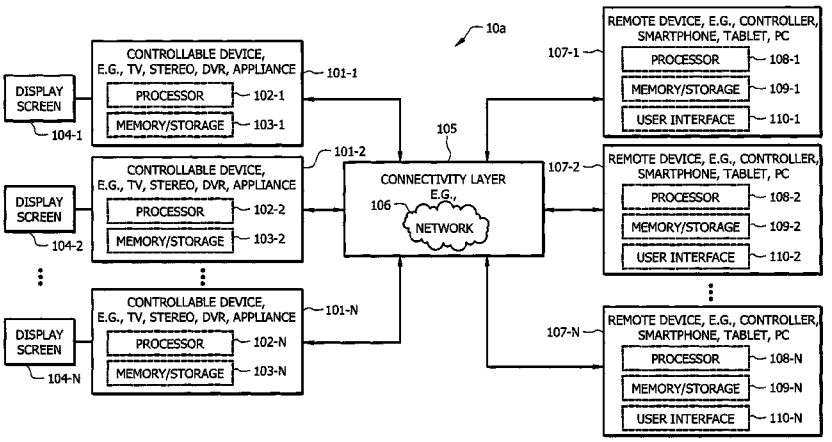
(Continued)

Primary Examiner — Brandon Miller
(74) *Attorney, Agent, or Firm* — Norton Rose Fulbright US LLP

(57) **ABSTRACT**

The present disclosure is directed to systems and methods in which a controllable device transfers to the remote device, such as to a remote control application ("app") located on a smartphone, a data structure identifying various functions that can be controlled by a remote device, together with the identity of the signal type that will achieve the desired operation. The remote device, upon accepting input directly from the remote device, can then allow the remote device user to select how controls of the various functions are to be configured and presented to, or otherwise selectively arranged for a user on a user interface of the remote device. In this way, the present disclosure provides a single highly customizable system. Distributors, resellers, and/or manufacturers of various electronic devices will be able utilize the same controllable device instructions, yet visually distinguish its brand name from other solutions using the same instructions.

47 Claims, 7 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

2008/0165024	A1*	7/2008	Gretton et al.	340/825.22
2008/0174449	A1*	7/2008	Schmidt et al.	340/825.22
2009/0156251	A1	6/2009	Cannistraro et al.	
2009/0195349	A1	8/2009	Frader-Thompson et al.	
2009/0239587	A1	9/2009	Negron et al.	
2009/0298535	A1*	12/2009	Klein et al.	455/556.1
2010/0017736	A1	1/2010	Kim	
2010/0134240	A1*	6/2010	Sims et al.	340/5.1
2010/0313169	A1*	12/2010	Huang et al.	715/835
2010/0321201	A1	12/2010	Huang et al.	
2010/0325565	A1	12/2010	Skinner et al.	
2010/0328547	A1	12/2010	Mayorga	
2011/0063506	A1	3/2011	Reams	
2012/0146918	A1*	6/2012	Kreiner et al.	345/173

OTHER PUBLICATIONS

"Turn Your Smartphone Into a Home Theater Remote Control," by Loyd Case, Mar. 14, 2010, http://www.pcworld.com/printable/article/id,214423/printable.html Mar. 23, 2011, pp. 1-18.

* cited by examiner

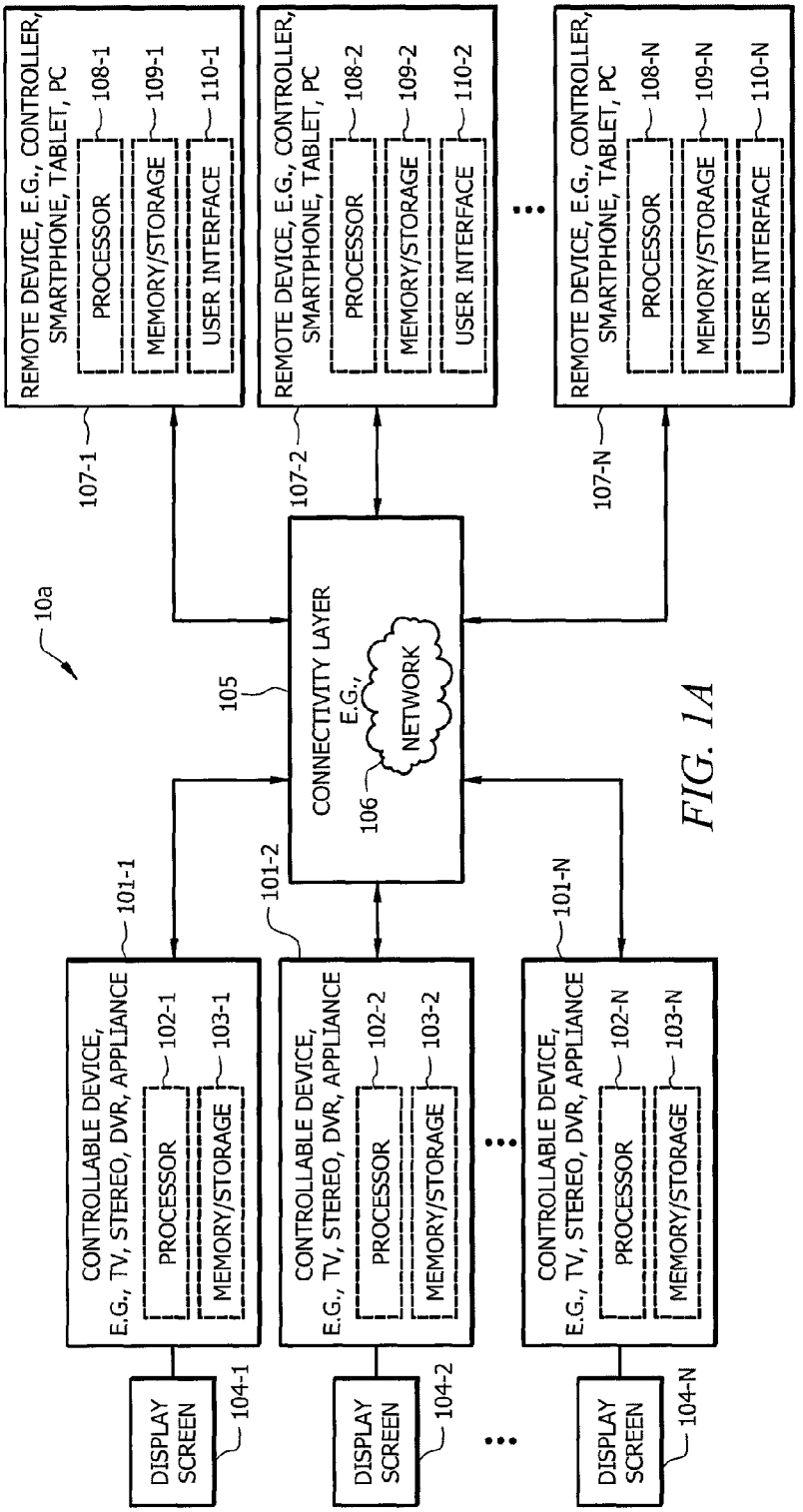

10a
REMOTE DEVICE, E.G., CONTROLLER, SMARTPHONE, TABLET, PC
PROCESSOR
MEMORY/STORAGE
USER INTERFACE
108-1
109-1
110-1
107-1
REMOTE DEVICE, E.G., CONTROLLER, SMARTPHONE, TABLET, PC
PROCESSOR
MEMORY/STORAGE
USER INTERFACE
108-2
109-2
110-2
107-2
REMOTE DEVICE, E.G., CONTROLLER, SMARTPHONE, TABLET, PC
PROCESSOR
MEMORY/STORAGE
USER INTERFACE
108-N
109-N
110-N
107-N
105
CONNECTIVITY LAYER
E.G.,
NETWORK
106
101-1
CONTROLLABLE DEVICE, E.G., TV, STEREO, DVR, APPLIANCE
PROCESSOR
MEMORY/STORAGE
102-1
103-1
101-2
CONTROLLABLE DEVICE, E.G., TV, STEREO, DVR, APPLIANCE
PROCESSOR
MEMORY/STORAGE
102-2
103-2
101-N
CONTROLLABLE DEVICE, E.G., TV, STEREO, DVR, APPLIANCE
PROCESSOR
MEMORY/STORAGE
102-N
103-N
DISPLAY SCREEN
104-1
DISPLAY SCREEN
104-2
DISPLAY SCREEN
104-N

FIG. 1A

10b

109-1

REMOTE DEVICE MEMORY/STORAGE

115 115'

CONTROLLABLE DEVICE 101-1			
FUNCTION 111-1	SIGNAL 112-1	STATUS 113-1	CONFIGURATION 114-1
ON - OFF	XY1	ON	BUTTON - RIGHT SIDE
MENU	XY2	ON	BUTTON - CENTER
VOLUME	XX1	ON ON	UP - RIGHT BOTTOM DOWN - LEFT BOTTOM
CHANNEL	ZZZ	ON	BUTTON - CENTER BOTTOM
INPUT	XY3	OFF	-

116 116'

