Ministero dello Sviluppo Economico
Ufficio Italiano Brevetti e Marchi

Domanda numero **102011901998156 (RE2011A000099)** Tipologia **Invenzioni**

N.B. *Non tutte le schede riportano la medesima struttura, essendo questa strettamente correlata alla tipologia.*
Dati aggiornati al **28 settembre 2017** (fonte: *www.uibm.gov.it*)

Data Deposito	N. Brevetto	Data Brevetto
21 novembre 2011	**0001408721**	**03 luglio 2014**
Stato Domanda	Anticipata accessibilità	Data di Pubblicazione
rilasciata	**no**	**22 maggio 2013**

Titolo
procedimento per il trasferimento verticale di un terminale mobile

Titolare
GUGLIELMO S.R.L. | **BIBBIANO** | **(RE)** |

Inventori
BUSANELLI STEFANO
FERRARI GIANLUIGI
IOTTI NICOLA
MARTALO' MARCO
SPIGONI GIOVANNI

Domicilio elettivo
ING. C. CORRADINI & C. S.R.L.

Indirizzo
VIA D. ALIGHIERI 4 - 42121 REGGIO EMILIA (RE)

Centro raccolta colture microrganismi
-

CLASSI

Codice Classi
H04W

PRIORITÀ

Nazione	Numero domanda	Data domanda
-	-	-

CCP/CCPF

Nel database non sono state trovate domande di CCP o CCPF

CONVERSIONE DELLA DOMANDA

Nel database non risultano pervenute domande di trasformazione o di deposito contemporaneo.

ANNOTAZIONI

Annotazione numero: **1** Tipologia della domanda di annotazione: **Fissa**

Numero Domanda	Data Deposito	Stato Domanda	Tipo Domanda Presentata	Causale
622014902237374 (RE2014F000008)	**26 febbraio 2014**	**agli atti**	**cambiamento di sede**	

Nome e indirizzo Studio
ING. C. CORRADINI & C. S.R.L. | **VIA D. ALIGHIERI 4 - 42121 REGGIO EMILIA (RE)** |
Da
LANGHIRANO (PR)
A
BIBBIANO (RE)

DESCRIZIONE

del Brevetto Italiano per Invenzione Industriale dal titolo:

"PROCEDIMENTO PER IL TRASFERIMENTO VERTICALE DI UN TERMINALE MOBILE"

a nome **GUGLIELMO S.r.l.**, con sede in **43013 PARMA (PR)**

* * * * *

La presente invenzione si riferisce ad un procedimento per il trasferimento di dati tra un terminale mobile e terminali remoti accessibili tramite connessioni di rete, mediante esecuzione di un trasferimento verticale (Vertical HandOver – VHO), e un metodo di VHO.

Più in particolare, un aspetto della presente invenzione si riferisce ad un sistema per eseguire un Vertical HandOver e un metodo di esecuzione di un Vertical HandOver che sia in grado di mantenere una elevata qualità di comunicazione, riducendo al minimo la perdita di dati acquisiti o di pacchetti di comunicazione, che si verifica quando viene eseguita la procedura di Vertical HandOver.

Come noto, per trasferimento verticale (Vertical HandOver – VHO) si intende generalmente un trasferimento della connessione tra due reti che usano differenti tecnologie, ad esempio GSM, UMTS, GPRS, 3G, WLAN, etc, permettendo in ogni istante l'utilizzo della connessione migliore secondo criteri specifici, o eventualmente passando da una prima rete che garantisce maggiori prestazioni ad una seconda rete con minori prestazioni, quando per una qualsiasi ragione la prima rete non è disponibile.

Ciò può avvenire perché, con lo sviluppo delle tecnologie di

comunicazione, si è venuto a creare uno scenario in cui sono presenti contemporaneamente reti eterogenee.

Si viene quindi a verificare, sempre più di frequente, la possibilità di connettersi a diverse reti di telecomunicazione disponibili contemporaneamente e nello stesso luogo fisico.

Le varie reti disponibili sono in generale diverse per caratteristiche tecniche, protocolli di riferimento, prestazioni e costi. Pertanto un utente, che utilizzi un dispositivo dotato delle interfacce per collegarsi alle varie reti disponibili, può scegliere la connessione migliore in ogni istante per le sue esigenze.

In questo contesto un singolo Terminale Mobile (MT) può eseguire un trasferimento verticale (VHO) fra un accesso multiplo a diverse delle suddette reti di comunicazione che siano disponibili, ovvero raggiungibili in modalità wireless dal terminale mobile stesso.

Un HandOver verticale (VHO) tra un terminale mobile ed un server può includere, ad esempio, una prima rete di comunicazione ed una seconda rete di comunicazione, in cui sia la prima che la seconda rete di comunicazione è una delle reti di comunicazione supportate secondo la standardizzazione dell'Institute of Electrical and Electronic Engineers (IEEE 802,21) o equivalente.

Una procedura VHO è composta da tre fasi principali: Inizializzazione, Decisione e Esecuzione.

Durante la fase di Inizializzazione, il Terminale Mobile (o network controller) attiva la procedura di VHO, in accordo con le condizioni specifiche della rete di partenza e di quella verso cui si

fa HandOver.

Nella seconda fase di Decisione, l'algoritmo di VHO sceglie il nuovo punto di accesso in accordo con un predefinito insieme di criteri, come ad esempio, il Received Signal Strength Indicator (RSSI), il tempo di connessione, la banda disponibile, il consumo di batteria, il costo economico, la sicurezza della rete e ovviamente le preferenze dell'utente.

Durante la fase finale di Esecuzione, sono portate a termine tutte le operazioni di segnalazione per stabilire la nuova comunicazione e il trasferimento dati.

Il più rilevante sforzo internazionale per la standardizzazione delle procedure di VHO è lo standard IEEE 802.21, che tuttavia si riferisce solo alle prime due fasi (Inizializzazione e Decisione) che sono relativamente indipendenti dalla tecnologia utilizzata, ma ignora la fase di Esecuzione.

Ci sono varie possibili classificazioni degli algoritmi di VHO. In particolare, essi possono essere distinti tra “no-coupling” e “coupling”.

Il primo gruppo è relativo ad uno scenario privo di ogni forma di cooperazione tra i soggetti coinvolti: utenti e operatori. Questa situazione presenta il massimo grado di libertà all'utente, al prezzo di un aumento della complessità di tutta la procedura di HandOver e di un degrado delle prestazioni.

Ovviamente con un livello maggiore di “coupling” sia esso di tipo “loose” o “tight”, sono facilmente raggiunti livelli di

prestazioni più elevati.

Consideriamo lo scenario “no-coupling”, in cui il Vertical HandOver è tipicamente più complicato e meno efficace.

In questa prospettiva si adotta l'approccio “Mobile Terminal-Controlled HandOver” (MCHO), in cui il Terminale Mobile è l'unica entità con un ruolo attivo nella procedura di VHO.

Inoltre, al fine di evitare ogni perdita di connettività durante la fase di Esecuzione del processo di VHO, è necessario adottare un approccio di tipo “make-before-break”. In altre parole, la vecchia connessione viene abbandonata solo dopo che quella nuova e stata stabilita, dando vita così a una fase di esistenza contemporanea delle due connessioni, durante la quale il Terminale Mobile è di fatto temporaneamente un Multi-Homed host.

La gestione di un Multi-Homed host durante la fase di Esecuzione è un problema aperto, senza una soluzione standardizzata e, al momento, ogni Sistema Operativo (OS) ha la propria soluzione.

Descriviamo – con riferimento alla figura 1 allegata – uno degli approcci di tecnica nota più diffusi al VHO, considerando che i limiti che si intendono superare con i miglioramenti che verranno descritti, sono comuni anche agli altri approcci al momento esistenti; le soluzioni proposte nella presente descrizione brevettuale non sono pertanto vincolate all'utilizzo dell'algoritmo descritto.

Allo stesso modo, l'algoritmo descritto, è spiegato in uno scenario di HandOver tra UMTS e WiFi, ma non si intende in alcun modo

vincolare le soluzioni proposte a questi due tipi di connessioni di rete.

Un algoritmo noto (si veda la figura 1) di tipo asimmetrico denominato Low Complexity RSSI-Based VHO di fatto è rappresentativo di un approccio generale al problema in cui l'interfaccia da utilizzare è scelta in base alla potenza di segnale ricevuta o, in generale, alla qualità del segnale, sia esso wireless o di altro tipo.

L'asimmetria dell'algoritmo è dovuta al fatto che generalmente le connessioni Wi-Fi hanno costi inferiori e prestazioni migliori, pertanto è stata assunta una preferenza di base per quel tipo di connessione.

Si descrive ora il funzionamento di questo algoritmo per il VHO, utilizzando il simbolo x per indicare entrambe le interfacce tra cui si intende possa avvenire l'HandOver. L'algoritmo è interamente basato sulla misura del RSSI, in particolare i due valori istantanei sulle diverse interfacce, denominati RSSIx, e il valore RSSIesa, ottenuti attraverso l'applicazione di un filtro definito: Exponential Smoothing Average, che non descriviamo nel dettaglio, essendo noto nella tecnica, ma che viene applicato al fine di contrastare l'effetto ping-pong che consiste nel continuo spostarsi tra le varie connessioni disponibili, senza raggiungere una situazione stabile.

I valori istantanei di RSSI sono paragonati rispetto a due coppie di soglie, chiamate TH^{U}_{x} e TH^{L}_{x}. Le soglie inferiori TH^{L}_{x} sono usate per determinare quando l'RSSI non è sufficiente per garantire

una connessione stabile e sono leggermente più elevate della rispettiva sensibilità dell'interfaccia.

Ovviamente quando si verifica la condizione RSSIx < TH^{L}_{x}, la connessione all'interfaccia x viene disattivata. Invece, le soglie superiori TH^{U}_{x} sono usate per determinare se l'RSSI misurato all'interfaccia di rete, è sufficiente per una connessione stabile; per questa ragione si assume la condizione $TH^{U}_{x} > TH^{L}_{x}$. L'utilizzo di due soglie è in primo luogo una contromisura nei confronti dell'effetto ping-pong.

Il valore filtrato RSSIesa, viene confrontato con un'altra coppia di soglie, chiamate TH^{esa}_{x}.

A differenza del RSSI istantaneo che viene utilizzato per prendere decisioni rapide, quello filtrato, come anticipato, rappresenta una sorta di valore medio, considerato per contrastare l'effetto ping-pong.

Come indicato in Figura 1, il Terminale Mobile (MT) può essere in tre stati definiti dal nome stesso: DISCONNECTED, WiFi CONNECTED, e UMTS CONNECTED.

L'algoritmo può essere compreso, attraverso una descrizione del comportamento nei vari stati possibili del Terminale Mobile.

Mentre è nello stato DISCONNECTED, il Terminale Mobile misura ogni T secondi il livello di RSSI su entrambe le interfacce e il risultato viene indicato come RSSIx con "x" sostituito da U o W a seconda dell'interfaccia considerata (UMTS o WiFi rispettivamente).

Appena un valore di RSSIx supera la relativa soglia superiore,

l'interfaccia x notifica l'evento al gestore del processo di VHO, scatenando l'esecuzione della procedura di Autenticazione, Autorizzazione e Accounting (AAA) per la rete x. Osserviamo che, nel caso di disponibilità di entrambe le reti, la priorità è sempre data al WiFi. Se la procedura AAA nella rete x ha successo, lo stato del Terminale Mobile cambia da DISCONNECTED a CONNECTED.

A causa dell'asimmetria dell'algoritmo, legata alla preferenza della rete WiFi rispetto all'UMTS, i due stati WiFi CONNECTED e UMTS CONNECTED, sono trattati separatamente.

