PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 29/06, G03G 15/00, H04N 1/32

A1

(11) International Publication Number: **WO 99/20024**

(43) International Publication Date: 22 April 1999 (22.04.99)

(21) International Application Number: PCT/NL98/00581

(22) International Filing Date: 9 October 1998 (09.10.98)

(30) Priority Data:
1007252 10 October 1997 (10.10.97) NL

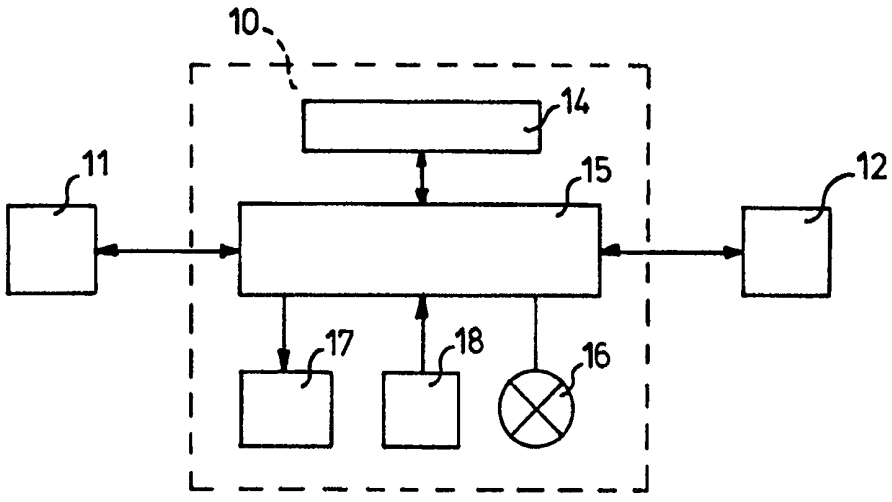
(71)(72) Applicant and Inventor: DE LA BRETONIERE, Ralph, Rogier [NL/NL]; Bijhouwerlommer 43, NL–2728 JK Zoetermeer (NL).

(74) Agent: DE BRUIJN, Leendert, C.; Nederlandsch Octrooibureau, Scheveningseweg 82, P.O. Box 29720, NL–2502 LS The Hague (NL).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
In English translation (filed in Dutch).

(54) Title: METHOD AND DEVICE FOR PROTECTING DATA COMMUNICATION



(57) Abstract

The invention relates to a method and a device for protecting data communication traffic between a first communication station (11) and a second communication station (12), in which the data is dispatched according to a data protocol from the second to the first communication station. The method comprises the steps of the comparison of the data protocol with at least one standardized protocol and the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station (11). For this purpose, the device (10) comprises memory means (14) in which data characteristics of at least one standardized protocol have been stored and comparison/forwarding means (15) which compare the stored data characteristics with the data protocol and forward only data of which the data protocol complies with the at least one standardized protocol.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

Method and device for protecting data communication

The invention relates to a method and a device for protecting data communication traffic between a first communication station and a second communication station, in which the data is dispatched according to a data protocol from the second to the first communication station. In particular, data communication links are protected which can be seized by third parties by means of public and/or private data and telecommunication infrastructure.

Appliances are found to an increasing extent on the market which are provided with an option which makes it possible to provide so-called remote service. This involves, in particular, installed fax equipment, network fax equipment, telephone modems, cable modems, combined fax/modem configurations, telephone sets, answering machines, telephone exchanges, copying machines, washing machines and other domestic, industrial appliances and operating appliances which can communicate with one another via the said infrastructures. This relates to appliances which are installed separately and also in combination with other equipment. This remote service, also known as "remote diagnostics" or "remote maintenance" has been developed in order to be able to deliver a flexible and cheap method of support to the (end) users of the equipment.

Remote service, furthermore referred to as RDS ("Remote DiagnosticS") makes it possible to subject the respective appliance to an analysis via the said infrastructure from the location of the supplier or another service point. In a number of cases, it is even possible for the service engineer to be able to carry out small repairs remotely. If it emerges that repair has nevertheless to be carried out at the location of the appliance, the respective maintenance engineer or technician can be sent out with the correct components. Specifically, it is already known via RDS what is wrong with the appliance and what measures have to be taken to remedy the fault.