CONTROLLABLE DEVICE 101-2			
FUNCTION 111-2	SIGNAL 112-2	STATUS 113-2	CONFIGURATION 114-2
ON - OFF	XX3	ON	RIGHT SIDE
VOLUME	XY5	ON	UP - DOWN - TOP
START	AB1	ON	GREEN LIGHT
STOP	AB2	ON	RED LIGHT
FAST FORWARD	AB3	ON	ARROW - RIGHT
FAST REWIND	AB4	ON	ARROW - LEFT
PAUSE	AB5	ON	BARS - BOTTOM
RECORD	XY6	ON	BUTTON RED

FIG. 1B

10c

CONTROLLABLE DEVICE MEMORY/STORAGE — 103-1

REMOTE DEVICE 107-1 = NAME : MASTER		
FUNCTION 119-1	STATUS 120-1	RULES 121-1
ON - OFF	YES	UNLIMITED
VOLUME	YES	UNLIMITED
MENU	YES	-
CHANNEL	YES	ALL
INPUT	NO	-

117

REMOTE DEVICE 107-2 = NAME : CHILD 1		
FUNCTION 119-2	STATUS 120-2	RULES 121-2
ON - OFF	YES	NOT AFTER MIDNIGHT
VOLUME	YES	OFF AFTER 9PM
MENU	NO	-
CHANNEL	YES	NOTHING ABOVE 100 NO PREMIUM NO PAY-PER-VIEW
INPUT	NO	-

118

FIG. 1C

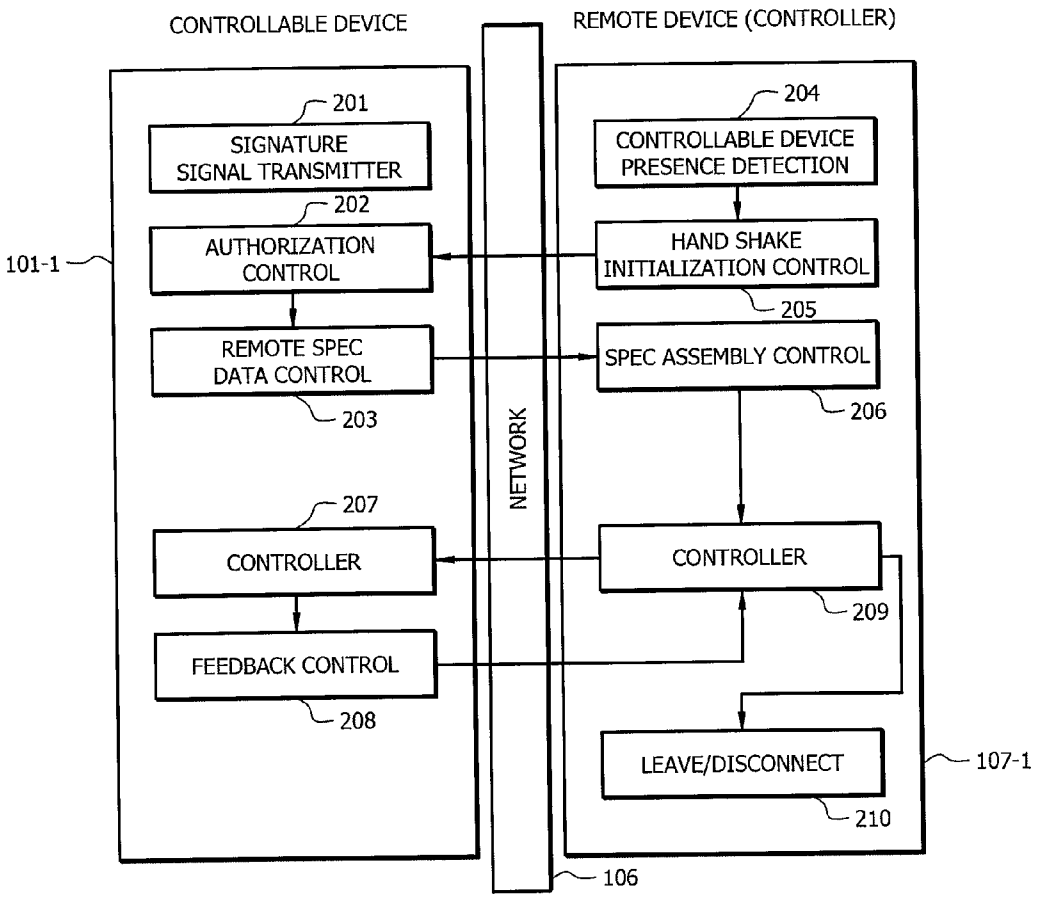

CONTROLLABLE DEVICE
REMOTE DEVICE (CONTROLLER)
201
SIGNATURE SIGNAL TRANSMITTER
202
AUTHORIZATION CONTROL
101-1
REMOTE SPEC DATA CONTROL
203
207
CONTROLLER
FEEDBACK CONTROL
208
NETWORK
204
CONTROLLABLE DEVICE PRESENCE DETECTION
HAND SHAKE INITIALIZATION CONTROL
205
SPEC ASSEMBLY CONTROL
206
CONTROLLER
209
LEAVE/DISCONNECT
210
107-1
106

FIG. 2

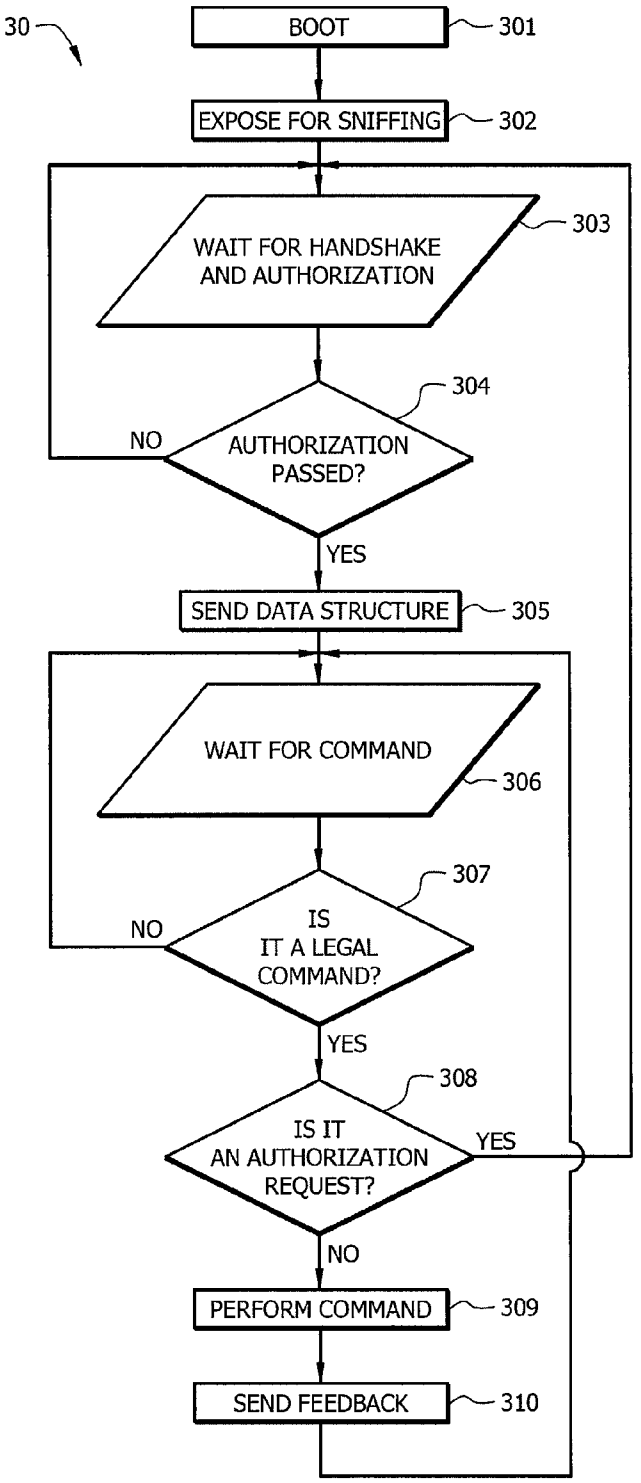

30
BOOT
301
EXPOSE FOR SNIFFING
302
WAIT FOR HANDSHAKE AND AUTHORIZATION
303
304
NO
AUTHORIZATION PASSED?
YES
SEND DATA STRUCTURE
305
WAIT FOR COMMAND
306
307
NO
IS IT A LEGAL COMMAND?
YES
308
IS IT AN AUTHORIZATION REQUEST?
YES
NO
PERFORM COMMAND
309
SEND FEEDBACK
310