Quando il Terminale Mobile è nello stato UMTS CONNECTED, periodicamente (ogni T secondi) si confronta RSSIu con la soglia inferiore TH^{L}_{U}.

Se si verifica la condizione RSSIu < TH^{L}_{U}, a causa dell'alto rischio di perdere la connessione, il gestore della procedura di HandOver, immediatamente inizia l'autenticazione per connettersi alla rete WiFi, dopo avere verificato la condizione RSSIw > TH^{U}_{W}.

Se questa ultima condizione non è verificata, il gestore del VHO forza la disconnessione alla rete UMTS e il Terminale Mobile raggiunge lo stato di DISCONNECTED. Se il livello di RSSIu rimane superiore a TH^{L}_{U}, il gestore del VHO, ha la possibilità di monitorare la condizione della rete WiFi, in modo da valutare continuamente la possibilità di fare HandOver.

In particolare, l'algoritmo effettua un doppio controllo verificando le condizioni RSSIw > TH^{U}_{W} e RSSIesaw > TH^{esa}_{W}.

Nel caso in cui le due condizioni siano verificate, il gestore

del VHO inizia le procedure di connessione alla rete WiFi, compreso il re-routing del traffico sull'interfaccia WiFi e inizia le procedure di disconnessione dalla rete UMTS. Ovviamente, nel caso che il doppio controllo effettuato dal Terminale Mobile non sia verificato, il Terminale Mobile è forzato a mantenere attiva ala connessione UMTS, restando nello stato UMTS CONNECTED.

Quando il Terminale Mobile è nello stato di WIFI CONNECTED, il comportamento dell'algoritmo di VHO è differente.

Infatti, in questo caso, finché il livello di RSSIw resta superiore a TH^{L}_{U}, il Terminale Mobile resta nella situazione di WIFI CONNECTED, ignorando di fatto l'interfaccia UMTS.

Solo quando la connettività WiFi viene meno (ovvero si verifica la condizione $RSSIw < TH^{L}_{U}$), il gestore del VHO confronta RSSIu con la soglia minima TH^{U}_{U}, in modo da iniziare la procedura di HandOver verso l'UMTS nel caso in cui l'RSSIu sia superiore alla soglia.

Infine, a causa della lunga durata delle procedure di autenticazione (AAA) necessarie per la connessione alla rete WiFi, durante il passaggio da UMTS CONNECTED a WIFI CONNECTED, ci sono alcuni stati transitori, non descritti per semplicità. In particolare si deve considerare la possibilità che la procedura di AAA sulla rete WiFi non abbia successo e si debba pertanto ritornare in uno stato UMTS CONNECTED o DISCONNECTED.

Questo approccio in certi casi è arricchito anche da una valutazione dell'effettivo goodput fornito dalle varie reti disponibili, ovvero dalle prestazioni permesse in termini di bit al

secondo (bit/sec) di informazione.

In generale lo stato dell'arte prevede che queste operazioni di VHO siano gestite attraverso algoritmi, simili a quello descritto, in cui la scelta dell'interfaccia viene effettuata in base a parametri scelti dall'utente, a una valutazione della qualità del segnale e ad una valutazione del goodput, inteso come bit al secondo di informazione resi disponibili dalla connessione.

Gli approcci noti presentano tre tipologie di limiti che sono riconducibili ai seguenti aspetti:

- Trasparenza rispetto alle applicazioni di livello superiore
- Attivazione della connessione e autenticazione dell'utente
- Valutazione delle prestazioni della rete.

Per quanto riguarda la trasparenza della procedura di VHO nei confronti delle applicazioni di livello superiore, il limite consiste nel fatto che gli algoritmi noti di VHO si occupano solo della scelta dell'interfaccia e dell'attivazione della connessione, indicativamente affrontando le problematiche principalmente codificate nei livelli 1 e 2 ISO-OSI normalmente utilizzati per classificare i protocolli di telecomunicazione.

I livelli superiori, fino alle applicazioni che utilizzano la connessione alla rete, di fatto registrano una discontinuità in corrispondenza delle operazioni di VHO e tutte le sessioni dovranno essere ricreate con conseguente discontinuità nel flusso dati verso le applicazioni.

A titolo di esempio possiamo fare riferimento a connessione alla

rete internet. In questo caso l'algoritmo di VHO è in grado di passare da una connessione all'altra minimizzando la discontinuità a livello 1 e 2 ISO-OSI, in quanto il passaggio viene effettuato quando entrambe le connessioni sono attive (make-before-break), ma una volta avvenuto l'HandOver, gli indirizzi IP (livello 3 della rete internet) pubblici assegnati direttamente o indirettamente al Terminale Mobile prima e dopo l'HandOver saranno in generale diversi e le applicazioni dovranno ricreare in generale tutte le connessioni di livello 4 TCP e riavviare eventuali download in corso.

Per quanto riguarda la procedura di attivazione della connessione e autenticazione del Terminale Mobile, il principale limite consiste nel fatto che certe reti prevedono, in questa fase, procedure, che possiamo definire genericamente di autenticazione, finalizzate alla tariffazione o per scopi legali o per applicare a ogni utente un particolare profilo.

I problemi introdotti da queste operazioni, si concretizzano nell'introduzione di ritardi che intaccano notevolmente le prestazioni dell'intera procedura di VHO.

Per quanto riguarda infine la valutazione delle prestazioni, lo scopo è quello di valutare le prestazioni in termini di bitrate (bit/sec) del goodput per decidere a quale rete connettersi, scegliendo quella con bitrate superiore.

Il limite principale è legato al fatto che tale valutazione viene effettuata direttamente scaricando una quantità di dati nota e misurando il tempo impiegato, o scaricando dati per un tempo fisso e

misurando la quantità di dati ricevuta.

Questo download viene effettuato contattando un host remoto. Il limite consiste nel fatto che per effettuare il download è necessario autenticare il Terminale Mobile alla rete prima dell'effettiva procedura di HandOver, ovvero mentre il Terminale Mobile sta ancora facendo traffico attraverso altre connessioni, solo per permettergli di raggiungere il target del Download. La principale conseguenza è che vengono effettuate connessioni, con relativi costi e ritardi (vedere punto precedente), finalizzate soltanto alla raccolta di dati per poi decidere se procedere o no all'HandOver.

Scopo della presente invenzione è quello di superare i succitati inconvenienti, mediante un procedimento per il trasferimento di connessione dati che sia trasparente dal punto di vista delle applicazioni funzionati sul Terminale Mobile.

Ulteriore scopo dell'invenzione è quello di creare un procedimento per il trasferimento di connessione che riduca o elimini la latenza nei trasferimenti di connessione tra diverse interfacce di rete.

Altro scopo dell'invenzione è quello di conseguire il suddetto risultato in modo pratico ed economico.

Detti scopi vengono raggiunti grazie ad un procedimento per il trasferimento verticale di un flusso di dati da un Terminale Mobile ad un terminale remoto tramite un Proxy server, ove il procedimento comprende le seguenti fasi:

- attivazione di una prima connessione tra il Terminale Mobile

ed il Proxy server;

- generazione di un flusso di dati che viene inviato al Proxy server mediante la prima connessione;
- attivazione di una seconda connessione tra il Terminale Mobile ed il Proxy server;
- creazione di un primo pacchetto di fine flusso dati, associato alla prima connessione, e di un pacchetto di inizio flusso dati, associato alla seconda connessione, ove sia il primo pacchetto di fine flusso dati, sia il pacchetto di inizio flusso dati, contengono informazioni necessarie per trasferire il flusso dati dalla prima connessione alla seconda connessione;
- alla ricezione del primo pacchetto di fine flusso dati da parte di un modulo di controllo del Terminale Mobile, inizia l' invio del flusso dati al Proxy server mediante la seconda connessione;
- ricezione del primo pacchetto di fine flusso dati da parte del Proxy server,
- uso delle informazioni contenute nel primo pacchetto di fine flusso dati per iniziare a leggere i dati provenienti dalla seconda connessione;
- alla ricezione del pacchetto di inizio flusso dati da parte del Proxy server, invio al Terminale Mobile di un secondo pacchetto di fine flusso dati attraverso la prima connessione per indicare al Terminale Mobile di interrompere la prima

connessione.

Un vantaggio di questa realizzazione del procedimento dell'invenzione è dato dal fatto che esso consente di trasferire la connessione dati da una prima connessione ad una seconda connessione senza interrompere il funzionamento delle applicazioni presenti sul Terminale Mobile.

Secondo un'altra realizzazione dell'invenzione, il traffico dati sulla prima connessione viene inviato tramite un primo buffer dati in uscita a bordo del Terminale Mobile ed è memorizzato in un primo buffer a bordo del Proxy server ed il traffico dati sulla seconda connessione viene inviato tramite secondo buffer dati in uscita a bordo del Terminale Mobile ed è memorizzato in un secondo buffer a bordo del Proxy server. Il già citato pacchetto di fine flusso è l'ultimo inserito sul buffer relativo alla prima connessione mentre quello di inizio flusso è il primo inserito nel buffer relativo alla seconda connessione.

Un vantaggio di questa realizzazione è dato dal fatto che essa contribuisce a creare un'infrastruttura per mantenere temporaneamente attive due connessioni dati tra il Terminale Mobile ed il Proxy server e dare continuità al flusso generale delle informazioni.

Secondo un'altra realizzazione dell'invenzione, alla ricezione del primo pacchetto di fine flusso dati da parte del modulo di controllo del Terminale Mobile, il modulo di controllo comunica ad un blocco di indirizzamento presente sul Terminale Mobile di spostare il flusso di dati sulla seconda connessione.

Un vantaggio di questa realizzazione è dato dal fatto che essa consente di predisporre l'inizio del trasferimento dati utilizzando la seconda connessione sfruttando un dato che viene trasferito tramite la prima connessione.

Secondo ancora un'altra realizzazione dell'invenzione, alla ricezione del primo pacchetto di fine flusso dati da parte del modulo di controllo del Terminale Mobile, il Terminale Mobile inizia ad inviare i dati estraendoli dal secondo buffer dati in uscita. Il primo pacchetto da inviare è quello di inizio flusso.

Un vantaggio di questa realizzazione è dato dal fatto che essa consente di iniziare il trasferimento dati utilizzando la seconda connessione sfruttando un dato che viene trasferito tramite la prima connessione.

Secondo un'ulteriore realizzazione dell'invenzione, alla ricezione del primo pacchetto di fine flusso dati da parte di un modulo di controllo a bordo del Proxy server, il Proxy server inizia a leggere i dati ricevuti tramite la seconda connessione su un secondo buffer di memoria.

Un vantaggio di questa realizzazione è dato dal fatto che essa consente di iniziare a ricevere dati utilizzando la seconda connessione, sfruttando un dato che viene trasferito tramite la prima connessione.

Secondo un'ulteriore realizzazione dell'invenzione, alla ricezione del primo pacchetto di fine flusso dati da parte di un modulo di controllo a bordo del Proxy server, il Proxy server

comunica ad un blocco di indirizzamento l'indirizzo IP della seconda connessione con il Terminale Mobile.

Un vantaggio di questa realizzazione dell'invenzione è dato dal fatto che essa permette al Proxy server di identificare la sorgente dei dati che vengono trasferiti grazie alla seconda connessione e di indirizzare correttamente il flusso dati in direzione opposta.

Secondo un'ulteriore realizzazione dell'invenzione, nel caso in cui il Proxy server inizi a ricevere i dati trasmessi tramite la seconda connessione mentre la prima connessione è ancora attiva, i dati ricevuti tramite la seconda connessione sono immagazzinati in un secondo buffer a bordo del Proxy server.

Un vantaggio di questa realizzazione dell'invenzione è dato dal fatto che essa consente di ovviare al problema ce si può creare se dovesse accadere che, a causa della diversa latenza dei collegamenti, la seconda connessione inizi a ricevere dati mentre la prima connessione è ancora in uso.

