(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 June 2006 (29.06.2006)

PCT

(10) International Publication Number
WO 2006/066315 A1

(51) International Patent Classification:
G06F 13/00 (2006.01)

(21) International Application Number:
PCT/AU2005/001912

(22) International Filing Date:
16 December 2005 (16.12.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2004907200 20 December 2004 (20.12.2004) AU

(71) Applicant *(for all designated States except US)*: **WEB-TRAF RESEARCH PTY LTD** [AU/AU]; 47 Bourbong Street, Bundaberg, QLD 4670 (AU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HOLLIS, Arron** [AU/AU]; 10 Hampson Street, Burnett Heads, QLD 4670 (AU). **WILTSHIER, Matthew, Ross** [AU/AU]; 115 Freshwater Court, Baffle Creek, Rosedale, QLD 4674 (AU). **SMIDT, Jeffrey** [AU/AU]; 10 Hampson Street, Bundaberg, QLD 4670 (AU).

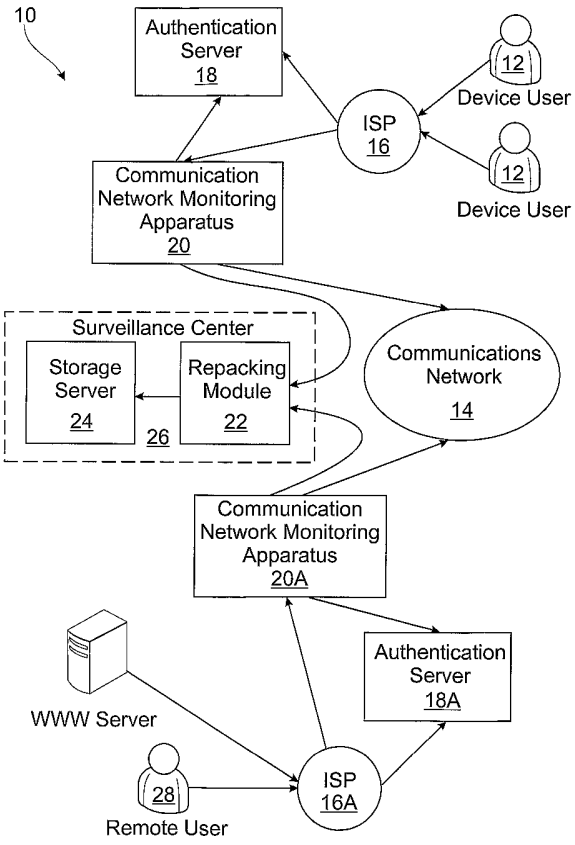
(74) Agent: **FISHER ADAMS KELLY**; Level 29, Comalco Place, 12 Creek Street, Brisbane, QLD 4001 (AU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT,

[Continued on next page]

(54) Title: COMMUNICATIONS NETWORK MONITORING SYSTEM, METHOD & APPARATUS



(57) Abstract: A system and method for monitoring a user of a communication network (14), comprises at least one monitoring apparatus (2) in communication with the communications network and a user device (12) coupled to the communications network, the at least one user device requiring entry of at least one authentication code to permit communication via the communications network. A repacking module (22) is coupled to be in communication with the at least one monitoring apparatus and a storage server (24) is in communication with the repacking module. The at least one monitoring apparatus reads headers of all packets of data transmitted to and/or from the at least one user device without affecting the transmission of the packets of data, analyses at least one component of the packets of data to determine one or more patterns between the different packets of data and determines users to be monitored from the patterns.

WO 2006/066315 A1

RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TITLE

COMMUNICATIONS NETWORK MONITORING SYSTEM, METHOD AND APPARATUS

FIELD OF THE INVENTION

The present invention relates to a communications network monitoring system, method and apparatus. In particular, but not exclusively, the present invention relates to a system, method and apparatus for covertly detecting and monitoring communications to, from and between users of concern/interest in a communications network.

BACKGROUND TO THE INVENTION

The ubiquitous nature of communications networks such as the World Wide Web, wireless and wired communications networks make them an attractive tool for the pursuit of undesirable and illegal activities such as organised crime, terrorism, paedophilia and undesirable espionage. In addition to threats originating in traditional ways, law enforcement and intelligence agencies are presented with the task of detecting, monitoring and preventing or attempting to prevent the aforementioned threats manifest over communications networks.

The ease with which such networks can be utilised by the everyday user, the availability of complex methods of encryption and the myriad different communication methods, such as email, virtual instant messaging and VoIP, to name but a few, exacerbate the problem faced by authorities of obtaining evidence of wrongdoing that is admissible in a court of law.

Existing methods of identifying and tracking nefarious activity on communications networks at internet gateways and/or across public or private network gateways include a number of drawbacks.

Difficulties in tracking include finding the source of spoofed IP addresses and the use of proxy servers to hide users' IP addresses.

Covert monitoring of communications network traffic places high demands on personnel. For example, covert monitoring of traffic at an Internet Service Provider (ISP) level currently requires a person to be physically present at the premises of the ISP, providing they have first obtained a court order permitting them to gain access and conduct monitoring where necessary. The person needs to electronically intercept the packets of data, which requires a lot of processing power and can noticeably degrade the performance of the ISP. Not only is the performance degradation commercially undesirable for the ISP, but it can alert users engaging in illegal behaviour to the covert monitoring thus prompting the users to suspend their activities to avoid detection.

