



- (51) **International Patent Classification:**
G06F 7/04 (2006.01)
- (21) **International Application Number:**
PCT/US2016/039009
- (22) **International Filing Date:**
23 June 2016 (23.06.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
62/183,411 23 June 2015 (23.06.2015) US
- (71) **Applicant:** THE TRUSTEES OF DARTMOUTH COLLEGE [US/US]; 11 Rope Ferry Road, Room 6210, Hanover, NH 03755 (US).
- (72) **Inventors:** PIERSON, Timothy, J.; 5 Lakeview Dr., Hanover, NH 03755 (US). LIANG, Xiaohui; 2 Meadowbrook Village, Apt. 12, West Lebanon, NH 03784 (US). PETERSON, Ronald; 107 Scott Road, Brattleboro, VT 05301 (US). KOTZ, David; 137 River Road, Lyme, NH 03768 (US).
- (74) **Agents:** BARTON, Steven, K. et al.; Lathrop & Gage LLP, 4845 Pearl East Circle, Suite 201, Boulder, CO 80301 (US).
- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,

[Continued on next page]

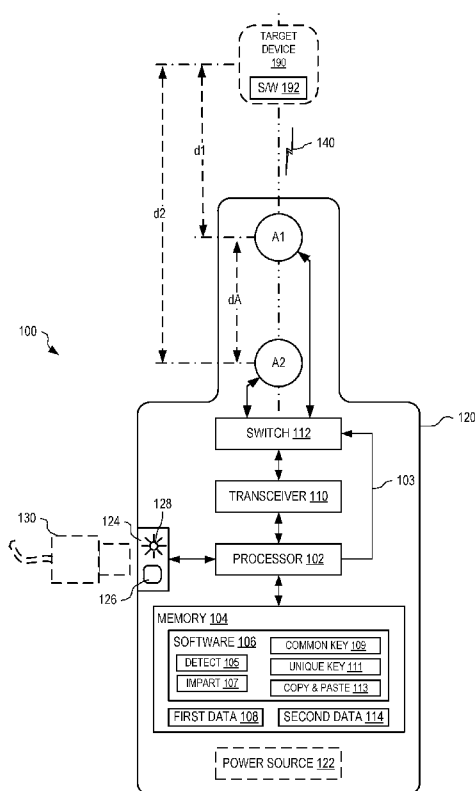
(54) **Title:** APPARATUS FOR SECURELY CONFIGURING A TARGET DEVICE AND ASSOCIATED METHODS

FIG. 1

(57) **Abstract:** Apparatus and method securely transfer first data from a source device to a target device. A wireless signal having (a) a higher speed channel conveying second data and (b) a lower speed channel conveying the first data is transmitted. The lower speed channel is formed by selectively transmitting the wireless signal from one of a first and second antennae of the source device based upon the first data. The first and second antenna are positioned a fixed distance apart and the target device uses a received signal strength indication (RSSI) of the first signal to decode the lower speed channel and receive the first data.



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

Published:

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

APPARATUS FOR SECURELY CONFIGURING A TARGET DEVICE AND ASSOCIATED METHODS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of priority to US Patent Application Serial Number 62/183,411, titled “Apparatus for Securely Configuring a Target Device and Associated Methods”, filed June 23, 2015, and incorporated herein by reference in its entirety.

BACKGROUND

[0002] Nearly every setting is increasingly populated with wireless and mobile devices – whether appliances in a home, medical devices in a health clinic, sensors in an industrial setting, or devices in an office or school. There are three fundamental operations when bringing a new device into any of these settings: (1) to configure the device to join the wireless local-area network, (2) to partner the device with other nearby devices so they can work together, and (3) to configure the device so it connects to any relevant individual or organizational account in the cloud.

[0003] Recently, predictions have been made of how the Internet of Things (IoT) is poised to make billions of everyday objects “smart” by adding wireless communication capabilities. The dream is that networks of these newly connection-enabled devices will give us greater insight into the behavior of complex systems than previously possible. The reality, however, is that configuring and managing billions of devices is extremely difficult.

[0004] As an illustration in the healthcare domain, imagine that a general-practice physician tells a patient that he’d like the patient to take home a wireless blood-pressure monitor and use it every day so that the physician can remotely monitor the patient’s health. The intention is that the blood-pressure measurements taken by the patient while at home will end up stored in the patient’s Electronic Health Record (EHR) at the physician’s clinic. The physician can then see the patient’s blood pressure on a daily basis and get automated alarms if any abnormal readings are recorded. At least three problems arise in making scenarios such as at-home blood-pressure monitoring a reality.

[0005] A first problem is that blood-pressure monitors, like many IoT sensors, do not come with long-range communication connections; they have only short-range radios such as Wi-Fi, Bluetooth, or Zigbee. The blood-pressure monitor must somehow get connected with other devices in the home such as a Wi-Fi access point (AP) in order to transmit its medical data to the physician's EHR system. Making those connections is difficult for many people, especially considering that different types of devices from different manufacturers often have different methods of making a connection and that the devices themselves often have very limited user interfaces.

[0006] A second problem with this blood-pressure scenario is that once a connection is made between the blood-pressure monitor and a device capable of transmitting data long distances, the blood-pressure readings must get to the right patient record in the right physician's EHR system. This implies that the blood-pressure readings must be augmented with additional credentials (e.g., patient ID, password) and destination information (e.g., a Restful API URL).

[0007] A third problem arises when devices partner with other nearby devices so they can work together in a peer-to-peer fashion, such as a blood-glucose monitor working with an insulin pump. In these peer-to-peer cases the devices may maintain a connection with a long-range communication device, but may also need a connection with neighboring devices using encryption based on a unique key for a specific pair of devices, rather than a common key shared by all devices. Establishing the encryption can be difficult if the devices have never met before and have never shared a secret key.

SUMMARY

[0008] In one embodiment, an apparatus securely transfers first data to a target device. The apparatus includes a first antenna, a second antenna positioned a fixed distance from the first antenna, a transmitter, and a processor configured to control the transmitter to transmit a first signal containing second data selectively from one of the first antenna and the second antenna based upon the first data. The first data may only be received by the target device when the target device within close proximity of the first and second antennae, and the second data does not include the first data.

[0009] In another embodiment, a method securely transfers first data from a source device to a target device. A wireless signal having (a) a higher speed channel

conveying second data and (b) a lower speed channel conveying the first data is transmitted. The lower speed channel is formed by selectively transmitting the wireless signal from one of a first and second antennae of the source device based upon the first data. The first and second antenna are positioned a fixed distance apart and the target device uses a received signal strength indication (RSSI) of the first signal to decode the lower speed channel and receive the first data.

[0010] In another embodiment, an apparatus securely transfers first and second data to a target device, where the first data includes encryption information. The apparatus includes a first antenna, a second antenna positioned a fixed distance from the first antenna, at least one transmitter, and a processor configured to selectively switch the transmitter between the first antenna and the second antenna based upon the first data, wherein the second data is encoded independently of the coupling of the at least one transmitter to the first and second antennae.

[0011] In another embodiment, a system securely transfers first data from a source device to a target device. The source device includes a first antenna, a second antenna positioned a fixed distance from the first antenna, a transmitter, and a processor configured to control the transmitter to transmit a first signal containing second data selectively from one of the first antenna and the second antenna based upon the first data. The target device includes an antenna configured for receiving the first signal from the source device, a receiver electrically coupled with the antenna and configured to determine a received signal strength indicator (RSSI) of the first signal, and a processor configured to receive the RSSI of the first signal from the receiver and to determine the first data therefrom. The first data may only be received by the target device when the target device within close proximity of the first and second antennae. The second data does not include the first data and the target device determines when it is positioned within a back lobe of the source device when polarity of received data is inverted.

BRIEF DESCRIPTION OF THE FIGURES

[0012] FIG. 1 shows one exemplary wand for securely configuring a target device, in an embodiment.

[0013] FIG. 2 shows another exemplary wand, similar to the wand of FIG. 1, but where the switch is omitted and a second transceiver is added, in an embodiment.

[0014] FIG. 3 shows three exemplary graphs illustrating distribution of received signal strength indication (RSSI) measurements returned by capturing 12,000 Wi-Fi packets sent between a Wi-Fi AP and the receiving antenna in each of a home, a coffee shop, and a Computer Science lab.

[0015] FIG. 4 shows one exemplary graph illustrating expected RSSI ratio plotted against distance between the transmitter and the nearest antenna A1.

[0016] FIG. 5 illustrates exemplary communication between the wand and the target device of FIG. 1 during operation of the detect primitive, in an embodiment.

[0017] FIG. 6 shows exemplary RSSI at a receiving antenna for 1,000 Wi-Fi packets transmitted from the antennae A1 and A2 of FIG. 1, in an embodiment.

[0018] FIG. 7 shows a first and second graphs illustrating exemplary reception of message *m* at distances of 3 cm and 30 cm, respectively.

[0019] FIG. 8 is a flow sequence showing exemplary operation of the impart primitive of FIG. 1, in an embodiment.

[0020] FIG. 9 is a flow sequence illustrating exemplary operation of a common key protocol of FIG. 1, in an embodiment.

[0021] FIG. 10 shows the wand of FIG. 1 implementing a unique key protocol for establishing a wireless connection between two devices, in an embodiment.

[0022] FIG. 11 is a flow sequence illustrating exemplary operation of the unique key protocol of FIG. 10, in an embodiment.

[0023] FIG. 12 shows the wand of FIG. 1 implementing a copy-and-paste protocol for copying data from a first device and pasting the data to a second device, in an embodiment.

[0024] FIG. 13 is a flow sequence illustrating exemplary operation of the copy-and-paste protocol of FIG. 12, in an embodiment.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0025] The disclosure herein presents a novel approach that accomplishes all three of the above goals.

[0026] FIG. 1 shows one exemplary wand 100 for securely configuring a target device 190. Wand 100 is an apparatus that includes a processor 102, a memory 104, a transceiver 110, a switch 112, and two antennae A1 and A2. FIG. 2 shows another exemplary wand 200, similar to wand 100, but where switch 112 is omitted and a

second transceiver 210 is added. FIGs. 1 and 2 are best viewed together with the following description. In one embodiment, processor 102 and memory 104 form part of a Raspberry Pi B+ computer. In the following description, references to wand 100 may also apply to wand 200. Wand 100 may be implemented in other forms without departing from the scope hereof. For example, wand 100 may be implemented with a mobile phone (e.g., smart phone) or other such similar device. That is, wand 100 is not limited in form to a long thin pointing type device as shown in FIGs. 1 and 2.

[0027] Wand 100 also includes a housing 120 that physically positions antenna A1 relative to antenna A2 with a distance dA therebetween. Antennae A1 and A2 and distance dA are selected based upon intended operating frequency of transceiver 110 and transceiver 210. In one embodiment, transceiver(s) 110, 210 operate at 2.4GHz (Wi-Fi), antennae A1 and A2 are Wi-Fi antennae, and distance dA is approximately 7 cm ($\frac{1}{2}$ wavelength is approximately 6.25cm). Where transceiver(s) 110, 210 operate at 5 GHz, distance dA is approximately 3 cm. As distance dA increases beyond $\frac{1}{2}$ wavelength, the effective range of wand 100/200 increases. Conversely, as dA decreases to be less than $\frac{1}{2}$ wavelength, operational range of wand 100/200 decreases. In one embodiment, housing 120 is shaped to indicate orientation of wand 100 and thus orientation of antennae A1 and A2, such that a user may 'point' wand 100 at target device 190. Target device 190 includes a processor, memory, and a receiver, for example.

[0028] Wand 100 may also include an interface 124 with one or more buttons 126 (e.g., a push button, capacitive input device, or other such input devices), one or more indicators 128 (e.g., a light emitting diode (LED) or other similar indicating device), and/or one or more audio emitters (e.g., speaker). Interface 124 may also include electrical coupling (e.g., a socket) for coupling with an external device via a plug or other similar devices. For example, first data 108 may be loaded from an external device (e.g., one of a computer, a router, and other such devices) via interface 124. Alternatively, first data 108 may be received wirelessly by wand 100 via transceiver 110, 210 and one of antenna A1, A2.

[0029] Wand 100 may also include a power source 122 that powers electronic components of wand 100 to allow portable operation. In one embodiment, transceivers 110, 210 operate at Wi-Fi frequencies (e.g., 2.4GHz, 5GHz), antenna A1 and A2 are selected accordingly, and positioned with separation dA equal to seven

centimeters (approximately half the wavelength of the transmitting frequency). Where dA is set to a distance of $\frac{1}{2}$ wavelength, it is difficult for an adversary device that is not proximate wand 100/200 to determine which antenna (A1 or A2) was used to transmit. Although wand 100/200 works at other antenna spreads, a distance of $\frac{1}{2}$ wavelength provides optimal operating range and security. Where antenna A1 is a distance $d1$ from the antenna of target device 190, antenna A2 will be a distance of $d1 + dA$ (e.g., 7 cm) when wand 100 is pointing directly at the antenna of target device 190.