FIG. 3

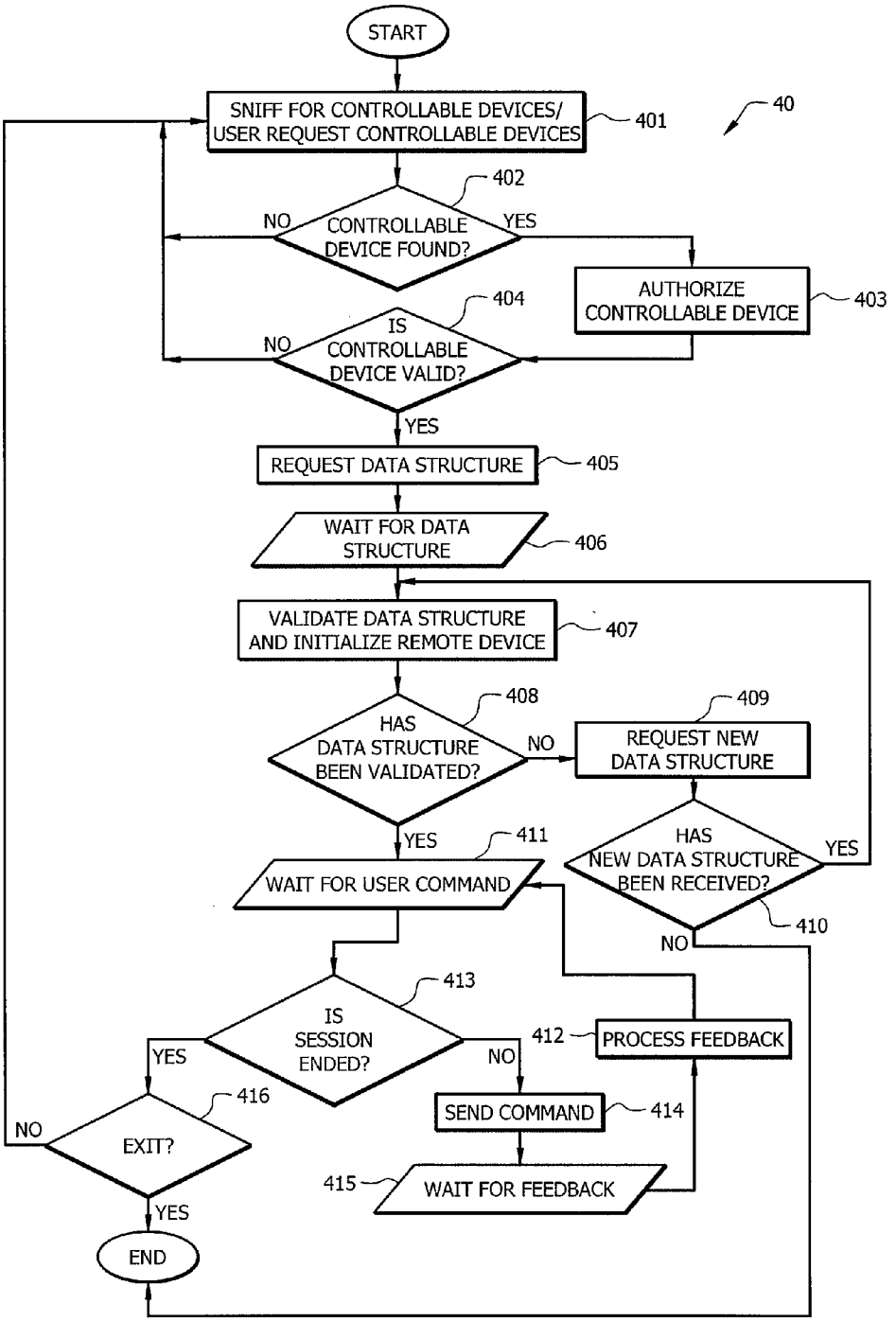

START
SNIFF FOR CONTROLLABLE DEVICES/ USER REQUEST CONTROLLABLE DEVICES
401
40
402
CONTROLLABLE DEVICE FOUND?
NO
YES
AUTHORIZE CONTROLLABLE DEVICE
403
404
IS CONTROLLABLE DEVICE VALID?
NO
YES
REQUEST DATA STRUCTURE
405
WAIT FOR DATA STRUCTURE
406
VALIDATE DATA STRUCTURE AND INITIALIZE REMOTE DEVICE
407
408
HAS DATA STRUCTURE BEEN VALIDATED?
NO
409
REQUEST NEW DATA STRUCTURE
YES
411
WAIT FOR USER COMMAND
HAS NEW DATA STRUCTURE BEEN RECEIVED?
YES
410
NO
413
IS SESSION ENDED?
YES
NO
412
PROCESS FEEDBACK
416
EXIT?
NO
YES
SEND COMMAND
414
415
WAIT FOR FEEDBACK
END

FIG. 4

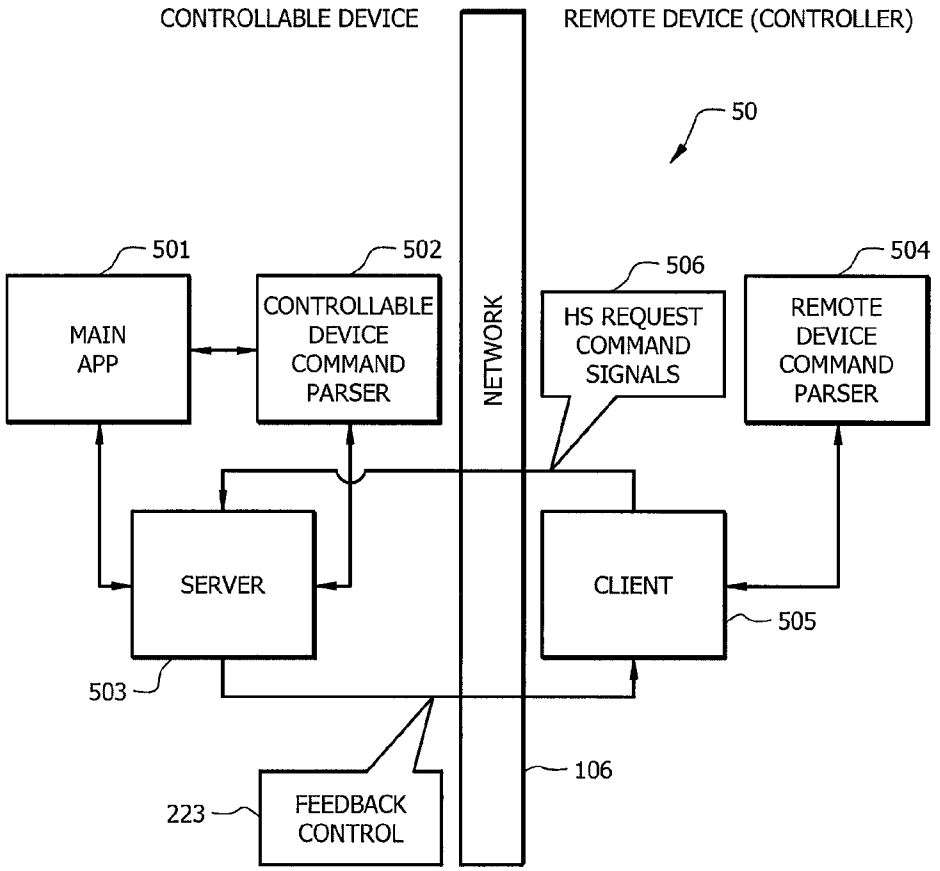

CONTROLLABLE DEVICE
REMOTE DEVICE (CONTROLLER)
50
501
MAIN APP
502
CONTROLLABLE DEVICE COMMAND PARSER
NETWORK
506
HS REQUEST COMMAND SIGNALS
504
REMOTE DEVICE COMMAND PARSER
SERVER
CLIENT
505
503
106
223
FEEDBACK CONTROL

FIG. 5

SYSTEMS AND METHODS FOR REMOTE CONTROL ADAPTIVE CONFIGURATION

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Application No. 61,482,361 filed on May 4, 2011 entitled, "ADAPTIVE METHOD OF CONFIGURING REMOTE CONTROL IP APPLICATION and U.S. Provisional Application No. 61/422,537 filed on Dec. 13, 2010 entitled, "ADAPTIVE METHOD OF CONFIGURING REMOTE CONTROL IP APPLICATION" the disclosures of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

It is known that a user can control certain functions of an electronic device, for example, the volume of a television or the record setting on a DVR, using a remote device (sometimes referred to as a "clicker," or simply a "remote control"). Such a remote device may be programmed to control several different electronic devices, or different types of specific electronic devices (i.e., one "universal" remote can be programmed to control various brands of televisions).

One known method of programming a remote device requires a user to select a button having a defined function and then select from a menu or list of codes related to the brand of electronic device to be controlled. Once the selection is made, the button will control a corresponding function of the electronic device. For example, assume a user desires to control the volume of a Sony TV. From the remote device, a user operates the button pre-defined as a volume-control button. The user is prompted to select or set a code corresponding to Sony TV's. If the selected code is proper for a Sony TV, the volume button on the remote device is "programmed" to control the volume of the Sony TV.

Another programming method allows a user to copy, into a clone remote device, programming signals from a source remote. Based on the copied information, the clone remote device can control an electronic device (e.g., the volume of a Sony TV) just like the source remote.

Such prior art programming methods for remotes are not sufficiently flexible nor customizable to meet the specific needs of users. For example, it would be difficult, if not impossible, to use prior art programming methods to configure a remote in one way for one user (for example, with the pause button on the top of the device), and the same remote configured another way for another user (for example, with the pause button on the bottom of the device).