Successful monitoring at the ISP level relies on the ISP maintaining security, which cannot be guaranteed. Breaches in security significantly reduce detection and prevention rates. Dishonest ISPs have been known to re-route traffic in an attempt to protect users.

Surveillance and monitoring of communications network traffic also requires expensive equipment to be deployed and the coordination of personnel and reporting. Furthermore, such equipment is not always capable of discovering undesirable and/or illegal behaviour because of, for example, difficulties in dealing with higher levels of encryption on the fly. Conventionally,

time is required to break such encryption, but such delays can alert users to the presence of surveillance and monitoring.

Routing protocols are known, such as "route always", "route never" and "route copy", which are used in routing data in communications networks. For example, the "route always" protocol always routes data via a specified route or to a specified destination, whereas the "route never" protocol never routes data to a particular destination or via a specified route. The "route copy" protocol makes a copy of data before routing. One problem with these protocols is their lack of selectivity in routing the data. For example, either all or none of the data is routed in a particular direction or all or none of the data is copied, which can lead to storage capacity problems because of the large amount of data being copied. This can additionally create undesirable levels of load on the network due to the proportional increase of data resulting from "route copy" activities. Furthermore, the majority of the data is likely to be irrelevant because all of the data is being copied and not selected data of interest.

Hence, there is a need for a communications network monitoring system and/or method and/or apparatus to address or at least ameliorate one or more of the aforementioned problems of the prior art.

In this specification, the terms "comprises", "comprising" or similar terms are intended to mean a non-exclusive inclusion, such that a method, system or apparatus that comprises a list of elements does not include those elements solely, but may well include other elements not listed.

SUMMARY OF THE INVENTION

In one form, although it need not be the only or indeed the broadest form, the invention resides in a system for monitoring at least one user of a communications network, said system comprising:

at least one monitoring apparatus coupled to be in communication with the communications network;

at least one user device coupled to be in communication with the communications network, the at least one user device requiring entry of at least one authentication code to permit communication via the communications network;

a repacking module coupled to be in communication with the at least one monitoring apparatus; and

a storage server coupled to be in communication with the repacking module;

wherein the at least one monitoring apparatus:

reads headers of all packets of data transmitted to and/or from the at least one user device without affecting the transmission of the packets of data;

analyzes at least one component of the packets of data to determine one or more patterns between the different packets of data; and

determines users to be monitored from the one or more patterns.

Suitably, the authentication code authenticates the user device.

Suitably, the authentication code authenticates the user of the user device.

Suitably, the communications network is the Internet and the user device is coupled to be in communication with the communications network via an

internet service provider.

Suitably, the at least one monitoring apparatus is physically connected to transmission and reception lines of the internet service provider.

Suitably, the at least one monitoring apparatus is physically connected to transmission and reception lines of an authentication server associated with the internet service provider.

In another form, the invention resides in an apparatus for monitoring at least one user of a communications network, the apparatus comprising a kernel for reading headers of all packets of data transmitted to and/or from a user device of the at least one user, analyzing at least one component of the packets of data to determine one or more patterns between the different packets of data and determining users to be monitored from the one or more patterns.

In a further form, the invention resides in a method for monitoring communications over a communications network via a monitoring apparatus coupled to be in communication with the communications network, at least one user device coupled to be in communication with the communications network, the at least one user device requiring entry of at least one authentication code to permit communication via the communications network, the method including:

reading headers of all packets of data transmitted to and/or from the at least one user device without affecting the transmission of the packets of data;

analyzing at least one component of the packets of data to determine one or more patterns between the different packets of data; and

determining users to be monitored from the one or more patterns.

The method may further include reading all payloads of packets of data transmitted to and/or from the user device of a user being monitored.

The method may further include copying at least some of the payloads of the packets of data transmitted to and/or from the user device of the user being monitored.

The method may further include transmitting the copied packets of data from the monitoring apparatus to a repackaging module coupled to be in communication with the monitoring apparatus.

The method may further include reconstructing the copied packets of data in the repackaging module into user readable format.

The method may further include dynamically allocating bandwidth available to one or more user devices on the basis of monitoring the one or more user devices.

The method may further include comparing a volume of traffic logged by the at least one monitoring apparatus with a volume of traffic logged by a telecommunications company to determine if the at least one monitoring apparatus is being circumvented.

The method may further include categorizing a user as a user of concern/interest when analysis of the at least one component of the packets of data determines that the user has communicated with a particular entity a threshold number of times.

Further features of the present invention will become apparent from the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

By way of example only, preferred embodiments of the invention will be described more fully hereinafter with reference to the accompanying drawings,

wherein:

FIG. 1 shows a schematic representation of the system according to an embodiment of the invention;

FIG. 2 is a flowchart illustrating the method according to two embodiments of the invention;

FIG. 3 is a schematic representation of a standard data packet;

FIG. 4 is a schematic representation of the IP header of the data packet of FIG. 3; and

FIG. 5 is a schematic representation of the TCP header of the data packet of FIG. 3.

DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG. 1, in accordance with an embodiment of the present invention, there is provided a system 10 comprising at least one user device 12 coupled to be in communication with a communications network 14. The user device 12 can be a desktop or tablet personal computer (PC), a laptop computer, a landline telephone, a VoIP telephone, a personal digital assistant (PDA), or other suitably enabled mobile communication device, such as a mobile telephone. The communications network 14 may be a global communications network, such as the Internet, or a conventional telephone network or a mobile telephone network.

