MINISTERO DELLO SVILUPPO ECONOMICO
DIREZIONE GENERALE PER LA TUTELA DELLA PROPRIETA' INDUSTRIALE
UFFICIO ITALIANO BREVETTI E MARCHI

UIBM

DOMANDA NUMERO	**101997900575825**
Data Deposito	**17/02/1997**
Data Pubblicazione	**17/08/1998**

Sezione	Classe	Sottoclasse	Gruppo	Sottogruppo
H	04	B		

Titolo

APPARECCHIO E METODO PER RILEVAMENTO ED INTERPRETAZIONE DI PROTOCOLLI APPLICATIVI DI SISTEMI DI TRASMISSIONE DATI SU RETE.

RM 97 A 000086

SIB 91225

DESCRIZIONE dell'invenzione industriale dal titolo:
"APPARECCHIO E METODO PER RILEVAMENTO ED INTERPRETAZIONE DI PROTOCOLLI APPLICATIVI DI SISTEMI DI TRASMISSIONE DATI SU RETE "
della ditta italiana ALGOTECH SISTEMI S.r.l.
con sede in ROMA - ITALIA

-!-!-!-

DESCRIZIONE

La presente invenzione si riferisce ad un apparecchio ed ad un metodo per il rilevamento e la interpretazione di protocolli applicativi di sistemi di trasmissione dati su rete.

Più in particolare, la presente invenzione permette una ricostruzione delle comunicazioni applicative intercorse sul tratto di rete sotto esame. Tramite la presente invenzione diviene pertanto possibile ricostruire un albero applicativo arricchito di informazioni di tipo statistico relativo ad esempio agli scambi di dati tra una molteplicità di utenti di un determinato servizio ed il servizio stesso. Un tale albero applicativo arricchito di informazioni di tipo statistico permette una certificazione dei dati e della correttezza della comunicazione a più livelli

compreso quello applicativo nonché il rilevamento di eventuali anomalie e la costruzione di statistiche di diagnostica.

La trasmissione di dati da un dispositivo di sorgente ad un dispositivo di destinazione può avvenire secondo modalità differenti. Al fine di assicurare uno scambio di dati con una ampia probabilità di mancanza di errori è però necessario adottare un insieme di regole o procedure di controllo. Tali regole o procedure sono note con il termine di "protocolli di comunicazione".

Un noto protocollo di comunicazione è l'"Open System Interconnection" (OSI) della International Standards Organization (ISO). Tale protocollo è organizzato secondo una suddivisione in sette livelli, mostrata in figura 1. Il livello 7 (applicazione) del lato sorgente contiene informazioni relative al semplice messaggio (M) da inviare verso il lato destinazione. I successivi livelli del lato sorgente aggiungono informazioni di controllo al messaggio: il livello 6 (presentazione) suddivide i dati del messaggio originale in blocchi (M1 ed M2); il livello 5 (sessione) aggiunge un titolo (S) per indicare il mittente, il destinatario ed alcune informazioni

relative alla sequenza; il livello 4 (trasporto) aggiunge informazioni (T) relative alla connessione logica tra il mittente ed il destinatario; il livello 3 (rete) aggiunge informazioni relative al percorso (N) ed il messaggio viene suddiviso in pacchetti che rappresentano l'unità standard di comunicazione in una rete; il livello 2 (collegamento dati) aggiunge una parte di titolo (B) ed una parte di coda (E) al messaggio per assicurare il corretto ordine dei vari pacchetti e correggere errori di trasmissione; i singoli bit del messaggio e delle informazioni di controllo via via aggiunte dai vari livelli vengono trasmessi sul mezzo fisico attraverso il livello 1. La freccia F1 verso il basso sul lato sorgente indica le modalità secondo le quali viene costruito il messaggio in partenza. Tutte le aggiunte al messaggio vengono verificate e rimosse dal corrispondente livello dal lato del destinatario. La freccia F2 verso l'alto sul dato destinatario indica le modalità secondo le quali viene ricostruito il messaggio in arrivo.

Il modello OSI fin qui schematicamente riassunto è solamente un modello concettuale. Un tipico protocollo normalmente adottato è ad esempio il protocollo TCP/IP (Transmission Control Protocol

and Internet Protocol). Tale protocollo, come anche altri protocolli di comunicazione adottati, è comunque spiegabile tramite riferimenti alla struttura a livelli del modello OSI. In ciascuno di tali protocolli infatti, un determinato livello di sorgente suddividerà i dati che riceve da un livello superiore aggiungendo agli stessi una intestazione e/o una coda per poi passare il tutto ad un livello inferiore. Dal lato destinazione avverranno le operazioni inverse.

Nel corso della presente descrizione si farà pertanto riferimento al modello concettuale OSI per comodità di riferimento; resta inteso che quanto descritto sarà facilmente applicabile a qualunque protocollo applicativo tramite ovvie modifiche, tipiche del rapporto che di volta in volta intercorre tra ciascun protocollo applicativo e lo standard OSI.

Sistemi di rilevamento dei dati trasmessi tra un nodo sorgente ed un nodo di destinazione sono già noti. Tali sistemi si limitano però all'analisi dei livelli OSI 2 (collegamento dati) e OSI 3 (rete). Il rilevamento e la successiva interpretazione dei dati a tali livelli permettono soltanto l'individuazione di anomalie nel

protocollo di scambio tra i vari componenti di un sistema di trasmissione dati su rete.

Uno svantaggio tipico di tali sistemi di tecnica precedente è pertanto l'impossibilità di decodificare l'informazione di tipo applicativo trasportata sulla rete, vale a dire l'informazione relativa ai livelli 4-7 dello standard OSI.

La presente invenzione ovvia a tale problema di tecnica precedente. Un primo scopo della presente invenzione è quello di permettere una ricostruzione, nei dati e negli istanti temporali, dello scambio di informazione tra un nodo di sorgente ed un nodo di destinazione. La ricostruzione negli istanti temporali sarà permessa tramite una unità di datazione. La ricostruzione dei dati sarà permessa tramite il confronto con dati predeterminati che rappresentano possibili interpretazioni dello scambio di informazione.

Un secondo scopo della presente invenzione è quello di poter costituire uno strumento affidabile e sicuro di certificazione delle sequenze applicative su rete di comunicazioni pubbliche, una volta che tali sequenze siano state ricostruite.

Un ulteriore scopo della presente invenzione è quello di rilevare e documentare l'eventuale

presenza di errori nelle applicazioni operanti sulla rete di comunicazione i cui dati sono stati rilevati ed interpretati.

Uno scopo ancora ulteriore della presente invenzione è quello di permettere una registrazione a fini amministrativi, contabili e di sicurezza dello scambio dati rilevato ed interpretato.

La presente invenzione prevede un apparecchio per il rilevamento e l'interpretazione di protocolli applicativi di sistemi di trasmissione dati su rete caratterizzato dal fatto di comprendere:

- un dispositivo di rilevamento di pacchetti di dati ad un livello corrispondente al livello OSI 2 comprendenti frame di controllo e frame di informazione, in cui i frame di informazione e di controllo contengono una parte di intestazione ed una parte di corpo, dette parti di intestazione essendo atte a permettere la distinzione tra un frame di informazione ed un frame di controllo;
- una unità di controllo ricevente in ingresso i dati provenienti dal dispositivo di rilevamento e comprendente mezzi atti a discriminare i frame di controllo dai frame di informazione;
- una unità di datazione collegata all'unità di

controllo e tale da associare un istante temporale di rilevamento ai frame di controllo ed ai frame di informazione;

- una unità di memorizzazione dei frame di controllo e dei frame di informazione e dell'istante temporale di rilevamento degli stessi, collegata in maniera bidirezionale all'unità di controllo; e

- una unità di memorizzazione di dati predeterminati, collegata in maniera bidirezionale all'unità di controllo, detti dati predeterminati rappresentando possibili interpretazioni dei frame di informazione o di controllo contenuti nell'unità di memorizzazione dei dati rilevati ed essendo atti ad essere confrontati, tramite l'unità di controllo, con i dati contenuti nella parte di corpo dei frame di informazione o di controllo memorizzati nell'unità di memorizzazione dei dati rilevati tramite il dispositivo di rilevamento in maniera tale da permettere:

- un ordinamento temporale e secondo il tipo di comunicazione delle parti di corpo dei frame di controllo e di informazione; e

- una ricostruzione di alberi applicativi arricchiti di informazioni di tipo statistico

secondo il tipo di comunicazione (ricostruzione multiprotocollo), in maniera da permettere certificazione delle comunicazioni ed il rilevamento di eventuali anomalie.

Viene inoltre previsto un metodo per il rilevamento e l'interpretazione di protocolli applicativi di sistemi di trasmissione dati su rete caratterizzato dal fatto di comprendere i seguenti passi:

- rilevare pacchetti di dati ad un livello corrispondente al livello OSI 2 comprendenti frame di controllo e frame di informazione, in cui i frame di informazione e di controllo contengono una parte di intestazione ed una parte di corpo, dette parti di intestazione essendo atte a permettere la distinzione tra un frame di informazione ed un frame di controllo;
- discriminare i frame di controllo dai frame di informazione;
- associare un istante temporale di rilevamento ai frame di controllo ed ai frame di informazione;
- memorizzare i frame di controllo ed i frame di informazione discriminati unitamente all'istante temporale di rilevamento degli stessi; e
- memorizzare dati predeterminati rappresentanti

possibili interpretazioni dei frame di informazione o di controllo, detti dati predeterminati essendo atti ad essere confrontati con i dati contenuti nella parte di corpo dei frame di informazione o di controllo memorizzati;

- ordinare temporalmente e secondo il tipo di comunicazione le parti di corpo dei frame di controllo o di comunicazione; e
- ricostruire alberi applicativi arricchiti di informazioni di tipo statistico secondo il tipo di comunicazione (ricostruzione multiprotocollo), in maniera da certificare comunicazioni e rilevare eventuali anomalie.

Ulteriori caratteristiche della presente invenzione sono definite nelle rivendicazioni dipendenti.

L'apparecchio ed il metodo secondo la presente invenzione sono pertanto in grado di eseguire analisi su tutti i livelli dello standard ISO/OSI fino a quello applicativo e livelli analoghi di altri standard. In tale maniera viene resa possibile la ricostruzione degli scambi di informazione intercorsi in un determinato intervallo temporale tra applicazioni operanti su elaboratori remoti.

L'apparecchio ed il metodo secondo la presente invenzione operano in modalità "trasparente", in quanto la trasmissione di dati tra sorgente e destinatario non viene influenzata dal rilevamento e dalla successiva interpretazione dei dati stessi.

L'apparecchio ed il metodo secondo la presente invenzione possono anche operare su reti di telecomunicazioni senza fili.

La presente invenzione verrà qui di seguito descritta secondo una sua forma di realizzazione preferita, illustrata a scopo esemplificativo e non limitativo. Verrà fatto riferimento alle figure allegate, in cui:

la figura 1, precedentemente descritta, mostra un diagramma schematico dello standard OSI;

la figura 2 mostra una rappresentazione schematica del tipo di dati utilizzati nelle comunicazioni su rete;

la figura 3 mostra uno schema a blocchi dell'apparecchio secondo la presente invenzione;

la figura 4 mostra uno schema di flusso che spiega il funzionamento dell'apparecchio secondo la presente invenzione;

le figure 5 e 6 mostrano ulteriori schemi di flusso per la comprensione di quanto descritto con

riferimento alla figura 4; e

le figure 7A e 7B mostrano un esempio di albero applicativo arricchito di informazioni di tipo statistico ottenuto tramite l'apparecchio secondo la presente invenzione.

Facendo riferimento allo standard OSI, l'unità di comunicazione in una rete è il pacchetto. I pacchetti solo a loro volta suddivisi in frame. L'inizio e la fine di ciascun frame vengono in genere stabiliti tramite caratteri di delimitazione. I frame sono a loro volta suddivisi in frame di informazione e frame di controllo. I frame di informazione servono al trasporto di dati relativi al messaggio da trasmettere lungo la rete, mentre i frame di controllo servono a gestire le modalità secondo le quali tale trasporto deve avvenire, vale a dire al controllo del flusso ed all'attivazione delle azioni di recupero degli errori. Sia i frame di informazione che i frame di controllo contengono una parte di intestazione che identifica il tipo di frame ed una parte di corpo tipica invece del frame stesso.

La struttura dei frame di informazione verrà descritta facendo riferimento alla figura 2. Nella parte superiore di tale figura è rappresentata in

maniera schematica la struttura generica di un pacchetto di livello OSI 2, comprendente cioè sia frame di informazione 1 che frame di controllo 2. La costituzione di un singolo frame di informazione (livello OSI 3) indica la presenza di una parte di intestazione 3, che contiene l'identificazione che il frame in oggetto è un frame di informazione, e di una parte di corpo 4. La parte di corpo (livelli OSI 4-7) contiene il messaggio 5 vero e proprio, unitamente ad una serie 6 di campi, rappresentati in maniera esemplificativa in figura con i caratteri C1, C2 e C3, tipici della particolare sintassi applicativa utilizzata. Per sintassi applicativa si intendono le informazioni relative al numero di campi contenuti all'interno della serie 6, al significato di ciascuno di tali campi ed ai dati in essi contenuti.

Verrà fatto ora riferimento alla figura 3. In tale figura vengono innanzitutto mostrati un nodo di sorgente 7 ed un nodo di destinazione 8, terminali del tratto di rete i cui dati vengono rilevati ed interpretati. Lungo il collegamento tra tali due nodi, rappresentato schematicamente dalle frecce F3, F4, F5, F6 e dal mezzo trasmissivo 23, viaggiano in maniera bidirezionale dati relativi a

più comunicazioni tra un primo insieme di elaboratori di sorgente (non indicati in figura) a monte del nodo di sorgente 7 ed un secondo insieme di elaboratori di destinazione (non indicati in figura) a valle del nodo di destinazione 8.

La presente invenzione prevede che tali dati vengano rilevati tramite un dispositivo 9 di rilevamento dati. Diversi sono i dispositivi di rilevamento del tipo noti sul mercato; è possibile citare ad esempio la scheda S508 della ditta canadese Sangoma. Tale scheda può operare con diversi standard a livello OSI 1 (livello fisico) quali ad esempio lo standard RS232 (o V.24) e lo standard RS422 (o V.35). Gli standard di livello OSI 2 (collegamento dati) con i quali tale scheda può operare sono ad esempio lo standard HDLC oppure lo standard X.25. Il tipo di dispositivo di rilevamento 9 da scegliersi ai fini della presente invenzione potrà comunque variare a seconda degli standard di livello OSI 1 o OSI 2 sui quali si desideri operare. Sarà infatti possibile pensare di utilizzare dispositivi di rilevamento che operino con standard implementativi differenti del livello OSI 2, quali ad esempio il "Frame Relay" o lo SDLC o ancora il BSC o altri similari. Tali dispositivi

sono comunque ben noti all'esperto del ramo e non verranno qui discussi in dettaglio.

Il rilevamento avviene in maniera "trasparente" tramite due connettori paralleli 10 ed 11, indicati schematicamente in figura, atti a permettere il rilevamento dei dati provenienti rispettivamente dal nodo di sorgente 7 e dal nodo di destinazione 8. Il dispositivo di rilevamento 9, mostrato nel suo complesso nel blocco indicato a tratteggio in figura, è tale da comprendere un ricevitore dei dati di sorgente 12, un ricevitore dei dati di destinazione 13 ed una interfaccia di connessione 14. Il ricevitore dei dati di sorgente 12 è tale da permettere la ricezione dei soli dati provenienti dal nodo di sorgente 7 secondo quanto schematicamente indicato dalla freccia F7; il ricevitore dei dati di destinazione 13 è tale invece da permettere la ricezione dei soli dati provenienti dal nodo di destinazione 8 secondo quanto schematicamente indicato dalla freccia F8. I dati così ricevuti vengono trasmessi alla interfaccia di connessione 14, secondo quanto indicato dalle frecce F9 ed F10.

Ciascun pacchetto di dati ad un livello corrispondente al livello OSI 2 letto tramite

l'unità di rilevamento 9 viene inviato ad una unità di controllo 15, come indicato dalla freccia F11. L'unità di controllo 15 verrà descritta oltre in dettaglio. A ciascuno di tali pacchetti viene associato un istante temporale di lettura tramite una unità 16 di datazione, rappresentata per comodità di presentazione all'esterno dell'unità di controllo 15 e collegata a quest'ultima come indicato tramite la freccia F12. Tale unità 16 di datazione può essere un qualsiasi dispositivo a tempo assoluto presente in commercio, in particolare via radio o satellitare. Nella modalità di realizzazione preferita delle presente invenzione si è utilizzato un orologio digitale radiocontrollato che si tara sull'ora CET (Central European Time) irradiata tramite satellite geostazionario.

Successivamente all'associazione dell'istante temporale di lettura tramite l'unità 16 di datazione, l'unità di controllo 15 provvede alla discriminazione dei frame di informazione dai frame di controllo. Nel caso in cui l'informazione venga ad esempio trasmessa in HDLC, l'ultimo bit della parte di intestazione di un frame di informazione è 0 mentre l'ultimo bit della parte di intestazione

di un frame di controllo è 1. All'interno dell'unità di controllo 15 sono pertanto presenti mezzi, non indicati in figura, atti alla discriminazione di tale ultimo bit, ad esempio un firmware contenuto in una ROM. In ogni caso, qualunque sia il codice di trasmissione dati utilizzato, saranno sempre note le modalità che distinguono un frame di controllo da un frame di informazione. Sarà pertanto sempre possibile prevedere mezzi atti a tale discriminazione. Tale discriminazione consente pertanto di immagazzinare i singoli frame di informazione privi della parte di intestazione e comprendenti la sola parte di corpo, contenente cioè le informazioni tipiche della particolare sintassi applicativa utilizzata, ed il messaggio da trasmettere.

I dati incorporanti l'istante temporale di rilevamento e suddivisi in frame di informazione e frame di controllo vengono immagazzinati all'interno di una unità 17 di memorizzazione dei dati rilevati, collegata in maniera bidirezionale all'unità di controllo 15 come rappresentato tramite la freccia F13. E' poi presente una unità 18 di memorizzazione di dati predeterminati, collegata in maniera bidirezionale all'unità di

controllo 15. Tali dati predeterminati rappresentano possibili interpretazioni dei frame di informazione o di controllo contenuti nell'unità di memorizzazione 17. Il loro utilizzo verrà spiegato in seguito con riferimento alle successive figure. Il collegamento tra l'unità di memorizzazione 18 e l'unità di controllo 15 è rappresentato tramite la freccia F14.

Verrà fatto successivamente riferimento alla figura 4, che mostra uno schema di flusso indicante le operazioni che vengono effettuate dall'unità di controllo 15 sui frame di informazione immagazzinati nell'unità 17 di memorizzazione. E' da intendersi che l'accesso a tale frame potrà eventualmente essere selettivamente regolato tramite sistemi di gestione privilegi ed autorizzazioni quali ad esempio password, codici di criptazione, decriptazione, lettori di badge e similari in possesso di utenti abilitati, a seconda dei casi.

Un primo passo S1 indica la lettura dei vari pacchetti avvenuta tramite l'unità 3 di rilevamento. Un secondo passo S2 indica la distinzione, precedentemente descritta, che l'unità di controllo 15 effettua tra i frame di

informazione ed i frame di controllo, unitamente all'associazione dell'istante temporale di rilevamento.

Sui frame di controllo, di basso livello (non applicativo), il cui utilizzo è marginale ai fini della presente invenzione, potrà comunque essere prevista una elaborazione statistica, effettuata nel passo S3. Tale elaborazione non viene qui descritta in dettaglio; le modalità con le quali essa avviene risulteranno chiare alla fine della presente descrizione. Il risultato finale di una tale elaborazione fornirà una elencazione dei vari frame di controllo, riportando inoltre il conteggio del numero di occorrenze di ciascuno di tali frame.

Per quanto concerne i frame di informazione, il flusso procede verso un passo S4 in cui i singoli frame di informazione vengono ricostruiti in base alla sintassi applicativa specifica degli stessi. Ai fini di tale ricostruzione, le strutture di sintassi applicativa dei singoli frame di informazione devono essere note. Esse sono infatti contenute all'interno dell'unità 18 di memorizzazione di dati predeterminati descritta con riferimento alla precedente figura 3. Tale unità 12 contiene, ad esempio in un "file" di testo, una

descrizione formale astratta di possibili interpretazioni dei frame di informazione o di controllo. Tali dati rappresentano le modalità secondo le quali può essere strutturata la parte di corpo di un singolo frame di informazione, ad esempio il codice di trasmissione macchina (vale a dire relativo ad un frame di informazione spedito dalla sorgente oppure dal destinatario), il numero di canale (vale a dire relativo ad uno specifico elaboratore a monte del nodo di sorgente oppure ad uno specifico elaboratore a valle del nodo di destinazione), numeri di protocollo, numeri meccanografici etc. E' da intendersi che tale unità 18 può contenere sintassi di molteplici protocolli applicativi, dei frame di informazione da ricostruire in quel momento.

Tramite un confronto sequenziale della parte di corpo di ciascun frame di informazione con ciascuna delle tipologie astratte presenti nell'unità 18, si ottiene una ricostruzione dei singoli frame di informazione.

Successivamente a ciò, si è in grado di ricomporre le varie sequenze applicative intercorse tra un determinato elaboratore di sorgente ed un determinato elaboratore di destinazione, vale a

dire un ordinamento temporale e secondo il tipo di comunicazione. Per sequenza applicativa verrà inteso nel corso della presente descrizione l'insieme dei frame di informazione scambiati tra un determinato elaboratore di sorgente ed un determinato elaboratore di destinazione all'interno di una singola comunicazione. La sequenza applicativa ordinata all'interno del passo S5 conterrà i singoli frame di informazione ordinati solamente secondo un criterio temporale e non anche secondo un criterio logico. L'ordinamento temporale è stato reso possibile dall'associazione dell'istante temporale avvenuta nel precedente passo S2.

Ai fini di un ordinamento anche logico dei dati all'interno di una specifica sequenza applicativa può rivelarsi utile, ma non necessaria, la presenza di un insieme di regole applicative che governano lo scambio di dati tra sorgente e destinazione. Tali regole applicative, tipiche della particolare tipologia di colloquio tra un determinato elaboratore di sorgente ed un determinato elaboratore di destinazione, devono essere predefinite e come tali sono anch'esse raccolte nell'unità 18 di memorizzazione di dati

predeterminati. Tali regole applicative sono un insieme di possibili interpretazioni di sequenze di frame di informazione contenuti nell'unità di memorizzazione 17 dei dati rilevati.

Un esempio di regole applicative è dato dalla seguente tabella 1, in cui si fa riferimento ad una comunicazione tra una sorgente che rappresenta uno studente (client) che voglia effettuare una iscrizione via terminale all'università, ed un destinatario (server) che rappresenta l'università cui lo studente vuole iscriversi.

TABELLA 1

1: AS ? FDB 15 AS ? FDB 5 AS ? FDB 0 La prenotazione dell'iscrizione è stata acquisita regolarmente
2: AS ? FDB 13 AS ? FDB 0 La posizione dell'utente non è regolare
.....
.....
.....

Ogni riga di tale tabella è una regola applicativa, indicante cioè una possibile sequenza applicativa di scambio dati tra sorgente e destinatario. Viene qui di seguito riportato il significato di ciascuna

di tali sequenze applicative. La prima riga indica ad esempio la seguente sequenza di frame di informazione:

- la sorgente (AS) interroga (?) il destinatario;
- il destinatario (FDB) risponde con l'attività numero 15;
- la sorgente (AS) interroga (?) nuovamente il destinatario;
- il destinatario (FDB) risponde con l'attività numero 5;
- la sorgente (AS) interroga (?) il destinatario; e
- il destinatario (FDB) risponde con l'attività numero 0.

Il risultato cui si perviene al termine di tale conversazione è che la prenotazione dell'iscrizione all'università è stata acquisita regolarmente. La tabella 1, meramente esemplificativa, potrebbe essere anche rappresentata tramite una struttura ad albero con più o meno ramificazioni, a seconda del numero di sequenze applicative previste. Ogni percorso fino ad una delle foglie dell'albero rappresenterebbe una particolare sequenza applicativa, vale a dire una particolare conversazione tra sorgente e destinatario, vale a dire ancora una particolare

sequenza di frame di informazione tra sorgente e destinatario.

Le regole applicative possono essere in numero qualunque. Maggiore sarà il numero di regole applicative fornito, maggiore sarà la possibilità di associare a ciascuna delle sequenze applicative temporalmente ricostruite nel passo S5 un significato logico ben definito, riscontrato tramite confronto con una particolare regola applicativa contenuta nell'unità di memorizzazione 18 di figura 3. In tale modo sarà dunque possibile verificare correttezza o anomalia della particolare sequenza applicativa in quel momento confrontata.

Nel passo S6 di figura 4 l'unità di controllo 15 verifica innanzitutto se tali regole applicative siano disponibili o meno. Supponendo che tali regole applicative siano note, il flusso può procedere o verso un passo S8 oppure verso un passo S9, a seconda di quanto scelto nel passo S7. Il passo S8 permette una semplice classificazione delle sequenze applicative. Ciascuna sequenza applicativa viene infatti classificata come appartenente ad un particolare percorso tra i vari percorsi possibili all'interno dell'albero delle regole applicative. Il passo S8 verrà spiegato in

maggiore dettaglio con riferimento alla successiva figura 5.

Nel passo S9 invece, viene ricostruito il percorso logico di tutte le sequenze applicative rilevate dall'apparecchio in un predeterminato intervallo temporale. Tale passo S9 verrà spiegato in maggiore dettaglio con riferimento alla successiva figura 6.

L'apparecchio secondo la presente invenzione consente di effettuare una ricostruzione del percorso logico delle sequenze applicative anche nel caso in cui non sia previsto un insieme di regole applicative. Il flusso procede in tale caso verso un passo S10, anch'esso successivamente descritto.

Verrà fatto ora riferimento alla figura 5, che spiega in maggiore dettaglio quanto sopra descritto con riferimento al passo S8 di figura 4. In un primo passo S11 viene selezionata la singola sequenza applicativa oggetto del confronto. In un successivo passo S12 vengono selezionati, all'interno della sequenza applicativa selezionata, gli elementi caratterizzanti ai fini del confronto. Nel caso esemplificativo precedentemente descritto di iscrizione all'università con riferimento alla

tabella 1 tali elementi caratterizzanti potranno essere: l'identificativo dell'elaboratore di sorgente, l'identificativo dell'utente che ha richiesto l'operazione di iscrizione, i dati forniti dalla sorgente ed i dati forniti dal destinatario. Nel passo S13 gli elementi caratterizzanti della sequenza applicativa in oggetto vengono confrontati con una delle regole applicative di cui alla precedente tabella 1 alla ricerca di una possibile corrispondenza. Nel caso in cui tale corrispondenza sia stata trovata, il flusso procede verso un passo S14 in cui tale corrispondenza viene segnalata e della quale andrà tenuto conto nei risultati dell'interpretazione. Il flusso torna poi a selezionare una successiva sequenza e a rieseguire il passo S11. Nel caso in cui la corrispondenza di cui al passo S13 non sia stata trovata, l'unità di controllo 15 passa ad una successiva regola nel passo S15 e nel caso in cui (passo S16) vi siano ancora regole con le quali effettuare il confronto l'unità di controllo ritorna ad eseguire il confronto di cui al passo S13. Nel caso in cui invece non vi siano regole ulteriori, l'unità di controllo segnala una anomalia nel passo S17. Una tale anomalia può

alternativamente significare:

- un tipo di sequenza che non sarebbe dovuto avvenire (anomalia vera e propria); oppure
- un tipo di sequenza non inserito per errore all'interno dell'albero delle regole applicative.

In ciascuno di tali casi il riscontro di una tale anomalia è sicuramente utile ai fini della certificazione delle tipologie di sequenze applicative intercorse nel tratto di rete posto sotto osservazione.

Verrà fatto ora riferimento alla successiva figura 6 che spiega in maggiore dettaglio quanto descritto nel passo S9 di figura 4.

I passi S18 ed S19 servono rispettivamente a selezionare la singola sequenza applicativa e gli elementi caratterizzanti della stessa, similmente a quanto descritto con riferimento alla precedente figura 5. Il passo S20 serve ad indicare il confronto tra la sequenza applicativa e le regole applicative predefinite contenute all'interno dell'unità 18 di memorizzazione di dati predeterminati. Nel caso in cui si sia trovata una corrispondenza, il flusso procede verso un passo S21 in cui viene tenuto conto della corrispondenza rinvenuta tramite aggiornamento dei relativi campi

statistici. I passi S18-S20 verranno successivamente ripetuti, fino ad esaurimento delle sequenze da classificare. Nel caso in cui invece non vengano trovate corrispondenze, la sequenza applicativa da classificare è nuova; essa può rappresentare una anomalia oppure semplicemente una sequenza che non è stata prevista. In questo caso il flusso procede verso un passo S22 in cui vengono inizializzati i campi statistici relativi a quella specifica sequenza. La sequenza riscontrata potrà inoltre inserita nella lista delle sequenza predefinite che servono ad effettuare la comparazione nel passo S20. Tale fatto è anche indicato dal doppio senso della freccia F14 della precedente figura 3. E' da intendersi che tali sequenze particolari, le probabili anomalie cioè, possono eventualmente essere marcate in maniera particolare in modo da essere riconosciute come tali. Successivamente a ciò vengono anche in questo caso ripetuti i passi S18-S20 fino ad esaurimento delle sequenze da classificare. In particolare, oltre a poter individuare il numero di attraversamenti di ciascun ramo dell'albero, sarà possibile individuare anche rami non percorsi.

Nel caso in cui non sia presente una sequenza

predefinita di regole applicative, l'unità di controllo sarà sempre in grado di effettuare una ricostruzione delle comunicazioni applicative intercorse sul tratto di rete sotto esame (passo S9 di figura 4). In tale caso ciascuna sequenza applicativa analizzata verrà confrontata non con sequenze predefinite, bensì con le sequenze precedentemente analizzate. L'albero applicativo arricchito di informazioni di tipo statistico verrà pertanto ricostruito tramite confronto reciproco di ciascuna parte di corpo dei frame di informazione con le altre. Verrà anche in questo caso formato un albero e sarà possibile conoscere il numero di attraversamenti di ciascun ramo. In questo caso non sarà ovviamente possibile individuare rami non percorsi, in quanto non si sarà a priori a conoscenza dell'esistenza di tali rami.

Verrà fatto infine riferimento alle figure 7A e 7B che mostrano rispettivamente una struttura esemplificativa di frame informativo ed una struttura esemplificativa di albero applicativo arricchito di informazioni di tipo statistico ottenuta tramite l'apparecchio secondo la presente invenzione.

In figura 7A è possibile scorgere quattro

campi differenti: un primo campo 19 che indica il nominativo dell'elaboratore di sorgente o dell'elaboratore di destinazione; un secondo campo 20 che indica il numero di collegamenti all'interno dell'intervallo di tempo di rilevamento, un terzo campo 21 che indica la durata media di ciascun collegamento, ad esempio in millisecondi, ed un quarto campo 22 che indica il codice dell'attività svolta.

La figura 7B indica l'albero ricostruito. Un primo elemento E1 dell'albero indica che AS (sorgente) si è collegato 20 volte, con una durata media di collegamento di 0 millisecondi (semplice apertura del collegamento con il destinatario) e ha effettuato l'attività con il codice 0. Un secondo elemento E2, unico "figlio" di E1, indica che in tutti e 20 questi collegamenti FDB (destinatario) ha risposto con l'attività con il codice 20, con una durata media di collegamento di 20 millisecondi. Due sono state le modalità con le quali si è proseguito. Per 18 volte (elemento E3) AS ha risposto con l'attività 0 e per due volte (elemento E4) AS ha risposto con l'attività 1. L'albero prosegue con altri elementi, il cui significato risulta ora chiaro dal contesto.

L'albero qui presentato è il risultato dell'ordinamento logico effettuato nei passi S9 o S10 della figura 4.

Si fa notare che l'individuazione dei contenuti del campo 19 e del campo 22 di ciascun elemento è stata effettuata tramite il passo S4 di figura 4. L'individuazione dei collegamenti tra i vari elementi, vale a dire il fatto che l'elemento E2 è "figlio" di E1 e che gli elementi E3 ed E4 sono "figli" di E2 è stata fatta o nel passo S9 oppure nel passo S10 di figura 4.

La presente invenzione è stata fin qui descritta con riferimento ad una sua forma di realizzazione illustrata a scopo esemplificativo e non limitativo. E' da intendersi ad esempio possibile una applicazione che preveda più apparecchi secondo la presente invenzione previsti lungo tratti di linea differenti.

E' da intendersi inoltre che altre siano le forme di realizzazione e le tipologie di servizio possibili rientranti nell'ambito della presente privativa industriale.

Ulberto Tonon
(Iscr. Albo n. 83)

RIVENDICAZIONI

1. Apparecchio per il rilevamento e l'interpretazione di protocolli applicativi di sistemi di trasmissione dati su rete caratterizzato dal fatto di comprendere:

- un dispositivo (9) di rilevamento di pacchetti di dati ad un livello corrispondente al livello OSI 2 comprendenti frame di controllo e frame di informazione, in cui i frame di informazione e di controllo contengono una parte di intestazione ed una parte di corpo, dette parti di intestazione essendo atte a permettere la distinzione tra un frame di informazione ed un frame di controllo;
- una unità di controllo (15) ricevente in ingresso i dati provenienti dal dispositivo di rilevamento (9) e comprendente mezzi atti a discriminare i frame di controllo dai frame di informazione;
- una unità (16) di datazione collegata all'unità di controllo (15) e tale da associare un istante temporale di rilevamento ai frame di controllo ed ai frame di informazione;
- una unità di memorizzazione (17) dei frame di controllo e dei frame di informazione e dell'istante temporale di rilevamento degli stessi, collegata in maniera bidirezionale all'unità di

controllo (15); e

- una unità (18) di memorizzazione di dati predeterminati, collegata in maniera bidirezionale all'unità di controllo (15), detti dati predeterminati rappresentando possibili interpretazioni dei frame di informazione o di controllo contenuti nell'unità di memorizzazione (17) dei dati rilevati ed essendo atti ad essere confrontati, tramite l'unità di controllo (15), con i dati contenuti nella parte di corpo dei frame di informazione o di controllo memorizzati nell'unità di memorizzazione (17) dei dati rilevati tramite il dispositivo di rilevamento (9) in maniera tale da permettere:

  - un ordinamento temporale e secondo il tipo di comunicazione delle parti di corpo dei frame di controllo e di informazione; e
  - una ricostruzione di alberi applicativi arricchiti di informazioni di tipo statistico secondo il tipo di comunicazione, in maniera da permettere certificazione delle comunicazioni ed il rilevamento di eventuali anomalie.

2. Apparecchio secondo al rivendicazione 1, caratterizzato dal fatto che il dispositivo (9) di

rilevamento dati comprende:

- un ricevitore dei dati di sorgente (12);
- un ricevitore dei dati di destinazione (13); e
- una interfaccia di connessione (14) atta a ricevere i segnali provenienti dal ricevitore dei dati di sorgente (12) e dal ricevitore dei dati di destinazione (13) ed a trasmettere gli stessi verso l'unità di controllo (15).

3. Apparecchio secondo la rivendicazione 1 o 2, caratterizzato dal fatto che la ricostruzione di detto albero applicativo arricchito di informazioni di tipo statistico avviene tramite confronto reciproco di ciascuna parte di corpo dei frame di informazione con le altre.

4. Apparecchio secondo la rivendicazione 1 o 2, caratterizzato dal fatto che la ricostruzione di detto albero applicativo arricchito di informazioni di tipo statistico avviene tramite confronto di ciascuna sequenza di parti di corpo dei frame di informazione con un insieme di sequenze predeterminate, rappresentanti possibili interpretazioni di sequenze di frame di informazione o di controllo contenuti nell'unità di memorizzazione (17) dei dati rilevati, dette sequenze predeterminate essendo contenute in detta

unità (18) di memorizzazione di dati predeterminati.

5. Apparecchio secondo una qualsiasi delle rivendicazioni precedenti, caratterizzato dal fatto che detta unità (16) di datazione è di tipo a tempo assoluto, in particolare via radio o satellitare.

6. Apparecchio sostanzialmente come descritto in precedenza con riferimento ai disegni annessi.

7. Metodo per il rilevamento e l'interpretazione di protocolli applicativi di sistemi di trasmissione dati su rete caratterizzato dal fatto di comprendere i seguenti passi:

- rilevare pacchetti di dati ad un livello corrispondente al livello OSI 2 comprendenti frame di controllo e frame di informazione, in cui i frame di informazione e di controllo contengono una parte di intestazione ed una parte di corpo, dette parti di intestazione essendo atte a permettere la distinzione tra un frame di informazione ed un frame di controllo;
- discriminare i frame di controllo dai frame di informazione;
- associare un istante temporale di rilevamento ai frame di controllo ed ai frame di informazione;
- memorizzare i frame di controllo ed i frame di

informazione discriminati unitamente all'istante temporale di rilevamento degli stessi; e

- memorizzare dati predeterminati rappresentanti possibili interpretazioni dei frame di informazione o di controllo, detti dati predeterminati essendo atti ad essere confrontati con i dati contenuti nella parte di corpo dei frame di informazione o di controllo memorizzati;
- ordinare temporalmente e secondo il tipo di comunicazione le parti di corpo dei frame di controllo o di comunicazione; e
- ricostruire alberi applicativi arricchiti di informazioni di tipo statistico secondo il tipo di comunicazione, in maniera da certificare comunicazioni e rilevare eventuali anomalie.

8. Metodo secondo la rivendicazione 7, caratterizzato dal fatto che detta operazione di ricostruzione di detto albero applicativo arricchito di informazioni di tipo statistico avviene tramite confronto reciproco di ciascuna parte di corpo dei frame di informazione con le altre.

9. Metodo secondo la rivendicazione 7, caratterizzato dal fatto che la ricostruzione di detto albero applicativo arricchito di informazioni

di tipo statistico avviene tramite confronto di ciascuna sequenza di parti di corpo dei frame di informazione, ordinate temporalmente e secondo il tipo di comunicazione, con un insieme di sequenze predeterminate rappresentanti possibili interpretazioni di sequenze dei frame di informazione o di controllo memorizzati.

10. Metodo secondo una qualsiasi delle rivendicazioni da 7 ad 9, caratterizzato dal fatto che l'operazione di associazione di un istante temporale di rilevamento ai frame di controllo ed ai frame di informazione avviene tramite una unità (16) di datazione di tipo a tempo assoluto, in particolare via radio o satellitare.

11. Metodo sostanzialmente come descritto in precedenza con riferimento ai disegni annessi.

p.p. ALGOTECH SISTEMI S.r.l.

Ulberto Tonon
(Iscr. Albo n. 89)

MINISTERO INDUSTRIA COMMERCIO E ARTIGIANATO
UFFICIO PROV. IND. COMM. E ART.
ROMA

p.p. ALGOTECH SISTEMI S.r.l.

Gilberto Tonon
(Iscr. Albo n. 83)

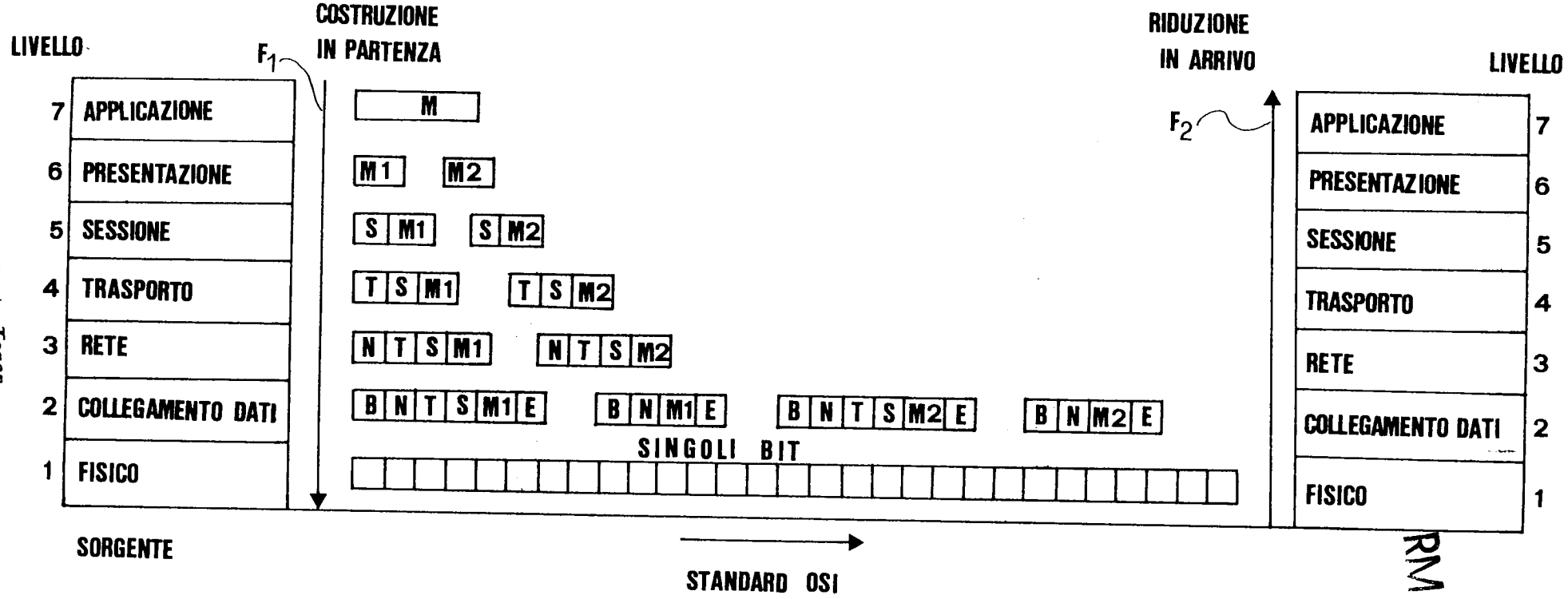

FIG 1

RM 97 A 000186

p.p. ALGOTECH SISTEMI S.r.l.
Gilberto Tonon
(Iscr. Albo n. 831)

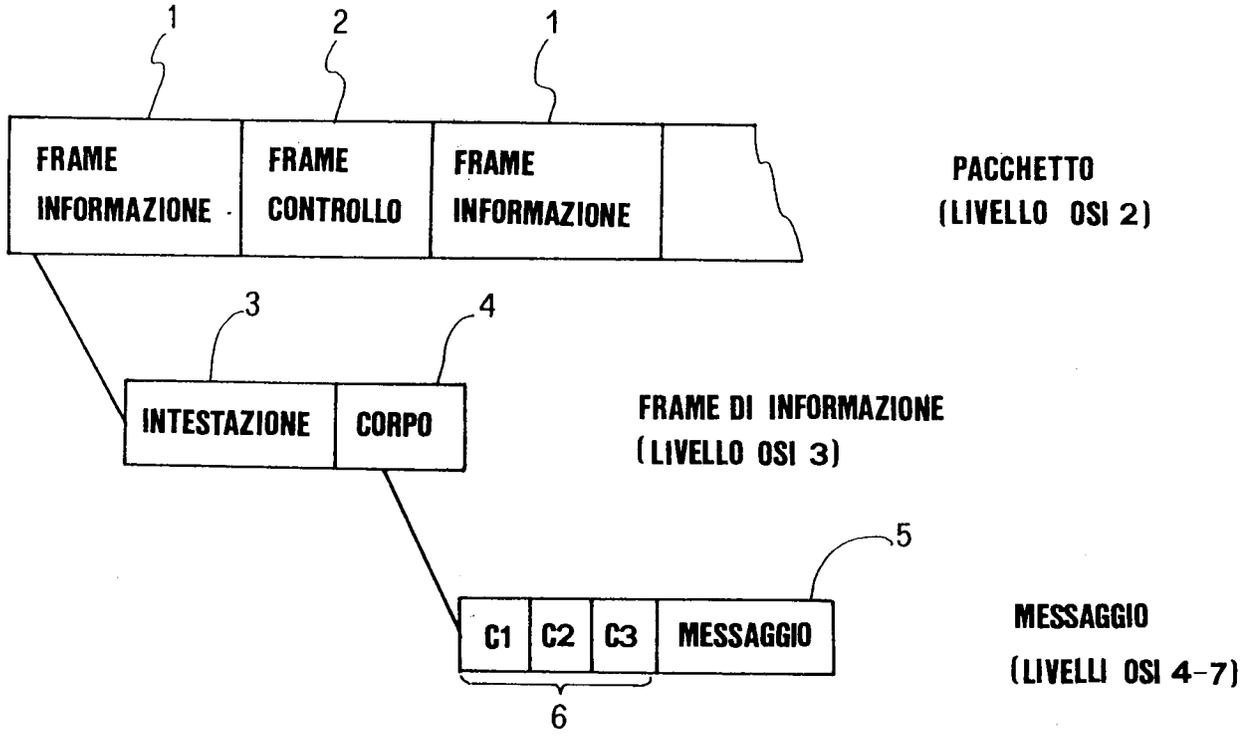

FIG 2

RM97A000086

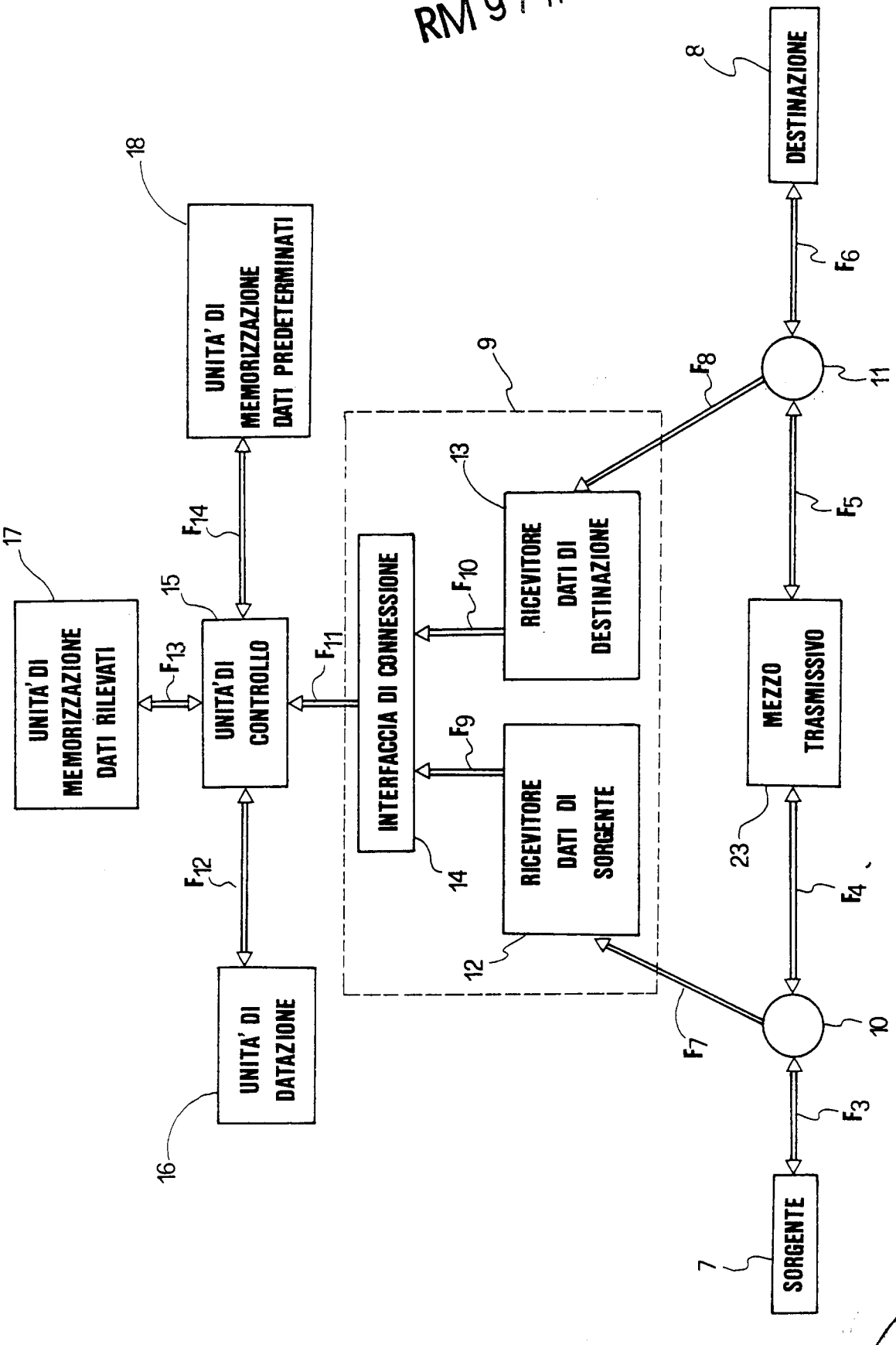

FIG 3

p.p. ALGOTECH SISTEMI S.r.l.

Gilberto Tonon
(Iscr. Albo n. 83)

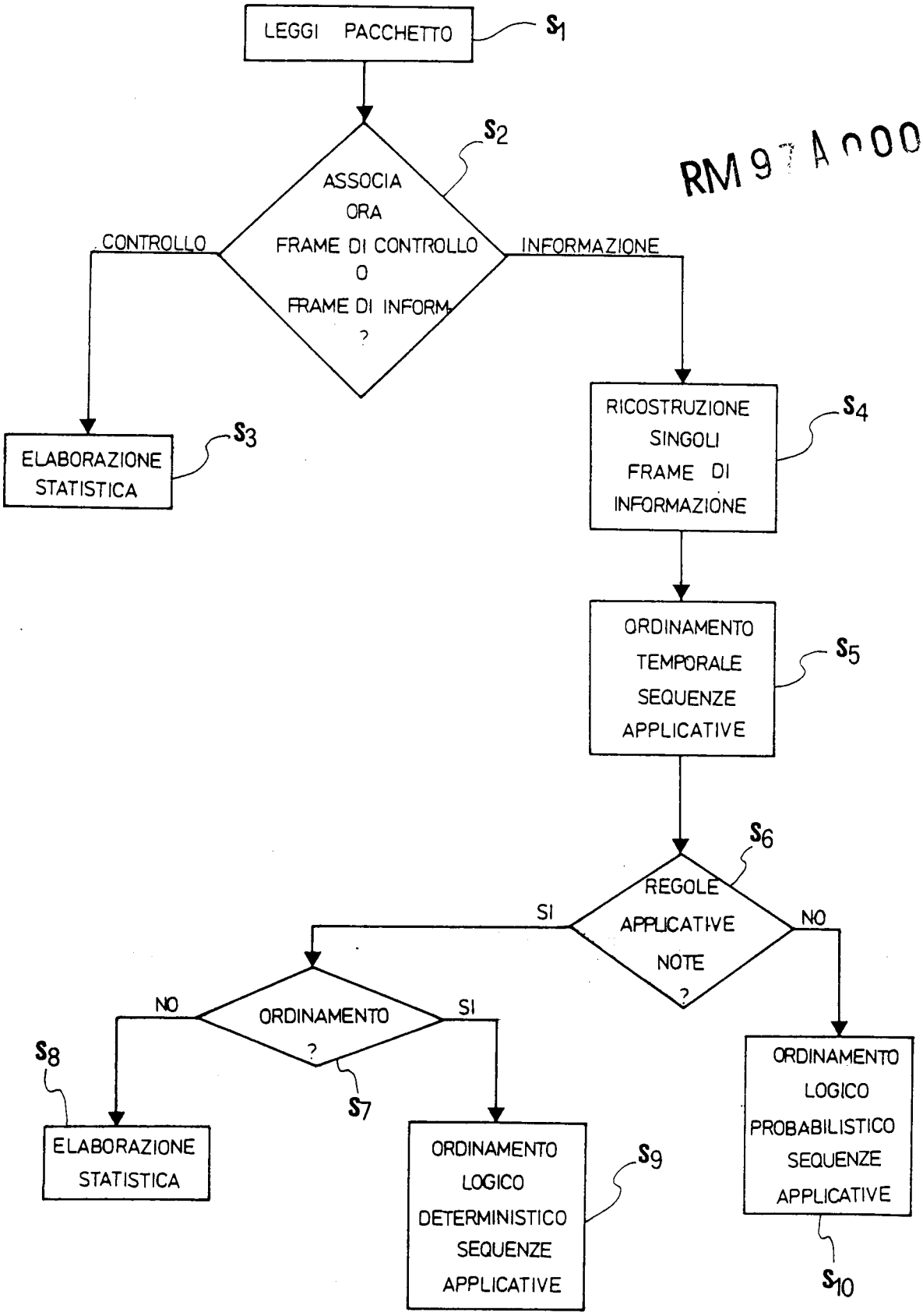

FIG 4

p.p. ALGOTECH SISTEMI S.r.l. *Gilberto Tonon* (Iscr. Albo n. 83)

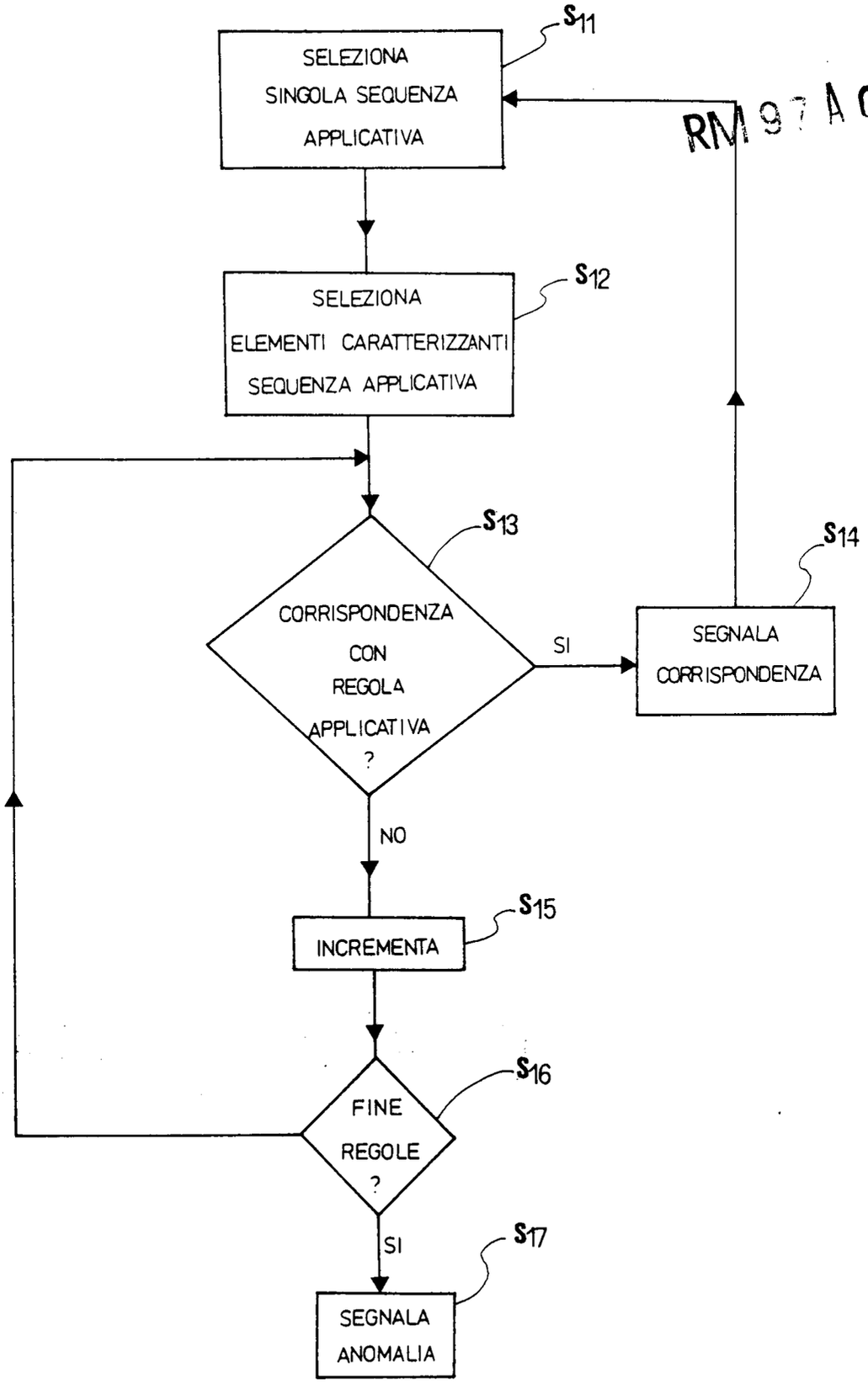

FIG 5

p.p. ALGOTECH SISTEMI S.r.l.

Gilberto Tonon
(Iscr. Albo n. 83)

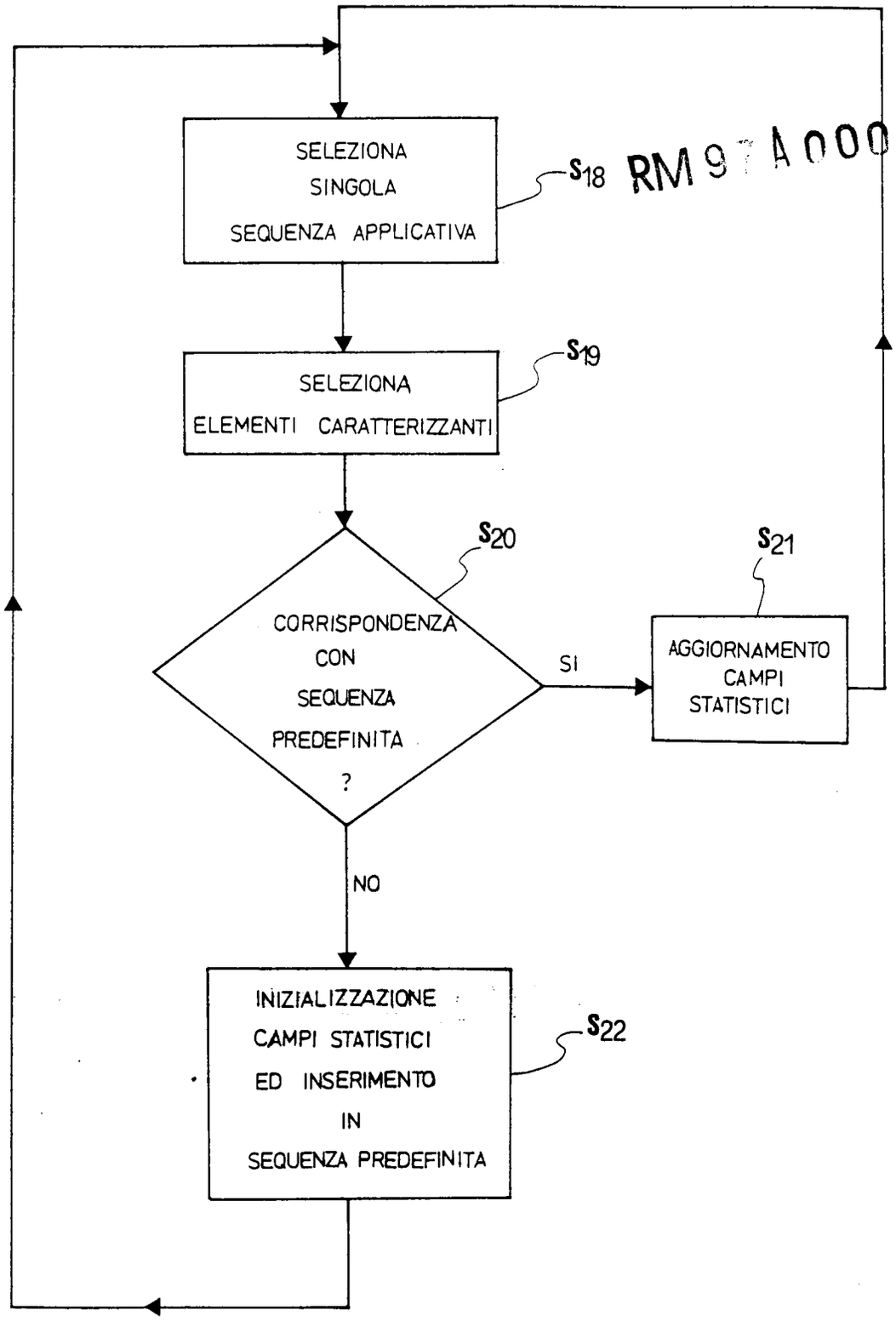

FIG 6

p.p. ALGOTECH SISTEMI S.r.l.

Gilberto Tonon
(Iscr. Albo n. 83)

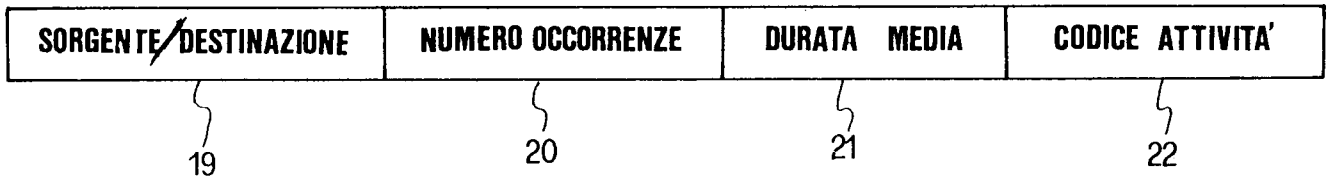

FIG 7A

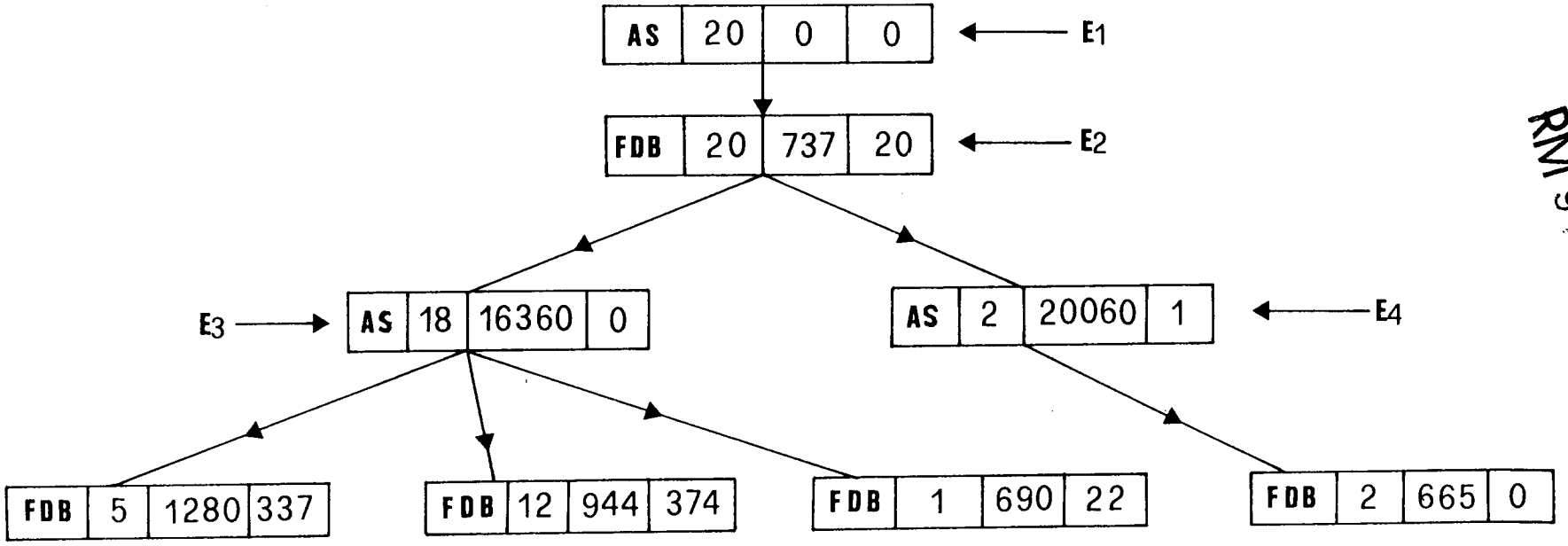

FIG 7B