(12) UK Patent Application (19) GB (11) 2 374 493 (13) A

(43) Date of A Publication 16.10.2002

(21) Application No 0109241.0

(22) Date of Filing 12.04.2001

(71) Applicant(s)
Mitel Knowledge Corporation
(Incorporated in Canada - Ontario)
350 Legget Drive, P.O. Box 13089,, Kanata, Ontario,
K2K 2W7, Canada

(72) Inventor(s)
Tonis Kasvand
Audil Virk
David Fram
James Hughes
Jon Moller
Kristan Stewart
Ryan Taylor

(74) Agent and/or Address for Service
Venner Shipley & Co
20 Little Britain, LONDON, EC1A 7DH,
United Kingdom

(51) INT CL^7
H04Q 7/34 // H04L 12/26 12/28

(52) UK CL (Edition T)
H4L LRNX

(56) Documents Cited
WO 2000/047003 A
WO 1996/016516 A
WO 2000/040049 A
US 5857190 A

(58) Field of Search
UK CL (Edition S) H4K KFMA , H4L LFMX LRNMT LRNR LRNX , H4P PPG
INT CL^7 H04L 12/26 12/28 , H04M 3/22 , H04Q 3/00 7/34
Online: WPI, EPODOC, JAPIO, INSPEC

(54) Abstract Title
Mobile interactive logging (MILog) of network devices

(57) A network administration system for an ad-hoc or 'sporatic' network where all logs are received and sent through a MILog agent at each network device. The MILog agents route and filter logs accordingly to instructions received via Mobile Interactive Logs (MILogs), and further provide other services such as creating MILogs. A user is able to create and dispatch a MILog at any time to any MILog-compliant component from a MILog agent authorized to create MILogs.

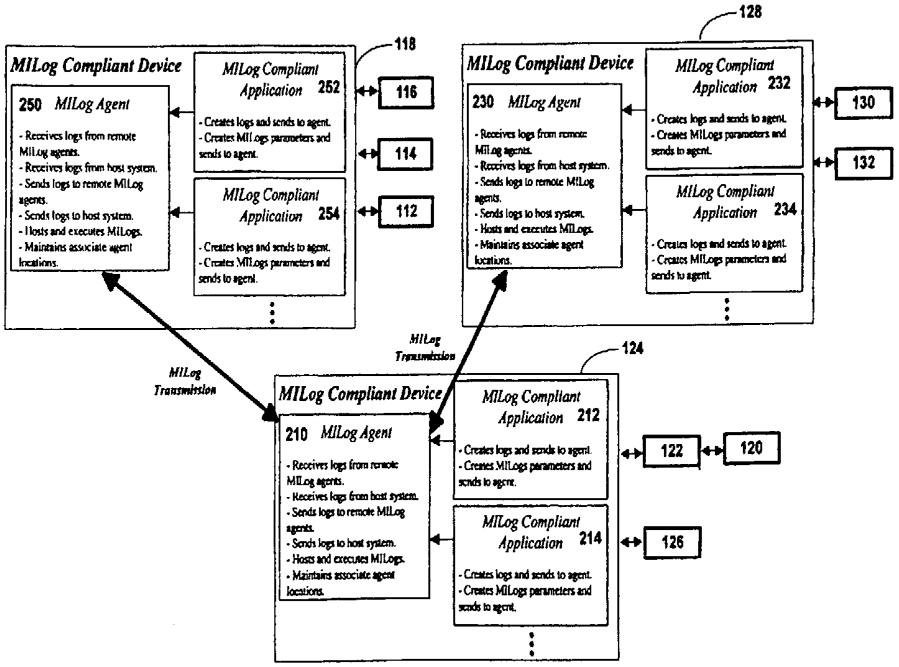

118
MILog Compliant Device
250 MILog Agent
- Receives logs from remote MILog agents.
- Receives logs from host system.
- Sends logs to remote MILog agents.
- Sends logs to host system.
- Hosts and executes MILogs.
- Maintains associate agent locations.
MILog Compliant Application 252
- Creates logs and sends to agent.
- Creates MILogs parameters and sends to agent.
MILog Compliant Application 254
- Creates logs and sends to agent.
- Creates MILogs parameters and sends to agent.
116
114
112
128
MILog Compliant Device
230 MILog Agent
- Receives logs from remote MILog agents.
- Receives logs from host system.
- Sends logs to remote MILog agents.
- Sends logs to host system.
- Hosts and executes MILogs.
- Maintains associate agent locations.
MILog Compliant Application 232
- Creates logs and sends to agent.
- Creates MILogs parameters and sends to agent.
MILog Compliant Application 234
- Creates logs and sends to agent.
- Creates MILogs parameters and sends to agent.
130
132
MILog Transmission
MILog Transmission
124
MILog Compliant Device
210 MILog Agent
- Receives logs from remote MILog agents.
- Receives logs from host system.
- Sends logs to remote MILog agents.
- Sends logs to host system.
- Hosts and executes MILogs.
- Maintains associate agent locations.
MILog Compliant Application 212
- Creates logs and sends to agent.
- Creates MILogs parameters and sends to agent.
MILog Compliant Application 214
- Creates logs and sends to agent.
- Creates MILogs parameters and sends to agent.
122
120
126

Figure 2

GB 2 374 493 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

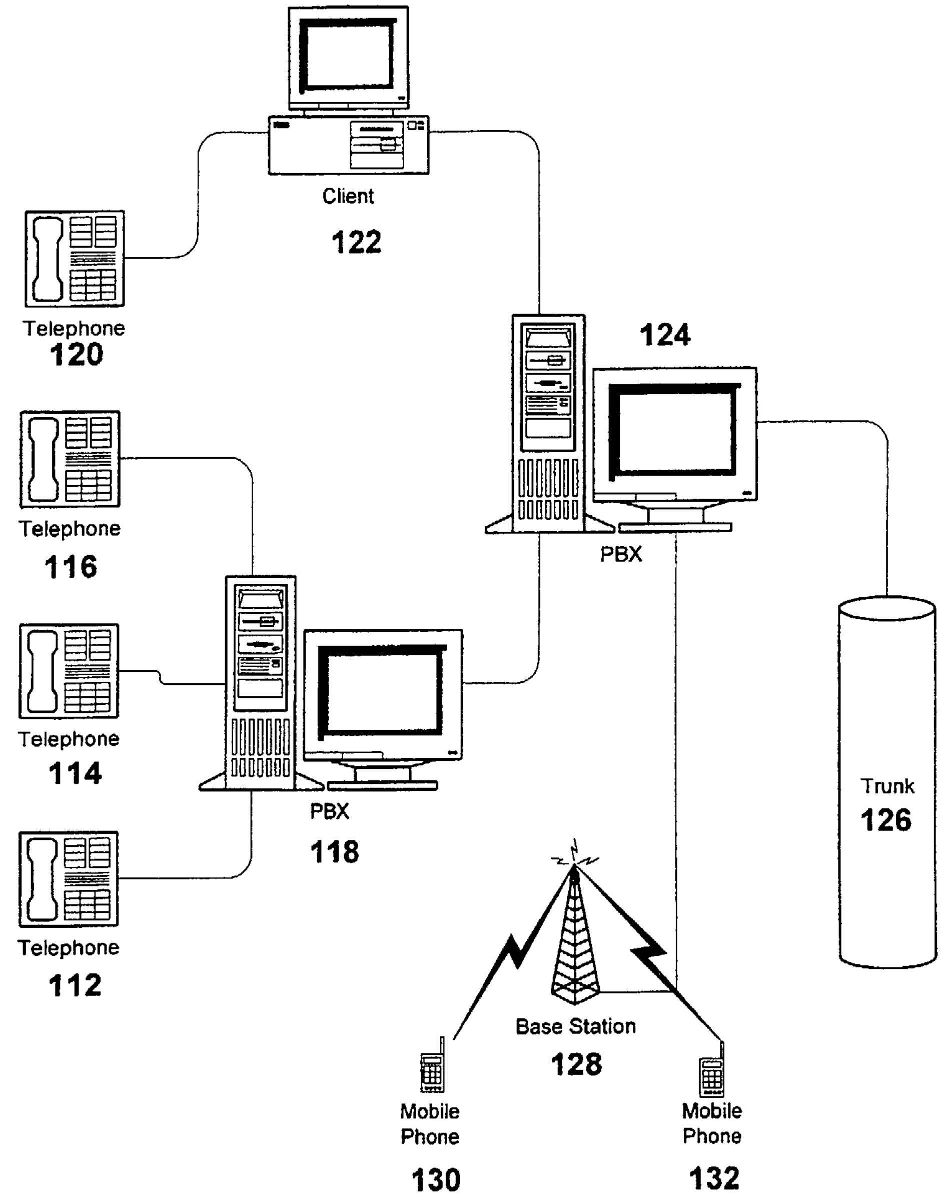

Client
122
Telephone
120
124
PBX
Telephone
116
Telephone
114
PBX
118
Trunk
126
Telephone
112
Base Station
128
Mobile
Phone
130
Mobile
Phone
132

Figure 1

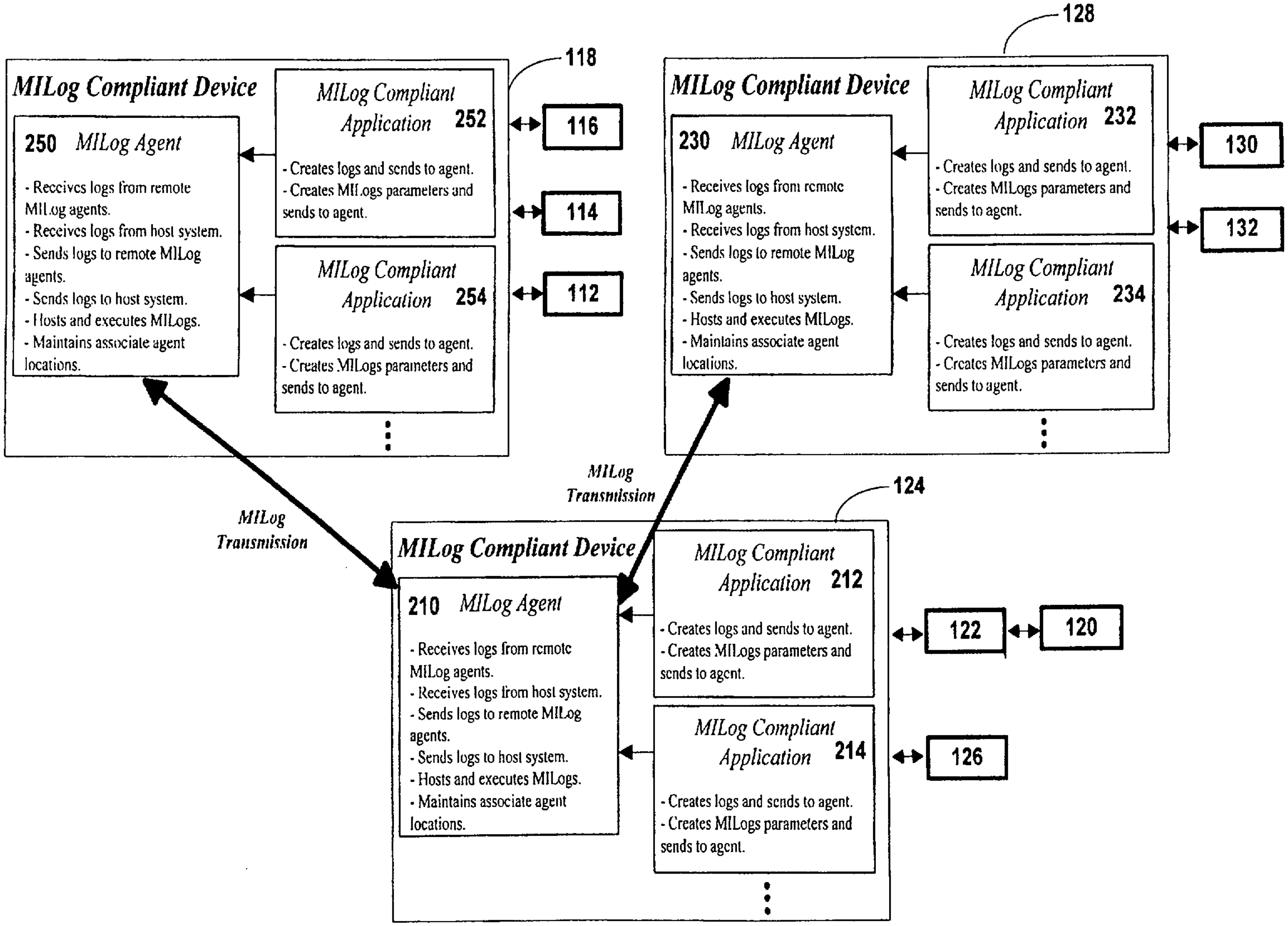
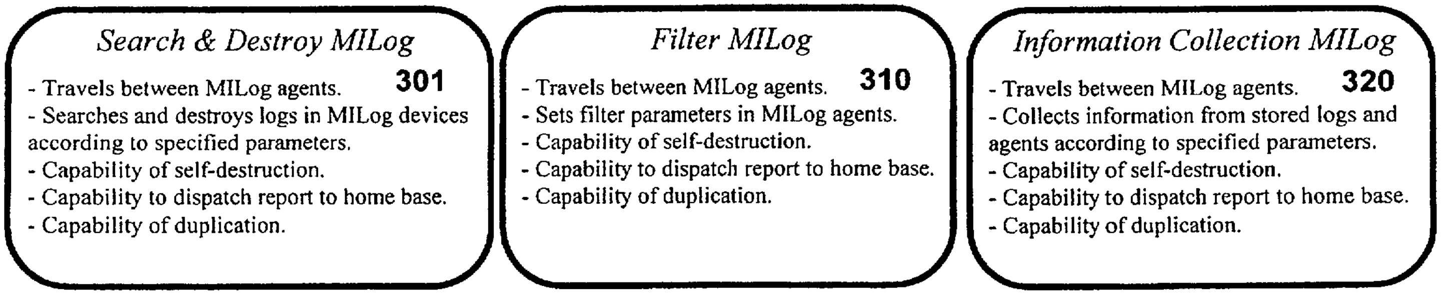

MILog Compliant Device
250 MILog Agent
- Receives logs from remote MILog agents.
- Receives logs from host system.
- Sends logs to remote MILog agents.
- Sends logs to host system.
- Hosts and executes MILogs.
- Maintains associate agent locations.
MILog Compliant Application 252
- Creates logs and sends to agent.
- Creates MILogs parameters and sends to agent.
MILog Compliant Application 254
- Creates logs and sends to agent.
- Creates MILogs parameters and sends to agent.
118
116
114
112
128
MILog Compliant Device
230 MILog Agent
- Receives logs from remote MILog agents.
- Receives logs from host system.
- Sends logs to remote MILog agents.
- Sends logs to host system.
- Hosts and executes MILogs.
- Maintains associate agent locations.
MILog Compliant Application 232
- Creates logs and sends to agent.
- Creates MILogs parameters and sends to agent.
MILog Compliant Application 234
- Creates logs and sends to agent.
- Creates MILogs parameters and sends to agent.
130
132
MILog Transmission
MILog Transmission
124
MILog Compliant Device
210 MILog Agent
- Receives logs from remote MILog agents.
- Receives logs from host system.
- Sends logs to remote MILog agents.
- Sends logs to host system.
- Hosts and executes MILogs.
- Maintains associate agent locations.
MILog Compliant Application 212
- Creates logs and sends to agent.
- Creates MILogs parameters and sends to agent.
MILog Compliant Application 214
- Creates logs and sends to agent.
- Creates MILogs parameters and sends to agent.
122
120
126

Figure 2



Search & Destroy MILog

- Travels between MILog agents.
- Searches and destroys logs in MILog devices according to specified parameters.
- Capability of self-destruction.
- Capability to dispatch report to home base.
- Capability of duplication.

Filter MILog

- Travels between MILog agents.
- Sets filter parameters in MILog agents.
- Capability of self-destruction.
- Capability to dispatch report to home base.
- Capability of duplication.

Information Collection MILog

- Travels between MILog agents.
- Collects information from stored logs and agents according to specified parameters.
- Capability of self-destruction.
- Capability to dispatch report to home base.
- Capability of duplication.

Figure 3

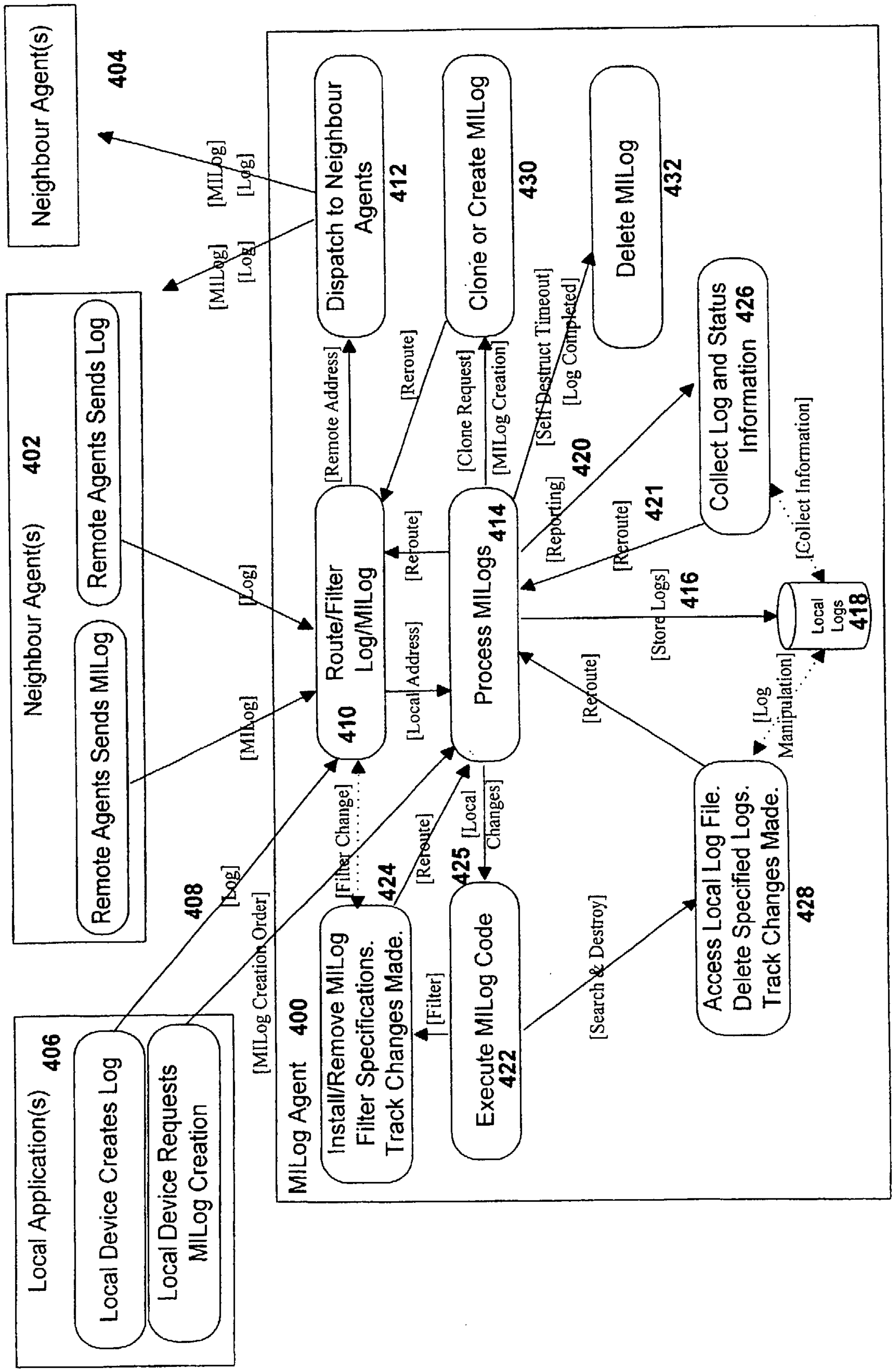

Neighbour Agent(s)
404
Neighbour Agent(s)
402
Remote Agents Sends MILog
Remote Agents Sends Log
Local Application(s)
406
Local Device Creates Log
Local Device Requests MILog Creation
408
[Log]
[MILog Creation Order]
[MILog]
[Log]
[MILog]
[Log]
[MILog]
[Log]
MILog Agent 400
Dispatch to Neighbour Agents
412
Clone or Create MILog
430
Delete MILog
432
Route/Filter Log/MILog
410
Process MILogs
414
Collect Log and Status Information
426
Local Logs
418
Install/Remove MILog Filter Specifications. Track Changes Made.
424
Execute MILog Code
422
Access Local Log File. Delete Specified Logs. Track Changes Made.
428
[Remote Address]
[Reroute]
[Clone Request]
[MILog Creation]
[Self Destruct Timeout]
[Log Completed]
[Reporting]
420
[Reroute]
421
[Collect Information]
[Store Logs]
416
[Log Manipulation]
[Reroute]
[Local Address]
[Reroute]
[Filter Change]
[Reroute]
425
[Local Changes]
[Filter]
[Search & Destroy]

Figure 4

Mobile Interactive Logs

Field of Invention

This invention relates to network administration and in particular to a network administration system for managing logs generated by network devices.

Background of the Invention

Logs are generated through out computer and communication networks for a number of purposes. Currently, network administrators maintain the logs manually; this is a time intensive proposition. It is difficult to manually collect or log information, or maintain log settings from each device on ad-hoc or 'sporatic' networks (peer to peer cell phones, Personal Digital Assistants (PDAs), and the like), where network devices continuously enter and leave the network. There are too many transient devices for administration by manual means. It is therefore desirable to provide a means to manage such administrative matters.

If many logs are being generated then large amounts of resources may also be consumed with log storage and log data transport over the network. Further, network management can be difficult as a result of the amount of log traffic being received by log analysis tools. The log analysis tools may not use all of the data contained in the logs. However, such data still consumes network bandwidth and processing time. It is therefore desirable to provide a means to manage logs in a more efficient manner.

Further, end users of the network devices have little or no control over the generated logs, and often have little or no knowledge of log data being transmitted and stored. There are a number of privacy laws in force or being enacted that limit how such log data can be used without the consent of the end users. For network administrators, the privacy laws could become a major administrative burden. It is therefore desirable to provide end users with a means to control the log data being stored to protect their privacy.

Summary of the Invention

According to the present invention, all logs are received and sent through a MILog agent at each network device. The MILog agents route and filter logs accordingly to instructions received via Mobile Interactive Logs (MILogs), and further provide other services such as creating MILogs. A user is able to create and dispatch a MILog at any time to any MILog-compliant component from a MILog agent authorized to create MILogs.

According to an aspect of the invention, there is provided a network administration system of a network for managing logs of MILog compliant network devices, comprising MILogs for traversing over the network to the network devices, each of the MILogs comprising instructions to manage the logs for execution on the network devices; and a MILog agent at each of the network devices for executing the instructions of the MILog.

According to another aspect of the invention, there is provided a method of managing logs of MILog compliant network devices of a network, comprising creating MILogs for traversing over the network to the network devices, each of the MILogs comprising instructions to manage the logs for execution on the network devices; and executing the instructions of the MILogs by MILog agents, where a MILog agent is present at each of the network devices.

According to another aspect of the invention, there is provided a network device which generates and manages logs, comprising a network interface for connecting to a network of other network devices; a memory for storing a MILog agent; and a processor for executing the MILog agent; where the MILog agent receives MILogs through the network interface from other network devices, each of the MILogs comprising instructions for managing the logs; and the MILog agent executing the instructions carried by the MILogs.

Brief Description of the Drawings

The present invention will be described in detail with reference to the accompanying drawings, in which like numerals denote like parts, and in which

Figure 1 is a block diagram of an exemplary network incorporating the present invention;

Figure 2 is an interface diagram of the network of Figure 1 and further shows Mobile Interactive Log interactions, according to the present invention;

Figure 3 shows three exemplary types of MILogs of Figure 1, according to the present invention; and

Figure 4 is a block diagram showing internal activities of a MILog Agent of Figure 1, according to the present invention.

Detailed Description of the Preferred Embodiments

Figure 1 shows an exemplary ad-hoc or sporatic network of network devices comprising a plurality of phones (112 to 116) connected to a server implemented PBX 118, a further phone 120 connected to a client server 122, both the client 122 and PBX 118 being connected to a PBX 124. The PBX 124 is connected to a T1 trunk 126 and to a wireless base station 128 in a well-known manner. The wireless base station 128 is in communication with cell phones (130 to 132). The cell phones (130 to 132) could also be PDA's or any other wireless device. Each of the network devices shown in Figure 1, with the exception of the T1 trunk 126, has the capability of generating logs. According to the present invention, all logs are received and sent through a MILog agent at each network device. The MILog agents route and filter logs according to instructions received via Mobile Interactive Logs (MILogs), and further provide other services such as creating MILogs. A user is able to create and dispatch a MILog at any time to any MILog-compliant component from a MILog agent authorized to create MILogs.

MILogs are logs, which also have functional capabilities instead of just carrying information. A MILog carries instruction code for execution by MILog agents on MILog compliant network devices that produce logging information. Agent technology is used to implement MILogs and MILog agents, and for MILogs to traverse heterogeneous ad-hoc networks. A MILog traverses a network from device to device on an itinerary. At each device, a MILog agent interacts with the MILog to execute the instruction code carried by the MILog. The instructions are to perform a number of functions including filtering log transmissions, deleting logs stored on network devices according to certain characteristics, cloning of the MILog, and managing other MILogs.

MILog agents are programs that have a number of functions including dispatching, creating, cloning, deleting and handling itinerary of MILogs. MILog agents also provide a run time execution environment for execution of the instruction code carried within MILogs. The functions of MILog agents further include bringing together instruction code and itinerary to create a MILog; controlling the mobility of MILogs including serialization and re-instantiation for traveling MILogs; checking the itinerary of MILogs and dispatching the MILogs to their next location if necessary; cloning a MILog for dispatching to the next location if so indicated in the MILog's instructions; and performing validation checks on MILogs for authentication.

A network device (hard-wired or wireless) is MILog compliant if the device hosts at least one MILog agent, passes all logs to the MILog agents for transmission, and receives logs via the MILog agents. For the purpose of MILog compliance, MILog agents do not have to be capable of creating MILogs. A MILog agent only has to be capable of accepting and otherwise supporting MILogs. The authorization to create and dispatch MILogs has to be carefully controlled, as certain MILogs can be destructive (i.e. deleting logs) if improperly handled.

Each of the network devices shown in Figure 1, with the exception of the T1 trunk 126, is MILog compliant. Figure 2 is an interface diagram of the network of Figure 1 and further showing an example of MILog agents and MILog Compliant Applications on of PBX 118, Base Station 128, and PBX 124. Each of the network devices (118, 128 and 124) comprises a MILog Agent (210, 230, 250) and a number of MIL Compliant Applications (212, 214, 232, 234, 252, 254). Each of the network devices (118, 128 and 124) can, however, host any number of applications including none (not shown). MILog agents and MILog Compliant Applications are similarly present on the other network devices (112 to 116, 120, 122, 126, 130, 132) (not shown).

The MILog Agent 210 hosts and executes MILogs, receives logs from its host system (i.e. PBX 124), sends logs to its host system (for example, to storage and log analysis tools), receives and sends logs and MILogs to and from, remove MILog agents, and maintains associate agent locations. The other MILog Agents including 230, 250 operate in a similar manner as MILog Agent 210. MILog Agents (210, 230, 250) on their respective devices interact with each other as well as receive logs from devices that send logs to the Agents (210, 230, 250) such as, for example, devices 116 or 132.

In this embodiment, for security purposes, MILogs are only created by authorized MILog agents, which are shown on Figure 2 as 210, 230, and 250. MILog Compliant Applications (212, 214, 232, 234, 252, 254) create and send logs to the MILog agents for handling as require for MILog compliance. Applications (212, 214, 232, 234, 252, 254) send instructions to their respective MILog Agent (210, 230, 250) to create the MILogs.

According to this invention, the MILog Agents (210, 230, 250) do not have to know the existence of all the devices in the network and this feature is particularly advantageous for ad hoc or 'sporatic' networks. For example, Agent 230 does not know Agent 250 exists. However, through neighbour association, the Agents (210. 230, 250) are able to communicate with any other agent connected to the network. For example, Agent 230 sends instructions for Agent 250 in a MILog to Agent 210, and Agent 210 passes the MILog to Agent 250. There can also be more than one agent on one device and these local agents can similarly interact with each other.

The architecture of a MILog includes the following fields: DESTINATION, an IP address and port of where to send the MiLog; AGENT SIGNATURE, the MILog's unique signature; TIME-OUT, the length of time the MILog is to be active on a host MILog agent; SEARCH & DESTROY RULE (S & D), a rule set used to search and destroy specific log(s); FILTERING LOGS RULE, a rule set used to filter specific log(s); RETURN HOME RULE, a rule set used to signal when this MILog is to return home (originating MILog agent); CLONE RULE, a rule set used to initiate a clone of this MILog; ITINERARY LIST, a list of network addresses that this MILog and its clones are to visit; NUMBER OF LOGS DELETED, the number of logs deleted by this MILog; and NUMBER OF LOGS FILTERED, the number of logs filtered by this MILog. Further, information, if any, is appended to the end of MILogs as required for transport by the MILogs. Using this architecture, it is possible to create a number of different MILogs with different attributes.

Figure 3 shows three exemplary types of MILogs that are more useful for managing logs in a heterogeneous ad-hoc network. The three exemplary types of MILogs are: Search & Destroy MILog 300, Filter MILog 310, and Information Collection MILog 320. Each of these MILogs is capable of carrying instructions for self-destruction, return to home (originating MILog agent), and duplication. The Search & Destroy MILog 310 travels between MILog agents searching and destroying logs in MILog compliant devices according to specified parameters. The Filer MILog 310 travels between MILog agents setting filter parameters in MILog agents. The Information Collection MILog 320 travels between MILog agents collecting information from stored logs and MILog agents according to specified parameters.

With the increase in the numbers of devices being networked, especially personal connectivity devices, privacy or anonymity is a major concern for end users. End users of, for example, cell phone 130 are provided with a capability send (or request) Search & Destroy MILogs to delete all personal information of the end users stored in logs of the network. This may become a very important security feature of any personal device interacting with a public or consumer based network.

A MILog agent comprises a MILog list, a Filter Rule Set, a Search & Destroy Rule Set, a Clone Rule Set, and a Return Home Rule Set. The MILog list is a list of all MILogs acting upon the MILog agent. The MILogs on this list are monitored and updated as MILogs expire and as the number of logs deleted/filtered changes. For example, if as a result of a particular MiLog, a log is filtered, then the MILog list is updated to increment that MiLog's NUMBER OF LOGS FILTERED by one.

The Filter Rule Set is a Rule Set consisting of all of the Filter Rules from every MILog in the MILog list. Each Rule is associated to its MILog in the MILog list. Each time a Filter Rule is satisfied, the NUMBER OF LOGS FILTERED field in the associated MILog is incremented.

The Search and Destroy (S & D) Rule Set is a Rule Set consisting of all of the Search and Destroy Rules from every MILog in the MILog list. Each Rule is associated to its MILog in the MILog list. Each time an S & D Rule is satisfied, the NUMBER OF LOGS DESTROYED field in the associated MILog is incremented.

The Clone Rule Set is a Rule Set consisting of all of the Clone Rules from every MILog in the MILog list. Each Rule is associated to its MILog in the MILog list. Each time a Clone Rule is satisfied, the appropriate IP/Port is extracted from the ITINERARY LIST and a clone of the associated MILog is created and sent to the address specified by the IP/Port. If there are no more IP/Ports, then no clone is created.

The Return Home Rule Set is a Rule Set consisting of all of the Return Home Rules from every MILog in the MILog list. Each Rule is associated to its MILog in the MILog list. Each time a Return Home Rule is satisfied the associated MILog is removed from the MILog list and sent home to the originating MILog agent.

Each time a MILog enters a MILog agent, it is checked to see whether the MILog is one that is returning home, or if it is a MILog sent by another MILog agent. If the MILog is returning home, its results are to be analyzed. If the MILog did not originate from the MILog agent, then the MILog is incorporated into the MILog agent's MILog list and the MILog's respective instructions are incorporated into the Agent's Filter Rule Set, S & D Rule Set, Clone Rule Set and Return Home Rule Set as appropriate.

Exemplary pseudo-code processing of MILogs of Figure 3 by the MILog agent is as follows:

When a MILog is received, the MILog agent checks the MiLog's AGENT SIGNATURE to see if the MILog agent originated the MiLog.

```
IF ( MILog AGENT SIGNATURE equals this MILog agent's AGENT SIGNATURE )
{
        The MILog is stored in a database where the returned results are extracted (i.e. number of logs deleted/filtered), and further appropriate action is initiated.
}
```

```
ELSE IF the MILog agent did not originate this MiLog, that is, the MiLog's AGENT
SIGNATURE is not equal to this MILog agent's AGENT SIGNATURE:
{
        Add the MILog to the MILog agent's MILog list.
        Parse(MiLog)
        {
                If ( FILTER RULE )
                        Add FILTER RULE to MILog agent's Filter Rule Set.

                If ( S & D RULE )
                        Add SEARCH & DESTROY RULE to MILog agent's
                                S & D Rule Set.

                If ( CLONE RULE and there are addresses in the ITINERARY LIST )
                        Add CLONE RULE to MILog agent's Clone Rule Set.

                If ( RETURN HOME RULE )
                        Add RETURN HOME RULE to MILog agent's
                                Return Home Rule Set.
}
}
```

Every time a Filter rule or S & D rule is satisfied, then within the MILog list, the associated MiLog's NUMBER OF LOGS FILTERED/DESTROYED is updated. If a clone rule is satisfied, a clone is generated and sent. If a return home rule is satisfied, the associated MILog is removed from the MILog list, and sent to its originating source. Every time the TIME_OUT value expires, the MILog is removed from the MILog list, including all of its Rules from the above Rule Sets, and then destroyed.

```
If ( Filter or S & L Rule Satisfied )
{
        Look-up associated MILog from MILog list and increment NUMBER OF LOGS
FILTERED/DELETED.
}

If ( Clone Rule Satisfied )
{
        Look-up associated MILog from MILog list.
        Make a copy of it.
        Remove the next destination IP/Port address from its itinerary and into the
        DESTINATION FIELD.
        Send clone.
}

If ( Return Home Rule Satisfied )
{
        Look-up and remove associated MILog from MILog list.
        Send MILog to originating source.
}

If ( TIME_OUT value expires )
{
        Look-up and remove associated MILog from MILog list.
        Destroy MiLog.
}
```

Figure 4 is a block diagram showing internal activities of a MILog Agent 400 and its interactions with Neighbour Agents 402, 404 and Local Application(s) 406 over a network. Route/Filter 410 is the routing and filtering mechanism of the MILog Agent 400. All logs and MILogs pass through the Route/Filter 410 for routing and filtering before entering or leaving the MILog Agent 400. The Route/Filter 410 has a Filter Rule Set. The Route/Filter 410 evaluates every log/MILog that is received to determine if the log/MILog is to be accepted by the MILog Agent 400 or is to be dispatched further on to Neighbour Agents 402, 404.

When logs and MILogs (logs/MILogs) arrive at the Route/Filter 410, each log/MILog is checked to determine if the log/MILog is to be used in the MILog Agent 400, dispatched to specific neighbours 402, or just passed onto a neighbour agent 404 for further transport. If the log/MILog is for the MILog Agent 400, the log/MILog is processed at the Process MILog Request 414. If the log/MILog is a log, the log is stored [store logs] 416 in the local logs database 418.

The Process MILog Request 414 analyzes the MILog's instruction code. If the instruction relates to collecting information from the MILog Agent 400 or from local logs [reporting] 420, the information is collected and attached 426 to the MILog. The updated MILog is then rerouted 421 back to Process MILog Request 414 for further processing according to the instruction code. The MILog is then rerouted to 410 and dispatched 412 accordingly.

If the instruction code relates to filtering logs, then the MILog instruction is executed in Execute MILog Code 422 [Local Changes]. The filtering rules are installed, removed, and changed 424, which changes the Filter Rule Sets of the Route/Filter 410 accordingly. All changes are tracked. Other MILog agents using MILogs are thus able to install filters for logs from MILog Agent 400 and in due course also remove their filters as desired. The MILog is then updated and rerouted to Process MILog Request 414 for further processing according to the instruction code, if required.

If the instruction code relates to searching and destroying logs, the MILog instruction is executed by Execute MILog Code 422 [Local Changes]. The logs in the local logs database 418 are accordingly manipulated by 428 [Log Manipulation]. All changes are tracked. The MILog is then updated and rerouted to Process MILog Request 414 for further processing according to the instruction code, if required.

If the instruction code relates to cloning the MILog, then a clone request [Clone Request] is made and the MILog is cloned 430 according to specified instructions. The clone(s) are then dispatched [Reroute] accordingly.

If the Process MILog Request 414 determines that the MILog has finished its instructions and no other action is necessary, then the MILog is deleted.

The Process MILog Request 414 further reviews and updates MILogs on its MILog list, and where a self-destruct instruction timeout of a MILog has timed-out or where a MILog has completed its instructions, the MILog is deleted [Self Destruct Timeout] / [Log Completed] and its instructions affecting the MILog Agent 400 reversed, if required.

The Local Application(s) 406 is able to request creation of a MILog 410 [MILog Creation Order]. When a MILog Creation Order is send by a local application then a MILog is created 430 according to the parameters specified by the local application.

The Local Application(s) 406 send their logs [Log] 408 to the Route/Filter 410 for handling. The logs are stored, filtered, and routed according to the rule set of the Route/Filter 410.

The above disclosure generally describes the present invention. A more complete understanding can be obtained by reference to the following specific Examples. These Examples are described solely for purposes of illustration and are not intended to limit the scope of the invention. Changes in form and substitution of equivalents are contemplated as circumstances may suggest or render expedient. Although specific terms have been employed herein, such terms are intended in a descriptive sense and not for purposes of limitation.

For an exemplary case of a cellular phone and a communications tower which are both MILog-compliant. The cellular phone emits a log every time it 'pings' the communications tower. The communications tower in this scenario is running MILog-compliant log tracking software and is analyzing and storing all incoming logs from all communications devices within its range.

If the cellular phone is 'pinging' the communications tower repeatedly, an administrator in charge of the tower may wish to filter out ping logs from the cellular phone. To execute, the administrator interfaces with a local application to dispatch a MILog to thereby filter out the undesired ping logs from the cellular phone.

To automate this process, a log analysis tool is configured so that a MILog is created and dispatched based on a set of logs. For example, when the logs indicate that the tower has received 10 'ping' logs from any single device then a 'Filter" MILog is dispatched and the MILog is set to self-destruct after a given time. This ensures that the cellular phone does not have the MILog filter resident indefinitely. If another pattern of 10 'pings' is received after the original MILog had self destructed (or returned home to report back on the number of 'pings' that it filtered), then a second MILog is sent out to repeat the process.

On the other side of this example, a user of the cellular phone may not wish for a trail of logs containing personal information to be left behind for analysis by another party (the tower in this case). If the cellular phone is authorized to create MILogs, then the user enters in a code on the cellular phone keypad that dispatches a 'Search and Destroy' MILog. This MILog is transmitted through the log stream to the tower. A MILog agent at the tower executes the instructions of the MILog and searches through the log storage files and removes any logs relating to the originating device (the cellular phone).

Exemplary rule sets for logs are disclosed in U.K. Patent Application No. 0008952.4 filed April 12, 2000, entitled "DYNAMIC RULE SETS FOR GENERATED LOGS".

It will be understood by those skilled in the art that MILogs could be created to have many combination of many functional possibilities beyond the Filter MILog, Search and Destroy MILog, and Information Collection MILog.

Although preferred embodiments of the invention have been described herein, it will be understood by those skilled in the art that variations may be made thereto without departing from the scope of the invention or the appended claims.

What is claimed is:

1. A network administration system of a network for managing logs of MILog compliant network devices, comprising

MILogs for traversing over the network to the network devices, each of the MILogs comprising instructions to manage the logs for execution on the network devices; and

a MILog agent at each of the network devices for executing the instructions of the MILog.

2. The network administration system of claim 1, wherein MILogs further comprises instructions for managing MILogs at MILog agents.

3. The network administration system of claims 1 or 2, wherein each of the MILogs traverses over the network on an itinerary.

4. The network administration system of claims 1, 2 or 3, wherein more than one of the MILog agents are able to create MILogs.

5. The network administration system of claims 1, 2 or 3, wherein one of the MILog agents is able to create MILogs.

6. The network administration system of any of claims 1 to 5, wherein the logs are generated according to rule sets.

7. The network administration system of any of claims 1 to 6, wherein the network is an ad-hoc or 'sporatic' network.

8. A method of managing logs of MILog compliant network devices of a network, comprising

creating MILogs for traversing over the network to the network devices, each of the MILogs comprising instructions to manage the logs for execution on the network devices; and

executing the instructions of the MILogs by MILog agents where a MILog agent is present at each of the network devices.

9. The method of claim 8, wherein MILogs further comprises instructions for managing MILogs at MILog agents.

10. The method of claims 8 or 9, wherein each of the MILogs traverses over the network on an itinerary.

11. The method of claims 8, 9 or 10, wherein more than one of the MILog agents are able to create MILogs.

12. The method of claims 8, 9 or 10, wherein one of the MILog agents is able to create MILogs.

13. The method of any of claims 8 to 12, wherein the logs are generated according to rule sets.

14. The method of any of claims 8 to 13, wherein the network is an ad-hoc or 'sporatic' network.

15. A network device which generates and manages logs, comprising
a network interface for connecting to a network of other network devices;
a memory for storing a MILog agent; and
a processor for executing the MILog agent;
where the MILog agent receives MILogs through the network interface from other network devices, each of the MILogs comprising instructions for managing the logs; and the MILog agent executing the instructions carried by the MILogs.

16. The network device of claim 15, wherein the MILogs further comprises instructions for managing MILogs at the MILog agent.

17. The network device of claims 15 or 16, wherein each of the MILogs traverses over the network on an itinerary.

18. The network device of claims 15, 16 or 17, wherein the MILog agent is able to create MILogs, where the MILogs created by the MILog agent are sent to MILog agents of the other network devices over the network for execution by the MILog agents to manage logs at the other network devices.

19. The network device of any of claims 15 to 18, wherein the logs are generated according to rule sets.

20. The network device of any of claims 15 to 19, wherein the network is an ad-hoc or 'sporatic' network.

The Patent Office

INVESTOR IN PEOPLE

Application No:	GB 0109241.0	**Examiner:**	Tom Sutherland
Claims searched:	1 - 20	**Date of search:**	4 December 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): H4L (LRNMT, LRNR, LRNX, LFMX), H4P (PPG), H4K (KFMA)

Int Cl (Ed.7): H04Q 3/00, 7/34; H04L 12/26, 12/28; H04M 3/22

Other: EPODOC, WPI, JAPIO, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	WO 00/47003 A	(MPATH INTERACTIVE) Whole document relevant.	1, 8 and 15 at least
X	WO 00/40049 A	(ERICSSON) See claim 1.	1, 8 and 15 at least.
A	WO 96/16516 A	(NORTHERN TELECOM)	
X	US 5857190	(MICROSOFT) Whole document relevant, note Fig. 1.	1, 8 and 15 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
		E	Patent document published on or after, but with priority date earlier than, the filing date of this application.
&	Member of the same patent family		