The present invention will be described with reference to an embodiment in which the user devices are computers that are coupled to be in communication with the communications network via an ISP 16. However, it will be appreciated that the invention is not limited to this embodiment.

Communication between the user device 12, ISP 16 and the communications network 14 may be via wireless communication using one of the communications protocols known to persons skilled in the art or may be via wired communication (optionally including optical fibre communication) or a combination of the two, such as wireless communication between the user device 12 and the ISP 16 and wired communication between the ISP 16 and the communications network 14 or vice versa.

Each ISP 16 includes an authentication server 18, which is shown separate from the ISP 16 in FIG. 1 for the sake of clarity. System 10 includes at least one communications network monitoring apparatus 20 coupled to be in communication with the ISP 16, including their authentication server 18, and the communications network 14. Monitoring apparatus 20 is also coupled to be in communication with repacking module 22. Repacking module 22 is coupled to be in communication with storage server 24 in which data can be stored and retrieved. Repacking module 22 and storage server 24 may be located at a surveillance centre 26 where collected information can be processed and analysed. System 10 can include at least one remote user device 28 coupled to be in communication with a second ISP 16A and a second monitoring apparatus 20A coupled to be in communication with authentication server 18A of ISP 16A and communications network 14.

The monitoring apparatus 20 can be in the same location as, or remote from, the ISP 16, but in each case is preferably coupled to be in communication with the authentication server 18. When in the same location as the ISP 16, the monitoring apparatus 20 is physically connected to the transmission and reception lines of the authentication server 18 such that all incoming and

outgoing traffic can be monitored. However, it should be noted that in some cases it may not be possible to connect directly to the authentication server 18. In this case, the information necessary to perform the invention is still obtainable from the headers of the packets of data transmitted via the ISP 16 and the further detail that is obtainable from a direct connection to the authentication server 18 to identify the user and their address and other such personal information can be obtained from the ISP 16 at a later date.

According to one embodiment, the monitoring apparatus 20 can be installed via a conventional bootable flash memory familiar to persons skilled in the art and does not require any other specialist software to be installed on the ISP 16 and reconfiguration of the ISP is not required. However, as specified above, connection to the authentication server 18 is required to obtain all the personal details of a user. The monitoring apparatus 20 works with any program or device that works over Internet Protocol (IP) configuration or Packet Switched Networks. The monitoring apparatus 20 only comprises RAM and communicates with boot ROM in the storage server 24 to upload the necessary encrypted software for reading packets of data, performing analysis of data to determine patterns and users of concern/interest as described below. Therefore, if the monitoring apparatus 20 is stolen from the ISP 16, no valuable information would remain in the monitoring apparatus 20 because it only comprises ROM.

Referring to FIG. 2, when a user 12 connects 100 to the ISP 16, the authentication server 18 authenticates 102 the user typically by verification of a username and password, although this could be by other means such as, but not limited to, an identifying numerical or alphanumerical code and other such combinations that may or may not be secured via a checksum or algorithm. The

user device requires entry of at least one authentication code to permit communication via the communications network. In one embodiment, the authentication code authenticates the user device. In another embodiment, the authentication code authenticates the user of the user device. In a further embodiment, both the user and the user device are authenticated.

Upon successful authentication 104, the ISP 16 permits the user to access the communications network 14. If authentication is unsuccessful, the user may retry. Since the monitoring apparatus 20 is coupled to be in communication with the ISP 16, all traffic communicated via the ISP is transmitted through the monitoring apparatus 20. Since the monitoring apparatus 20 is coupled to the authentication server 18, the monitoring apparatus 20 is able to identify users 12 by recording 106 the authentication details provided by the user 12.

According to one embodiment, initially the monitoring apparatus 20 monitors 108 all traffic flowing through the ISP 16 from which traffic patterns can be identified 110. With reference to FIGS 3-5, monitoring is carried out by reading the IP header 200 and the TCP header 201 of the data packet 204. Under current legislation, without specific authorization, it is not permissible to view the contents of the communications stored in the payload 202 of the data packet 204, however this can be copied for later inspection. Regarding monitoring, for example, a frequency of visits to a destination of concern, such as a particular website, can be monitored. The user visiting the website of concern can be traced and if the frequency of visits exceeds a threshold, the user can be placed on, for example, a list of users of concern/interest. The threshold may be set at zero such that any visit to a particular website causes

the user to be included on the list. Alternatively, the threshold may be set at one to account for accidental visits to a particular website and to account for automatic redirects to the website of concern that are not the responsibility of the user. In another embodiment, the threshold can be set at another predetermined figure such as 5 visits per month or other such frequency. In another example, a user may send or receive images on a regular basis to or from one or more users or sources already under surveillance and such activity would cause the user not already under surveillance to be entered on the list.

This enables the determination 112 of users of interest/suspicion/concern who may be placed on a list to be monitored. The monitoring apparatus 20 will then monitor 114 all traffic to and from this user, which may include, but is not limited to, emails sent and received by the user, attachments thereto, images downloaded and/or uploaded by the user, the size and type of such files/data, information relating to users with whom the user of interest has been communicating, and other relevant information.