Secondo un'altra realizzazione dell'invenzione, la prima e la seconda connessione sono connessioni di tipo Virtual Private Network (VPN).

Un vantaggio di questa realizzazione dell'invenzione è dato dal fatto che essa consente la creazione di collegamenti tunnel tra il terminale Mobile ed il Proxy server, ovvero collegamenti dedicati al trasferimento dati per la procedura di trasferimento della connessione. In questo modo inoltre si può avere il controllo degli indirizzamenti utilizzati nella comunicazione tra Terminale Mobile e

Proxy in quanto le VPN permettono di utilizzare un indirizzamento di tipo privato che prescinde dagli indirizzi eventualmente assegnati dai provider.

Secondo un'altra realizzazione dell'invenzione, una procedura di eventuale autenticazione viene effettuata successivamente al collegamento alla seconda connessione (VPN B).

Un vantaggio di questa realizzazione dell'invenzione è dato dal fatto che essa, dilazionando la procedura di autenticazione, consente di ridurre i tempi di collegamento tra le varie connessione, aumentando quindi le prestazioni della procedura di trasferimento della connessione.

Secondo un'altra realizzazione dell'invenzione, se la procedura di autenticazione non ha successo il collegamento alla seconda connessione viene interrotto ed il collegamento alla prima connessione viene ripristinato.

Un vantaggio di questa realizzazione dell'invenzione è dato dal fatto che essa consente comunque un controllo sulla correttezza o meno della procedura di autenticazione.

Secondo un'altra realizzazione dell'invenzione, un server remoto mette a disposizione un file raggiungibile senza autenticazione tramite la prima o la seconda connessione, detto file avendo una quantità nota di Bytes, al fine di stimare il goodput della rete misurando il tempo per ricevere una quantità nota di Bytes o i Bytes ricevuti in un intervallo di tempo noto.

Un vantaggio di questa realizzazione dell'invenzione è dato dal

fatto che la stima del goodput non necessita di autenticazione, eliminando i costi e ritardi relativi.

L'invenzione prevede anche un sistema per effettuare un procedimento di trasferimento verticale di un flusso di dati come alle rivendicazioni precedenti, il sistema comprendendo un Terminale Mobile atto ad essere connesso a terminali remoti tramite connessioni di rete, ed un Proxy server sempre connesso ai terminali remoti, ove il suddetto Terminale Mobile ed il Proxy server presentano mezzi per instaurare e mantenere due connessioni reciproche per il trasferimento dati.

Ulteriori caratteristiche e vantaggi dell'invenzione risulteranno evidenti dalla lettura della descrizione seguente fornita a titolo esemplificativo e non limitativo, con l'ausilio delle figure illustrate nelle tavole allegate, in cui:

- la figura 1 è uno schema che illustra l'algoritmo decisionale di una procedura VHO secondo la tecnica nota;

- la figura 2 è uno schema che raffigura i principali componenti impiegati per attuare un procedimento secondo una realizzazione preferita dell'invenzione;

- le figure da 3 a 6 raffigurano alcune fasi dell'interazione tra un terminale mobile e diverse reti di telecomunicazione secondo il procedimento di una realizzazione preferita dell'invenzione;

- le figure da 7 a 10 raffigurano alcune fasi dell'interazione tra un Server Proxy e diverse reti di telecomunicazione secondo il procedimento di una realizzazione preferita dell'invenzione;

– le figure da 11 a 13 illustrano alcune fasi di una seconda realizzazione preferita dell'invenzione, e

– la figura 14 illustra un'ulteriore realizzazione preferita dell'invenzione.

Dalle menzionate figure si rileva un Proxy server 20 raggiungibile via rete internet 30 da parte di un Terminale Mobile (MT) 10.

Più in particolare, il Terminale Mobile (MT) 10 presenta due interfacce 10A, 10B per il collegamento a due rispettive Virtual Private Networks VPN A e VPN B, eventualmente tramite i Provider 40,50, come meglio illustrato nel seguito e che possono instaurare collegamenti VPN tra Proxy server 20 e Terminale Mobile 10.

Il Terminale Mobile (MT) 10 presenta un primo modulo software 12 ed il Proxy server 20 un secondo modulo software 22, ove entrambi i moduli 12, 22 possono avvalersi di buffer di memoria.

Sul Terminale Mobile (MT) 10 sono attive alcune applicazioni 14 le quali accedono a dati su terminali remoti. L'accesso a questi dati avviene attraverso una connessione di rete. Il Terminale Mobile 10 ha più possibilità di connettersi alla rete, rappresentate da diverse interfacce 10A,10B.

In generale, nel procedimento descritto il Proxy server 20 contatterà le sorgenti dei flussi dati per le applicazioni 14 del Terminale Mobile 10, svolgendo un ruolo sostanzialmente di tramite, tra queste e il Terminale Mobile 10.

In questo modo le connessioni con le sorgenti dei dati non

vengono cambiate dalla procedura di Vertical HandOver (VHO) che investe solamente le connessioni tra il Terminale Mobile 10 ed il Proxy server 20; di conseguenza, le connessioni aperte presso le sorgenti dei dati non dovranno essere ripristinate, ma potranno continuare ad esistere inalterate dal processo di VHO.

Il Terminale Mobile 10 è collegato al Proxy server 20 utilizzando le interfacce di rete coinvolte nel processo di VHO, ma tra i due host viene implementata una VPN per ogni interfaccia coinvolta. In questo modo tra Terminale Mobile 10 e Proxy server 20 si instaurano dei tunnel che permettono di fare traffico tra interfacce virtuali, una presso il Proxy server 20, l'altra presso il Terminale Mobile 10, che avranno un indirizzamento IP indipendente da quello della connessione fisica attiva. Questo collegamento deve essere attivo a prescindere dall'esito di eventuali processi di autenticazione.

Resta da affrontare il problema della continuità del flusso dati evitando trasmissioni doppie o parti mancanti; questo aspetto è preso in carico dai moduli software denominati 12 e 22, rispettivamente a bordo del Terminale Mobile 10 e del Proxy server 20.

Entrambi i moduli 12 e 22 controllano il flusso di dati, lato Proxy 20 e Terminale Mobile 10, avvalendosi ciascuno di due buffer di memoria, in generale uno per ogni connessione attiva in uscita ed in ingresso.

In particolare il modulo 12 del terminale Mobile 10 presenta un primo buffer di uscita 13 (Buffer-OUT 1) ed un secondo buffer di

uscita 15 (Buffer-OUT 2) ed un buffer in entrata 17 (Buffer-IN).

Il modulo 22 del Proxy server 20 presenta un primo Buffer VNP 23 ed un secondo Buffer VPN 25.

Grazie all'approccio “make before break” esiste una fase durante il processo di VHO in cui entrambe le connessioni sono attive con i relativi tunnel VPN, mentre il flusso dati è agganciato ancora alla prima connessione, quella che si sta per abbandonare.

Una realizzazione preferita del procedimento dell’invenzione prevede le fasi descritte nel seguito.

La situazione di partenza, illustrata in Figura 2, mostra un’unica connessione attiva attraverso l’interfaccia 10A.

Il traffico generato dalle applicazioni 14 utilizza un primo buffer di uscita 13 (Buffer-OUT 1) a bordo del Terminale Mobile 10 prima di esser incapsulato nel tunnel VPN A.

Il tunnel VPN A si chiude sul Proxy server 20 dove il traffico appare generato con l’indirizzo della interfaccia virtuale della VPN attivata sull’interfaccia 10A del Terminale Mobile 10 ed arriva, tramite un modulo VPN 28, al primo Buffer VPN 23.

Il traffico viene quindi inoltrato sulla rete 30 con l’indirizzo sorgente di un’interfaccia Wide Area Network (WAN) 26 del Proxy server 20.

A questo punto (Figura 3) viene attivata una seconda VPN, denominata nel seguito VPN B, sulla seconda interfaccia disponibile 10B, ovvero quella su cui sta avvenendo il Vertical HandOver.

Vengono quindi portate a termine tutte le procedure di

associazione e autenticazione necessarie ed una nuova VPN è quindi creata attraverso l'interfaccia 10B. A questo punto un Client VPN 116 a bordo del Terminale Mobile 10 comunica ad un primo Buffer Controller 16 che è disponibile la seconda connessione.

Una volta che il Terminale Mobile 10 ha ricevuto conferma che la VPN B è utilizzabile, viene creato un pacchetto dati di Fine Flusso (FF) 49 e viene inviato al primo buffer in uscita 13 (Buffer-OUT 1) associato alla connessione VPN A ed un pacchetto dati di Inizio Flusso (IF) 41 è inviato ad un secondo buffer in uscita 15 (Buffer-OUT 2) associato alla connessione VPN B (Figura 4).

Sia il pacchetto di Fine Flusso (FF) 49, sia il pacchetto di Inizio Flusso (IF) 41, contengono le informazioni necessarie per identificare la connessione che si sta abbandonando, sia quella che si sta per utilizzare a beneficio del Proxy server 20.

In particolare, il pacchetto di Fine Flusso (FF) 49 ed il pacchetto di Inizio Flusso (IF) 41 contengono al loro interno tutte le informazioni sulle connessione A e B e le relative VPN A e VPN B e tutti i dati che posso servire al Proxy server 20 per associare le due VPN allo stesso Terminale Mobile 10.

Da quel momento il Terminale Mobile 10 inizia ad inviare i pacchetti dati in uscita al secondo buffer in uscita 15 (Buffer-OUT 2) associato alla connessione VPN B.

Come illustrato in Figura 5, da quando il pacchetto di Fine Flusso 49 arriva ad un modulo di controllo 114 del Terminale Mobile 10, il modulo di controllo 114 comunica ad un blocco di

indirizzamento 112 presente sul Terminale Mobile 10 di portare il flusso di dati sulla nuova VPN B disponibile.

Il modulo di controllo 114 comunica anche ad un secondo Buffer Controller 18 di iniziare a leggere i dati in uscita dal secondo buffer in uscita 15 (Buffer-OUT 2).

Quindi quando il pacchetto di Fine Flusso 49 arriva allo stadio di uscita dal Terminale Mobile 10, questo evento origina il passaggio alla lettura del buffer in uscita 15 (Buffer-OUT 2) del terminale Mobile (10) associato alla connessione VPN B e l'invio dei dati estratti sulla connessione B attraverso la VPN B partendo dal pacchetto di Inizio Flusso 41.

Nel frattempo il Proxy server ha attive le due VPN A e B associate ai relativi buffer.

Il flusso dati inizia ad utilizzare la VPN B e la VPN A può essere terminata (in 48) in seguito alla ricezione del pacchetto di Fine Flusso 59 (Figura 6) generato dal Proxy a titolo di conferma.

Quando il Proxy 20 riceve attraverso la VPN A il pacchetto di Fine Flusso 49, ne estrae tutte le informazioni per associare i flussi dati provenienti dal VPN A e la VPN B come originati dallo stesso Terminale Mobile 10.

Ciò comprende anche la gestione dei diversi indirizzi associati alla due diverse VPN attivate dal Terminale Mobile.

Come conseguenza delle informazioni ricevute, il Proxy 20 si mette in ascolto sul buffer associato alla connessione B in attesa del pacchetto di Inizio Flusso 41.

Quando viene creata la seconda VPN B, nonostante il Terminale Mobile 10 indirizzi il flusso dati sempre solo su una delle due VPN, a causa della latenza dei collegamenti, è possibile che la VPN B inizi a ricevere dati mentre anche la VPN A è ancora in uso.

In questo caso i dati ricevuti dalla VPN B sono immagazzinati in un secondo Buffer VPN 25 del Proxy 20. Quando viene ricevuto il pacchetto di Inizio Flusso 41, i dati di servizio relativi alle connessione da questo portati sono inviati ad un modulo di controllo 214 del Proxy 20 (Figura 7).