A further issue is that manufacturers of different controllable electronic devices have proprietary internal structures that accept signals from remote devices and then convert the received signals into specific actions. The various functions that are performed for different devices vary from device to device and different devices use different data structures to achieve their operations.

Also known are "smart" devices, such as iPhones, iPads and the like, having applications thereon that enable the smart device to remotely control one or more specific electronic devices. Since the electronic devices to be controlled typically have unique signal control instructions, the smart device must be programmed in the manner described above, or alternatively, a set of control instructions must be download. Such control instructions may be downloaded from a common store or website compatible with the smart device. Thus, if a user desires his or her smart device to remotely control three

different electronic devices, the control instructions for each of the three controlled electronic devices must be delivered individually from a remote location. This is inefficient, impossible where there is no Internet connection, and may be costly due to downloading fees.

Going on-line to acquire programming information for smart device remote control applications is also problematic in some situations because it requires each manufacturer to make public its signal control sets and to do so in versions that interface properly with the latest hardware/software version of each smart device. This can become a most difficult task to manage and may require a sophisticated tracking network to maintain over a period of time.

BRIEF SUMMARY OF THE INVENTION

Disclosed herein is a system and method for remote control adaptive configuration. According to one aspect of the present invention, a controllable device (controlled device) is responsible for specifying functions available for control by a remote device (controlling device), while the remote device is responsible for creating a graphical representation and applying visual effects that will be presented to a user at the remote device exercising such control. In this way, the present disclosure provides a single highly customizable common system. A distributors, reseller, and/or manufacturer of various electronic devices, such as DVD players, automobiles, Bluetooth headsets, etc., will be able utilize the same controllable device function specification, yet visually distinguish its brand name from other solutions using the same specification.

In one embodiment, a controllable device transfers to a remote device, such as to a remote control application ("app") located on a SmartPhone, a data structure identifying various functions that can be controlled by a remote device, together with the identity of the signal type that will achieve the desired operation. The remote device, upon accepting input directly from the remote device, can then allow the remote device user to select how controls of the various functions are to be configured and presented to, or otherwise selectively arranged for a user on a user interface of the remote device.

In one embodiment, the data structure transferred is relatively small, so that transfer occurs quickly and may be repeated periodically, such as at each new session between the remote device and the controllable device. Small data files also enable the remote device to store many different data structures so as to accommodate protocols for different remote devices and users. This, in turn, allows different users to have control functions unique to the user and/or unique to the remote device type. The small file size also leaves room to store data that will heighten security. One such security function could be that the controllable device's data structure stored on the remote device is renewed during each session, such that if it had been hacked or changed in any manner, the new data structure would replace the changed data structure and the protocols established for the remote device would be maintained.

In one embodiment, all the controllable devices at a location that can be controlled by a particular remote device can be displayed to a user of the remote device. Controllable devices can range from TVs and DVRs to printers, computers, and cameras, or even kitchen appliances or automobiles. In some embodiments, the controllable device and/or remote device can be password protected such that unknown or unwanted users cannot access the controllable device and/or remote device, change protocols without an owner's permission, or a user can be recognized facilitating delivery of the proper data structure to the remote device.

The foregoing has outlined rather broadly the features and technical advantages of the present invention in order that the detailed description of the invention that follows may be better understood. Additional features and advantages of the invention will be described hereinafter which form the subject of the claims of the invention. It should be appreciated by those skilled in the art that the conception and specific embodiment disclosed may be readily utilized as a basis for modifying or designing other structures for carrying out the same purposes of the present invention. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the invention as set forth in the appended claims. The novel features which are believed to be characteristic of the invention, both as to its organization and method of operation, together with further objects and advantages will be better understood from the following description when considered in connection with the accompanying figures. It is to be expressly understood, however, that each of the figures is provided for the purpose of illustration and description only and is not intended as a definition of the limits of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, in which:

FIG. **1**A shows one embodiment of a system utilizing the concepts discussed herein;

FIG. **1**B shows one embodiment of a portion of memory of a remote device that has been "programmed" with the data structure from two controllable devices in accordance with the present invention;

FIG. **1**C shows one embodiment of a portion of a data structure for controlling a controllable device in accordance with the present invention;

FIG. **2** shows one embodiment of the operation of a remote device working in cooperation with a controllable device in accordance with the present invention;

FIG. **3** shows one embodiment of a typical life cycle of a controllable device in accordance with the present invention;

FIG. **4** shows one embodiment of a typical life cycle of a remote device in accordance with the present invention; and

FIG. **5** shows one embodiment of data flow in the system configured according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

According to one aspect of the present invention, a controllable device (controlled device) is responsible for specifying functions (providing limited instructions) for control by a remote device (controlling device or controller), while the remote device is responsible for creating a graphical representation and applying visual (or other sensory) effects that will be presented to a user at the remote device exercising control. In this way, the present invention provides a highly customizable system by which distributors, resellers, and manufacturers of various electronic devices will be able utilize the same controllable device instructions, yet visually distinguish its brand name from other solutions using the same instructions.

FIG. **1**A shows one embodiment of a system, such as embodiment **10***a*, that utilizes the concepts discussed herein. In the embodiment shown, one or more controllable devices, **101-1** to **101**-N, are capable of being paired with one or more remote devices, **107-1** to **107**-N, via connectivity layer **105**, such that a remote device may be used to control specific operations and functions of the controllable device during a paired session. Controllable functions vary with the controllable device and can be related to any operation of the controllable device. Exemplary functions to control of a TV include on/off, channel, and volume; of a DVR include play, fast-forward, and record; of a coffee maker include on/off and brew. Additional exemplary functions are described with reference to FIGS. **1**B and **1**C, and at FUNCTION columns **111-1**, **111-2**, **119-1**, and **119-2** of same.

Controllable devices **101-1** to **101**-N may be any one or combination of various types of processor-controlled programmable electronic devices, including, for example, set-top boxes, cable boxes, televisions, digital video recorders, cameras, printers, small and large appliances, and vehicles. Each controllable device **101-1** to **101**-N has a processor **102-1** to **102**-N, respectively, memory/storage **103-1** to **103**-N, respectively, and optionally, a display screen (or other user interface) **104-1** to **104**-N, respectively. Processors **102-1** to **102**-N may include circuitry and/or other components (e.g., wireless transmitter, wireless receiver, multiplexors, demultiplexors, etc.) as is well-known in the art for executing various logical operations (i.e., based on computer logic, code, software, applications, firmware, etc.) of controllable devices **101-1** to **101**-N (e.g., delivering a data structure of a controllable device to a remote device, sending feedback to a remote device, accepting and parsing command signals from a remote device, manipulating a display in accordance with received command signals, executing authorization/handshake routines, managing and allocating system resources, selecting data transmission channels, connecting to a data transmission network, and more as discussed further below). Memory/storage **103-1** to **103**-N may include a variety of types of tangible mediums for storing such logic, code, software, applications, and/or firmware, including, for example, hard drive media, optical media, RAM, EPROM, EEPROM, cartridge media, flash memory, ROM, and/or memory stick.

Connectivity layer **105** may include, for example, network **106** and/or one or more of various types of communication and/or data transmission systems and protocols, such as Bluetooth® short-range wireless connection, Wi-Fi, Internet, phone/data networks (e.g., 3G, 4G, Long Term Evolution (LTE), Unlicensed Mobile Access technology (UMA)), or a light-modulated system. Hence, the data transfer between controllable devices **101-1** to **101**-N and **107-1** to **107**-N may include multiple networks. The type of connectivity layer **105** (and number of networks involved) will depend on various factors that may include functionality of controllable devices **101-1** to **101**-N and remote devices **107-1** to **107**-N, the location of controllable devices **101-1** to **101**-N and remote devices **107-1** to **107**-N, the proximity of controllable devices **101-1** to **101**-N to remote devices **107-1** to **107**-N, the power of such devices, the availability of certain networks, and capacity for memory/storage **103-1** to **103**-N and **109-1** to **109**-N at such devices. In some situations, connectivity layer **105** between controllable devices **101-1** to **101**-N and remote device **107-1** to **107**-N may be wired, in whole or in part. The only requirement for connectivity layer **105** is that both controllable devices **101-1** to **101**-N (or a proxy working in conjunction with the controllable device) and remote devices **107-1** to **107**-N be capable of establishing a communication path between or among them so as to facilitate an exchange of data.

In the embodiment shown, controllable devices **101-1** to **101**-N have stored in memory/storage **103-1** to **103**-N, respectively, data structures that are available for communi-

cation to one or more remote devices **107-1** to **107**-N. The data structures may be factory loaded (i.e., at the time of manufacture of controllable devices **101-1** to **101**-N) or later downloaded by a reseller or user to the controllable device. Further, data structures may be updated or modified (manually by a user or automatically) from time to time. For example, a device may acquire a new function—the data structure would be updated to identify the new function and its associated command signal. Such data structures may be received, for example, via connectivity layer **105** if designed to extend into the world outside system **10***a*, e.g., where network **106** is the Internet and/or a global communication pathway. Otherwise, data structures may be received through a wired or wireless connection separate from connectivity layer **105**, and/or by whatever means are used to upgrade/modify software or firmware of controllable devices **101-1** to **101**-N during the normal course of operation of such devices.