In an alternative embodiment, a user may already be of interest or concern on the basis of behaviour identified prior to installation of the monitoring apparatus 20. In this case, the user's activity can be monitored 114 from the outset.

The monitoring apparatus 20 copies 116 the packets of data 204 being transmitted to and from the user being monitored and transmits 118 the copied data packets to the repacking module 22, which reconstructs 120 the packets of data into human readable/viewable format. The reconstructed data can then be viewed in real time or substantially real time and/or can be stored 122 in storage server 24. Where the data is encrypted, it is likely the data will be stored in

storage server 24 for subsequent decryption and analysis. However, the data need not be encrypted.

In the case of peer to peer traffic, i.e. where the user of interest is communicating with a remote user 28, the monitoring apparatus 20 coupled to be in communication with the ISP 16 of the user of interest attempts communication with the second monitoring apparatus 20A coupled to be in communication with the second ISP 16A to which the remote user 28 is connected. Where connection to the second monitoring apparatus 20A is successful, identity information relating to the remote user 28 can be sent by the second monitoring apparatus 20A to the repacking module 22.

As packets of data 204 pass through the kernel of the monitoring apparatus 20, the size of each packet is extracted and then collated to provide usage records at a very high level of speed and accuracy. Typically traffic can be accurately recorded at speeds far in excess of 200Mb/s, but speeds are envisaged to increase as technology develops. Further speed increases are envisaged to be achievable by conversion to enable execution in solid state processors. The kernel inspects each packet header 200, 201 for its destination address enabling reading of the packets without slowing the network and enabling the present invention to maintain monitoring performance as networks and traffic volumes grow. The data packets 204 are read and, as required, all or parts of the selected packets 204 or their contents or string(s) are copied or mirrored and sent to the repacking module 22 and the storage server 24. According to one embodiment, in a proactive mode of operation in which all traffic is being monitored and no particular users are being monitored, only the headers 200, 201 of the data packets 204 are read and optionally copied.

However, once authorisation is provided to monitor a particular user, the payload 202 can also be read and copied.

Address spoofing by a proxy server can be detected by the present invention and the traffic recorded regarding the user and/or account at the ISP by extracting the source and destination from the data packets. This can be done providing the monitoring apparatus 20 is installed in the system 10 before the user's traffic reaches the proxy server. In the event of a proxy server being installed between the user and the monitoring apparatus 20, the monitoring apparatus would identify such destination traffic from a proxy server and a remedy could be sought. The destination and origin of such traffic will be in common, these being the IP address of the proxy server.

Monitoring apparatus 20 is also optionally capable of dynamically controlling and allocating bandwidth available to terminals with which the monitoring apparatus 20 is coupled to be in communication. Bandwidth may be controlled to individual user devices on a per user basis or on a group basis, such as all user devices coupled to be in communication with a specific ISP. Therefore, when, for example, there is a real threat to national security involving communications networks, the apparatus 20 can be employed to restrict bandwidth availability or to share bandwidth that is not required for those services, such as governmental services, requiring communications capability. This means that civil networks, whilst being dynamically controlled, could be allowed to continue partially or, if the need is such, to fully commandeer all such resources for matters of national urgency/priority. Additionally, this provides the ability to block communications or connections of an undesirable nature.

The monitoring apparatus 20 and method of the present invention could

also be applied to client software for the tracking of individual computers or for applications controlling internal or local traffic. The apparatus and method may process all or selective data and store such data on location for manual collection such as, for example, within or attached to a Wide Area Network (WAN) that has no connection to external networks such as, but not limited to, the internet. It should be appreciated that the monitoring apparatus 20, repacking module 22 and storage server 24 could be present in a single device.

Hence, the method, system and apparatus of the present invention thus provide a solution to the aforementioned problems of the prior art by identifying specific users of interest and monitoring their activity on the communications network. This may be achieved by monitoring some or all of the traffic and identifying patterns in the traffic or by monitoring one or more specific users known to be of concern from the outset. Since the present invention copies the data packets and no degradation in the performance of the ISP is experienced, users can be monitored covertly without alerting the users to the presence of the monitoring. Routing tables will also show no evidence that a user is being monitored because the routing tables will show that data packets are being routed normally. Once the apparatus is installed at the ISP, personnel do not need to be present and traffic can be monitored remotely. This reduces demands on personnel and the risk of raising suspicion. Specific users can be monitored and therefore only selected data needs to be stored relating to specific users and/or specific activities and not all data transmitted through a specific route, thus addressing the storage capacity problems of the prior art.

In the event that the ISP is dishonest and, for example, re-routes traffic such that it is not monitored by the monitoring apparatus 20, this is detectable by

comparing the volume of traffic logged by the telecommunications company providing the infrastructure for the ISP with the volume of traffic logged by the monitoring apparatus 20. The two volumes should be the same. However, where less traffic passes through the monitoring apparatus 20 than the telecommunications company, this suggests that the ISP is circumventing the monitoring apparatus 20 by re-routing data.

The data stored in the storage server 24 will comprise a date and time stamp relating to its acquisition thus making the electronic evidence more readily acceptable in a court of law.

It is currently difficult and manpower intensive to collect evidence, especially "Best Evidence", sufficient to justify the issue of legal and/or ethical permission to invade privacy. The initial monitoring and building of profiles will greatly reduce such costs and dramatically improve the efficiency and effectiveness of such activities whilst reducing current response times on such matters.