[0030] Memory 104 stores software 106 that includes machine-readable instructions that are executed by processor 102. In wand 100, software 106 is configured to control switch 112, via control signal 103, to electrically couple one of antennae A1 and A2 with transceiver 110, where only one of antenna A1 and A2 is electrically coupled with transceiver 110 at any time. In wand 100, software 106 is also configured to control, based upon information of first data 108, transceiver 110 and switch 112 to cooperatively transmit a wireless signal 140 to target device 190. Within wand 100, operation of switch 112 forms a lower speed secure data channel within signal 140. Simulation may be performed to take into account PCB parasitic effects and antennae interaction to verify that the antennae do not interact and operate as a directional antenna. In wand 200, software 106 is configured to control, based upon information of first data 108, one of transceivers 110, 210 to transmit signal 140, via a corresponding one of antennae A1 and A2 within wireless signal 140 to target device 190. Thereby, within wand 200, control of transceivers 110, 210 forms the lower speed secure data channel of signal 140.

[0031] Information of first data 108 is not included within content (e.g., within conventional data packets of the higher speed channel) of signal 140. Rather, for each bit of information of first data 108, a portion of signal 140 (e.g., one packet) is transmitted from a selected one of antenna A1 and A2 based upon the value (0 or 1) of the bit. Thus, although wireless signal 140 conveys a second data (e.g., second data 114) conventionally within conventional data packets of the higher speed channel, reading and decoding this higher speed channel (e.g., the data portion of the data packets) does not result in gaining first data 108. However, when wand 100 is within sufficiently close proximity to target device 190, the receiver within target device 190 may decode the lower speed channel by detecting a received signal

strength indication (RSSI) ratio between received portions (e.g., data packets) of signal 140 based upon which antenna (A1, A2) was used to transmit that portion of signal 140 from wand 100. The information of first data 108 within the lower speed channel is thereby received by target device 190 as an amplitude modulated (AM) signal; however, this lower speed channel may only be decoded when target device 190 is sufficiently close to wand 100/200. Second data 114 may be conveyed within the higher speed channel (e.g., within conventional data packets) independently of data conveyed by the slower speed channel. Signal 140 may use one of amplitude modulation (AM), frequency modulation (FM), and quadrature amplitude modulation (QAM), and so on. That is, signal 140 is a conventional signal that conveys second data conventionally within the higher speed channel. In one embodiment, this higher speed channel is based upon Wi-Fi protocols that include data packets.

[0032] The lower speed channel is used to convey first data (e.g., first data 108) that may include authentication and encryption keys only to target device 190 when sufficiently close to wand 100/200. That is, first data is only intended to be received by target device 190 and is therefore sent over the lower speed channel. The higher speed channel may convey second data, such as a MAC address, cyclic redundancy check, sequence number, optional payload, within conventional packets of the used protocol and this higher speed channel may be received by devices that are not proximate wand 100/200. In one example of use, the higher speed channel is used to convey second data that is encrypted using a secure key (e.g., known only to wand 100/200), where this secure key is conveyed as first data over the lower speed channel and is thereby only received by target device 190 when proximate to wand 100/200. The higher speed channel may be used to convey status, retransmission requests for specific bits of first data 108, and/or a request to retransmit the entire message. Thus, the higher speed channel may be used to verify first data 108 and to reconstruct missing bits of first data 108 as necessary without including first data 108.

[0033] Wand 100 may be used to connect wireless devices, where first data 108 represents a wireless protocol and key configuration that is imparted from wand 100 to each wireless device. Wand 100 may be used to impart any type of information securely onto a targeted, nearby device, without the requirement for specialized hardware (or any hardware changes) in the target device. Use of wand 100 does not use complex algorithms or complicated cryptography libraries, and does not require

target device 190 to be adjacent, or even movable. Wand 100 may be used to wirelessly and securely configure large appliances as well as small mobile devices by using a wireless capability already found on the target device. Once the target device is configured, wand 100 is not needed for further communication.

[0034] Target device 190 is assumed (a) to have at least one radio antenna that it can use to transmit and receive wireless data, (b) to be able to measure the signal strength of wireless communication packets, and (c) to be able to run a small piece of software that implements a read protocol. Target device 190 need not have sensors such as cameras, microphones or accelerometers, and it need not be altered to add new hardware. That is, target device 190 need not have a specific user interface, such as typically included to allow configuration of the device.

[0035] Wand 100 is assumed (i) to be trusted to generate a secret key, (ii) to include wireless capability (e.g., transceivers 110, 210) compatible with that of target device 190 and two antennae located approximately one half wavelength apart, (iii) to be portable such that it may be brought close to and pointed at target device 190, and (iv) to run the communication protocol.

[0036] In one embodiment, only a transmitter section of transceiver 110 is switched between antenna A1 and antenna A2, and a receiver section of transceiver 110 remains coupled to a single antenna (e.g., one of antenna A1 or A2) at any given moment. In another embodiment, transceivers 110 and 210 are implemented as two transmitter sections, each electrically coupled to a different one of antennae A1 and A2, and a single receiver section electrically coupled to one of antennae A1 and A2.

[0037] Wand 100 provides a novel approach for imparting information onto target device 190, even where target device 190 is otherwise unknown and does not have any secret keys pre-installed. Wand 100 provides a consistent, fast, easy, and secure method for imparting any kind of information onto target device 190, regardless of device type or manufacturer of target device 190, and without hardware modifications to the target device. Wand 100 may implement an efficient and robust proximity-detection technique, a protocol for imparting a common key (e.g., a Wi-Fi service set identifier (SSID) and password) onto a new device, a protocol for introducing two devices so they may establish secure, user-intended, communication, and a protocol for imparting a cloud identity and credentials into a new device.

[0038] A radio signal transmitted by an antenna attenuates, or fades, as it travels through the air according to the well-known free-space propagation model given in Equation (1):

$$P_r = P_s G_s G_r \left(\frac{\lambda}{4\pi d} \right)^2 \quad (1)$$

where P_r is the power received in watts, P_s is the power at the surface of the sending antenna in watts, G_s and G_r are the gains of the sending and receiving antennae, respectively, λ is the frequency of the signal, and d is the distance between the sending and receiving antennae.

[0039] This model assumes the radio waves travel through free space without bouncing off any surfaces before striking a receiving antenna. Equation (1) tells us that as the distance between the transmitter and receiver increases, the signal strength at the receiver decreases. Because wand 100 does not change antennae or frequencies, the received power is driven by the distance d between the transmitter and receiver.

[0040] It is sometimes useful to consider signal strength in relation to a known amount of power. In that case, dBm (which expresses power in decibels compared to one milliwatt (mW)) is often used. The conversion is given by Equation (2) where $\log$ refers to the base 10 logarithm:

$$\text{dBm} = 10 \log \left(\frac{P_r}{1\text{mW}} \right) \quad (2)$$

[0041] Using Equation (2), Equation (1) may be rewritten in dBm for free space, as shown in Equation (3):

$$P_r = P_0 - 10\alpha \log \left(\frac{d}{d_0} \right) \quad (3)$$

[0042] where P_r is now the received power in dBm, P_0 is the power in dBm received at a distance of d_0 from the transmitter, and α , called the path-loss exponent, represents the reduction in power as the signal travels. In free space α is 2.

[0043] P_x is used to indicate power in dBm predicted by radio signal propagation models, and RSSI is used to indicate power measured in dBm by actual hardware.

[0044] Equation (3) is a good approximation of signal attenuation in free space, but in the real world obstacles, moving and fixed, may attenuate a signal or cause reflections that create multiple paths between a transmitter and a receiver. The result is that multiple copies of the transmitted signal, each with a different attenuation,

delay, and phase shift, arrive at the receiver superimposed upon each other. This superposition can result in either constructive interference where multiple copies of the signal add to each other, or destructive interference where multiple copies of the signal cancel each other. The change in signal strength caused by obstacles is often called fading.

[0045] There are two types of fading: slow and fast. Slow fading occurs when changes to the signal strength happen slowly over time. Shadowing, where an obstacle such as a building lies between the transmitter and receiver, is an example of slow fading. In this case the alteration to the signal strength is normally constant unless the transmitter or receiver moves. Fast fading occurs when changes to the signal strength happen quickly such as when a moving obstacle comes between a transmitter and receiver.

[0046] Fading may be accounted for by altering Equation (3) to add a noise component, which gives us the log-normal shadow model:

$$P_r = P_0 - 10\alpha \log\left(\frac{d}{d_0}\right) + \chi_\sigma \quad (4)$$

[0047] where χ_σ is a Gaussian random variable representing noise with zero mean and standard deviation σ (in the case of slow fading) or follows a Rayleigh or Rician distribution (in fast fading environments). As noted above, in free space α is 2, but it in real-world dynamic environments α normally ranges from 1.2 to about 8.

[0048] In a dynamic environment where there are multiple moving objects, χ_σ in Equation (4) may change rapidly, making actual measurements of RSSI highly variable.

[0049] In this kind of dynamic environment, the moving objects are changing their position relative to the transmitter – which slightly changes the length of the path from the transmitter to the receiver. The difference in path length, in turn, slightly alters the phase of the received signal. This change in phase may change how the multiple copies of the signal add up to create constructive or destructive interference. Finally, the Doppler effect of the moving obstacle slightly changes the frequency of the received signal, and interference has been shown to vary greatly depending on the frequency of the signal.

[0050] In addition to the environmental variables, the signal strength captured by real equipment is also subject to manufacturing variability as well as thermal noise in the antenna. Wand 100 exploits the variability from manufacturing and thermal noise, together with variability from obstacles in the environment, to make it difficult for an adversary to eavesdrop on communications between wand 100 and target device 190.

[0051] To understand the role environment plays in signal propagation, the signal strength of Wi-Fi packets exchanged between a computer and a Wi-Fi AP were captured in three very different (but realistic) locations where wand 100 might be used. The first location was a quiet home environment where no one was moving, the second location was a local coffee shop where a small number of customers were milling about, and the third location was a busy computer science lab bustling with student activity. A MacBook Pro laptop connected to an Alfa Networks AWUS036H external Wi-Fi antenna was used and the RSSI returned by the Alfa card in the form of RadioTap headers were captured using a Python program written with Scapy. In all cases the receiving antenna was stationary while packets were exchanged with the AP.

[0052] FIG. 3 shows three exemplary graphs 302, 304, 306 illustrating distribution of RSSI measurements returned by capturing 12,000 Wi-Fi packets sent between a Wi-Fi AP and the receiving antenna in a home, in a coffee shop, and in a computer science lab, respectively. Each graph 302, 304, 306 shows a histogram of RSSI values measured, and a best-fit Gaussian distribution for the RSSI values. In the home and computer science lab, the distance between the access point and the receiver was approximately 4 meters. In the coffee shop the distance was approximately 8 meters. The differences in distance led to differences in RSSI, but as expected, due to moving obstacles, there is a wide range in variability of the RSSI. When packets were captured in the quiet home environment the RSSI readings were tightly grouped and had little variation; increased variability was noted in the coffee shop, and a great deal of variability in the busy lab. Table 1 provides details on the mean, standard deviation, and range of the packet RSSIs captured.

Location	Mean	Std Dev	Range
Home	-60	0.69	8
Coffee shop	-84	1.50	10
CS lab	-61	3.48	19

Table 1 RSSI mean, standard deviation, and range of 12,000 Wi-Fi packets captured at three different locations. The standard deviation and range of RSSI measurements increased as the number of moving obstacles increased.

[0053] Although the variability in RSSI is lower in environments where there is little activity, it is important to note that there is still variability – RSSI readings were not the same for all packets. In the quiet home environment, there was still a range of eight RSSI values observed. Other researchers have found that even in an underground concrete tunnel where outside signals and the effects of moving obstacles are not present, there is still a variation of at least two dBm away from the mean.

[0054] Two insights may be gleaned from the above concepts. A first insight is that if a device has two antennae, it can determine when it is in close proximity to another device that is transmitting a radio signal. A second insight is that when a device with two antennae determines it is in close proximity to another device, it may use its two antennae to securely impart information to the other device. As shown in FIG. 1, wand 100 has two antennae A1 and A2.