The data structures stored in controllable devices **101-1** to **101**-N may be generic or specific. A data structure may be generic so as to be compatible with more than one remote device or more than one type of remote device **107-1** to **107**-N. Alternatively, data structures may be tailored to optimize their delivery to, compatibility with, or use by a specific brand, model, or category of remote devices **107-1** to **107**-N, for example, remote devices running a Google operating system or Apple operating system.

Because, in a typical embodiment, the data structure is small (taking up little memory or memory/storage **103-1** to **103**-N), several data structures may be stored at the controllable device. When a particular remote device has been paired to a particular controllable device, e.g., controllable devices **101-1** to **101**-N, that controllable device is thus able to store, under control of processor **102-1** to **102**-N, supplemental data structures unique to and compatible with each historically and/or currently paired remote device **107-1** to **107**-N. A single paired remote device may also be associated with multiple data structures stored on a particular controllable device. Further, one or more data structures may be associated with a particular user, e.g., either by virtue of his or her use or ownership of a particular remote device, protocols established by a user, or use of a particular ID/password or other credential indicating compatibility. Therefore, a controllable device, such as controllable device **101-1**, may store a plurality of data structures, generic to all paired users and/or remote devices, specific to a remote device, and/or specific to a user.

FIG. **1**A also illustrates remote devices **107-1** to **107**-N. These may be, for example, a smart clicker, smartphone, tablet computer, personal computer, or any other programmable processor-based device. Such remote devices include a processor **108-1** to **108**-N, memory/storage **109-1** to **109**-N, and user interface **110-1** to **110**-N. Processors **108-1** to **108**-N may include circuitry and/or other components (e.g., wireless transmitter, wireless receiver, multiplexors, demultiplexors, etc.) as is well-known in the art for executing various logical operations (i.e., logic, code, software, applications, firmware) of remote devices **107-1** to **107**-N (e.g., sending command signals to controllable devices, allowing a user to establish an ID and password, sniffing for controllable devices, verifying compatibility with a controllable device, disconnecting from a controllable device, accepting and parsing data structures of a paired controllable device, managing and allocating system resources, selecting data transmission channels, connecting to a data transmission network, and more as discussed further below). Memory/storage **109-1** to **109**-N may include a variety of types of tangible mediums for storing such logic, code, software, applications, and/or firmware, including, for example, a hard drive media, optical media, RAM, EPROM, EEPROM, cartridge media, flash memory, ROM, and/or memory stick. Remote devices **107-1** to **107**-N also include user interfaces **110-1** to **110**-N that allow a user to control operation of a paired controllable device by various methods, including buttons (via touch screen or mechanical), voice, and motion.

A user of system according to the present disclosure, such as system **10***a* described in FIG. **1**A, may establish protocols or rules customized for a specific remote device or for a specific user. Protocols or rules may apply to all functions or selected functions. Such protocols or rules may define, for example, what remote devices are recognized and/or authorized to control the controllable device (e.g., based on a Media Access Control Address ("MAC address"), phone number, any other unique network or device identification, or user entered ID/password); how function controls (for inputting commands) are presented at a user interface (e.g., CONFIGURATION columns **114-1** and **114-2** of FIG. **1**B); whether a remote device is permitted to change protocols or rules; which of the stored data structures is delivered to a remote device; when a data structure is delivered to a remote device (e.g., after a certain function (on/off), after a set period of time, or upon initiation of a new paired session); and other permissions and limitations that a user may desire (e.g., rules limiting accessible TV channels such as shown in RULES columns **121-1** and **121-2** of FIG. **1**C).

One such protocol may require an ID, password, and/or other credentials (entered manually or sent automatically) to authorize control of the controllable device and/or remote device. In this manner, a single remote device can be used by different users who enter an ID and/or password to gain access to controllable device functions, or a subset of such functions. Such ID and password may be associated with a specific protocol established for the particular remote device or user. That protocol may limit, for example, what data structure is delivered to the remote device from the controllable device (where such protocols are stored at the controllable device), and/or what function controls (function selections) are displayed at a user interface. This may be particularly useful where a parent wishes to limit TV channels that may be viewed or recorded by a young child user; give broader access privileges to a teenage user; and give full unrestricted access to an adult user. Hence, in response to a user entering a young child's ID and password, a user interface **110-1** of remote device **107-1** may not display the function control (e.g., button) for "record" as related to operation of controllable device **101-1**; but such function control would appear in response to entry of an adult's ID/password information. Such customization may be likewise implemented on a remote-by-remote basis.

Protocols may be managed in a variety of ways. In one embodiment, the user of a remote device configures protocols for that remote device by entering a password and then manipulating settings. In another embodiment, a master remote may be used, or the Internet. In this manner, a parent could program a child's remote device using the parent's ID and password, then at the next session, the child's protocol would be all that can be used from the child's remote device until such time as the parent changes the protocol. In the master/child remote scenario, any type of communication path between the master and child remote may be used to program the child's remote. In another embodiment, protocols are managed using a master list of all historically or currently paired remote devices. The user identifies all the functions allowed (or allowable) to be controlled or seen by each remote device. The person with the master remote device and/or master ID/password then changes or updates

permissions/limitations for each function, remote device, and/or user (e.g., TV channels or otherwise as shown and described with respect to FIG. **1**C). Such changes and updates may be done at the master remote or through a display (e.g., display screens **104-1** to **104**-N) at the controllable device, depending on the type of protocol and where the protocol is stored. In this manner, the actual appearance of the controls on each remote would be particular to the remote device type and capabilities of the remote device. The controllable device might send a generic set of protocols for those who do not wish to customize their remote devices and these then would be tailored to work with different remote device types. Thus, the CONFIGURATION column from table **115'**, for example (as will be discussed hereinafter with respect to FIG. **1**B) could come preloaded with a standard configuration and then be customized by the user, if desired.

In another embodiment, the remote device, e.g., remote devices **107-1**, based on a limited data structure (i.e., only an identification of functions that may be controlled and the proper associated command signal for controlling each function, and therefore a relatively small data size) sent from the controllable device via connectivity layer **105**, constructs the proper command signals to send back to the controllable device for control purposes and also constructs its own look and feel for function control, based jointly on its own capabilities and on the capabilities of the remote device itself. The look and feel includes such features as placement, arrangement, and appearance of buttons, size of buttons, use of soft buttons for one or more functions, blocking of certain functions, time control so that different functions (such as sound levels, channels, etc.) are available only at particular times of the day or only under particular conditions. In some situations, the remote device will give the user a generic template of function controls and configurations and then, if desired, the user creates his or her own customized configuration.

In some situations, the user of the remote device, such as device **107-1**, will download from a third party (typically an "app store") a control application that is designed to control controllable devices. The downloaded control application, typically in code format, is stored in a memory, such as memory/storage **109-1**, on remote device **107-1** and runs on a processor, such as on processor **108-1**, also contained on remote device **107-1**. Downloading control applications from an app store is now well-known in the art and can be accomplished in any one of a number of ways, including via Internet, WiFi, or telephone network. In some situations, the control application will be pre-loaded onto the remote device by the manufacturer of the remote device. The user, from time to time, may add features or otherwise upgrade the control application to provide additional features. In operation of one embodiment, then, the remote device receives the data structure from the controllable device to be controlled, and under a control application, either on its own or with user input, assembles the functions/signals together with the proper protocol (as shown and described with respect to FIGS. **1**B and **1**C) such that the functions of the controllable device may be controlled from the remote device.

FIG. **1**B shows an embodiment **10***b* of a portion of memory/storage **109-1** of remote device **107-1** that has been "programmed" with data structures of two controllable devices: controllable device **101-1** (memory portion **115** having table **115'**) and controllable device **101-2** (memory portion **116** having table **116'**). The data structures were delivered to remote device **107-1** through connectivity layer **105**. In this embodiment, controllable device **101-1** is a TV, controllable device **101-2** is a DVR, and remote device **107-1** is a smartphone. Although discussed in this embodiment as controlling only two controllable devices, a remote device configured according to the present disclosure could control additional controllable devices, to the extent such controllable devices are compatible with the remote device. The data structures (similar to tables stored in memory portions **115** and **116**) for the additional controllable devices would likewise be stored in memory/storage **109-1** of remote device **107-1**. When a remote device controls multiple controllable devices, a user will typically be presented with an option, via a user interface, such as user interface **110-1** (e.g., screen, speaker, and/or other sensor) to select (e.g., by touch, voice, and/or motion) the controllable device to be controlled. Alternatively, if only one controllable device is within detectable signal range of the remote device, the remote device may automatically default to presenting the user with function controls at the user interface related to the detected controllable device. In another embodiment, the user's ID and/or password may dictate what controllable devices a user may "see" and/or select for controlling, and thus, the functions presented.

In FIG. **1**B, FUNCTION columns **111-1** and **111-2** and SIGNAL columns **112-1** and **112-2** contain the data structures delivered from their respective controllable devices **101-1** and **101-2**. In the embodiment shown, the data structure in table **115'** identifies a plurality of exemplary functions or commands (e.g., on-off, menu, volume, channel, input) associated with a plurality of exemplary command signals (e.g., XY1, XY2, XX1, ZZZ, XY3) that when sent from remote device **107-1** to controllable device **101-1**, the function/command is carried out. Similarly, the data structure in table **116'** identifies a plurality of exemplary functions or commands (e.g., on-off, volume, start, stop, fast forward ("FF"), fast rewind, pause, and record) associated with a plurality of exemplary command signals (e.g., XX3, XY5, AB1, AB2, AB3, AB4, AB5, XY6) that when sent from remote device **107-2** to controllable device **101-2**, the function/command is carried out.