Throughout the specification the aim has been to describe the invention without limiting the invention to any one embodiment or specific collection of features. Persons skilled in the relevant art may realize variations from the specific embodiments that will nonetheless fall within the scope of the invention.

CLAIMS:

1. A system for monitoring at least one user of a communications network, said system comprising:

at least one monitoring apparatus coupled to be in communication with the communications network;

at least one user device coupled to be in communication with the communications network, the at least one user device requiring entry of at least one authentication code to permit communication via the communications network;

a repacking module coupled to be in communication with the at least one monitoring apparatus; and

a storage server coupled to be in communication with the repacking module;

wherein the at least one monitoring apparatus:

reads headers of all packets of data transmitted to and/or from the at least one user device without affecting the transmission of the packets of data;

analyzes at least one component of the packets of data to determine one or more patterns between the different packets of data; and

determines users to be monitored from the one or more patterns.

2. The system of claim 1, wherein the authentication code authenticates the user device.

3. The system of claim 1, wherein the authentication code authenticates the user of the user device.

4. The system of claim 1, wherein the communications network is the Internet and the user device is coupled to be in communication with the communications network via an internet service provider.

5. The system of claim 4, wherein the at least one monitoring apparatus is physically connected to transmission and reception lines of the internet service provider.

6. The system of claim 5, wherein the at least one monitoring apparatus is physically connected to transmission and reception lines of an authentication server associated with the internet service provider.

7. An apparatus for monitoring at least one user of a communications network, the apparatus comprising a kernel for reading headers of all packets of data transmitted to and/or from a user device of the at least one user, analyzing at least one component of the packets of data to determine one or more patterns between the different packets of data and determining users to be monitored from the one or more patterns.

8. A method for monitoring communications over a communications network via a monitoring apparatus coupled to be in communication with the communications network, at least one user device coupled to be in

communication with the communications network, the at least one user device requiring entry of at least one authentication code to permit communication via the communications network, the method including:

reading headers of all packets of data transmitted to and/or from the at least one user device without affecting the transmission of the packets of data;

analyzing at least one component of the packets of data to determine one or more patterns between the different packets of data; and

determining users to be monitored from the one or more patterns.

9. The method of claim 8, further including reading all payloads of packets of data transmitted to and/or from the user device of a user being monitored.

10. The method of claim 8, further including copying at least some of the payloads of the packets of data transmitted to and/or from the user device of the user being monitored.

11. The method of claim 8, further including transmitting the copied packets of data from the monitoring apparatus to a repackaging module coupled to be in communication with the monitoring apparatus.

12. The method of claim 8, further including reconstructing the copied packets of data in the repackaging module into user readable format.

13. The method of claim 8, further including dynamically allocating bandwidth available to one or more user devices on the basis of monitoring the one or more user devices.

14. The method of claim 8, further including comparing a volume of traffic logged by the at least one monitoring apparatus with a volume of traffic logged by a telecommunications company to determine if the at least one monitoring apparatus is being circumvented.

15. The method of claim 8, further including categorizing a user as a user of concern/interest when analysis of the at least one component of the packets of data determines that the user has communicated with a particular entity a threshold number of times.