The functionality of RDS may comprise many advanced options:

- The reading-out of the various counter positions; when a service is necessary can be determined by interpreting the counter positions.
- The switching-on and switching-off of the visual and audible signals, for example, in the case of a fax machine; as a result it is possible to analyse the appliance remotely without disturbing the immediate environment.

- The reading-out of a fax/telephone number list; in the event of an alteration of (service) telephone numbers, these can be altered remotely.
- The reading-out of a fax log; the log usually contains the error codes of the last fax messages sent and these can be used by the technical support for the purpose of analysing the appliance.
- The manipulation of the fax memory; this is intended to offer a final possibility for erasing the memory if this is not possible by means of the prescribed manner.
- The alteration of the configuration settings; as a service, the appliance can be configured remotely in accordance with the wishes of the client.
- The adding of connecting-through numbers; the service centre can then examine any damaged faxes itself and infer therefrom what the possible cause of the fault is.

Although the functionality mentioned is concentrated on fax machines, a comparable functionality may be present in the other equipment mentioned above. The RDS functionality can, in principle, comprise all the functionality which relates to operations concerning the memories (RAM, ROM, EEPROM) present in the appliance.

Many manufacturers of data communication devices make use of so-called custom chip sets (standard integrated circuits produced in large numbers) or accommodate hardware produced in large numbers and delivered to many manufacturers in a separate housing. The specifications of the manufacturer will, in many cases, describe only the functions desired by the manufacturer. It is therefore possible that (RDS) functionality is present in custom chip sets or hardware which is not made known to the end user.

In the modern information society, knowledge is power. Information is, of course, well protected by means of physical and organizational protection measures of all kinds. Documents may, for example, be seen only by a select group of individuals, after which they are securely stored in the safe. For the purpose of rapid decision-making and refreshing the information situation, consultation will often be made by telephone, in which case use is frequently made of the fax machine to transmit the documents to be discussed to one another. It is here that there is a weak point in the entire security chain. Essentially, the respective documents are made available to third parties, the intention

being precisely to avoid that. Said third parties, who possibly have direct business interests or operate in the world of information brokerage, may acquire possession of valuable information. This may take place even without the owner of the sensitive information even having any indication until it is too late. The industrial spy therefore appears to be very near at hand and works, it is to be noted, together with the individual who has protected his own information with every means.

A fax machine has, for example, RDS functionality, whether this is known to the end user or not, and can thereby be manipulated by a third party. Said third party can ensure, for example, that the respective fax machine responds to certain fax numbers and/or fax identification numbers. During the transmission and/or reception of faxes from/to these fax numbers, the fax machine will transmit, for example, an additional copy to the fax number specified by said third party. The user of the fax machine does not, however, notice anything in this case because the visual and audible signals can be switched off, the so-called fax through-connection number does not have to figure in the list of fax through-connection numbers and even the fax log does not have to report this operation. If necessary, a copy of the fax involved is transmitted only during the night hours when no-one is present in the company.

In the case of a network fax or a modem fax incorporated in a network system within a company, it is conceivable that a third party obtains access via said fax or said modem to the network system. As a result, it might be possible also to extract information in the manner mentioned above from the network system, which is believed to be safe.

The object of the present invention is to provide a method and a device for protecting data communication traffic in order to prevent third parties being able to make unnoticed use of functionality present in a communication station.

According to the invention, the object is achieved by means of a method of the type defined in the introduction, characterized by the steps of the comparison of the data protocol with at least one standardized protocol and the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station.

Repetitions of commands, or certain combinations of commands, which each belong per se to the standardized protocol but do not lead to normal, effective data communication traffic, are deemed not to belong to the standardized protocol. Specifically, it is possible that such

repetitions or combinations of commands are used to switch on certain RDS functionality.

Before a fax machine, for example, can proceed to the reception and/or transmission of documents, the appliances at both ends of the communication link have to inform one another about the status they are in. After this so-called "handshake" procedure, the information exchange is mutually adapted. Both appliances are now ready and will carry out the desired task. This procedure and the information exchange proceeds according to internationally specified standards, also referred to as protocols, which are specified in part in the so-called ISO, ETSI and ANSI standards or in the ITU regulations. Before, during or after the "handshake" procedure, a check can take place on the presence of certain RDS functionality. To use RDS functionality, a manufacturer will use protocols which are not (entirely) incorporated in the standards. This means that the use of a so-called exotic protocol can indicate the use of RDS functionality. It indicates in any case that the other party is not adhering to the standard protocols. The negation of the standard indicates that the link made is being used in a manner other than that which the user intended.

As a result of using the method according to the invention, an attempt of a third party to switch on (concealed) RDS functionality from the outside will be unsuccessful, as a result of which the probability that information can leak out via the communication equipment used becomes substantially smaller.

Because, according to the invention, the data protocol is compared with standardized protocols, the method according to the invention can be used worldwide.

In an embodiment of the method according to the invention, the user of a communication station is warned if it emerges during the comparison of the data protocol that the latter does not belong to a known standardized protocol. As a result, the user is warned of an attempt of a third party to manipulate his communication station, whereupon the user can take direct action.

In a further embodiment of the method according to the invention, the link is interrupted if it emerges during the comparison of the data protocol that the latter does not belong to a standardized protocol. This has the result that any attempt to manipulate the communication station by a third party will be unsuccessful.

In a preferred embodiment of the method according to the

invention, after ascertaining that the data protocol does not belong to a certain standardized protocol, a data file containing data of the data communication traffic and the second communication station is prepared. As a result of recording said data, the user is enabled to obtain as complete a picture as possible of the user of the second communication station, after which appropriate measures can be taken.

Another aspect of the invention provides a device suitable for carrying out the method according to the invention. For this purpose, the device is provided with memory means for storing data characteristics of a standardized protocol and comparison/forwarding means for the comparison of the stored data characteristics with the data protocol and the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station.

With the device according to the invention, it is possible to use the abovementioned method in a data communication environment. An advantage of the device according to the invention is that the user can determine himself, regardless of the brand and type of appliance, whether RDS functionality is permitted. Because the device can be used separately from the local communication station, there is no need to pay attention to any RDS functionality present when purchasing the local communication station.

As a result of the small number of components required, it is possible to manufacture the device in a compact, lightweight and robust form and to adapt it to the situation in which it is used. Furthermore, the operation and the connection of the device are simple.

Preferably, the memory means are designed as a ROM memory. As a result, it is impossible for the contents of the memory means to be manipulated during use, but it is still simple to adapt the device to the latest standardized protocols by replacing the ROM memory.

In an embodiment of the device, the device furthermore comprises warning means. If data is detected of which the data protocol does not comply with the at least one standardized protocol, the user is warned, for example by visual and/or audible warning means. As a result, the user will always be warned if an attempt is made to manipulate the first communication station, even if an attempt is made in these circumstances to switch off indications of the first communication station.

A further embodiment of the device according to the invention comprises display means linked to the comparison/forwarding means, the

display means displaying data relating to the data communication traffic and the second communication station which are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol. This can be implemented, for example, as a display screen on the device itself.

As an addition, the device can be provided, in a further embodiment, with input means linked to the comparison/forwarding means for inputting commands relating to the display of the data.

An alternative embodiment of the invention is to provide it with interface means instead of the display means and/or the input means. Said interface means ensure the exchange of data relating to the data communication traffic and the second communication station with an external processing device, which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol. Said processing device may be, for example, a computer with which the data are processed further and can be displayed.

By means of the display of said data, the user is enabled to obtain as complete a picture as possible of the attempt to manipulate the local communication station, after which appropriate measures can be taken.

According to an embodiment of the invention, the device can be integrated with the local communication station.

The method and the device according to the invention will now be explained further by reference to the drawings.

Figure 1 shows a diagram of an embodiment according to the invention; and

Figure 2 shows a flow chart of the method according to the invention.

Figure 1 shows a diagram of a preferred embodiment according to the invention in which the device 10 for protecting data communication traffic is linked to a first communication station 11 and a second communication station 12. The device 10 comprises comparison/forwarding means 15 which can communicate during operation both with the first communication station 11 and the second communication station 12. The device 10 furthermore comprises memory means 14 linked to the comparison/forwarding means 15. In the preferred embodiment of the invention shown, the device 10 furthermore comprises warning means 16, display means 17 and input means 18, all linked to the

comparison/forwarding means 15. The communication stations 11 and 12 may be, for example, fax or copying machines provided with an RDS functionality.

In the memory means 14, the characteristics of the data communication are stored according to at least one standardized protocol. The comparison/forwarding means 15 serve to compare the data protocol of data which the second communication station wishes to dispatch to the first communication station 11 and to forward only data of which the data protocol complies with the at least one standardized protocol to the local communication station 11.

In the preferred embodiment shown, the device 10 also comprises warning means 16, which give a warning after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol. The figure indicates that the warning means 16 are implemented as a warning lamp. However, it is possible to use other visual or audible warning means for this purpose.

In the preferred embodiment of the invention shown, the device 10 also comprises display means 17 for displaying data relating to the data communication traffic and the second communication station 12 which have been stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol. Furthermore, the device comprises input means 18 for inputting commands relating to the display of the data. It is possible, for example, to input commands to display only a certain portion of the data on the display means.

In an embodiment of the invention not shown, the device 10 comprises, instead of the display means 17 and input means 18, interface means which can be linked to an external processing device. This processing device may be, for example, a computer with which the data can be processed further, stored and displayed.

Figure 2 shows the flow chart of the method according to the invention. The method begins with the reception of data from the second communication station 12 in block 1. In decision block 2, the data protocol of the data received in block 1 is compared with the standardized protocol. If the data protocol complies with the at least one standardized protocol, the data is forwarded to the first communication station 11 in forwarding block 3. The method then returns to block 1 to check the further data received.

If the data protocol does not comply with the at least one

standardized protocol, the method continues the procedure in warning block 4, in which the user is warned. The following step in the procedure comprises the interrupt block 6, in which the link to the second communication station is interrupted. In a preferred embodiment of the method according to the invention, in block 5, a data file is stored in which data of the data communication traffic and the second communication station are stored in parallel with warning block 4 and interrupt block 6.

Using the method and device shown in the figures for protecting data communication traffic, an attempt of a third party to switch on (concealed) functionality from the outside will be unsuccessful, as a result of which the probability that information can leak out via the communication equipment used becomes appreciably smaller.

As a result of warning the user and recording data relating to the data communication traffic and the second communication station 12, the user is enabled to obtain as complete a picture as possible of the user of the second communication station, after which appropriate measures can be taken.

An advantage of the device described is that the user can determine himself, regardless of the brand and type of appliance whether RDS functionality is permitted. Because the device can be used separately from the first communication station, there is no need to pay attention to any RDS functionality present when purchasing the first communication station. Of course, the device 10 can also be physically incorporated in the first communication station 11. In that case, the comparison/forwarding means 15 can form an integral component of a processor present in the first communication station 11.

As a result of the comparison of the data protocol of the received data with standardized protocols, the method according to the invention can be used worldwide.

As a result of the small number of components required, it is possible to manufacture the device in a compact, lightweight and robust form and to adapt it to the situation in which it is used. Furthermore, the operation and the connection of the device are simple.

If the memory means are designed as a ROM memory, it is impossible for the contents of the memory means 14 to be manipulated during use, but it is still simple to adapt the device to the latest standardized protocols by means of replacing the ROM memory.

Although the device has been described for the protection of

data communication traffic between two communication stations, it is, of course, also possible to protect the data communication traffic between a plurality of communication stations, such as, for example, in a network environment.

CLAIMS

1. Method for protecting data communication traffic between a first communication station (11) and a second communication station (12), in which the data is dispatched according to a data protocol from the second to the first communication station, characterized by the following steps:

(i) the comparison of the data protocol with at least one standardized protocol;

(ii) the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station (11).

2. Method according to Claim 1, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, a warning is generated.

3. Method according to Claim 1 or 2, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, the data communication traffic is interrupted.

4. Method according to one of the preceding claims, characterized in that, after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol, a data file containing data of the data communication traffic and the second communication station (12) is stored.

5. Device for protecting data communication traffic between a first communication station (11) and a second communication station (12), data being dispatched according to a data protocol from the second to the first communication station, characterized in that the device (10) comprises:

- memory means (14) in which data characteristics of at least one standardized protocol are stored;

- comparison/forwarding means (15) for the comparison of the stored data characteristics with the data protocol and the forwarding only of data of which the data protocol complies with the at least one standardized protocol to the first communication station (11).

6. Device according to Claim 5, characterized in that the device furthermore comprises warning means (16) linked to the comparison/forwarding means (15) which give a warning after it has emerged during the comparison of the data protocol that it does not

belong to the at least one standardized protocol.

7. Device according to Claim 5 or 6, characterized in that the device furthermore comprises display means (17) linked to the comparison/forwarding means (15), the display means (17) displaying data relating to the data communication traffic and the second communication station (12), which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol.

8. Device according to Claim 7, characterized in that the device furthermore comprises input means (18) linked to the comparison/forwarding means (15) for inputting commands relating to the display of the data.

9. Device according to Claim 5 or 6, characterized in that the device comprises interface means for exchanging data relating to the data communication traffic and the second communication station (12) with an external processing device, which data are stored after it has emerged during the comparison of the data protocol that the latter does not comply with the at least one standardized protocol.

10. Device according to one of Claims 5 to 9, characterized in that the device (10) is integrated in the first communication station (11).

Fig 1

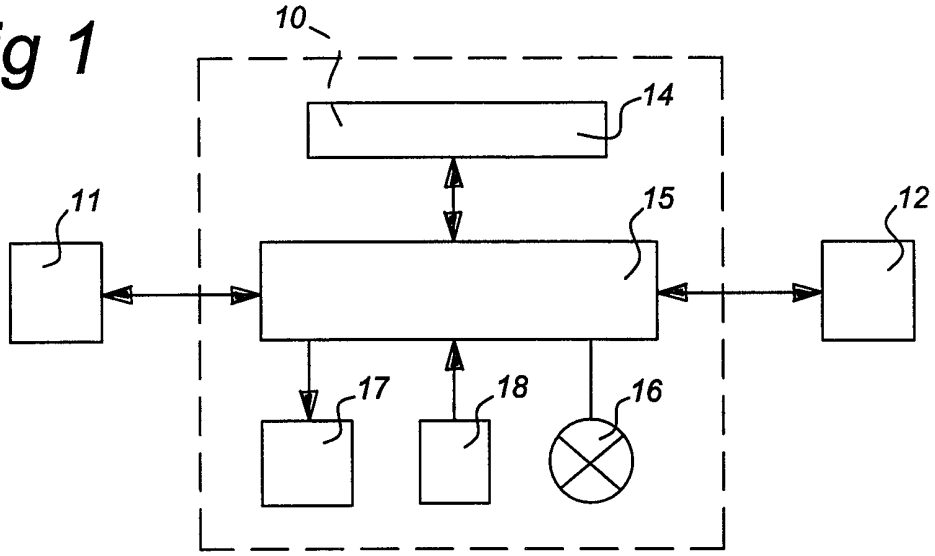
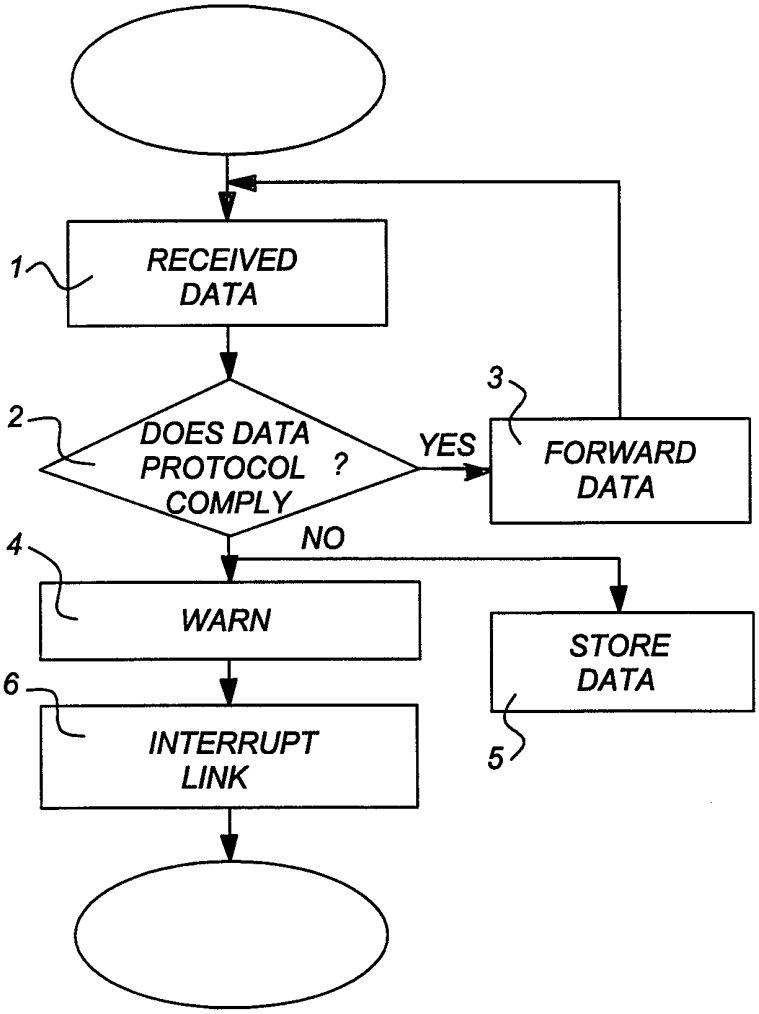

10
14
11
15
12
17
18
16

Fig 2


RECEIVED DATA
1
DOES DATA PROTOCOL COMPLY ?
2
YES
3
FORWARD DATA
NO
4
WARN
STORE DATA
5
6
INTERRUPT LINK

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/NL 98/00581

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06 G03G15/00 H04N1/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04M G03G H04N G06G G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 5 124 984 A (ENGEL FERDINAND) 23 June 1992 see abstract see column 1, line 12-66 see column 2, line 38 - column 5, line 7 see column 6, line 35-55 see column 8, line 30 - column 12, line 18 see figures 1,2 ---	1-3,5 4,6,9,10
Y A	US 5 675 510 A (COFFEY STEVEN R ET AL) 7 October 1997 see abstract see column 2, line 34 - column 3, line 5 ---	4,9 7,8
Y	US 5 057 941 A (MORIYA DAISUKE) 15 October 1991 see abstract see column 2, line 7-23 --- -/--	6

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 March 1999	17/03/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lievens, K

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/NL 98/00581

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 245 658 A (BUSH GEORGE ET AL) 14 September 1993 see column 5, line 39 - column 6, line 15 ---	10
A	US 5 337 349 A (FUROHASHI IKUKO ET AL) 9 August 1994 see abstract see column 1, line 55 - column 2, line 3 ---	7,8
A	US 5 226 074 A (HAN SANG-HO) 6 July 1993 see abstract see column 1, line 33-44 ---	1-10
A	EP 0 509 525 A (CANON KK) 21 October 1992 see abstract see column 2, line 44 - column 3, line 20 ---	1-10
A	GB 2 265 158 A (TOKYO SHIBAURA ELECTRIC CO) 22 September 1993 see abstract see page 1, line 1 - page 3, line 12 ---	10
A	US 4 805 206 A (BEOM-CHAE JEONG) 14 February 1989 see abstract see column 4, line 40-49 -----	1-10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ional Application No
PCT/NL 98/00581

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5124984 A	23-06-1992	WO 9203001 A	20-02-1992
US 5675510 A	07-10-1997	AU 701813 B	04-02-1999
		AU 6273996 A	30-12-1996
		CA 2223919 A	19-12-1996
		DE 843946 T	04-03-1999
		EP 0843946 A	27-05-1998
		JP 10510647 T	13-10-1998
		NO 975728 A	06-02-1998
		WO 9641495 A	19-12-1996
US 5057941 A	15-10-1991	JP 3010448 A	18-01-1991
		DE 69025648 D	11-04-1996
		DE 69025648 T	02-10-1996
		EP 0401804 A	12-12-1990
US 5245658 A	14-09-1993	NONE	
US 5337349 A	09-08-1994	JP 5145658 A	11-06-1993
		JP 5145694 A	11-06-1993
US 5226074 A	06-07-1993	DE 4108127 A	05-03-1992
		FR 2666469 A	06-03-1992
		GB 2249457 A,B	06-05-1992
		JP 2525084 B	14-08-1996
		JP 6090317 A	29-03-1994
EP 0509525 A		NONE	
GB 2265158 A	22-09-1993	JP 5317571 A	03-12-1993
		KR 9701016 B	25-01-1997
US 4805206 A	14-02-1989	NONE	