For example, from smartphone (remote device **107-1**), a user may enter a command, e.g., turn TV on, by pressing a right side button of the function controls presented via user-interface **110-1**. This command will be converted to a command signal. Based on the data structure of the controllable device, the proper command signal for "on" is known to be XY1. Command signal XY1 is therefore sent to the TV (controllable device **101-1**) causing the TV to turn on. In an another example, the user may enter at the same smartphone (remote device **107-1**) a command to display a menu of options or programs by pressing a center button of the function controls presented via user-interface **110-1**. The entered command is translated into command signal, XY2, which is recognizable by the controllable device and then sent to the controllable device, which responds by displaying the menu via display screen **104-1**. In another example, from the same smartphone (remote device **107-1**), a user is presented (automatically or by manual selection) at user interface **110-1** a view of function controls for DVR (controllable device **101-2**) rather than the TV (controllable device **101-1**). The user may send a command to turn the DVR "off" by using the function control on the right side of user interface **110-1**. This command is translated into the proper command signal, which is then communicated via connectivity layer **105** to the DVR. The DVR responds by turning off.

Command signals (e.g., SIGNAL columns **112-1** and **112-2**) for implementing a change in the state of a controllable device's function can be any type of signal required for control purposes, typically a frequency set or a coded IR signal generated in the well-known manner by, for example, remote

device **107-1**, such as are discussed in U.S. Pat. No. 4,623,887, entitled "Reconfigurable Remote Control," hereby incorporated herein by reference. Alternatively, the data structure can be a new or proprietary structure known only to a specific controllable device or to a family of controllable devices. In some situations this signal may be a Bluetooth signal or any other type of signal desired. In the embodiment shown, the notation used in SIGNAL columns **112-1** and **112-2** denote the type of signal as well as the code or code sequence of the signal. Further, the functions listed in FUNCTION columns **111-1** and **111-2** are merely representative functions, and are not limited to those shown. It should be understood by those skilled in the art that any function or combination of functions could be used.

Still referring to FIG. **1**B, STATUS columns **113-1** and **113-2** and CONFIGURATION columns **114-1** and **114-2**, are protocol columns and contain information populated by a template and/or by the user. Protocols may originate in whole or in part from a number of sources, including controllable devices **101-1** and **101-2**, remote device **101-1**, master remote device (such as shown and described in FIG. **1**C), or from various other data sources. In the embodiment shown, protocols are configurations specific to a particular remote device, and define the appearance, arrangement, and/or assignment of function controls (e.g., left, center, right, button, up, down, button, arrow, one-click, two-click, key word) for a specific function of a controllable device, and an associated status (e.g., on or off). For example, in the embodiment shown, the on/off function is enabled, i.e., "on," and may be manipulated using the button on the right side of user interface **110-1**. It should be understood by those skilled in the art that any number of rows and columns can be used to store specialized information, preferences, associations, and/or restrictions.

Note that the configuration for each function could further include a code or other identification marker related to the operation of that function control. By doing this, anytime that code or marker appeared, the remote would know to use the same user display symbol across all controllable devices being controlled. Using the fast forward signal as an example, a special FF code can be established that is associated with FF in all controllable devices. Thus, regardless of what controllable device the remote device is currently controlling, the FF display (which can be the user's preference) will be the same. In this manner, the control application will be able to put the same FF display at the same location and/or format regardless of what actual device is being controlled at the time for a consistent user interface across multiple controllable devices.

Further, protocols applied in any particular session between a remote device and controllable device may be based on the user ID and/or password entered at the remote device **101-1**, or other selection of a user (e.g., selection of a controllable device to control). Further, in the embodiment shown in FIG. **1**B, the protocol and its association with a received data structure is stored at remote device **101-1** in memory/storage **109-1**.

Although CONFIGURATION columns **114-1** and **114-2** shown in FIG. **1**B assume buttons, bars, and arrows, whether hard or programmable, that are physically pushed or touched by the user, this form of entering a command by the user need not be so limited. Any type of input from the user can be utilized. Thus, voice commands, motion commands (e.g., with the user waiving his or her finger), and/or motion commands (e.g., with the remote device itself being moved), can be used for one or more of the functions performed by the remote device, such as remote device **107-1**. In this manner, the input stimuli to the remote device is independent of the command signal that is actually passed from the remote device to the controllable device, with the translation being made in the remote device as will be discussed hereinafter.

FIG. **1**C shows one embodiment **10***c* of a portion of a data structure for controlling a controllable device, such as controllable device **101-1**. In the embodiment shown, data structure tables **117** and **118** are part of memory/storage **103-1** of controllable device **101-1**. The controllable device is a TV in this embodiment. In an alternate embodiment, data structure tables **117** and **118** are part of memory/storage **109-1** of remote device **107-1** (as discussed with reference to FIG. **1**B above). In that alternate embodiment, data structure tables are contained in a specification ("spec") assembly control as discussed in more detail with respect to FIG. **2**.

Further, in FIG. **1**C, controllable device **101-1** has been paired with two remote devices; therefore each may control function of the controllable device. The paired remote devices are remote device **107-1** (named Master, table **117**, associated with a parent) and **107-2** (named Child 1, table **118**, associated with a young child). Although this embodiment uses a master/child relationship for tables **117** and **118**, other roles and relationships between remote devices and/or users may be employed in other embodiments. In this embodiment, tables **117** and **118** each have a plurality of specific functions that may be controlled, FUNCTION columns **119-1** and **119-2**, associated with a status, such as yes or no, in STATUS columns **120-1** and **120-2**, and notes in RULES columns **121-1** and **121-2**. In this embodiment, the child's profile (i.e., protocols established for the child) has restrictions, e.g., remote device **107-2** (table **118**) will not be allowed to control various channels, such as pay-per-view, premium, or those numbered above 100. In addition, the volume is limited after 9:00 PM and the entire remote goes inactive after midnight. Of course, this is an example, and any combination of features and controls can be implemented on a remote-by-remote and/or user-by-user basis

In the embodiment shown in FIG. **1**C, RULES **121-1** and **121-2** were established by entering commands at master remote device **107-1**. In another embodiment, such rules may be established through another connection to the controllable device, or through controls on the controllable device.

Based on such rules, the data structure delivered to a remote device may include only a subset of all possible functions. Alternatively, the full data structure (including all possible functions) may be delivered from a controllable device but restricted by a protocol residing on the controllable device or remote device. The actual data structure delivered from a controllable device to a remote device may further depend on the ID, password, or other credential associated with a data structure. Hence, the delivered data structure may vary with the credential information.

FIG. **2** shows one embodiment of the operation of the remote device working in cooperation with a controllable device. When a controllable device, such as controllable device **101-1**, is turned on, signature signal transmitter **201** begins sending out signals that can be "sniffed" (i.e., detected) by particular devices such as remote devices. Bluetooth or any protocol can be used for this purpose and in this example, network **106** is used. Any compatible remote device in sufficient proximity of device **101-1** (or in the vicinity of network **106** or other connectivity layer **105**) will, using its internal controllable device presence detector, such as controllable device presence detector **204**, begin a handshaking (HS) process between handshake initialization control **205** in remote device **107-1** and authorization control **202** in controllable device **101-1**. If remote device **107-1** has not already been paired with this particular controllable device **101-1**, and if the devices are compatible, remote spec data control

203 sends a data structure, for example the information used to populate the FUNCTION and SIGNAL columns of table 115' as shown in FIG. 1B, to spec assembly control 206 for subsequent use by controller 209. Spec assembly control 206 aides in building the table shown at table 115' and in some cases (as noted above) table 117.

Once a pairing has been authorized (via authorization control 202, handshake initialization control 205), controller 209, working from data contained in the tables located in spec assembly control 206 responds to a human "press" of a displayed function control by sending the proper signals (as obtained from table 115') to controller 207 in the paired controllable device 101-1. These command signals are sent by IR, Bluetooth, or in any other manner, over network 106. Controller 207 handles any received command signal from any of the paired remote devices. In some situations, feedback control 208 sends feedback information to remote device 107-1. This feedback information can be any type of information desired. For example, the channel number and program information can be communicated to remote device 107-1, along with the name of the controllable device 101-1. Other instructions can also be sent to remote device 107-1 to assist in controlling controllable device 101-1. This feature can be helpful, for example, when the controllable device does not have a display screen, or is not within visible range of the user operating remote device 107-1. The feedback can be simply an acknowledgment of the received command signal.