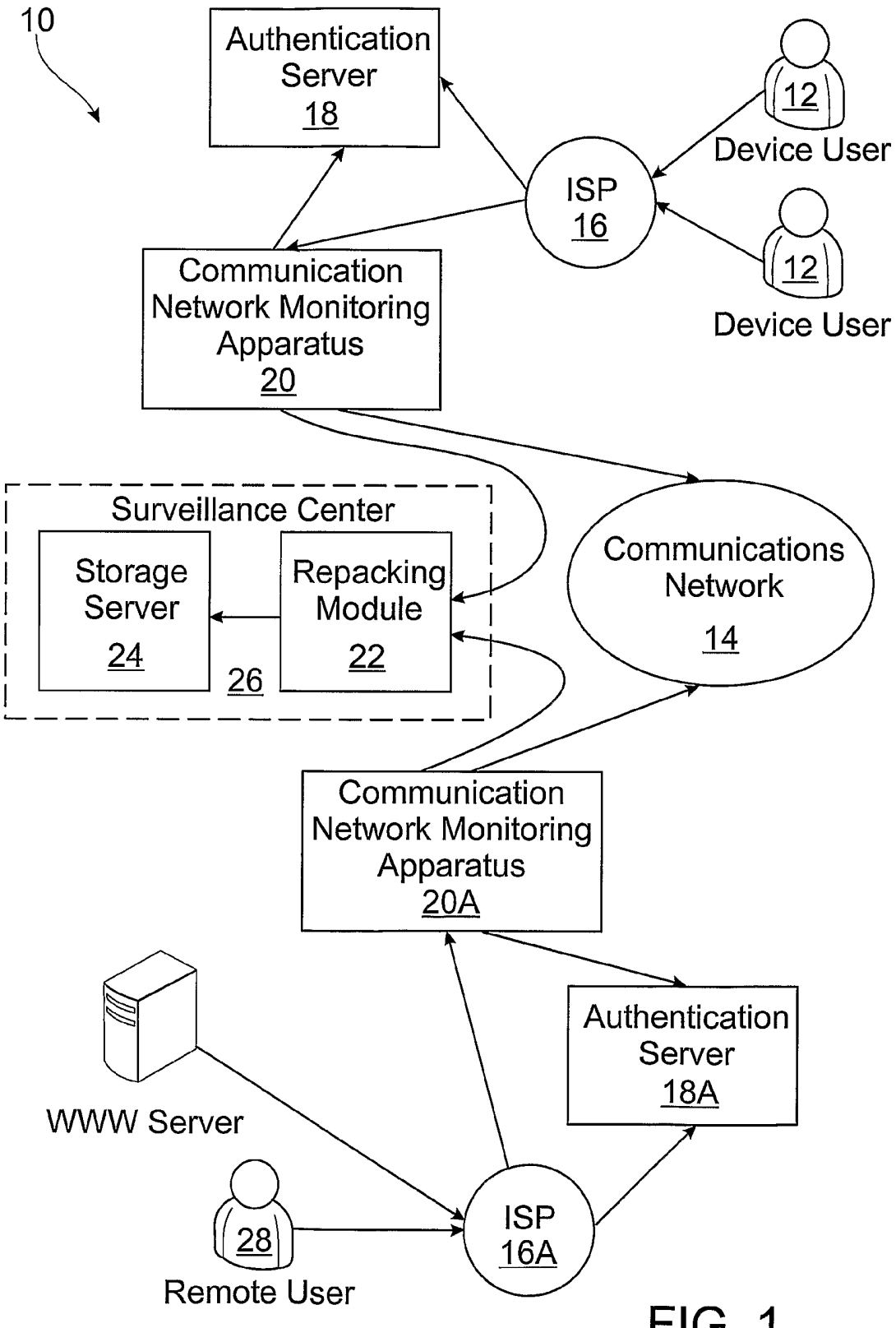

10
Authentication Server 18
12
Device User
ISP 16
12
Device User
Communication Network Monitoring Apparatus 20
Surveillance Center
Storage Server 24
Repacking Module 22
26
Communications Network 14
Communication Network Monitoring Apparatus 20A
Authentication Server 18A
WWW Server
28
Remote User
ISP 16A