Quando sulla VPN A si esaurisce il flusso di dati viene ricevuto il pacchetto di Fine Flusso 49 generato dal Terminale Mobile 10 (Figura 8).

Quando viene ricevuto dal modulo di controllo 214 del Proxy 20 il pacchetto di Fine Flusso 49 generato dal Terminale Mobile 10 hanno origine i seguenti eventi, illustrati in Figura 9.

In primo luogo il modulo di controllo 214 del Proxy 20 comunica ad Buffer Controller 27 del Proxy 20 di iniziare a leggere i dati ricevuti dalla VPN B immagazzinati nel secondo Buffer VPN 25 del Proxy 20.

Inoltre viene comunicato ad un blocco di indirizzamento 212 del Proxy 20 che, da quel momento, il Terminale Mobile 10 remoto è raggiungibile attraverso l'indirizzo associato alla VPN B.

Infine, al momento in cui viene processato dal modulo di controllo 214 del Proxy 20 il pacchetto di Inizio Flusso 41 estratto dal Buffer VPN 25, viene inviato al terminale Mobile 10, attraverso

la VPN A, un pacchetto di Fine Flusso 59, generato dal Proxy 20; che conferma la possibilità di abbattere la VPN A.

A procedura ultimata, il traffico dati utilizza la VPN B associata alla nuova connessione (Figura 10).

Per dare continuità nel passaggio da un flusso all'altro il Terminale Mobile 10 ed il Proxy 20 utilizzano i pacchetti di Fine Flusso 49,59 ed il pacchetto di Inizio Flusso 41 per avvisarsi reciprocamente del fatto che termina l'utilizzo di quella VPN per l'invio dei dati e che si inizia ad utilizzare la VPN nuova.

Il collegamento tra il Proxy 20 e gli host remoti resta inalterato per tutto il tempo.

Viene quindi raggiunto l'obiettivo di cambiare l'interfaccia di connessione alla rete (processo di VHO) in modo del tutto trasparente dal punto di vista delle applicazioni.

Secondo un ulteriore realizzazione della presente invenzione è possibile ridurre la latenza introdotta dall'autenticazione durante la procedura di HandOver.

L'idea di base è quella di invertire la logica dell'autenticazione, ovvero in questo caso al Terminale Mobile 10 viene permesso l'accesso alla rete 30 (es: internet) immediatamente al momento della connessione, senza attendere l'esito dell'autenticazione (Figura 11), per poi eventualmente bloccarlo nel caso in cui il processo di autenticazione, svolto in background, non abbia successo, il tutto differisce dal normale modo di procedere, secondo cui il Terminale Mobile 10 non può raggiungere internet se

prima non è stato autenticato.

La sequenza degli eventi, pertanto è la seguente.

L'algoritmo decide di effettuare l' HandOver dalla rete alla quale è collegato tramite la connessione 55 con il Provider A, alla rete mediante il provider B in base ai dati in suo possesso.

Non appena viene stabilita la connessione 45 per collegarsi alla rete 30 tramite il provider B, ovvero indicativamente sono state svolte le funzionalità di livello ISO-OSI 1, 2 e 3, il gestore del VHO immediatamente inizia a usare questa nuova connessione per fare traffico, sfruttandone a pieno i servizi, senza attendere l'autenticazione. In questo modo si accelerano notevolmente i tempi dell'HandOver e la connessione 55 può essere immediatamente rilasciata con risparmio di risorse ed eventualmente di costi.

Mentre l'utente continua ad usufruire della connessione 45 alla rete 30, contemporaneamente il processo di autenticazione ha luogo.

Quando l'esito dell'autenticazione è disponibile, in base al fatto che abbia avuto o no successo, l'utente potrà rispettivamente: continuare ad essere collegato alla rete B o sarà disconnesso.

Eventualmente prima della disconnessione dalla rete B, il gestore del VHO può ripristinare il collegamento con la rete A.

Secondo ancora un’altra realizzazione della presente invenzione, è previsto un procedimento per la stima del goodput.

In un contesto in cui l'algoritmo sta valutando la possibilità di fare HandOver dalla rete A alla rete B, con la rete B che richiede l'autenticazione del Terminale Mobile.

Il provider di servizi di connettività di una delle reti coinvolte nel processo di VHO, mette a disposizione un file 100 ospitato su un host remoto (fig.14) 70, che definiamo Target, raggiungibile utilizzando la rete denominata in precedenza, ovvero la rete B. Gli apparati attraverso cui viene fornito il servizio di connettività alla rete B, con l'autorizzazione dello stesso provider, devono permettere l'accesso al file Target 100 senza autenticazione.

In questo modo il software che gestisce il VHO potrà realizzare la stima del goodput, semplicemente facendo il download del file Target 100 e misurando o il tempo per ricevere una quantità nota di Bytes, o i Bytes ricevuti in un intervallo di tempo noto. Seguendo questa procedura, è possibile effettuare una stima del goodput senza effettuare l'autenticazione, limitando così la latenza introdotta da questa operazione e evitando che gli utenti con profili a scalare consumino del tempo di connessione per questa operazione di servizio.

In questa descrizione si è fatto riferimento generico a reti denominate A e B, in quanto la stessa procedura è applicabile a qualsiasi scenario che preveda l'autenticazione del Terminale Mobile 10, anche se il caso più tipico è quello in cui le connessioni A e B sono di fatto connessioni ad internet e l'host Target è a sua volta un server raggiungibile attraverso internet.

Ovviamente all’invenzione così come descritta potranno essere apportate modifiche o migliorie dettate da motivazioni contingenti o particolari, senza per questo uscire dall’ambito dell’invenzione come sotto rivendicata.

RIVENDICAZIONI

1. Procedimento per il trasferimento verticale di un flusso di dati da un Terminale Mobile (10) ad un terminale remoto tramite un Proxy server (20), ove il procedimento comprende le seguenti fasi:

- attivazione di una prima connessione (VPN A) tra il Terminale Mobile (10) ed il Proxy server (20);
- generazione di un flusso di dati che viene inviato al Proxy server (20) mediante la prima connessione (VPN A);
- attivazione di una seconda connessione (VPN B) tra il Terminale Mobile (10) ed il Proxy server (20);
- creazione di un primo pacchetto di fine flusso dati (49), associato alla prima connessione (VPN A), e di un pacchetto di inizio flusso dati (41), associato alla seconda connessione (VPN B), ove sia il primo pacchetto di fine flusso dati (49), sia il pacchetto di inizio flusso dati (41), contengono informazioni necessarie per trasferire il flusso dati dalla prima connessione (VPN A) alla seconda connessione (VPN B);
- alla ricezione del primo pacchetto di fine flusso dati (49) da parte di un modulo di controllo (114) del Terminale Mobile (10), iniziare l'invio del flusso dati al Proxy server (20) mediante la seconda connessione (VPN B);
- ricezione del primo pacchetto di fine flusso dati (49) da parte del Proxy server (20),
- uso delle informazioni contenute nel primo pacchetto di fine

flusso dati (49) per iniziare a leggere i dati provenienti dalla seconda connessione (VPN B);

- alla ricezione del pacchetto di inizio flusso dati (41) da parte del Proxy server (20), invio al Terminale Mobile (10) di un secondo pacchetto di fine flusso dati (59) per indicare al Terminale Mobile (10) di interrompere la prima connessione (VPN A).

2. Procedimento come alla rivendicazione 1, in cui il flusso dati sulla prima connessione (VPN A) viene inviato tramite un primo buffer dati in uscita (13) a bordo del Terminale Mobile (10) ed è memorizzato in un primo buffer VPN (23) a bordo del Proxy server (20) ed il flusso dati sulla seconda connessione (VPN B) viene inviato tramite un secondo buffer dati in uscita (15) a bordo del Terminale Mobile (10) ed è memorizzato in un secondo buffer VPN (25) a bordo del Proxy server (20).

3. Procedimento come alla rivendicazione 1, in cui alla ricezione del primo pacchetto di fine flusso dati (49) da parte del modulo di controllo (114) del Terminale Mobile (10), il modulo di controllo (114) comunica ad un blocco di indirizzamento (112) presente sul Terminale Mobile (10) di spostare il flusso di dati sulla seconda connessione (VPN B).

4. Procedimento come alla rivendicazione 2, in cui alla ricezione del primo pacchetto di fine flusso dati (49) da parte del modulo di controllo (114) del Terminale Mobile (10), il Terminale Mobile (10) inizia ad inviare i dati tramite il secondo buffer dati in uscita

(15).

5. Procedimento come alla rivendicazione 2, in cui alla ricezione del primo pacchetto di fine flusso dati (49) da parte di un modulo di controllo (214) a bordo del Proxy server (20), il Proxy server (20) inizia a leggere i dati ricevuti tramite la seconda connessione (VPN B) sul secondo buffer di memoria (25).

6. Procedimento come alla rivendicazione 2, in cui alla ricezione del primo pacchetto di fine flusso dati (49) da parte di un modulo di controllo (214) a bordo del Proxy server (20), il Proxy server (20) comunica ad un blocco di indirizzamento (212) l'indirizzo IP della seconda connessione (VPN B) con il Terminale Mobile (10).

7. Procedimento come alla rivendicazione 2, ove nel caso in cui il Proxy server (20) inizi a ricevere i dati trasmessi tramite la seconda connessione (VPN B) mentre la prima connessione (VPN A) è ancora attiva, i dati ricevuti tramite la seconda connessione (VPN B) sono immagazzinati nel secondo buffer (25) a bordo del Proxy server (20).

8. Procedimento come alla rivendicazione 1, in cui la prima e la seconda connessione (VPN A,VPN B) sono connessioni di tipo Virtual Private Network (VPN).

9. Procedimento come alle rivendicazioni precedenti, in cui una procedura di autenticazione viene effettuata successivamente al collegamento alla seconda connessione (VPN B).

10. Procedimento come alla rivendicazione 9, in cui se la procedura di autenticazione non ha successo il collegamento alla seconda

connessione (VPN B) viene interrotto ed il collegamento alla prima connessione (VPN A) viene ripristinato.

11. Procedimento come alle rivendicazioni precedenti, in cui un server remoto mette a disposizione un file (100) raggiungibile senza autenticazione tramite la prima o la seconda connessione (VPN A,VPN B), detto file avendo una quantità nota di Bytes, al fine di stimare il goodput della rete misurando il tempo necessario per ricevere una quantità nota di Bytes o i Bytes ricevuti in un intervallo di tempo prefissato.

12. Sistema per effettuare un procedimento di trasferimento verticale di un flusso di dati come alle rivendicazioni precedenti, il sistema comprendendo un Terminale Mobile (10) atto ad essere connesso a terminali remoti tramite connessioni di rete, ed un Proxy server (20) sempre connesso ai terminali remoti, ove il suddetto Terminale Mobile (10) ed il Proxy server (20) presentano mezzi per instaurare e mantenere due connessioni reciproche per il trasferimento dati.

Tecnica Nota

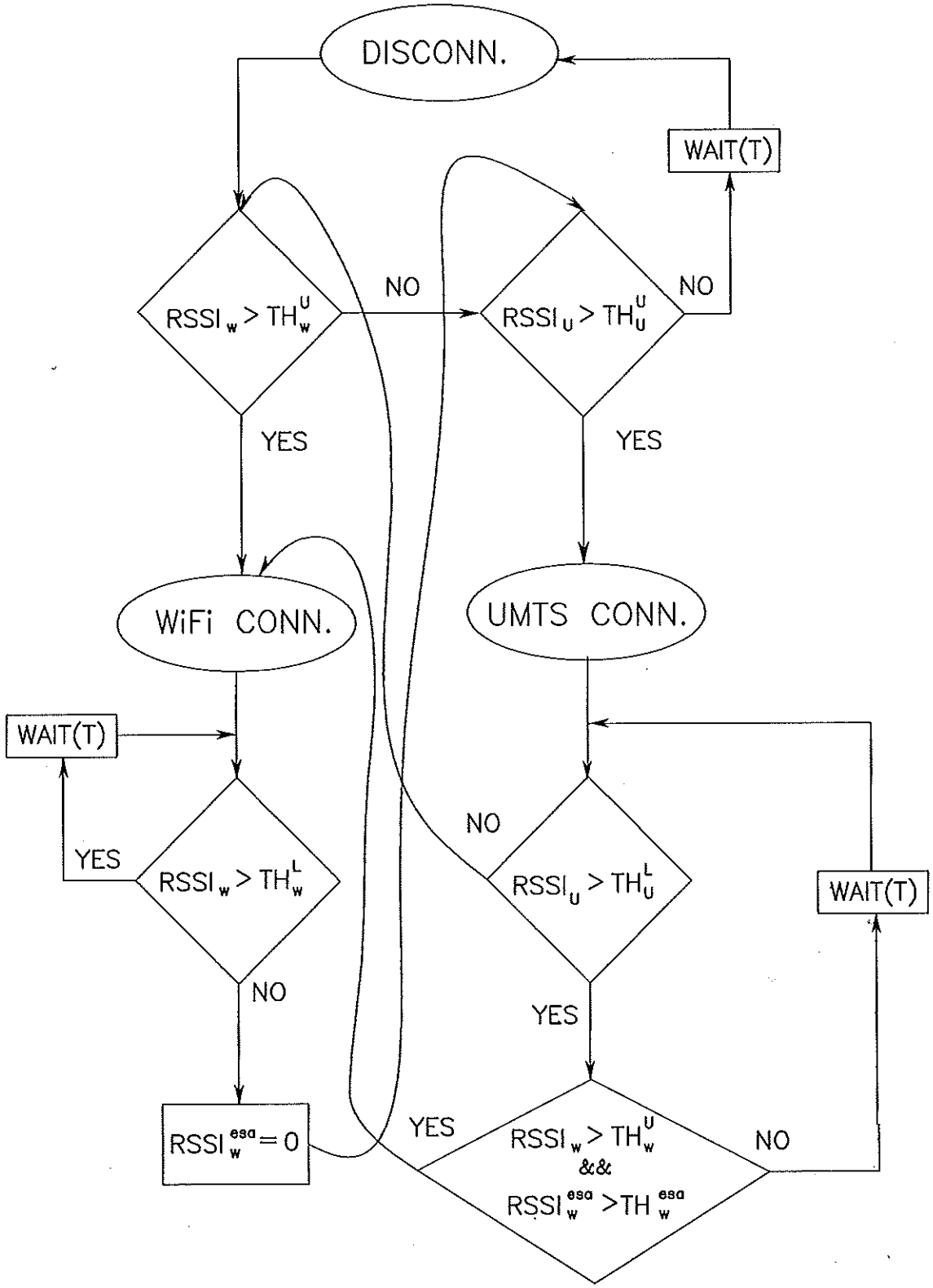

FIG.1

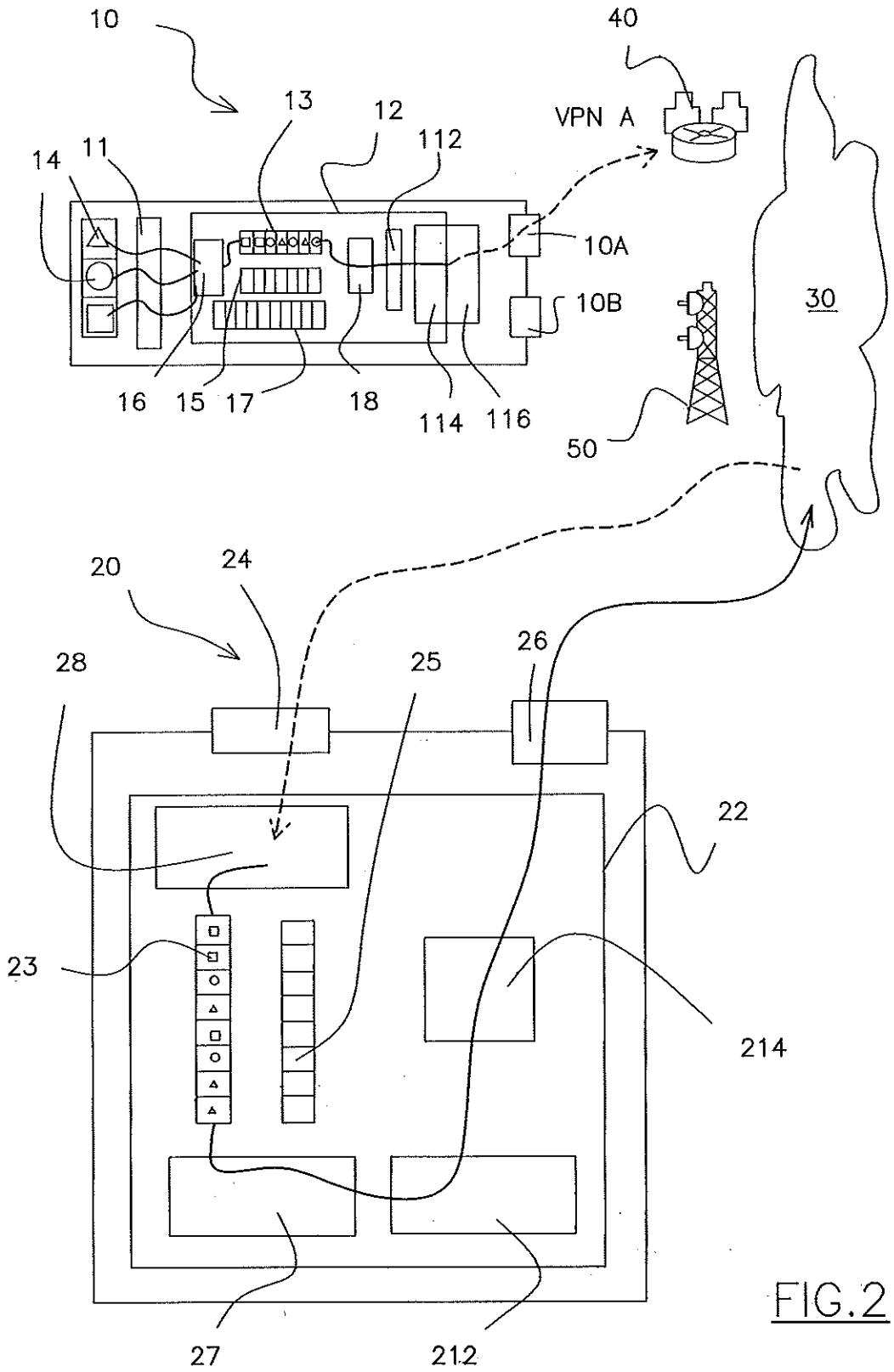
10
13
12
112
40
VPN A
14
11
10A
10B
30
16
15
17
18
114
116
50
20
24
26
28
25
22
23
214
27
212

FIG.2

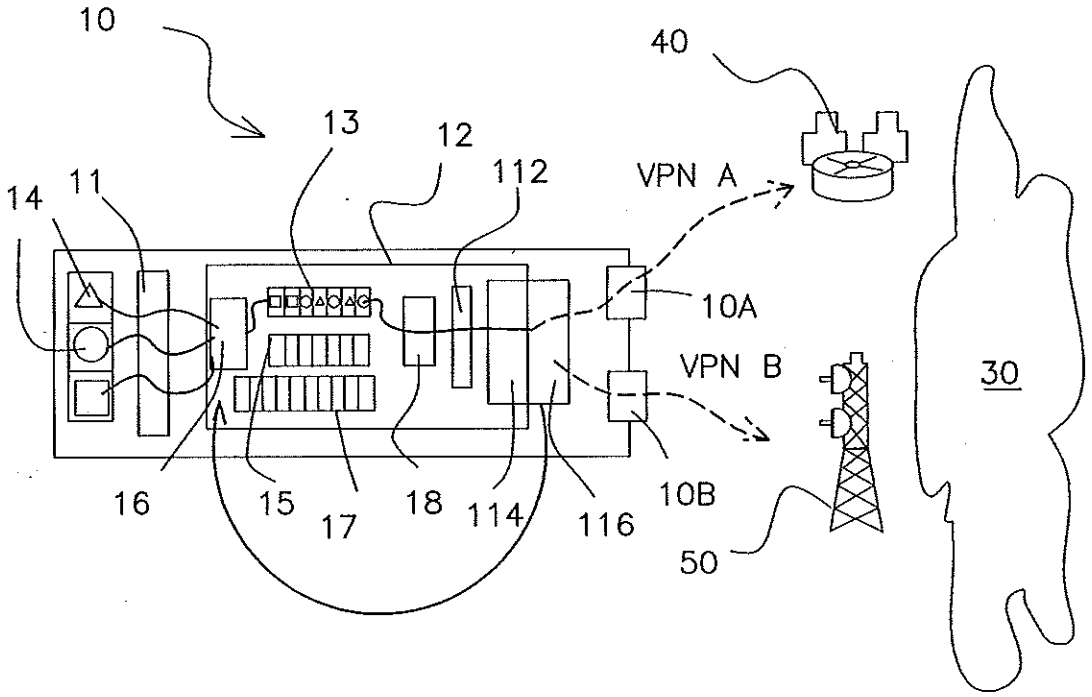
10
40
13
12
112
VPN A
14
11
10A
VPN B
30
16
15
17
18
114
116
10B
50

FIG.3

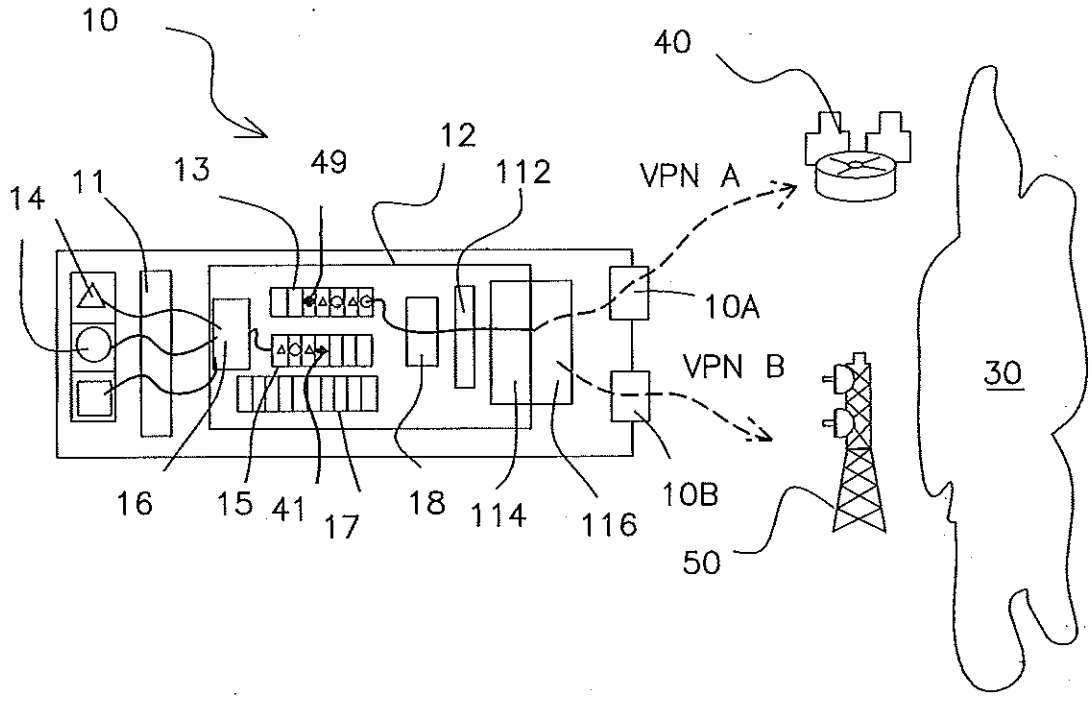
10
40
12
13
49
112
VPN A
14
11
10A
VPN B
30
16
15
41
17
18
114
116
10B
50

FIG.4

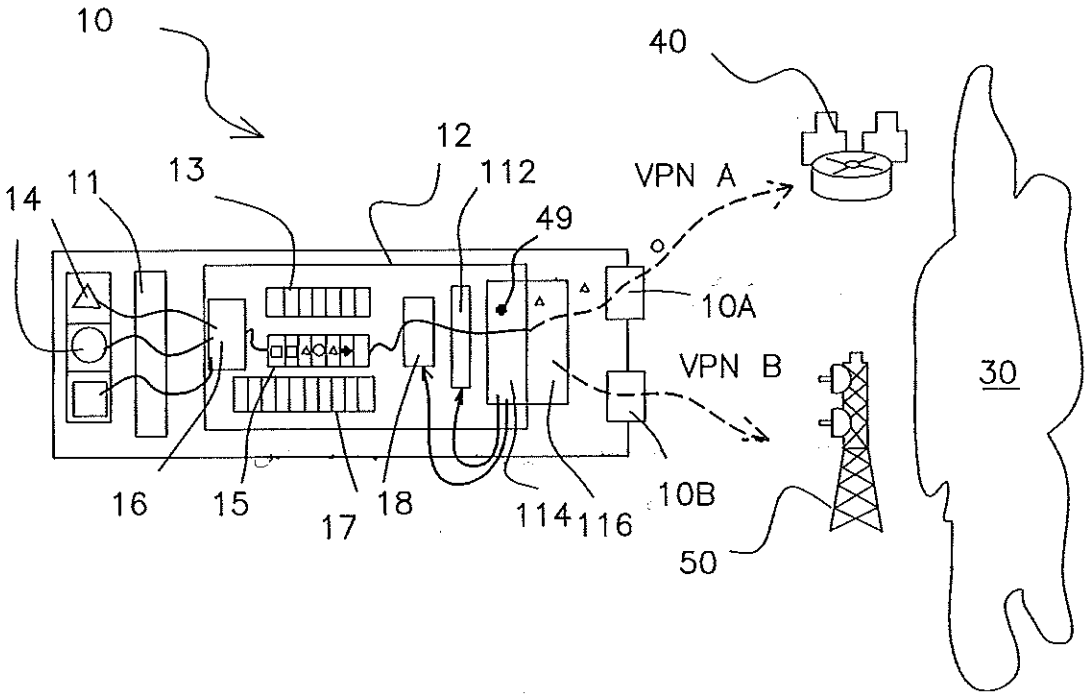
10
40
12
13
112
VPN A
14
11
49
10A
VPN B
30
16
15
17
18
114
116
10B
50

FIG.5

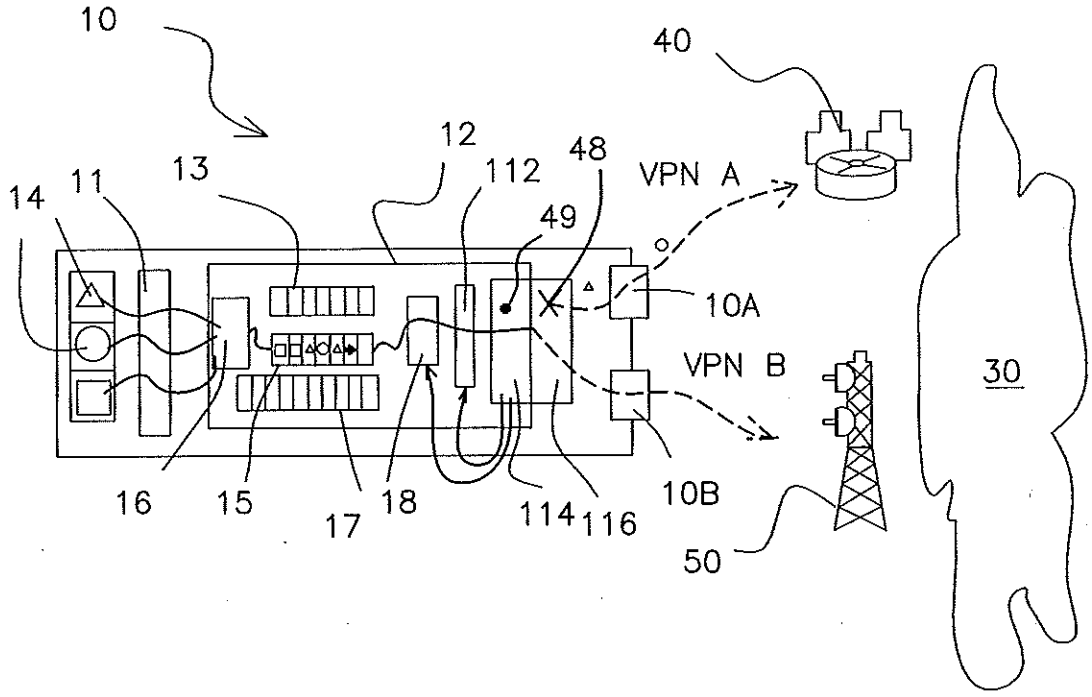
10
40
12
48
13
112
VPN A
14
11
49
10A
VPN B
30
16
15
17
18
114
116
10B
50

FIG.6

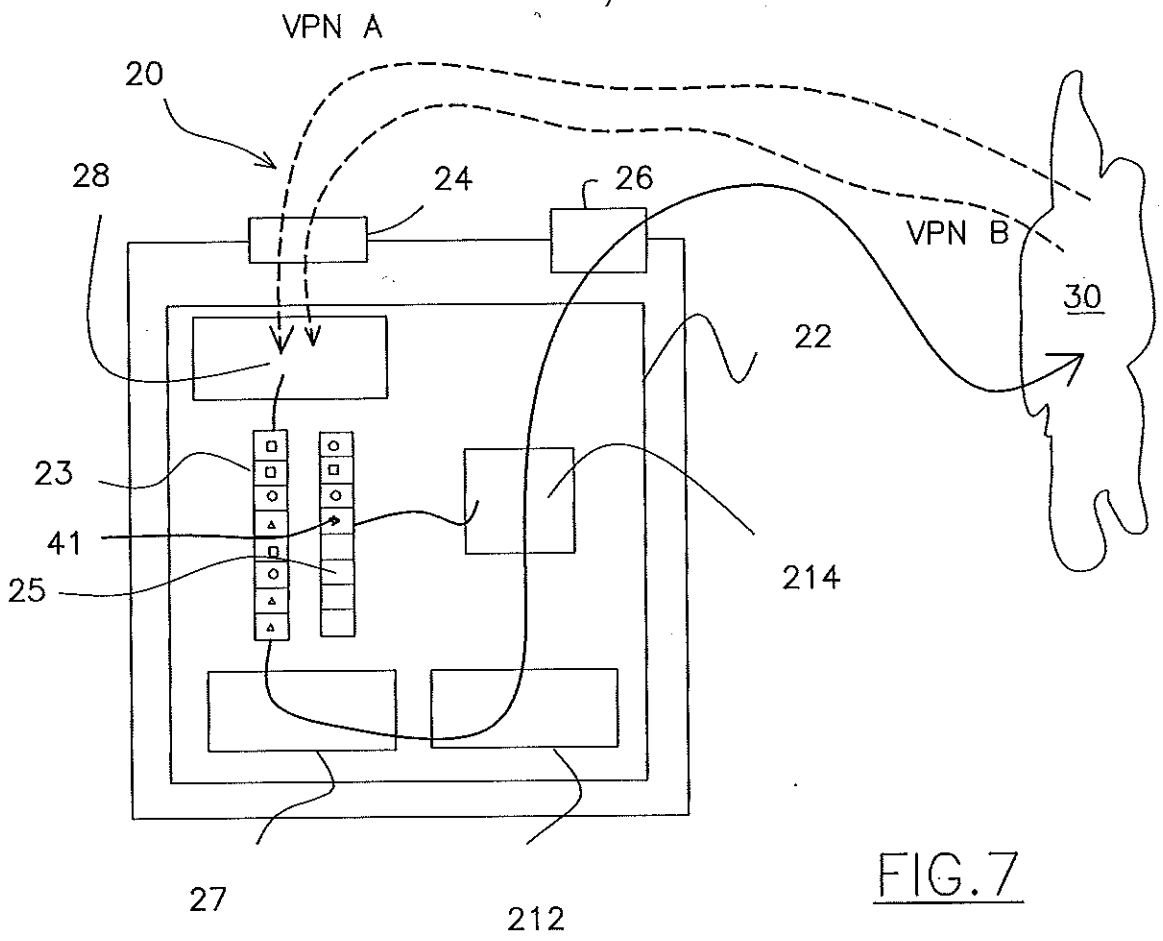
VPN A
20
28
24
26
VPN B
30
22
23
41
25
214
27
212

FIG.7

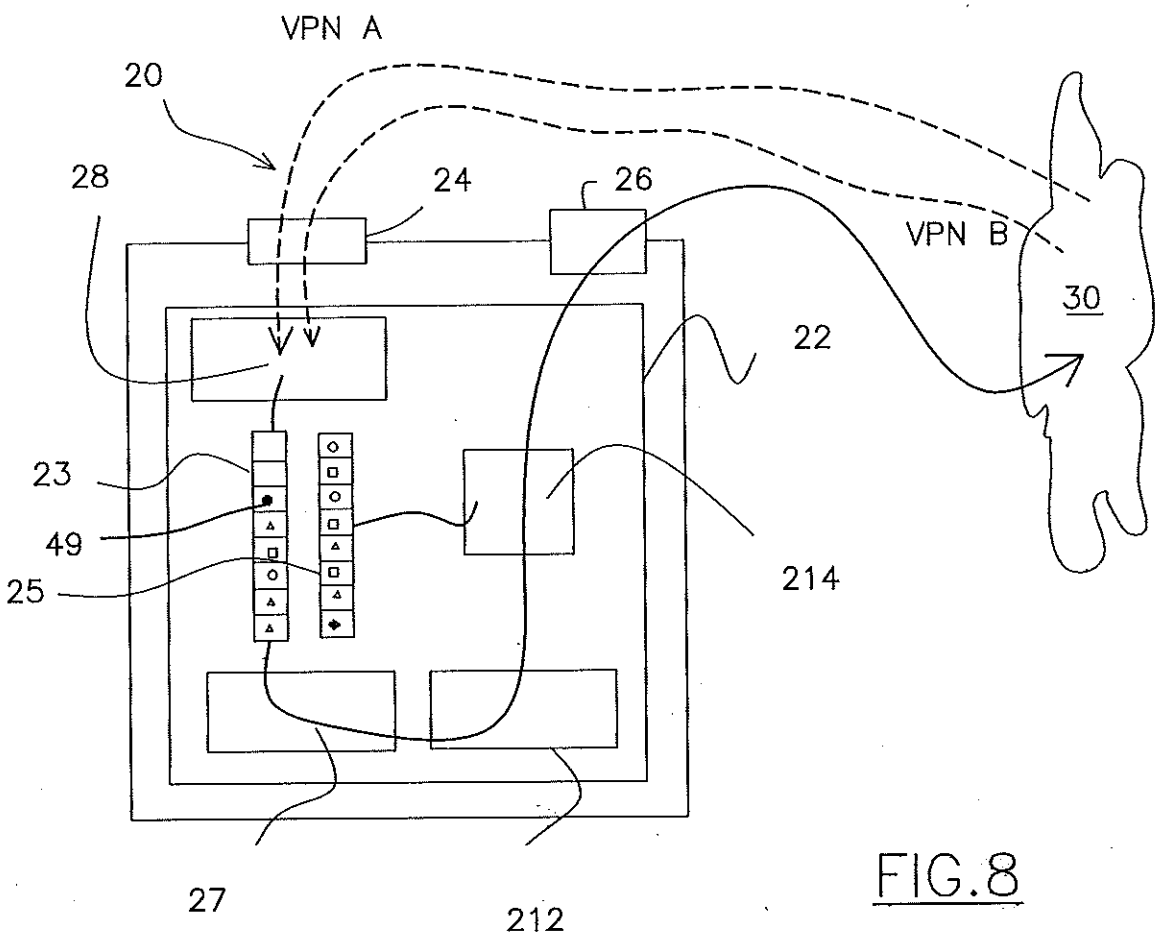
VPN A
20
28
24
26
VPN B
30
22
23
49
25
214
27
212

FIG.8

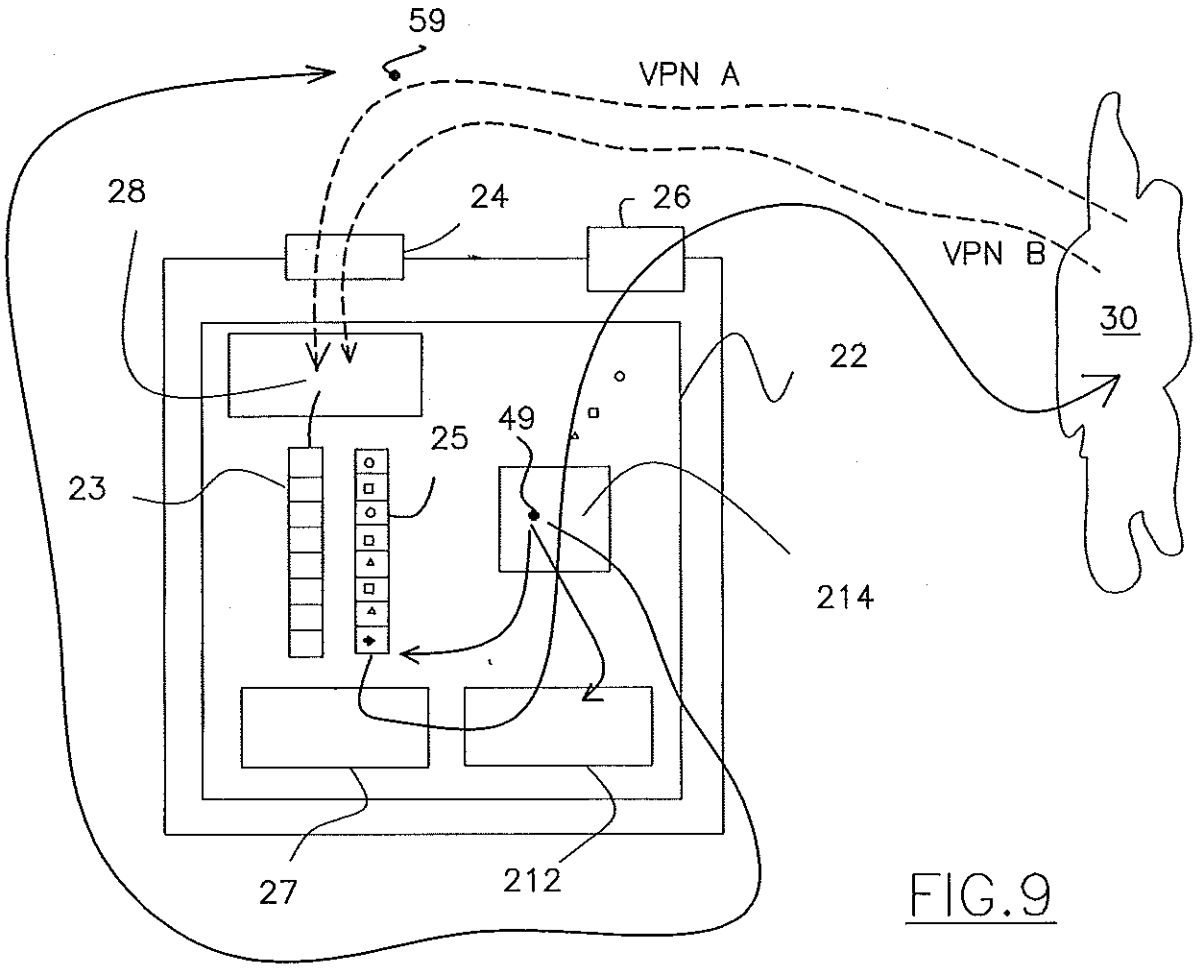
59
VPN A
28
24
26
VPN B
30
22
49
25
23
214
27
212

FIG.9

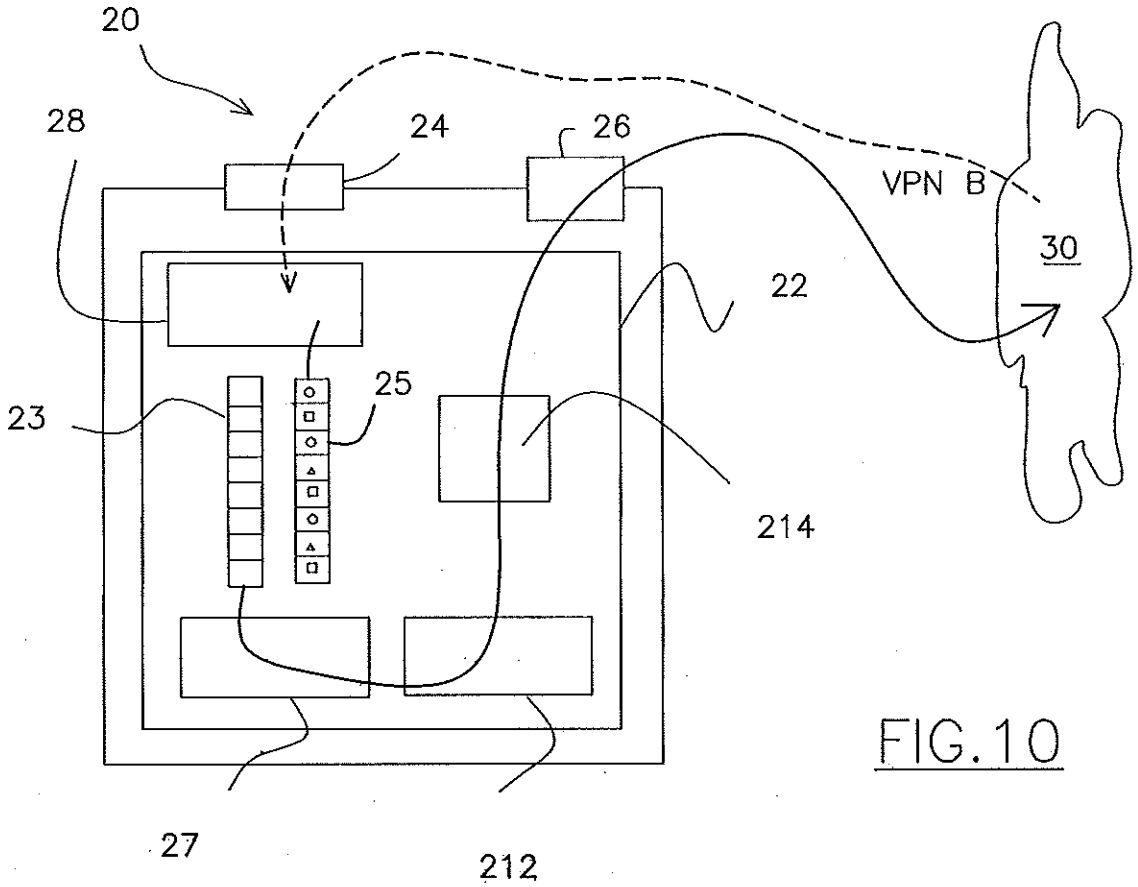
20
28
24
26
VPN B
30
22
25
23
214
27
212

FIG.10

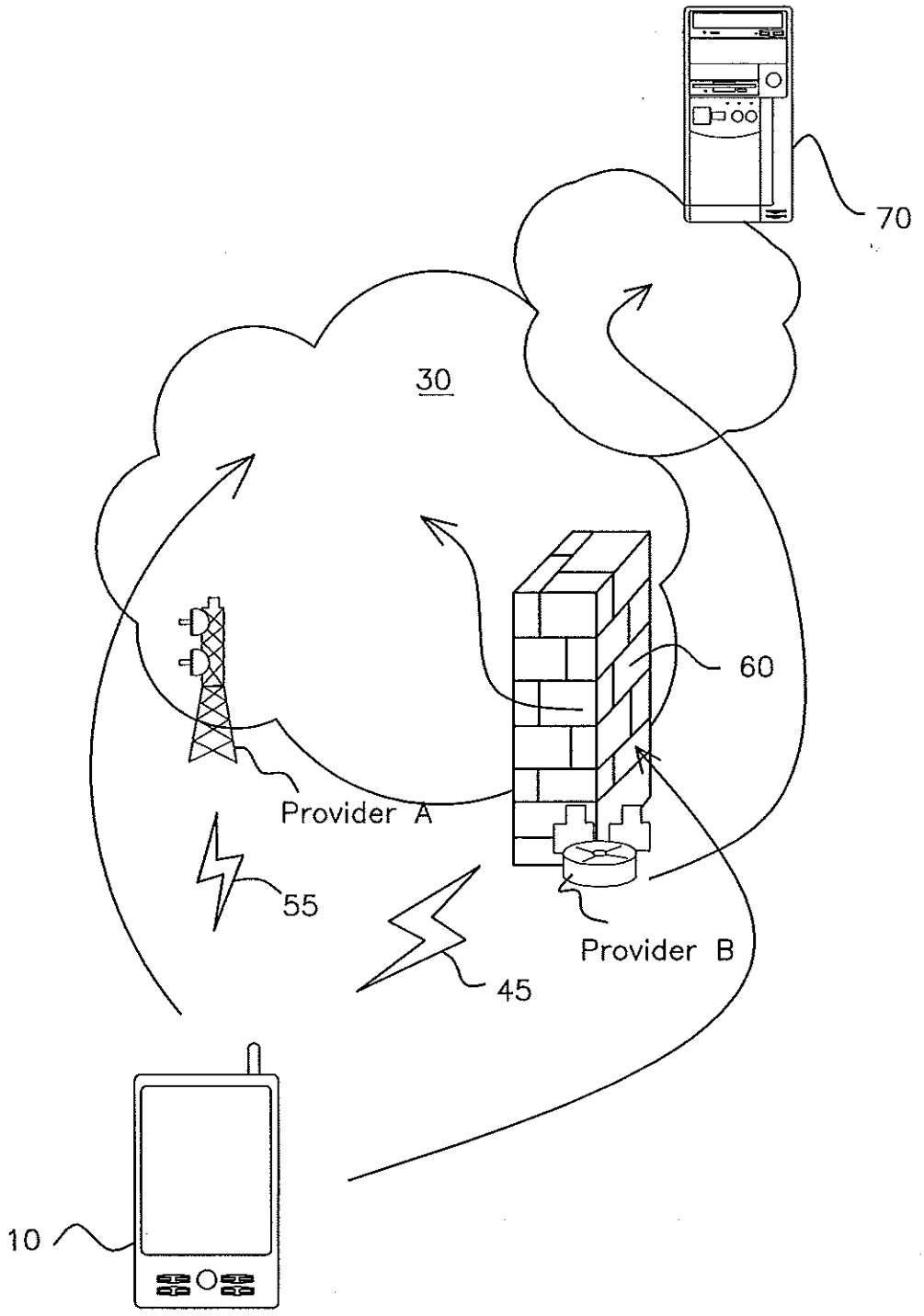

FIG. 11

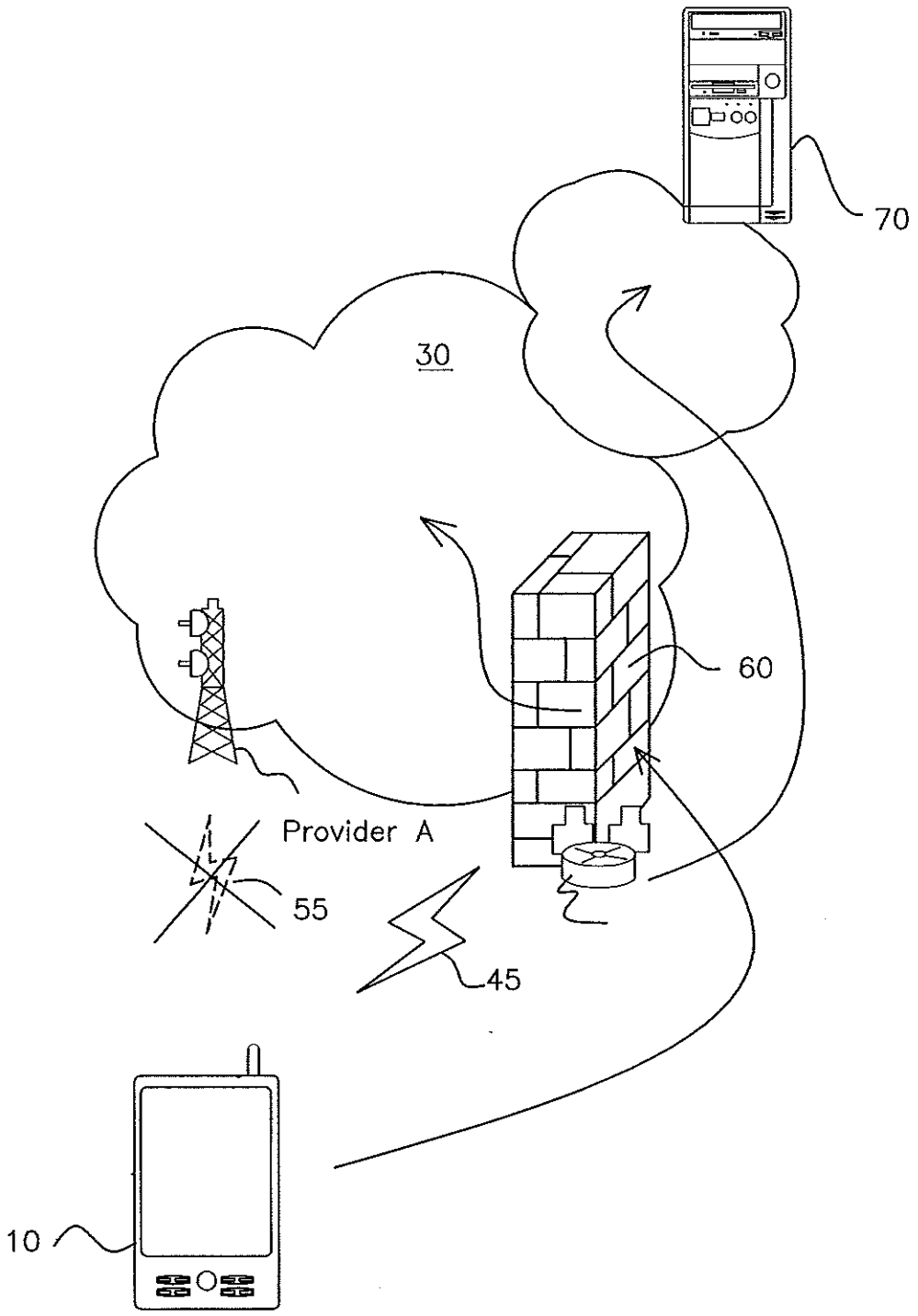

FIG.12

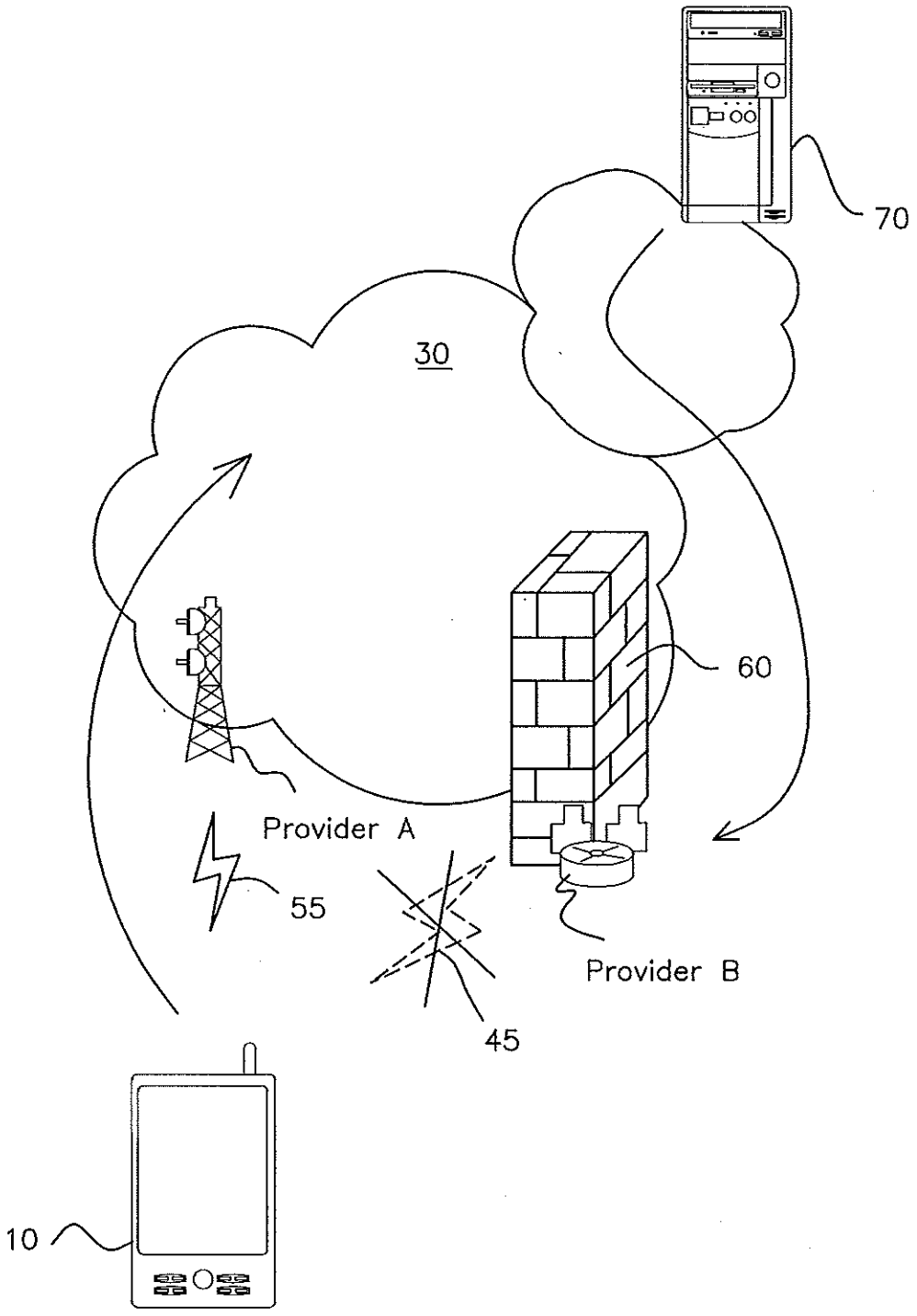

FIG.13

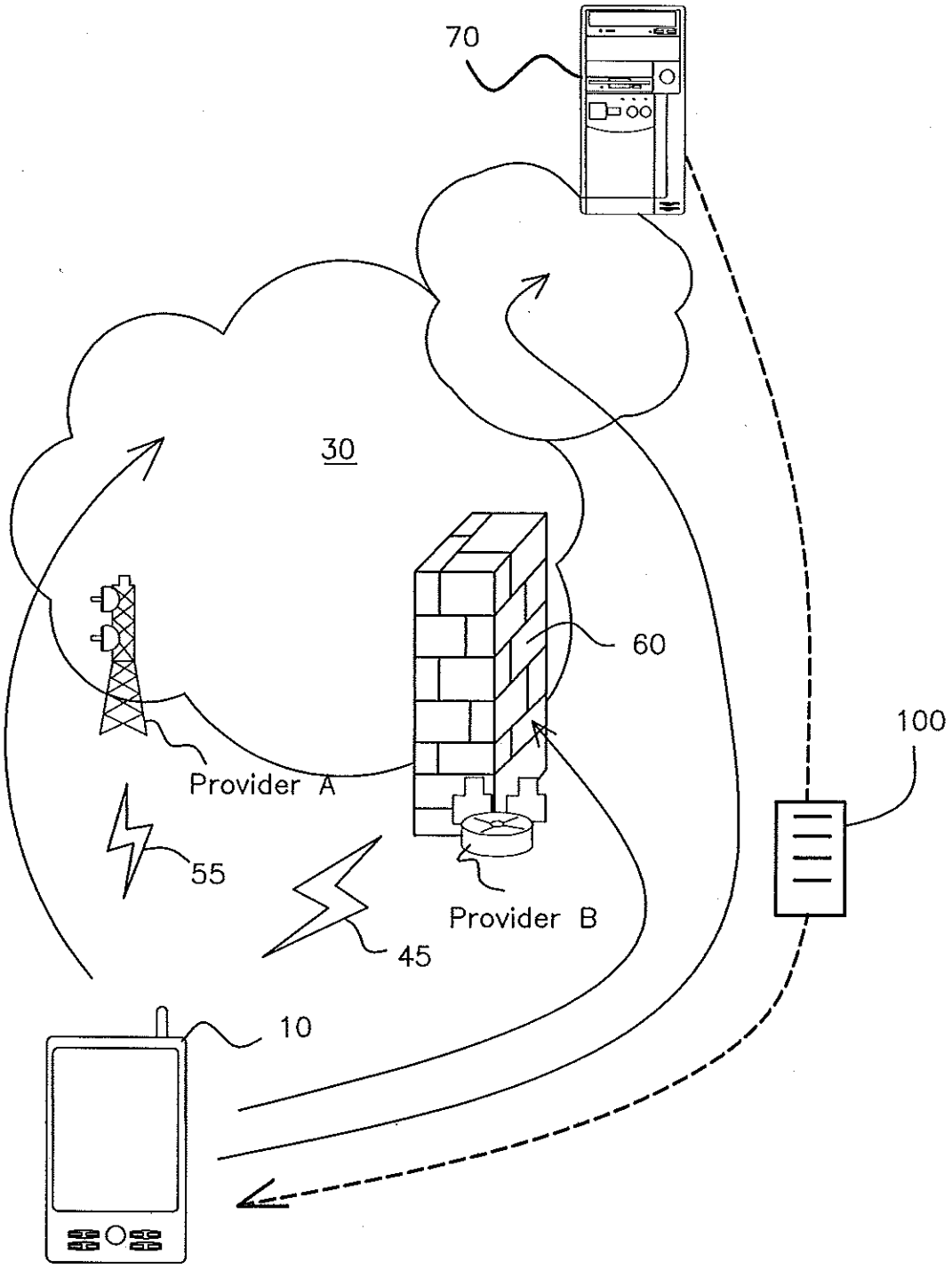

FIG.14