[0055] Wand 100 may implement detect primitive 105 to determine if it is in close proximity to another device transmitting a radio signal. Wand 100 independently measures the RSSI of the radio signal on each of the two antennae A1 and A2. Building on Equation (4), the RSSI values received on the two antennae of wand 100 will be:

$$P_1 = P_0 - 10\alpha \log\left(\frac{d_1}{d_0}\right) + \chi_\sigma \quad (5a)$$

$$P_2 = P_0 - 10\alpha \log\left(\frac{d_2}{d_0}\right) + \chi_\sigma \quad (5b)$$

where P_0 is the power in dBm measured at a distance of d_0 from the transmitter, P_i is the power in dBm measured at receiving antenna A_i , and d_i is the distance between the transmitter and receiving antenna i .

[0056] Armed with the equations in (5a) and (5b), the difference in signal strength between the two antennae A1 and A2 is calculated as follows:

$$P_1 - P_2 = P_0 - 10\alpha \log\left(\frac{d_1}{d_0}\right) + \chi_\sigma - \left(P_0 - 10\alpha \log\left(\frac{d_2}{d_0}\right) + \chi_\sigma \right) \quad (6a)$$

$$= -10\alpha \left(\log\left(\frac{d_1}{d_0}\right) - \log\left(\frac{d_2}{d_0}\right) \right) \quad (6b)$$

$$= -10\alpha \log\left(\frac{d_1}{d_2}\right) \quad (6c)$$

[0057] Antennae A1 and A2 are physically close together (e.g., 7 cm apart in one embodiment –approximately ½ wavelength). Because they are close together, the environmental factors represented by χ_σ are likely to be similar on each antenna. By taking the difference in signal strength observed on two antennae, sometimes called the RSSI Ratio, the environmental factors cancel out. This suggests that some of the randomness of the environment, shown in FIG. 3, may be minimized in the RSSI Ratio on wand 100.

[0058] When the distance between antennae A1 and A2 is small relative to distances d_1 and d_2 between these antennae and the transmitter, then the RSSI determined for each antenna A1, A2, may be approximately equal. This happens when the receiving device is far away from the transmitting device. For example, where antennae A1 and A2 are 7 cm apart and are aligned with the transmitting antenna such that A2 is 7 cm farther away from the transmitting antenna than A1 (see FIGs. 1 and 2), then $d_2 = d_1 + 7$ cm. Further, where the distance d_1 between A1 and the transmitting antenna is 30 cm (i.e., more than 4 times the distance dA between antennae A1 and A2), then using Equation (6c) and assuming $\alpha = 2$ yields a difference, Δ , of:

$$d_1 = 30 \text{ cm}$$

$$d_2 = 30 \text{ cm} + 7 \text{ cm} = 37 \text{ cm}$$

$$\Delta = -10 \alpha \log(30/37), \text{ approx } 1.8 \text{ dBm} \quad (7)$$

[0059] When the distance to the transmitter is small relative to the distance between antennae A1 and A2, then the difference between received power on the two antennae will be large. That is, when wand 100 is close to target device 190, the distance, d_1 , between antenna A1 and the antenna on target device 190 is much smaller than distance dA between antennae A1 and A2, and the difference between received power on antennae A1 and A2 is large. For example, where target device

190 is located 1 cm from A1, then $d_1 = 1$ cm and $d_2 = 8$ cm, giving an expected difference in RSSI of $\Delta = -10\alpha \log(1/8)$, which is approximately 18.1 dBm.

[0060] Thus, when wand 100 is in close proximity to target device 190, the difference in RSSI readings between antennae A1 and A2 will be significantly larger than the difference between the power readings when the device is far away. In this example there is an expected 10-fold increase in the RSSI Ratio when wand 100 moves from 30 cm to 1 cm between target device 190 and A1. FIG. 4 shows one exemplary graph 400 illustrating expected RSSI ratio, according to Equation 6C, plotted against distance between the transmitter and the nearest antenna A1. As shown, as wand 100 moves close to the transmitter, the RSSI ratio increases dramatically, thereby allowing wand 100 to determine when it is in close proximity to target device 190.

[0061] Software 106, when executed by processor 102, is configured to determine when wand 100 and target device 190 are in close proximity by periodically calculating an average RSSI Ratio according to the following equations:

$$\bar{\delta} = \frac{1}{\omega} \sum_{i=1}^{\omega} r_1(i) - r_2(i) \quad (8a)$$

$$close = \begin{cases} True & \text{if } \bar{\delta} \geq \tau \\ False & \text{if } \bar{\delta} < \tau \end{cases} \quad (8b)$$

where i is the i^{th} packet transmitted and $r_1(i)$ is the RSSI for packet i measured on antenna A1, $r_2(i)$ is the RSSI for the same packet measured on antenna A2, τ is a fixed-value (e.g., 6) threshold to determine if the devices are close, and ω is a window size of the number of RSSI packets received. τ may be adjusted; as τ is made larger, wand 100 and target device 190 need to be closer together before wand 100 indicates sufficiently close proximity, and as τ is made smaller wand 100 and target device 190 may be further apart, but this may introduce errors when transferring data from wand 100 to target device 190. In one embodiment, τ is set to 6 to ensure wand 100 indicates sufficiently close proximity when wand 100 and target device 190 are about 6 cm apart.

[0062] If the average difference $\bar{\delta}$ rises above τ , then wand 100 determines that it is in close proximity to target device 190. Wand 100 may wait to check for proximity until it has received at least ω packets, and re-checks for proximity every $\omega/2$ packets afterward using the last ω RSSI values until it detects it is close to the

device or times out. Using detect primitive 105, wand 100 may determine when it is in close proximity to target device 190, even if the target device has only a single antenna. If target device 190 has multiple antennae, wand 100 assumes that the target device transmits packets using only one of its antennae and does not change its transmitting antenna while wand 100 is executing detect primitive 105.

[0063] FIG. 5 illustrates exemplary communication between wand 100 and target device 190 during operation of detect primitive 105. Upon initiation (e.g., button press on target device 190) by a user, software 192 with target device 190 may cause target device 190 to broadcast an AssocReq packet 502 (e.g., Wi-Fi or similar) every 100ms indicating that it is looking to connect with another device. Wand 100 receives these AssocReq packets 502 and determines whether wand 100 is in close proximity to target device 190 based upon Equations (8a, 8b). In one embodiment, wand 100 provides its user some visual or audio feedback to encourage the user to move wand 100 closer if needed. To provide that feedback, wand 100 uses the difference between the RSSI values of AssocReq packets received on antenna A1 vs. antenna A2. If the spread between RSSI readings is increasing, wand 100 is getting closer to target device 190. If the spread is reducing, wand 100 is getting farther away from target device 190. Wand 100 may indicate (e.g., using one or more indicators 128, or other means such as by generating an audio tone) whether wand 100 is getting closer or farther from target device 190. Where the location of the antenna in target device 190 is not obvious, a visual indicator such as a sticker bearing a recognizable logo could be affixed to target device 190 proximate the antenna to make detect easier. The user could then simply move wand 100 close to the sticker and initiate the detect process.

[0064] Once wand 100 determines that it is in sufficiently close proximity to target device 190, it transmits an AssocAck packet 504 to target device 190. Upon receiving the AssocAck packet 504, target device 190 stops transmitting AssocReq packets.

[0065] Once wand 100 has determined, using detect primitive 105, that it is close proximity to target device 190, it may invoke an impart primitive 107 that exploits a property of radio wave propagation called reciprocity to impart information onto target device 190. Reciprocity says that a signal will experience the same multipath properties (e.g., attenuation phase shifts, delays) in both directions of the link. This means that fading characteristics that occurred for transmissions from target device

190 to wand 100 will be substantially the same for a signal transmitted from wand 100 to target device 190. That is, due to reciprocity, target device 190 should see a large difference in RSSI when wand 100 transmits from antenna A1 vs. when wand 100 transmits from antenna A2.

[0066] Software 192 within target device 190 exploits this expected difference in RSSI to receive the imparted information. Wand 100 first converts information of first data 108 into a binary string m and then sends m one bit at a time. To send a 1, wand 100 may send a packet using the closest antenna, A1. To send a 0, wand 100 may send a packet using the farthest antenna, A2. Antenna A1 and A2 may be swapped without departing from the scope hereof. Close proximity of wand 100 to target device 190 results in software 192 determining a large difference in RSSI depending on which antenna A1, A2 of wand 100 was used for transmission of the data packet. Continuing with the above example, where antennae A1 and A2 are 7 cm apart, wand 100 is pointing directly at target device 190 so that $d2 = d1 + 7$ cm, and distance $d1$ is 3 cm, then with $\alpha = 2$ the signal-strength difference as received on the device would be about 10.5 dBm based upon Equation (6). Thus, RSSI of packets sent from antenna A1 will be significantly higher than RSSI of packets sent from antenna A2.

[0067] FIG. 6 shows exemplary RSSI for 1,000 Wi-Fi packets transmitted from antenna A1, located 3 cm from the receiving antenna of target device 190, intermixed with 1,000 Wi-Fi packets sent from antenna A2, located 10 cm from the receiving antenna of target device 190. As shown in FIG. 6, there is a large difference in RSSI depending on the antenna transmitting the packet. In this case, the RSSI values are consistent with Equation (6) with the path loss exponent $\alpha = 1.6$.

[0068] To decode the message m sent by wand 100, software 192 within target device 190 calculates the average RSSI over all packets received and then compares the RSSI value for each individual packet with the average RSSI. If the RSSI for the individual packet is above the average, software 192 determines that the received packet represents a 1. If the RSSI of the individual packet is below the average, software 192 determines that the received packet represents a 0. More formally:

$$\bar{r} = \frac{1}{n} \sum_{i=0}^n r(i) \quad (9a)$$

$$\hat{m}(i) = \begin{cases} 1 & \text{if } r(i) \geq \bar{r} \\ 0 & \text{if } r(i) < \bar{r} \end{cases} \quad (9b)$$

where $r(i)$ is the RSSI measured on the single antenna of the target device for packet i and $\hat{m}(i)$ is the i^{th} bit in the message received. Once this process is complete the device will have a string $\hat{m}$ representing the string m sent by wand 100.

[0069] To illustrate operation of impart primitive 107, the message “hello” is converted into binary and sent to target device 190 using impart primitive 107. FIG. 7 shows a first exemplary graph 702 illustrating reception of message m where target device 190 is at a distance of 3 cm from antenna A1 of wand 100, and a second graph 704 illustrating reception of message m where target device 190 is at a distance of 30 cm from antenna A1 of wand 100. In FIG. 7, packets representing bit values of 1 should be received on the target device with an RSSI above the average and packets representing bit values of 0 should be received below the average. Circles represent bits received correctly and X’s represent errors. In the example of FIG. 7, message m was received without error at 3 cm, but had numerous errors at 30 cm.

[0070] To ensure target device 190 is not missing any bits in message m due to dropped packets, each packet sent by wand 100 may include an increasing sequence number in the payload. Target device 190 uses this sequence number of each received packet to determine whether any packets have been missed. After it has received the last packet from wand 100, if any packets are missing target device 190 requests a resend of only those missing packets; otherwise it sends an empty list to wand 100.

[0071] To be clear, the information is transferred using the RSSI alone – the packets themselves sent do not contain portions of the message m . The payload of transmitted packets contains only the sequence number to allow target device 190 to identify any missing bits.

[0072] To execute impart primitive 107, wand 100 sends *Message* packets to target device 190, where each packet represents one bit in message m , transmitted from one of antenna A1 and A2 based upon the value of the bit. Wand 100 sends the entire message without waiting for any acknowledgement from target device 190. When all message bits have been transmitted, wand 100 sends a *Done* packet. The *Done* packet is like a *Message* packet, but it also includes a hash of m in the payload. Target device 190 records the RSSI for all of the *Message* packets and searches for missed packets upon receiving the *Done* packet from wand 100. If target device 190 detects any missed packets, it transmits a list of missing sequence numbers to wand 100 in the payload of a *DoneAck* message. If no packets are missing, target device

190 transmits the *DoneAck* with an empty payload. If the payload of the *DoneAck* is not empty, wand 100 resends only those missing packets followed by another *Done* packet. If the Wand does not receive a *DoneAck* packet, the Wand resends the *Done* packet. In an embodiment, each packet (i.e., each bit of message m) is acknowledged rather than waiting until all message bits have been transmitted.

[0073] Once target device 190 has received and stored RSSI values for each bit of message m , it computes the average RSSI of the packets received. Target device 190 then compares each of the stored RSSI values with the average RSSI to determine whether the corresponding bit of message m was a 1 or 0 as described above. This creates a message $\hat{m}$ on the device.

[0074] Finally, target device 190 hashes $\hat{m}$ and compares it with the hash of m included in the *Done* packet received from wand 100. If the computed hash matched the received hash, target device 190 knows that all packets have been received correctly. Where the hashes do not match, target device 190 tries flipping each bit in $\hat{m}$, one bit at a time; each time it re-hashes $\hat{m}$ and compares the re-hash with the received hash. If, after flipping all bits of $\hat{m}$, a match has not been found, target device 190 follows a similar pattern and tries flipping two bits each time. If target device 190 still does not compute a re-hash that matches the received hash, target device 190 signals wand 100 to restart by sending a Restart packet to wand 100. If target device 190 does find a match, target device 190 transmits a Success packet to wand 100.

[0075] FIG. 8 is a flow sequence 800 showing exemplary operation of impart primitive 107, illustrating *Message* packets $m(1) \dots m(n)$ being sent from wand 100 to target device 190, followed by a *Done* packet containing a hash of m . Target device 190 then sends a *DoneAck* packet with a list of missing packet numbers to wand 100, and wand 100 retransmits any missing packets. Target device 190 derives a message $\hat{m}$ from the RSSI values of each received packets from wand 100, and confirms that message $\hat{m}$ matches message m by comparing the hashes of $\hat{m}$ and m . If the hashes do not match, target device 190 tries flipping bits in $\hat{m}$ to get a match.

[0076] In one embodiment, where the length of message m is long, wand 100 may divide message m into smaller messages to enable target device 190 to efficiently flip bits. On the other hand, short messages may be susceptible to an adversary discovering the message by brute-force flipping bits and hashing. Therefore, wand

100 may divide long messages and pad short message into 128-bit messages, for example.

[0077] As described above, wand 100 (and software 192 within target device 190) uses the primitive operations configured within detect primitive 105 and impart primitive 107 described above to build higher level protocols for configuring target device 190 (e.g., where target device 190 is to be configured for communication on a local-area network). The detect primitive 105 and the impart primitive 107 are used to implement three exemplary protocol operations: (1) common key, where a target device is imparted with parameters and a key that are common to all devices in a local-area network, (2) unique key, where two partnering devices connect using parameters and a key that is unique to the partnering devices, and (3) copy and paste, where wand 100 copies data from a first device and pastes it into another device without creating a lasting bond between devices.

[0078] As shown in FIG. 1 (and FIG. 2), software 106 includes a *common key protocol* 109 that is used for configuring target device 190 with common information, such as when target device 190 is new and is to be configured with parameters that are common to all devices in a local-area network. FIG. 9 is a flow sequence 900 illustrating exemplary operation of the common key protocol 109. FIGs. 1, 2 and 9 are best viewed together with the following description. In one example, where a patient receives a blood-pressure monitor and wishes to connect the blood-pressure monitor to a Wi-Fi network, the blood-pressure monitor needs to be configured with an SSID and a password (e.g., a key) of the Wi-Fi network access point (AP).

[0079] First data 108 may include the SSID and password of the AP, previously loaded into wand 100 using a wired universal serial bus (USB) connection (for example). In one embodiment, wand 100 is configured as a stick-shaped device that couples with a USB port of the AP, keeping its batteries charged until needed, and using the USB interface to securely receive connectivity parameters from the AP.

[0080] Common key protocol 109 and software 192 within target device 190 (e.g., the blood-pressure monitor) cooperate to first implement detect primitive 105 to ensure that wand 100 and target device 190 are within sufficient proximity of one another, and then use impart primitive 107 to transfer first data 108 (e.g., the SSID and password) from wand 100 to target device 190. Once target device 190 has confirmed it has properly received the SSID and password message, flipping bits if

necessary as described above, target device 190 may connect to the Wi-Fi AP using the SSID and password parameters.

[0081] Thus, wand 100 gives only the target device 190 (i.e., the blood-pressure monitor) the information needed to connect with the Wi-Fi AP, after which the wand 100 is not required for future communications between the Wi-Fi AP and target device 190. First data 108 may represent other information, whether secret or not, that is to be transferred to target device 190, and is not limited to this Wi-Fi connection parameter example.

[0082] FIG. 10 shows wand 100 implementing a *unique key protocol* 111 for establishing a wireless connection between two devices 1090 and 1096, where the wireless connection is secured by a key meant to be known only to devices 1090 and 1096. Device 1090 includes a processor 1091 and a memory 1093 that cooperate to provide functionality of device 1090. Device 1096 includes a processor 1097 and a memory 1099 that cooperate to provide functionality of device 1096. Devices 1090 and 1096 each also includes at least a receiver to receive signals from wand 100/200. FIG. 11 is a flow sequence 1100 illustrating exemplary operation of unique key protocol 111. FIGs. 10 and 11 are best viewed together with the following description.

[0083] Within wand 100, unique key protocol 111 first generates a random key 1008. Wand 100 and target device 1090 run detect primitive 105 such that wand 100 determines when they are within sufficient proximity of one another for communication. Wand 100 then sends random key 1008 to device 1090 using impart primitive 107. Target device 1090 includes its unique identifier 1092 (e.g., one or more of internet protocol (IP) address, media access control (MAC) address, and other such identification) in the payload of the success message at the end of impart primitive 107 and unique key protocol 111 stores ID 1092 within memory 104.

[0084] Unique key protocol 111 then uses detect primitive 105 with the second device, target device 1096. Once proximity is established between wand 100 and target device 1096, unique key protocol 111 uses impart primitive 107 to send random key 1008 and ID 1092 to target device 1096. Once device 1096 has confirmed it has successfully received random key 1008 and ID 1092, wand 100 is no longer required. Device 1096 may then open direct communication with device 1090 by sending a hash of random key 1008 to device 1090 using ID 1092 obtained from wand 100.

Device 1090 receives the hash from device 1096, notes the address of device 1096, and hashes its own copy of random key 1008. If the hashes match, then device 1090 may bootstrap a MAC or IP layer connection with device 1096 using random key 1008 as an initial key. If the hashes do not match, device 1090 may not attempt the connection.

[0085] One example where copying and pasting information would be useful is for the blood-pressure monitor scenario described above. FIG. 12 shows wand 100 implementing a *copy-and-paste protocol* 113 for copying data from a doctor device 1290 and pasting the data to a target device 1296. Device 1290 includes a processor 1291 and a memory 1293 that cooperate to provide functionality of device 1290. Device 1296 includes a processor 1297 and a memory 1299 that cooperate to provide functionality of device 1296. Devices 1090 and 1096 each also includes at least a receiver to receive signals from wand 100/200. FIG. 13 shows exemplary operation of copy-and-paste protocol 113. FIGs. 12 and 13 are best viewed together with the following example.

[0086] Doctor device 1290 and target device 1296 have no need to form a relationship, such as for communication as used in the example for common key protocol 109 and unique key protocol 111 described above. Continuing with the above example, the patient uses the blood-pressure monitor at home to take his/her blood pressure every day with the intention that the blood-pressure readings are to be stored on the physician's Electronic Health Record (EHR) system. As described above, wand 100 may use common key protocol 109 to configure the blood-pressure monitor for communication with his/her Wi-Fi AP, and while that adds long-range communication capability to the short-range blood-pressure monitor, it does not solve the problem of transferring the blood-pressure reading from the blood-pressure monitor into the EHR. To allow the blood-pressure readings to be stored within the EHR, the blood-pressure monitor (or optionally the Wi-Fi AP) is configured with the specific communication details that define how and where to send the blood-pressure readings. These specific communication details may include a Restful API URL and the patient's credentials such as ID and password for example. With these specific communication details, the medical readings from the blood-pressure monitor may be delivered to and stored within corresponding patient records in the EHR.

[0087] Continuing with the medical example, the patient brings wand 100 to the doctor's office and invokes the *copy* part of copy-and-paste protocol 113, which first generates a random key 1208 and then uses detect primitive 105 and impart primitive 107 to securely transfer random key 1208 to a computer (i.e., doctor device 1290) in the doctor's office that contains the patient's credentials 1292. Doctor device 1290 encrypts the patient's credentials 1292 using random key 1208 to generate a cypher 1294 and sends cypher 1294 to wand 100. Wand 100 stores cypher 1294 and the patient returns home with wand 100. The patient then performs the *paste* portion of copy-and-paste protocol 113, using detect primitive 105 and impart primitive 107, to send random key 1008 and cypher 1294 to target device 1296 (i.e. the blood-pressure monitor). Target device 1296 then decrypts cypher 1294 and uses credentials 1292 to send blood-pressure readings to the EHR and wand 100 deletes cypher 1294 (and optionally deletes random key 1008). In this way, copy-and-paste protocol 113 is used to securely copy data from one device (e.g., doctor device 1290) and to securely paste that data onto another device (e.g., target device 1296), even though devices 1290, 1296 are physically far apart.

[0088] The use of wand 100 alleviates (a) the complexity of manually configuring a device with sensitive communication parameters and other sensitive data, (b) the need to store unencrypted information on a third-party device. When performing the copy part of the copy and paste protocol, wand 100 may protect itself from storing malicious data by ensuring any received packets have a large RSSI ratio. This ensures the data is received from a nearby target device, and not from a distant attacker attempting to exploit wand 100.

[0089] Wand 100/200 may determine, based on the RSSI of the received signal on each of its antennas, when the transmitting device is in front or behind. For example, where the determined RSSI ratio between the two antennae is negative, then the target device is behind wand 100/200. Where the ratio is positive (as is normally assumed), the target device is in front of wand 100/200. In embodiments, target devices 190, 1090, 1096, 1290, and 1296, are configured to differentiate between front-lobe operation and back-lobe operation of wand 100/200 to prevent inadvertent configuration of the target device when proximate but behind wand 100/200. For example, where wand 100/200 is used to configure a first target device positioned in front of wand 100/200, such as on a patient, and a second target device is located on

the user of wand 100/200, such as a care-giver, polarity of received bits of first data 108 within the lower speed secure channel indicates whether the target device is in front of or behind wand 100/200, since the positions of antennae A1 and A2 relative to the target devices are reversed. Such differentiation within target device 190 may prevent incorrect transfer and configuration of devices within the back-lobe of wand 100/200.

[0090] Changes may be made in the above methods and systems without departing from the scope hereof. It should thus be noted that the matter contained in the above description or shown in the accompanying drawings should be interpreted as illustrative and not in a limiting sense. The following claims are intended to cover all generic and specific features described herein, as well as all statements of the scope of the present method and system, which, as a matter of language, might be said to fall therebetween. In particular, the following embodiments are specifically contemplated, as well as any combinations of such embodiments that are compatible with one another:

- A. Apparatus for securely transferring first data to a target device, including a first antenna, a second antenna positioned a fixed distance from the first antenna, a transmitter, and a processor configured to control the transmitter to transmit a first signal containing second data selectively from one of the first antenna and the second antenna based upon the first data. The first data may only be received by the target device when the target device within close proximity of the first and second antennae, and the second data does not include the first data.
- B. The apparatus of embodiment A, the fixed distance between the first and second antenna being approximately a half of a wavelength of the first signal.
- C. The apparatus of either of embodiments A and B, the first signal being transmitted such that the first data may be determined by the target device from received signal strength indication (RSSI) of the first signal.
- D. The apparatus of any of the embodiments of A through C, further including a switch configured to electrically couple each of the first antenna and the second antenna to the transmitter under control of the processor.
- E. The apparatus of any of the embodiments of A through D, for each of a plurality of bits of the first data, the processor sequentially controlling the

transmitter and the switch to transmit the first signal from the first antenna when the bit has a first value and the processor controlling the transmitter to transmit the first signal from the second antenna when the bit has a second value different from the first value.

- F. The apparatus of any of the embodiments of A through E, further including a wand shaped housing for positioning the second antenna at the fixed distance from the first antenna.
- G. The apparatus of any of the embodiments of A through F, the housing being shaped to indicate orientation of the first and second antennae to a user of the apparatus.
- H. The apparatus of any of the embodiments of A through G, the transmitter including a first transmitter electrically coupled to the first antenna and a second transmitter electrically coupled to the second antenna, the processor selectively controlling one of the first and second transmitters to transmit the signal based upon values of bits of the first data.
- I. The apparatus of any of the embodiments of A through H, the processor configured to determine proximity of the target device to the apparatus based upon a ratio of received signal strength indication (RSSI) for a second signal transmitted by the target device and received by both of the first and second antennae, the processor controlling the transmitter to transmit the first signal only when the target device is in line with and in close proximity to the first and second antennae to decode the first data.
- J. The apparatus of any of the embodiments of A through I, the spacing and orientation of the first and second antennae ensuring that the first data is detectable within the first signal only when (a) an antenna of the target device is within a predefined proximity of the first and second antennae and (b) the antenna of the target device is positioned substantially in line with the first and second antennae.
- K. A method for securely transferring first data from a source device to a target device, including the step of transmitting a wireless signal having (a) a higher speed channel conveying second data and (b) a lower speed channel conveying the first data, wherein the lower speed channel is formed by selectively transmitting the wireless signal from one of a first and second

antennae of the source device based upon the first data. The first and second antenna being positioned a fixed distance apart and the target device using a received signal strength indication (RSSI) of the first signal to decode the lower speed channel and receive the first data.

- L. The method of embodiment K, the fixed distance corresponding to approximately a half of a wavelength of the first signal.
- M. The method of either of the embodiments K and L, further including, before the step of transmitting, determining proximity of the target device to the source device based upon an RSSI ratio of a second signal received from the target device by each of the first and second antennae, wherein the step of transmitting is started when the RSSI ratio is greater than a predefined threshold that indicates that the target device is within sufficiently close proximity of the first and second antennae to decode the lower speed channel.
- N. The method of any of the embodiments of K through M, the higher speed channel conveying the second data within data packets, where each data packet corresponds to one bit of the first data within the slower speed channel.
- O. The method of any of the embodiments of K through N, further including sending a hash value of the first data within one of the data packets to allow the target device to determine whether part of the first data is incorrect or incomplete based upon the hash value.
- P. The method of any of the embodiments of K through O, further including receiving, within a data packet transmitted by the target device, a request to retransmit the part of the first data that is incorrect and retransmitting at least the incorrect or incomplete part of the first data.
- Q. The method of any of the embodiments of K through P, the target device flipping bits of received data until a hash of the received data matches the hash value.
- R. The method of any of the embodiments of K through Q, the first data including data copied from another device for pasting into the target device. The first data is copied from the other device using a copy portion of a copy and paste protocol, and then the first data is transferred to the target device using a paste portion of the copy and paste protocol.

- S. The method of any of the embodiments of K through R, the first data corresponding to encryption of information within the second data.

CLAIMS

What is claimed is:

1. Apparatus for securely transferring first data to a target device, comprising:
a first antenna;
a second antenna positioned a fixed distance from the first antenna;
a transmitter; and
a processor configured to control the transmitter to transmit a first signal
containing second data selectively from one of the first antenna and the
second antenna based upon the first data;
wherein the first data may only be received by the target device when the
target device within close proximity of the first and second antennae;
and
wherein the second data does not include the first data.
2. The apparatus of claim 1, wherein the fixed distance between the first and
second antenna is approximately a half of a wavelength of the first signal.
3. The apparatus of claim 2, wherein the first signal is transmitted such that the
first data may be determined by the target device from received signal strength
indication (RSSI) of the first signal.
4. The apparatus of claim 3, further comprising a switch configured to
electrically couple each of the first antenna and the second antenna to the transmitter
under control of the processor.
5. The apparatus of claim 4, for each of a plurality of bits of the first data, the
processor sequentially controlling the transmitter and the switch to transmit the first
signal from the first antenna when the bit has a first value and the processor
controlling the transmitter to transmit the first signal from the second antenna when
the bit has a second value different from the first value.

6. The apparatus of claim 5, further comprising a wand shaped housing for positioning the second antenna at the fixed distance from the first antenna.
7. The apparatus of claim 6, wherein the housing is shaped to indicate orientation of the first and second antennae to a user of the apparatus.
8. The apparatus of claim 7, the transmitter comprising a first transmitter electrically coupled to the first antenna and a second transmitter electrically coupled to the second antenna, the processor selectively controlling one of the first and second transmitters to transmit the signal based upon values of bits of the first data.
9. The apparatus of claim 8, the processor configured to determine proximity of the target device to the apparatus based upon a ratio of received signal strength indication (RSSI) for a second signal transmitted by the target device and received by both of the first and second antennae, the processor controlling the transmitter to transmit the first signal only when the target device is in line with and in close proximity to the first and second antennae to decode the first data.
10. The apparatus of claim 9, wherein the spacing and orientation of the first and second antennae ensures that the first data is detectable within the first signal only when (a) an antenna of the target device is within a predefined proximity of the first and second antennae and (b) the antenna of the target device is positioned substantially in line with the first and second antennae.
11. A method for securely transferring first data from a source device to a target device, comprising:
 - transmitting a wireless signal having (a) a higher speed channel conveying second data and (b) a lower speed channel conveying the first data, wherein the lower speed channel is formed by selectively transmitting the wireless signal from one of a first and second antennae of the source device based upon the first data;
 - wherein the first and second antenna are positioned a fixed distance apart; and

wherein the target device uses a received signal strength indication (RSSI) of the first signal to decode the lower speed channel and receive the first data.

12. The method of claim 11, wherein the fixed distance corresponds to approximately a half of a wavelength of the first signal.
13. The method of claim 12, further comprising, before the step of transmitting, determining proximity of the target device to the source device based upon an RSSI ratio of a second signal received from the target device by each of the first and second antennae, wherein the step of transmitting is started when the RSSI ratio is greater than a predefined threshold that indicates that the target device is within sufficiently close proximity of the first and second antennae to decode the lower speed channel.
14. The method of claim 13, the higher speed channel conveying the second data within data packets, where each data packet corresponds to one bit of the first data within the slower speed channel.
15. The method of claim 14, further comprising sending a hash value of the first data within one of the data packets to allow the target device to determine whether part of the first data is incorrect or incomplete based upon the hash value.
16. The method of claim 15, further comprising:
 - receiving, within a data packet transmitted by the target device, a request to retransmit the part of the first data that is incorrect; and
 - retransmitting at least the incorrect or incomplete part of the first data.
17. The method of claim 16, wherein the target device flips bits of received data until a hash of the received data matches the hash value.
18. The method of claim 17, the first data comprising data copied from another device for pasting into the target device.
19. The method of claim 18, the first data corresponding to encryption of information within the second data.

20. Apparatus for securely transferring first and second data to a target device, the first data comprising encryption information, the apparatus comprising:

a first antenna;

a second antenna positioned a fixed distance from the first antenna;

at least one transmitter; and

a processor configured to selectively switch the transmitter between the first antenna and the second antenna based upon the first data, wherein the second data is encoded independently of the coupling of the at least one transmitter to the first and second antennae.

21. A system for securely transferring first data from a source device to a target device, comprising:

the source device, comprising:

a first antenna;

a second antenna positioned a fixed distance from the first antenna;

a transmitter; and

a processor configured to control the transmitter to transmit a first signal containing second data selectively from one of the first antenna and the second antenna based upon the first data;

the target device, comprising:

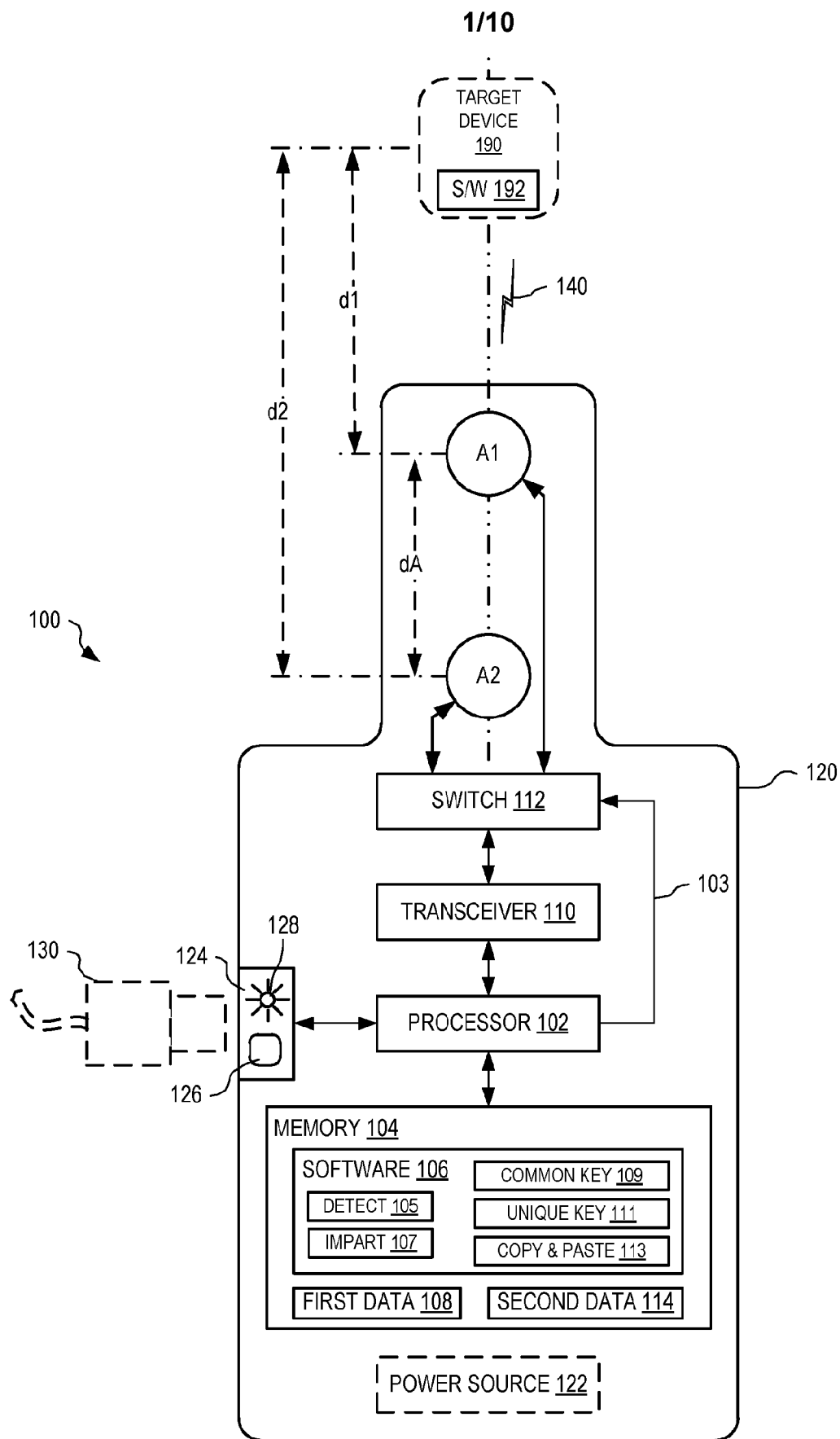
an antenna configured for receiving the first signal from the source device;

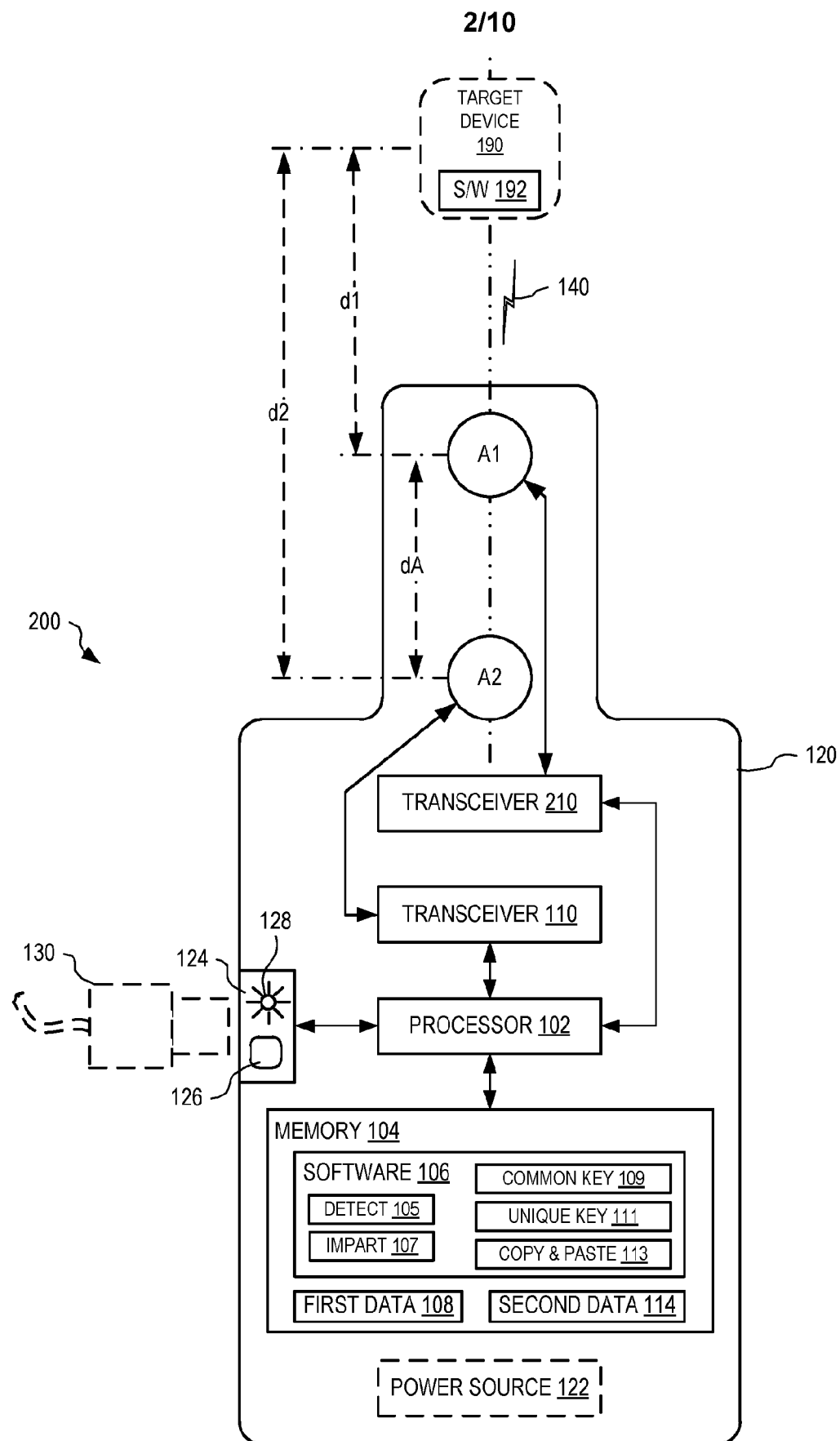
a receiver electrically coupled with the antenna and configured to determine a received signal strength indicator (RSSI) of the first signal; and

a processor configured to receive the RSSI of the first signal from the receiver and to determine the first data therefrom;

wherein the first data may only be received by the target device when the target device within close proximity of the first and second antennae;

wherein the second data does not include the first data; and
wherein the target device determines when it is positioned within a back lobe
of the source device when polarity of received data is inverted.

**FIG. 1**



3/10

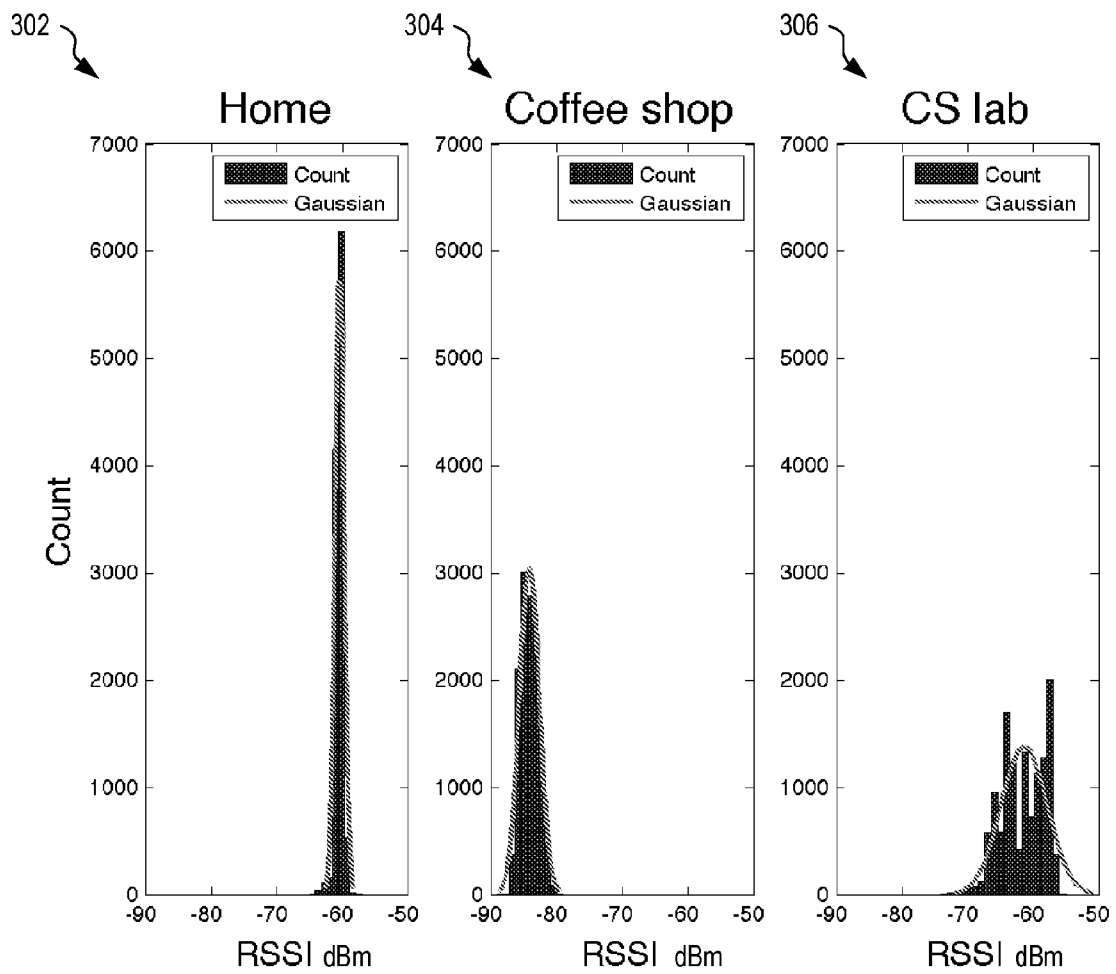


FIG. 3

4/10

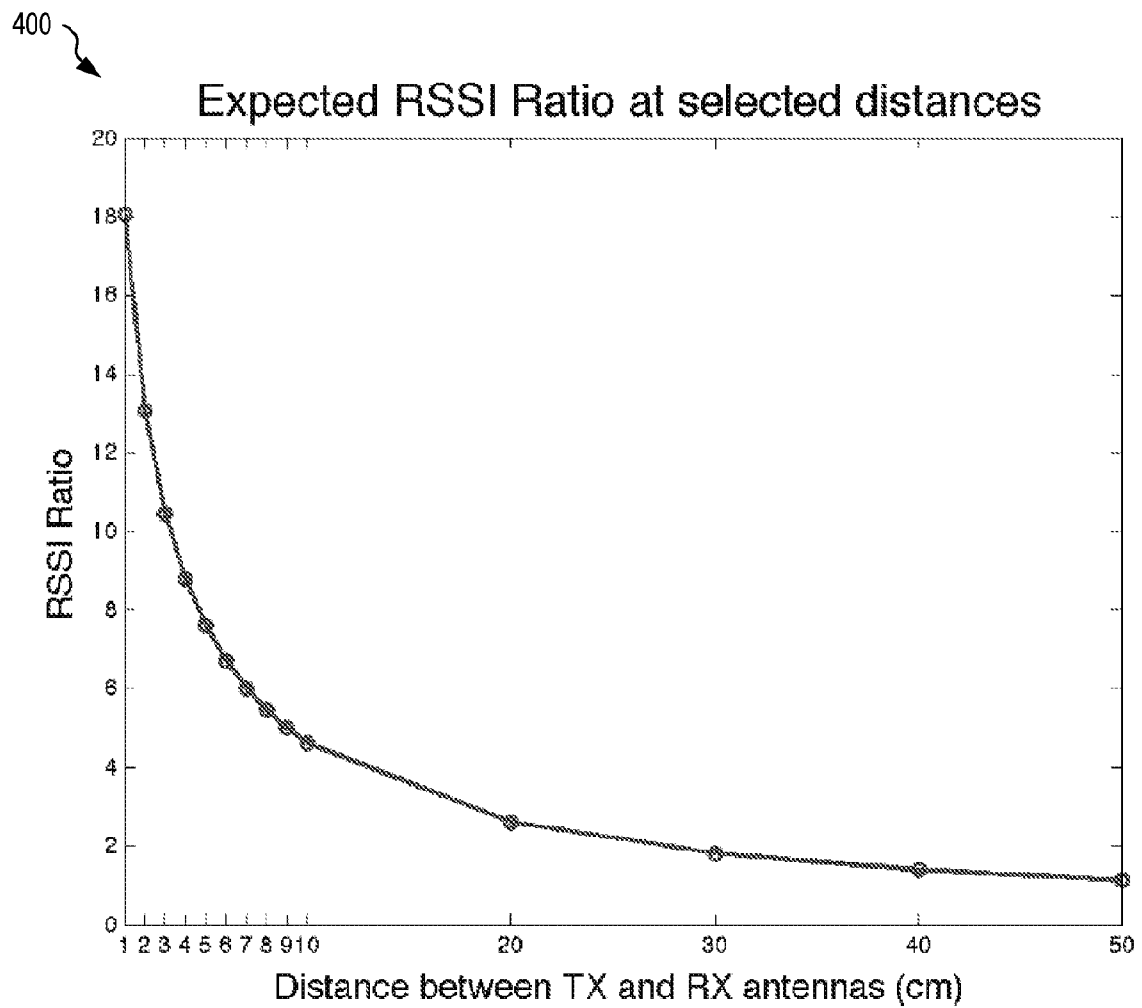


FIG. 4

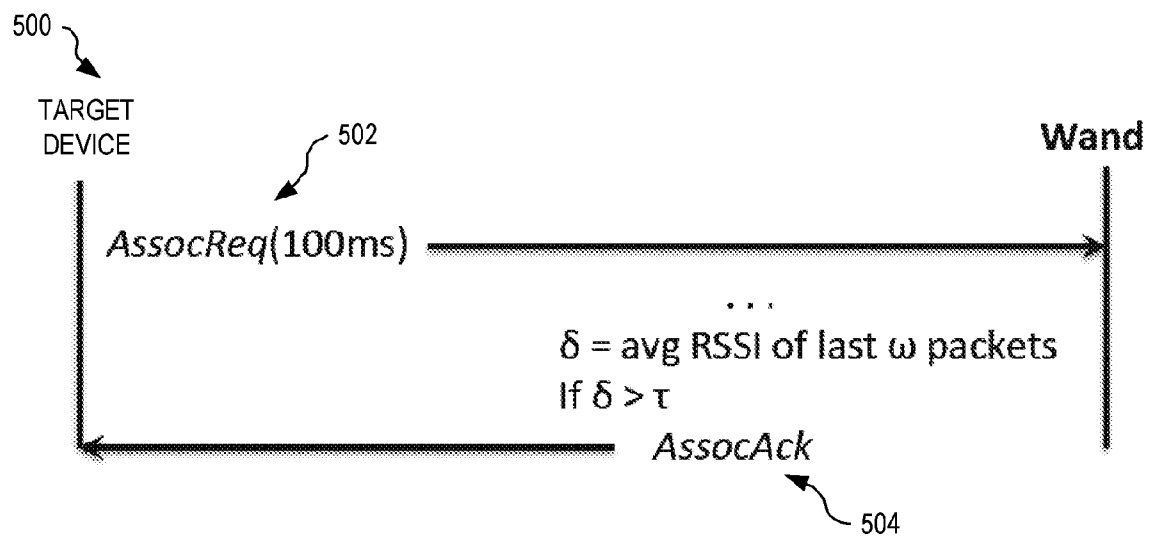


FIG. 5

5/10

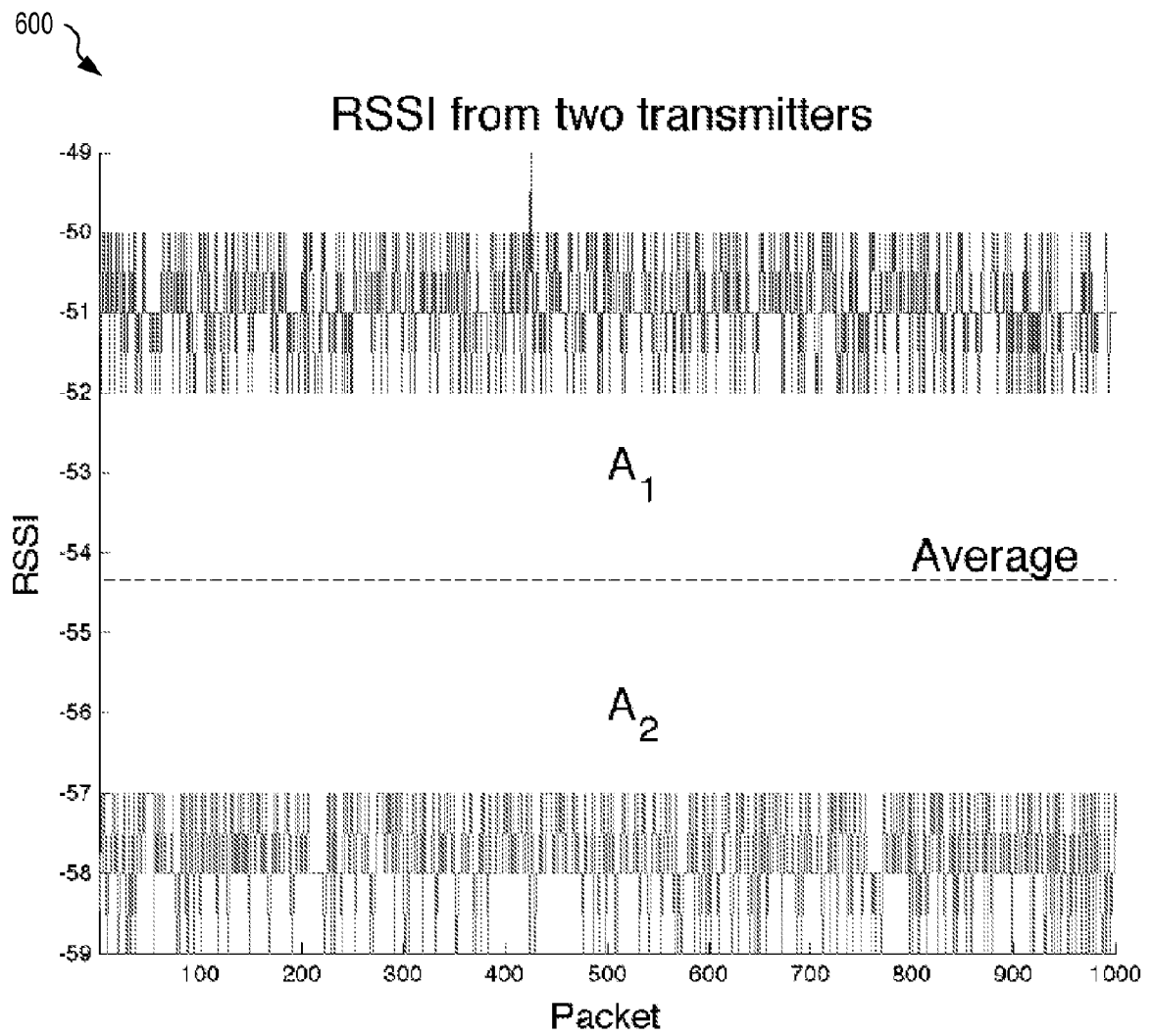


FIG. 6

6/10

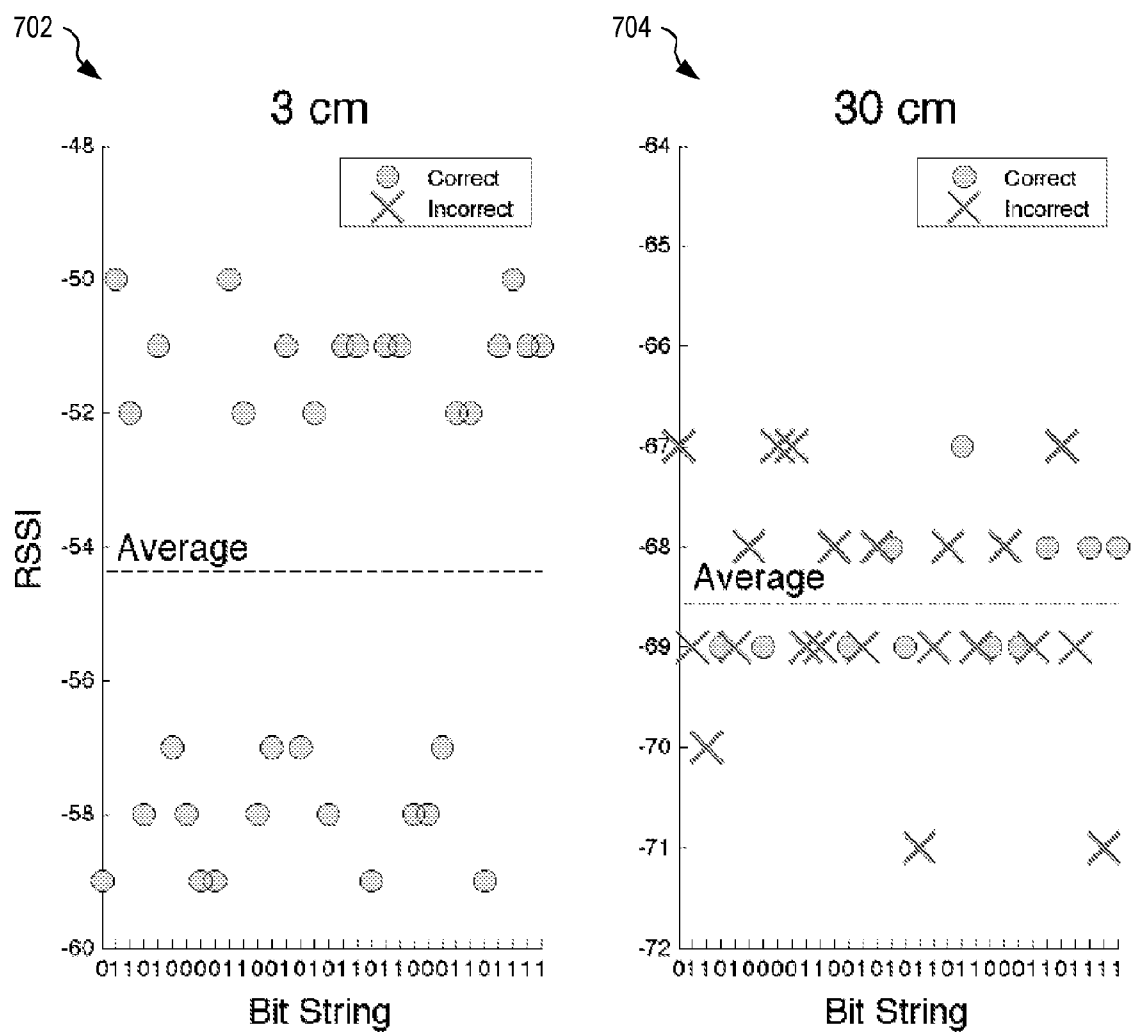


FIG. 7

7/10

800

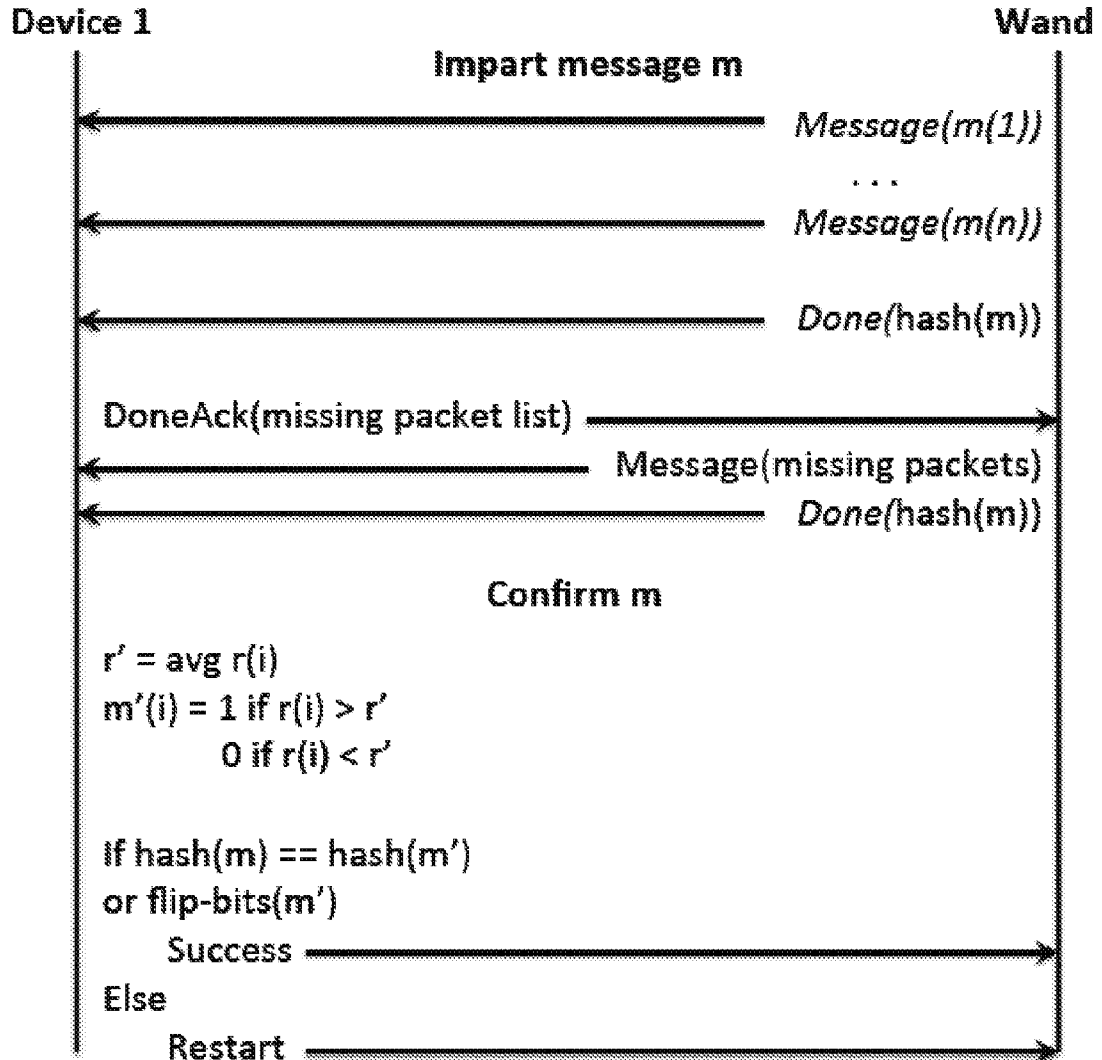


FIG. 8

900

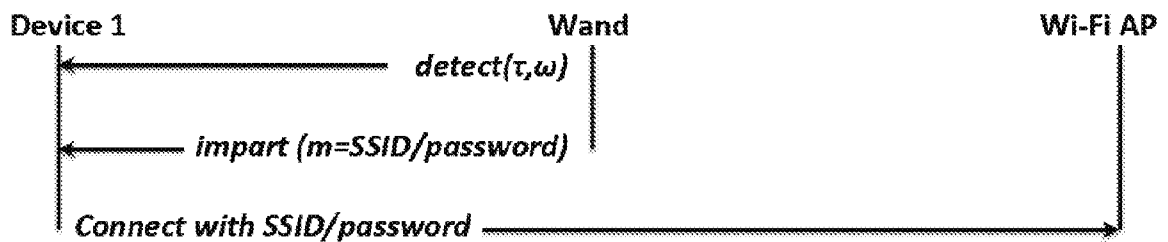


FIG. 9

8/10

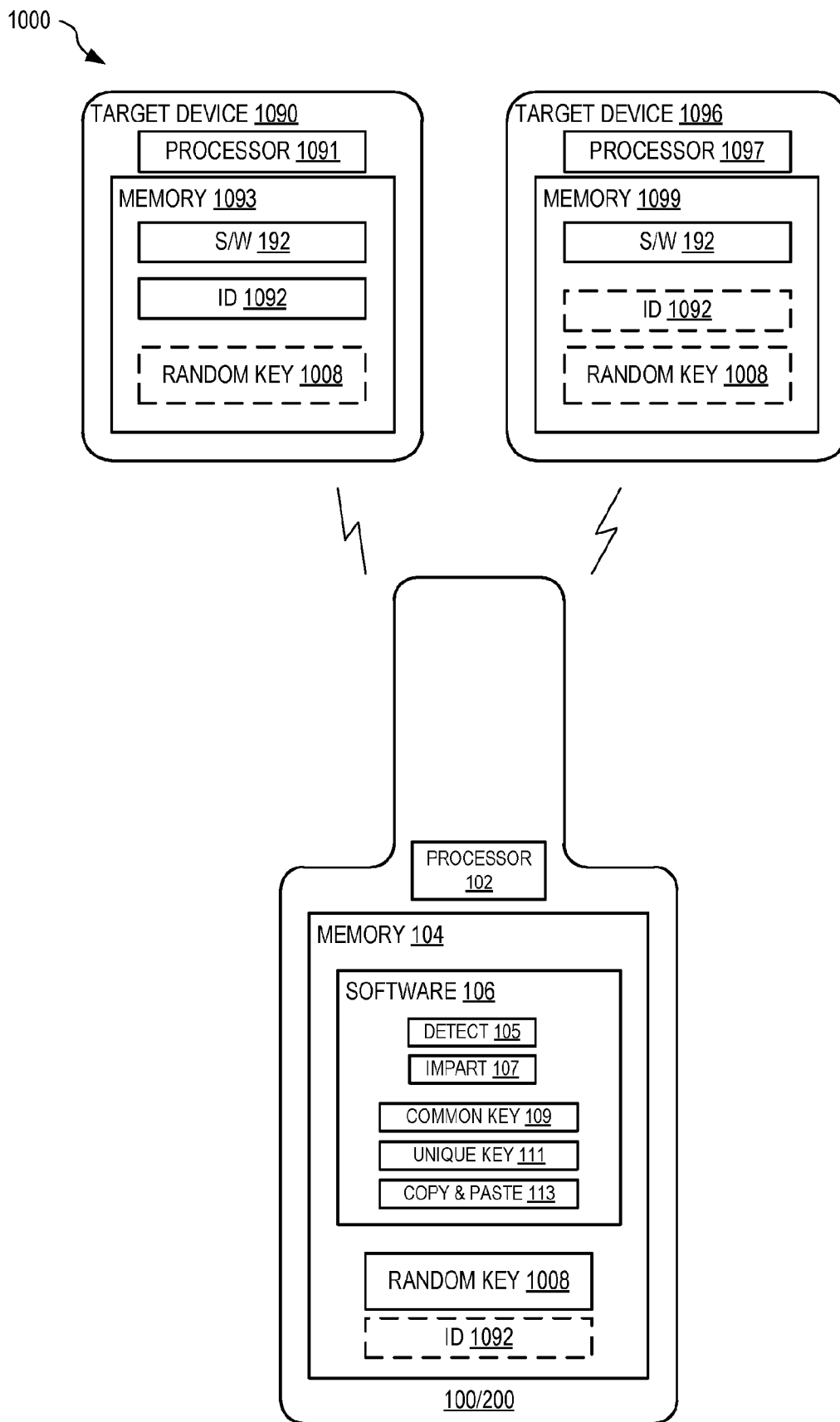


FIG. 10

9/10

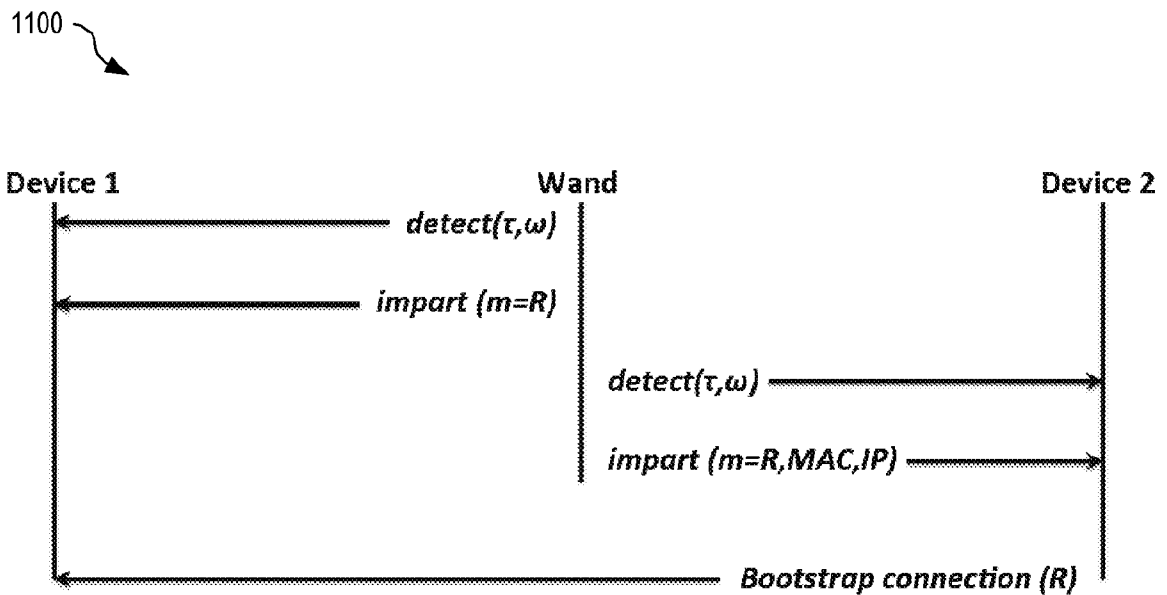


FIG. 11

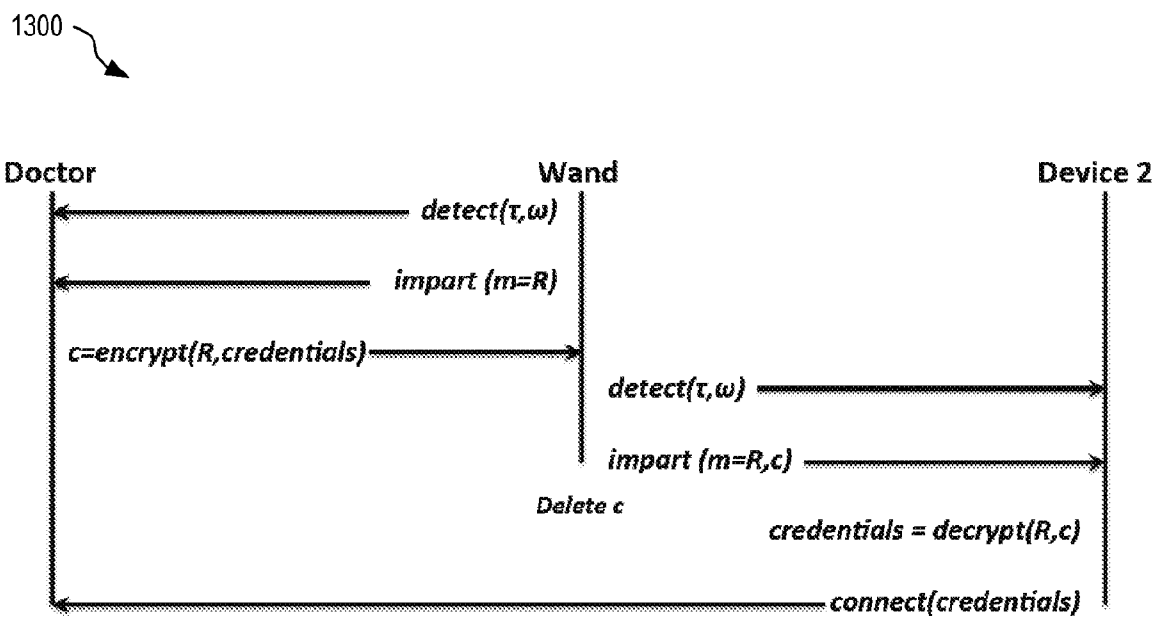


FIG. 13

10/10

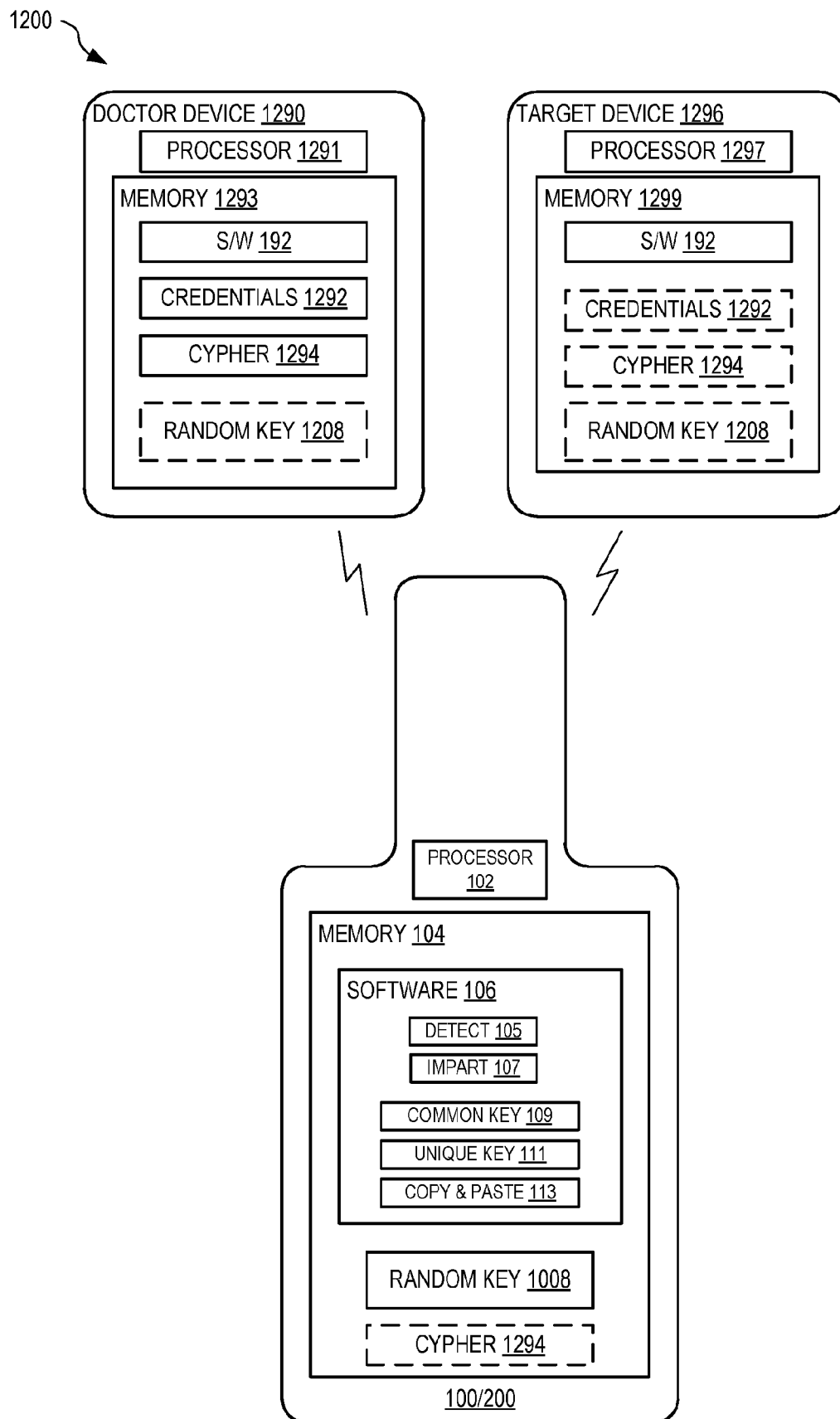


FIG. 12

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 16/39009

A. CLASSIFICATION OF SUBJECT MATTER IPC(8) - G06F 7/04 (2016.01) CPC - H04L 67/02, H04L 63/12, G06F 21/604 According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) IPC(8)-G06F7/04 (2016.01); CPC-H04L67/02, H04L63/12, G06F21/604 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched IPC(8)- H04L 29/06 (01.2016); CPC-H04W12/08, H04L63/20, G06F21/577, H04L63/1433, H04L29/06 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) PatBase, Google Patents/Scholars: terms-Source device emitter transmitter secure transfer first signal channel convey containing second data to target device within proximity selective switch first antenna position space apart fix distance second antenna based upon first data target device		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2013/0307727 A1 (HE et al.) 21 November 2013 (21.11.2013), para [0040]-[0041], [0044] [0047]-[0048], [0055], [0065]; figs. 3-5.	1-21
A	US 2013/0308554 A1 (Ngai et al.) 21 November 2013 (21.11.2013), entire document.	1-21
A	US 2014/0022125 A1 (Zhu et al.) 23 January 2014 (23.01.2014), entire document.	1-21
A	US 2012/0214402 A1 (Shany et al.) 23 August 2012 (23.08.2012), entire document.	1-21
A	US 2012/0268308 A1 (Tuttle) 25 October 2008 (25.10.2008), entire document.	1-21
☐ Further documents are listed in the continuation of Box C. ☐		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 10 August 2016 (10.08.2016)		Date of mailing of the international search report 08 SEP 2016
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300		Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774