FIG. 1

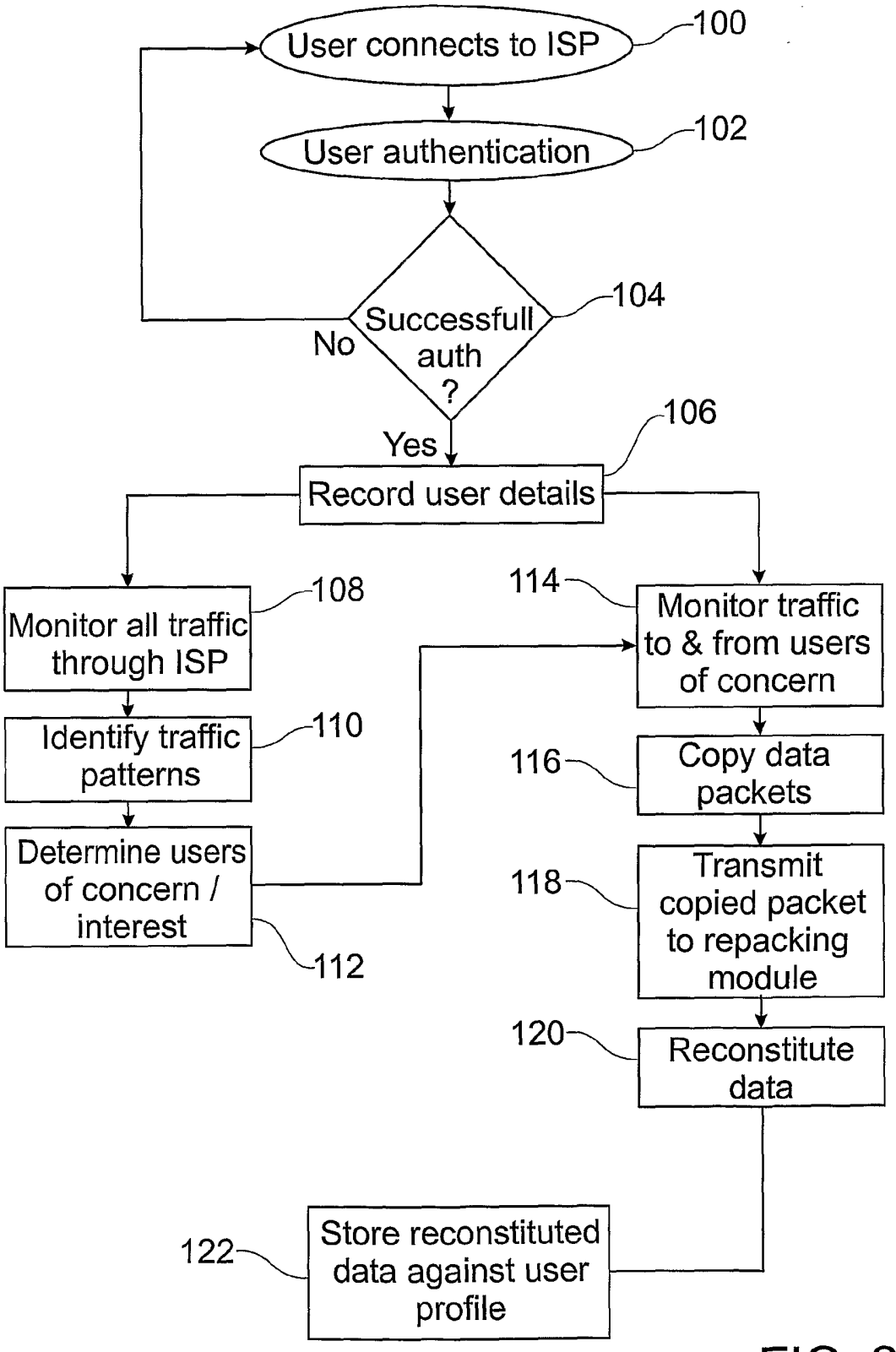

User connects to ISP
100
User authentication
102
Successfull auth ?
104
No
Yes
Record user details
106
Monitor all traffic through ISP
108
Identify traffic patterns
110
Determine users of concern / interest
112
114
Monitor traffic to & from users of concern
116
Copy data packets
118
Transmit copied packet to repacking module
120
Reconstitute data
122
Store reconstituted data against user profile

FIG. 2

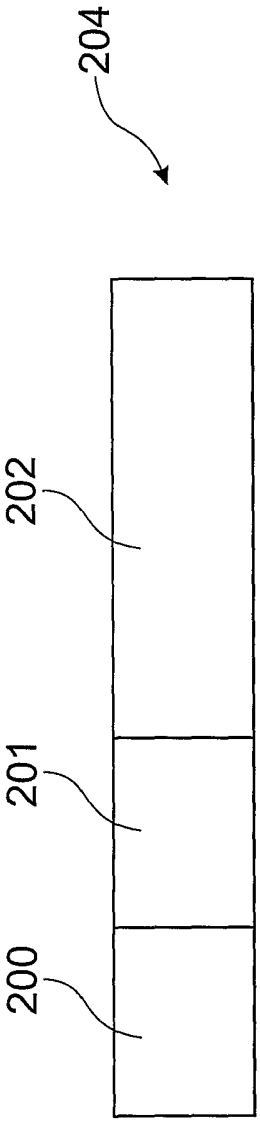

204
202
201
200

FIG. 3

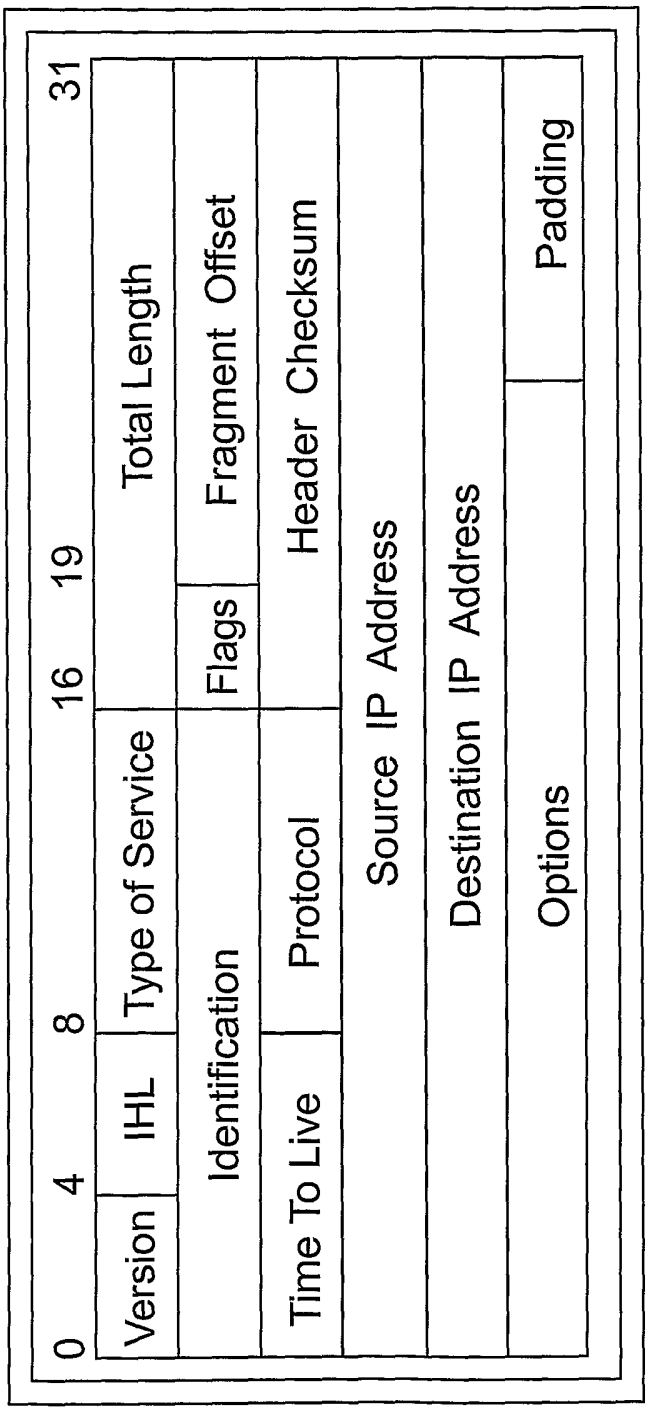

0
4
8
16
19
31
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time To Live
Protocol
Header Checksum
Source IP Address
Destination IP Address
Options
Padding