The identification and authorization process can be any well-known process and, if desired, actual user-entered ID, password, or other credential may be required. Any unique ID or credential that the remote device (controller or controlling device) might have can be used. Further, authorization procedures may be performed at both a controllable device and a remote device. To further facilitate a more secure environment (e.g., system 10*a* of FIG. 1), it might be helpful to re-deliver (refresh) data structures (signal specifications/instructions) upon the happening of an event, even if the remote device and the controllable device have already been paired successfully historically or currently. For example, upon a subsequent pairing of the remote device to the controllable device, upon the lapse of a pre-defined period of time (e.g., once every half-hour, hour, week, or year), upon change in state of the controllable device or remote device (e.g., turned off or on), upon a change in protocols, rules, or functions of the controllable device, or upon determining that a command signal received is not permitted based on credential information, an updated data structure may be sent to the remote device. Thus, if a remote was hacked, and protocols changed without the owner's permission, i.e., giving access to an restricted TV channel or DVR function, the data structure, and accompanying limitations/restrictions, would be renewed upon the happening of an event as described above, e.g., a new paired session. The new data structure and rules (if any) would be applied to the remote device in the new session, overriding any previously delivered data structure and/or protocol that is outdated or unauthorized.

If an ID, password, or other credential is required, rules such as those contained in table 117 of FIG. 117 of FIG. 1C, would most likely be stored on the controllable device and not in the remote device to minimize any effect of the remote device being hacked (e.g., unauthorized changes to protocols/rules). Otherwise, a delivered data structure may be stored, at least temporarily, at the remote device and available from time to time so that a user may control specific functions of a controllable device without requiring further delivery of the previously stored data structure.

Another security feature may use other credential information to verify one or more of the remote devices, such as a MAC address and/or any other network-type identification. In some situations, new remote devices may not be added without express permission from a particular "master" remote device. In some embodiments, when the session is over, for example, when the remote leaves the vicinity of the controllable device, or when the controllable device is turned off, leave/disconnect 210 can sever the temporary pairing. In such an event, the process of authorizing a re-pairing will occur when a new session begins, and preferably a new set of data structures (signal specifications/instructions) will be exchanged between the controllable device and the remote device.

FIG. 3 shows one example 30 of a typical life cycle of the controllable device. Process 30 begins with boot process 301 which turns on the system and causes process 302 to expose a signal for discovery by a remote device. In the system shown, the remote device will search for the controllable device and initiate communication. In another embodiment, the controllable device will seek out remote devices detected. Returning to example 30, the system then waits under control of process 303 for a remote to "sniff" its transmitted signal and to respond with a handshake offer. When such an offer arrives, process 304 either accepts the pairing or rejects it. If accepted, process 304 causes process 305 to send the proper data structure to the remote device. At this stage, the initialization is finished and process 306 causes the controllable device to wait for a command signal to be received from any of its paired remote devices.

When process 306 detects receipt of a command signal or other event from a remote device, that command signal is checked by process 307 to determine if it is a "legal" (i.e., permitted or valid) command from an authorized remote device or if it is an authorization request. If the command is an authorization request, then process 308 diverts the request to process 303.

If the received signal corresponds to a proper command then process 309 performs the command delivered by the command signal and if desired, process 310 furnishes feedback to the remote device. The process then returns to process 306 to await an additional command signal or other event.

FIG. 4 shows a typical life cycle 40 of a remote device. Process 401 sniffs for controllable devices in proximity to the remote device. Process 402, upon finding a possible controllable device, enables process 403 to begin an authorization process as discussed above with reference to FIGS. 2 and 3. If process 404 determines that the found controllable device is indeed a proper one for control (and assuming the controllable device likewise finds the remote device to be proper) then process 405 requests a data structure from the controllable device in order to know which signals to send to the controllable device for proper control. Process 406 waits for the requested data structure.

Process 407, upon receipt of the controllable devices' data structure, validates the received data structure to be certain the remote device can properly operate the controllable device. If process 408 determines that the received data structure is not proper or not one it can handle, then optionally a new data structure can be requested under control of process 409. When process 410 determines that a new data structure has been received process 407 is reentered. If no new data structure is received, life cycle 40 ends and the remote is non-functional with respect to this particular controllable device. Note that while the process discussed herein assumes a standard set of data structures (signal specifications/instructions) for controlling the controllable device, perhaps

adjusted for the type of remote device that is requesting the data structures, it should be understood that the remote device could request certain formats and/or formats for certain functions. Thus, the "standard" communication of data structures from the controllable device need not cover all possible functional controls if the remote device is not capable of using all such controls. In operation, the standard package can be augmented function-by-function, or in function packages, using codes that apply across product-lines to identify function sets the remote device is capable of handling.

Once process **408** determines that a received data structure is acceptable, then process **411** waits for an input command from a user of the remote device. While process **411** is waiting, if process **413** determines the session has ended, process **416** determines if the remote device is going to turn off or alternatively, resume sniffing for new controllable devices.

When a command is received from a user while the session remains active, then process **414** sends the associated command signal to the paired controllable device using the proper signal set as obtained from its memory (e.g., from SIGNAL column **112-1** as discussed above with respect to FIG. **1**B). If feedback has been received by process **415**, it is controlled by process **412** and the appropriate action taken (such as shown and described with respect to FIG. **2** and feedback control **208**).

FIG. **5** shows one embodiment **50** of data flow in the system according to the present disclosure. Shown are server **503** and client **505**. Client **505** runs in the remote device (controller), such as remote devices **101-1** to **101**-N of FIG. **1**, while server **503** runs in the controllable device, such as controllable devices **107-1** to **107**-N of FIG. **1**.

Server **503** sends the data structures and feedback (e.g., acknowledgment of receipt of command signal) to client **505**. The data structure can be any desired function, signal, and/or other structure as discussed above with reference to FIGS. **1**B and **1**C. In a typical system, the data structure will be limited, that is, it will include only the identity of the functions that may be controlled, and the associated command signal (or other like instruction) for remotely controlling the function. In other embodiments, the exchanged data structure may be more robust and include protocols, rules, or other information useful to carrying out remote control of the controllable device.

Client **505** sends the handshake (HS) request and command signals **506** to controllable device server **503**. Client **505** sends data structures received from server **503** to command parser **504**. In one embodiment, command parser **504** is a control application downloaded from an app store or received from some other source. Command parser **504** also contains the graphical layer of the control application that accepts the data and represents it to the user in a manner that is user friendly at a user interface, e.g., **110-1**. The same graphical layer of the control application parses the user initiated input (such as touching the displayed volume button) and sends such command signals (event information) to client **505** for delivery to server **503**. As discussed above with reference to FIG. **1**A, the input could take any form, from verbal to motion and can differ for different controllable devices. Thus, shaking the remote device during a live sports event might cause the motion on the screen to slow down whereas shaking the remote while watching a movie on a Blu-ray player might pause the movie. Since the translation (conversion) of the user input (into command signals) is made under control of command parser **504** and the control application currently resident on the remote device, the controllable device remains neutral to how such input is received, since the controllable device acts only on signals sent from the remote device. Such command signals have already been put into the form demanded by the controllable device and as previously communicated to the remote device as part of the data structure.

On the controlled side, when server **503** receives a new command signal, it sends that command to command parser **502** for analysis. Command parser **502** drives main application **501** (e.g., an application within a set-top box) within the controllable device. Main app (i.e., main application) **501** handles the command as received from the remote device, and, if appropriate, sends feedback to server **503** for subsequent delivery to client **505**. The control application, as contained in the remote device commands parser **504** then takes action based on the feedback. This action can take any number of forms, from displaying information to the user via the user interface (see, e.g., user interface **110-1** of FIG. **1**), to changing the code structure, or to initiating additional response actions.

Although the present invention and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of the invention as defined by the appended claims. Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure of the present invention, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized according to the present invention. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

What is claimed is:

1. A method of controlling an electronic device remotely, said method comprising:

determining that a controllable device and a controlling device are in proximity to each other;

establishing pairing compatibility between said controllable device and said controlling device determined to be in proximity to each other, wherein said establishing said pairing compatibility comprises determining an identity of said controlling device;

selecting, by said controllable device, a data structure that is compatible with said identity and associated with a recognized user recognized by said controllable device; and

delivering, from said controllable device of said established pairing to said controlling device of said established pairing, said data structure compatible with said identity of said controlling device and associated with said recognized user, wherein said data structure allows said recognized user to control, with said controlling device, specific functions of said controllable device, where the specific functions are specific to said user,

wherein said accepted data structure is stored, at least temporarily, at said controlling device, so as to be usable by said controlling device for sending command signals to said controllable device for a period of time without accepting any further data structures from said controllable device.

2. The method of claim **1** wherein said control application establishes on said controlling device a function control inter-

face for accepting commands from said recognized user to exercise said control of said specific functions of said controllable device.

3. The method of claim **2** wherein said data structure compatible with said identity of said controlling device is specific to said controlling device.

4. The method of claim **2** wherein identifying at least one specific user further comprises identifying a plurality of specific users; wherein said control application establishes on said controlling device a unique function control interface for each specific user in said plurality of specific users, said unique function control interface specific to said each specific user, and said unique function control interface accepting commands from said each specific user to exercise said control of said specific functions of said controllable device.

5. The method of claim **1** wherein said delivered data structure consists of:

an identification of said specific functions of said controllable device; and

an identification of a command signal associated with each of said specific functions, wherein said specific functions and said command signals are unique to said identified controlling device.

6. The method of claim **1** wherein said delivered data structure is stored, at least temporarily, at said controlling device.

7. The method of claim **6** wherein said delivered data structure is re-delivered upon an occurrence of a specified event, wherein said re-delivered data structure overrides the previously delivered data structure.

8. The method of claim **7** wherein said specified event is initiation of a subsequent establishment of pairing compatibility between said controllable device and said controlling device.

9. The method of claim **8** further comprising:

allowing said recognized user of said controlling device to selectively configure function controls of said specific functions.

10. The method of claim **6** wherein said stored data structure comprises at least one generic function control interface for presenting function controls of said specific functions to said recognized user.

11. The method of claim **10** further comprising:

allowing said recognized user of said controlling device to configure said function control interface.

12. The method of claim **1** further comprising:

allowing said recognized user to establish rules for said specific functions.

13. The method of claim **1** wherein said controlling device is a smartphone, and wherein said control of said specific functions is at least partially enabled by said control application stored on said smartphone.

14. The method of claim **1** further comprising:

detecting that said controlling device is in proximity to a second controllable device other than said paired controllable device;

establishing pairing compatibility between said controlling device and said second controllable device;

delivering from said second controllable device of a second established pairing to said controlling device a second data structure that would allow said recognized user of said controlling device to control specific functions of said second controllable device; and

allowing said recognized user to control said controllable device and said second controllable device with same said controlling device.

15. The method of claim **14** wherein said delivered data structures from at least one of said controllable devices includes protocols for maintaining a consistent function control interface across multiple controllable devices.

16. The method of claim **1** wherein said delivered data structure further consists of an identification of said identified at least one user.

17. The method of claim **1** wherein said credentials comprises a combination of a username and a password.

18. A remotely controllable electronic device comprising:

means for exchanging identification signals between said controllable electronic device and a remote device;

means for determining that said remote device is a compatible remote device by determining compatibility of said remote device with said controllable electronic device based at least in part on said exchanging of said identification signals;

means for identifying, by said controllable electronic device, a data structure to deliver from said controllable electronic device to said compatible remote device, wherein said data structure is associated with a recognized user recognized by said controllable electronic device; and

means for delivering from said controllable electronic device to said compatible remote device said data structure configured to allow control of specific functions of said controllable electronic device from said compatible remote device, where the specific functions are specific to said user,

wherein said delivered data structure is stored, at least temporarily, at said compatible remote device and available for control of said specific functions at said controllable electronic device without requiring a second delivery of said data structure.

19. The device of claim **18** further comprising:

means for delivering supplemental data structures to said compatible remote device intermittently.

20. The device of claim **18** wherein said delivered data structure is tailored, at least in part, to satisfy requirements of said compatible remote device.

21. The device of claim **18** wherein said delivered data structure comprises at least one generic function control interface for presenting function controls to a user of said compatible remote device.

22. The device of claim **18** wherein said delivered data structure includes protocols for maintaining a consistent function control interface across multiple controllable devices.

23. The device of claim **18** further comprising:

means for delivering to said compatible remote device feedback pertaining to functions selected from said compatible remote device.

24. The method of claim **18** wherein said credentials comprises a combination of a username and a password.

25. A programmable remote device comprising:

an application running on said programmable remote device, said application configured to:

recognize a user, said recognizing based on reading credentials associated with said recognized user;

accept a data structure unique to said programmable remote device from at least one controllable device, wherein said data structure defines command signals for controlling specific functions of said controllable device, and wherein said data structure is determined, by said controllable device, to be associated with said

recognized user recognized by said controllable device based on reading said credentials associated with said recognized user;

establish on said programmable remote device a user interface, wherein said user interface is under at least partial control of said application;

accept commands of said recognized user at said user interface; and

convert said commands of said recognized user into said command signals recognizable by said controllable device, said converting utilizing said accepted data structure;

wherein said accepted data structure is stored, at least temporarily, at said programmable remote device, so as to be usable by said programmable remote device for sending said command signals to said controllable device for a period of time without accepting any further data structures from said controllable device.

26. The programmable remote device of claim **25** wherein said application is further configured to:

allow said recognized user to configure said user interface of available ones of said specific functions.

27. The programmable remote device of claim **25** wherein said application is further configured to:

allow said recognized user of said programmable remote device to establish protocols for selected ones of said specific functions.

28. The programmable remote device of claim **25** wherein said programmable remote device is a smartphone, and wherein control of said specific functions from said smartphone is at least partially enabled under control of said application program resident on said smartphone.

29. The programmable remote device of claim **25** wherein said application is further configured to:

apply protocols delivered with said accepted data structure, said protocols established for selected ones of said specific functions.

30. The programmable remote device of claim **25** wherein said application is further configured to:

accept a second data structure from a second controllable device, wherein said second data structure defines other command signals for controlling specific functions of said second controllable device;

establish on said programmable remote device a second user interface, wherein said second user interface is under at least partial control of said application;

accept said other commands of said recognized user at said second user interface; and

convert said other commands of said user into other command signals recognizable by said second controllable device, said converting utilizing said accepted data structure.

31. The programmable remote device of claim **30** wherein said second data structure accepted from said second controllable device is stored, at least temporarily, at said programmable remote device so as to be usable by said programmable remote device for sending said other command signals to said second controllable device for a period of time without accepting any further data structures from said second controllable device.

32. The method of claim **25** wherein said credentials comprises a combination of a username and a password.

33. The programmable remote device of claim **25** further configured to:

identify a plurality of users,

wherein said application establishes on said remote device a unique user interface for each specific user in said plurality of specific users, said unique user interface specific to said each specific user, and said unique user interface accepting commands from said each specific user.

34. An electronic device controller comprising:

means for exchanging identification signals with potential controllable devices;

means for assisting in determining compatibility of said potential controllable device with said electronic device controller in response to an exchange of identification signals;

means for sending credentials from said electronic device controller to a controllable device of determined compatibility, said credentials associated with a user;

means for processing a data structure unique to said credentials from said compatible controllable device, said data structure determined, by said controllable device, to be associated with said user recognized by said controllable device based on reading said credentials, and said data structure allowing specific functions of said compatible controllable device to be controlled from said electronic device controller; and

means for storing a data structure, at least temporarily, at said electronic device controller, so as to be usable by said electronic device controller for sending said command signals to said controllable device for a period of time without accepting any further data structures from said controllable device.

35. The device of claim **34** wherein a delivered data structure is stored, at least temporarily, at said electronic device controller and available intermittently for control of said specific functions at said compatible controllable device without requiring further delivery of said data structure.

36. The device of claim **34** further comprising:

means for communicating to said compatible controllable device requirements of said electronic device controller for said processing of said data structures communicated from said compatible controllable device.

37. The device of claim **34** further comprising:

means for utilizing feedback from said compatible controllable device pertaining to said specific functions selected from said electronic device controller.

38. The method of claim **34** wherein said user credentials comprises a combination of a username and a password.

39. A system for controlling devices, said system comprising:

at least one controllable device;

at least one remote device;

at least a temporary communication link between said controllable devices and available ones of said remote devices;

a protocol for pairing ones of said controllable devices with ones of said remote devices; and

a delivery mechanism for communicating a data structure from each paired controllable device to a paired remote device, said data structure associated with a recognized user recognized by said paired controllable device, unique to said paired remote device, and allowing said remote device to control specific functions of said paired controllable device, where the specific functions are specific to said user,

wherein a control application establishes on said remote device a unique function control interface for each specific user in a plurality of specific users, said unique function control interface specific to said each specific user, and said unique function control interface accept-

ing commands from said each specific user to exercise said control of said specific functions of said controllable device.

40. The system of claim **39** wherein a delivered data structure is stored, at least temporarily, at said paired remote device and available intermittently to said paired remote device for said control of said specific functions of said paired controllable device without requiring further delivery of said data structure.

41. The system of claim **39** further comprising:

means for communicating to said controllable device from said paired remote device requirements of said paired remote device for processing said data structures communicated from said paired controllable device.

42. The system of claim **39** further comprising:

means at said paired remote device for utilizing feedback from said paired controllable device pertaining to said specific functions selected from said paired remote device.

43. The method of claim **39** wherein said user credentials comprises a combination of a username and a password.

44. An application program product for controlling a programmable remote device, said application program product comprising a non-transitory computer readable medium having program code recorded thereon, the program code configured to perform the steps of:

accepting user credentials;

accepting a data structure from at least one controllable device, wherein said data structure is specific to said user credentials authorized by said at least one controllable device;

establishing on said programmable remote device a user interface for allowing a user to input selected commands to said programmable remote device, wherein a configuration of said user interface is specific to said user credentials;

converting inputted commands into command signals recognizable by said at least one controllable device, said converting utilizing said accepted data structure; and

storing said data structure, at least temporarily, at said programmable remote device, so as to be usable by said programmable remote device for sending said command signals to said at least one controllable device for a period of time without accepting any further data structures from said at least one controllable device.

45. The program product of claim **44** wherein said configuration of said user interface includes an arrangement of function controls for available commands.

46. The program product of claim **44** further configured to perform the step of:

allowing said user of said programmable remote device to establish rules for selected ones of said commands.

47. The method of claim **44** wherein said user credentials comprises a combination of a username and a password.

* * * * *