FIG. 4

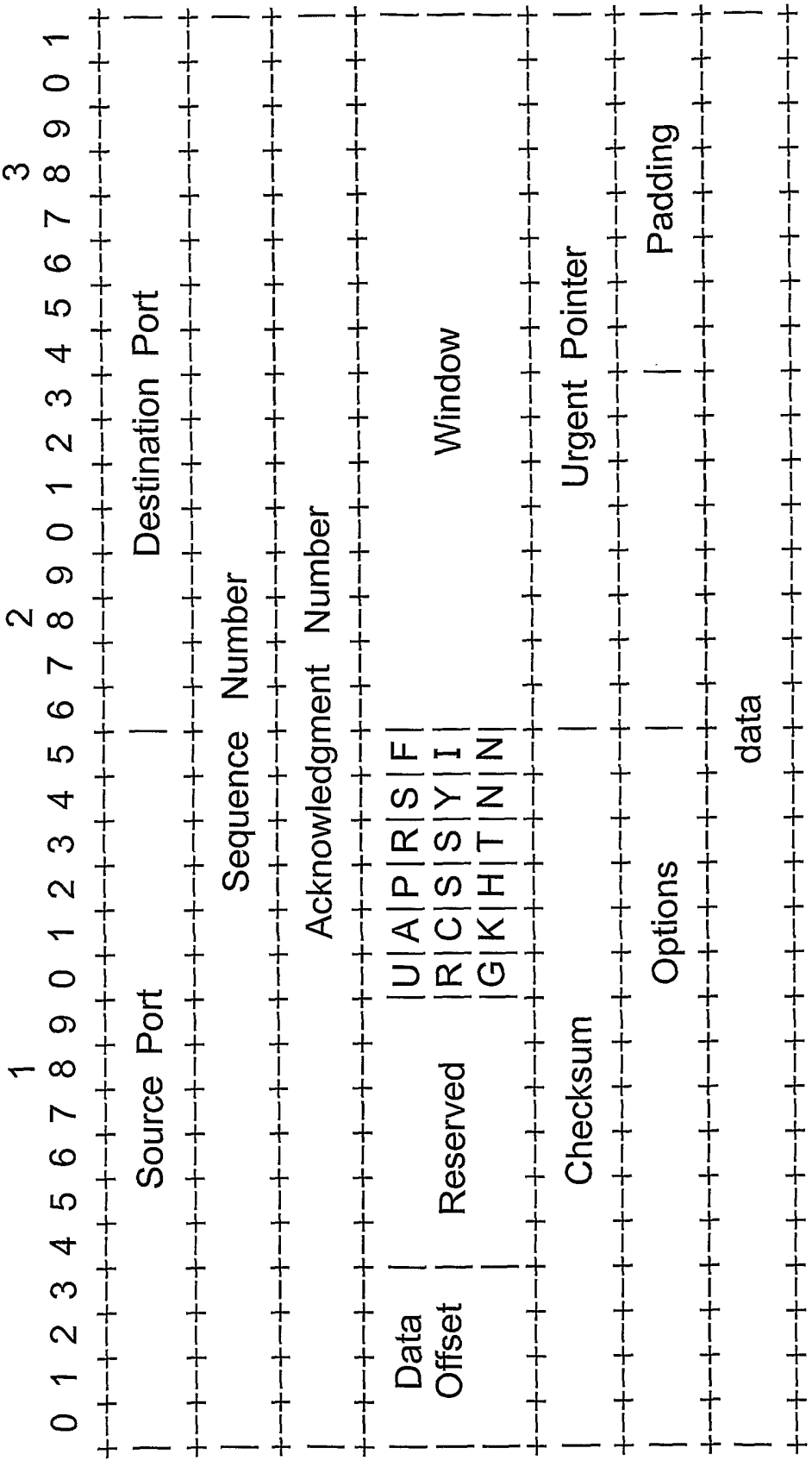

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Source Port
Destination Port
Sequence Number
Acknowledgment Number
Data Offset
Reserved
U A P R S F
R C S S Y I
G K H T N N
Window
Checksum
Urgent Pointer
Options
Padding
data

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2005/001912

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

G06F 13/00 (2006.01)

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)

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 practicable, search terms used)
WPAT: network, internet, monitor, surveillance, header, packet, pattern, analyse, server and similar terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2001/001272 A2 (APPTITUDE INC), 4 January 2001 (Pages 1 – 17, 24 – 33, 38 -50)	1 – 15
A	US 6182146 B1 (GRAHAM-CUMMING, JR), 30 January 2001. Whole document	1 – 15
A	US 5787253 A (McCREERY et al), 28 July 1998. Whole document	1 – 15

☐ Further documents are listed in the continuation of Box C ☒ See patent family 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 application or patent but published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
02 February 2006	10 FEB 2006
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	**DEREK BARNES** Telephone No : (02) 6283 2198

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU2005/001912

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	2001001272	AU	60685/00	CN	1399742	CN	1571403
		CN	1571404	CN	1574789	CN	1578259
		CN	1578260	EP	1196856	US	6651099
		US	6665725	US	6771646	US	6789116
		US	6839751	US	6954789	US	2004083299
		US	2004199630				
US	6182146						
US	5787253						

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX