(12) UK Patent Application (19) GB (11) 2564430 (13) A

(43) Date of A Publication 16.01.2019

(21) Application No: 1711016.4

(22) Date of Filing: 07.07.2017

(71) Applicant(s):
Gurulogic Microsystems Oy
Linnankatu 34, Turku FI-20100, Finland

(72) Inventor(s):
Tuomas Kärkkäinen
Mikko Sahlbom

(74) Agent and/or Address for Service:
Basck Ltd
16 Saxon Road, CAMBRIDGE, Cambridgeshire,
CB5 8HS, United Kingdom

(51) INT CL:
H04L 9/08 (2006.01) *H04L 12/44* (2006.01)

(56) Documents Cited:
US 7096355 B1
US 20160065548 A1
US 20130195272 A1
US 20100031063 A1
US 20090122984 A1

(58) Field of Search:
INT CL **H04L**
Other: **EPODOC, WPI, Patent Fulltext**

(54) Title of the Invention: **Data communication system and method**
Abstract Title: **Interconnection of local star networks of client and bot services centered on a hub node service, with transmission of key store IDs used for encryption**

(57) A network node 102 provides a service to clients or bots executing on network devices 106 arranged around the node in a programmatic star configuration to create a local network 108. Communication data between clients/bots is relayed through the node. A client/bot encrypts communication data by employing a key store, the store being associated with an owner of the client/bot. Similar local star networks may be interconnected such that a client/bot on one local network can communicate data to another in the same or different local network through the corresponding service network nodes. Metadata indicative of a unique identifier (ID) of the key store and a key index of a key material to be derived from the key store for decryption of data may be transmitted with said data. The metadata may be encrypted or unencrypted, and may further comprise group information relating to clients/bots that form a receiving group. A given network node service may validate and authenticate local services provided by clients or bots within its own local network. These client/bot services may be registered with a registration service 104 as a private or public service.

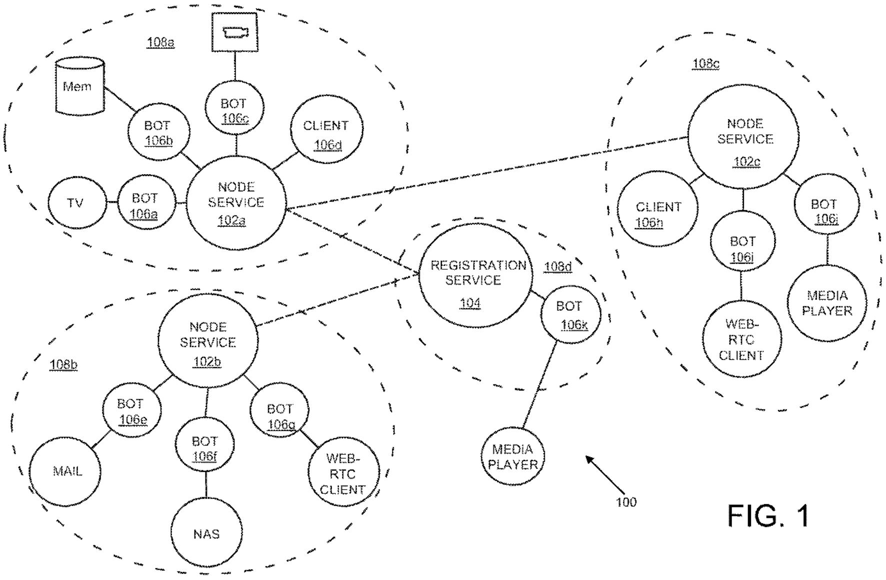

FIG. 1

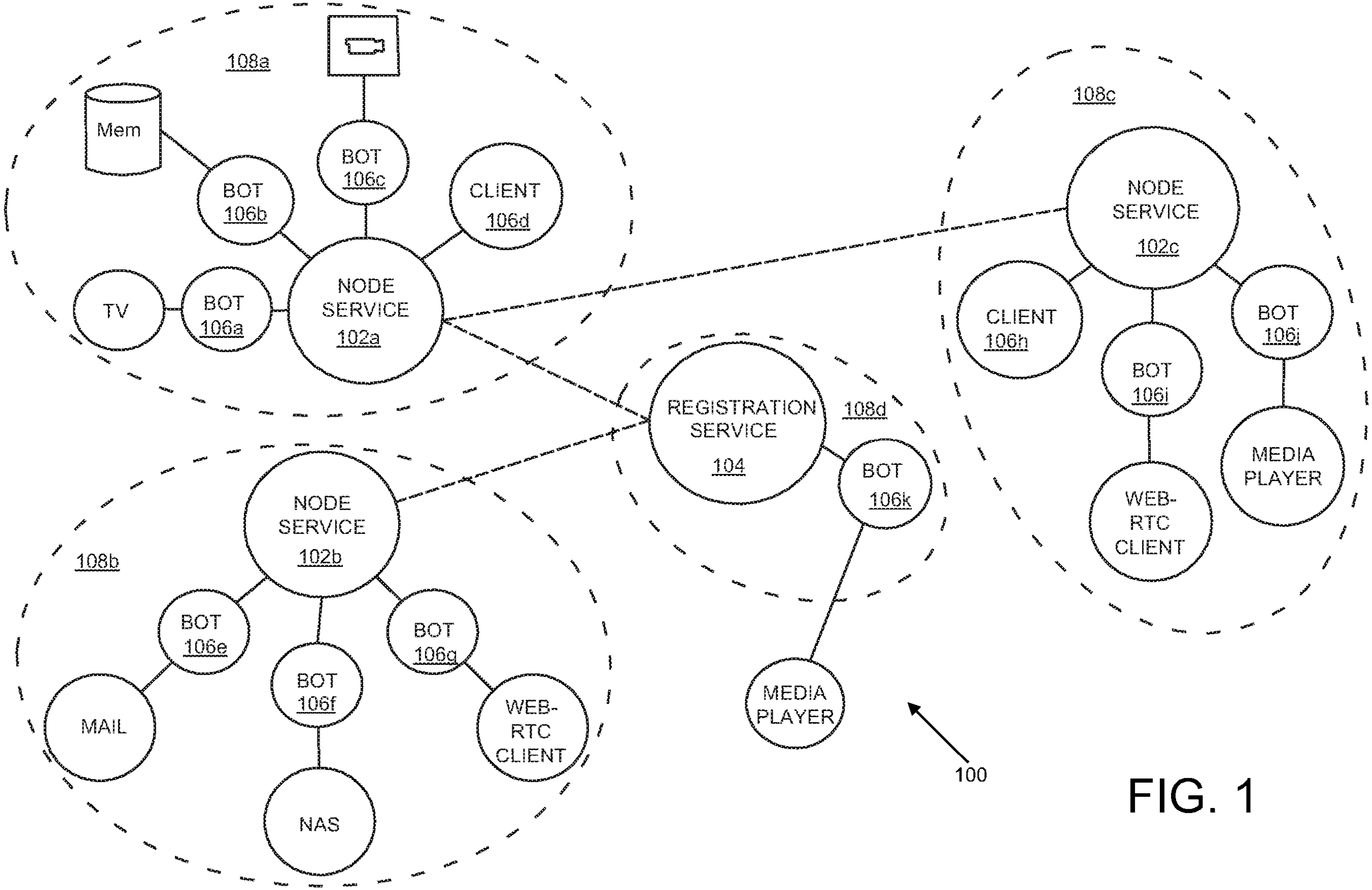
108a
Mem
BOT
106b
BOT
106c
CLIENT
106d
TV
BOT
106a
NODE
SERVICE
102a
108c
NODE
SERVICE
102c
CLIENT
106h
BOT
106i
BOT
106j
MEDIA
PLAYER
WEB-
RTC
CLIENT
REGISTRATION
SERVICE
104
108d
BOT
106k
MEDIA
PLAYER
108b
NODE
SERVICE
102b
BOT
106e
BOT
106f
BOT
106g
MAIL
NAS
WEB-
RTC
CLIENT
100

FIG. 1

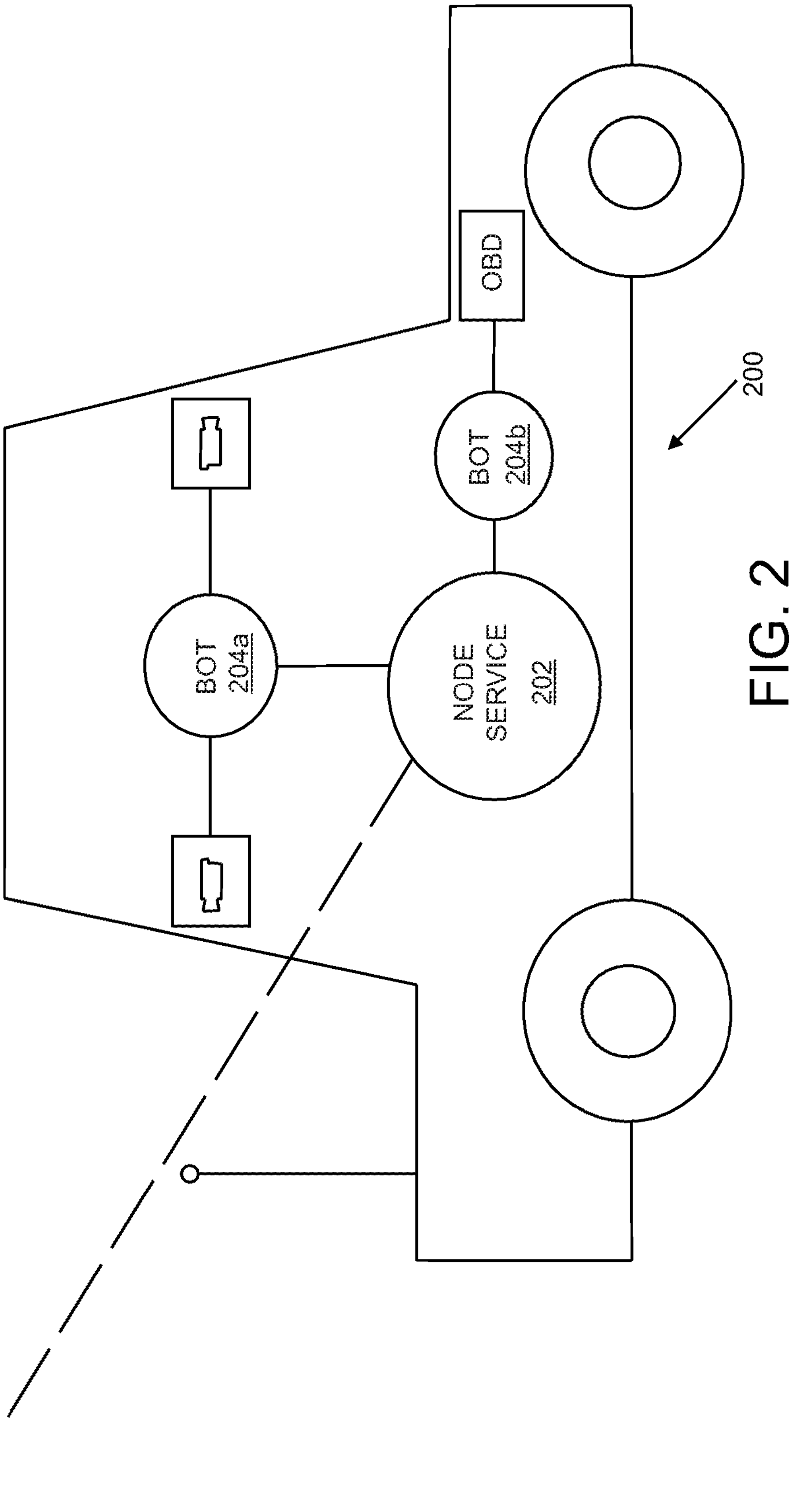

FIG. 2

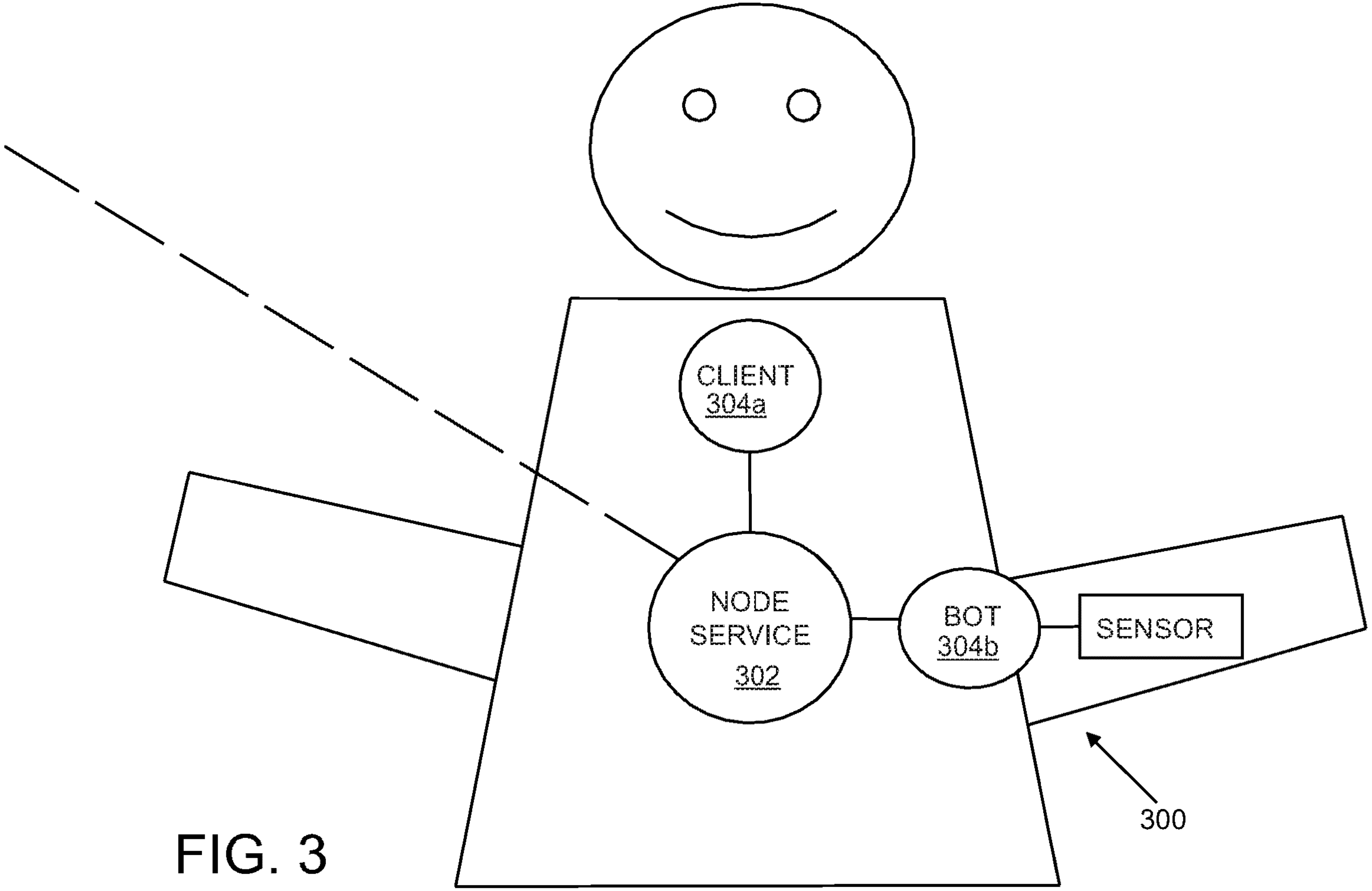

FIG. 3

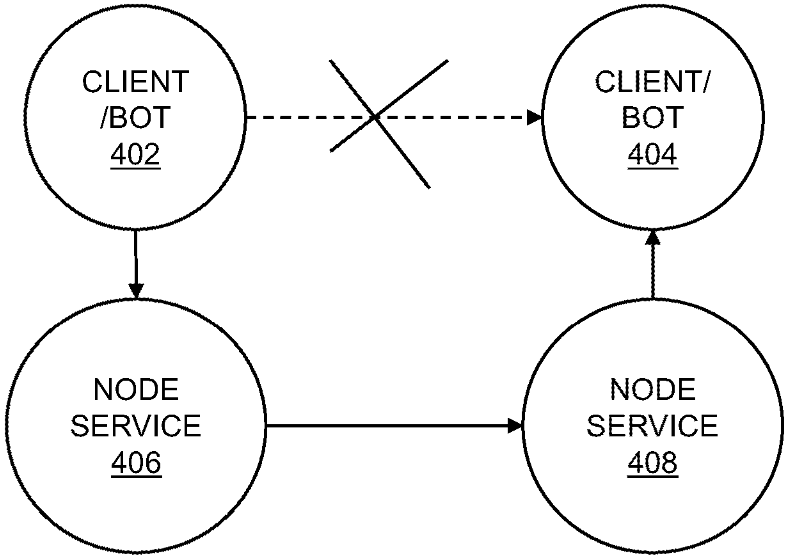
CLIENT
/BOT
402
CLIENT/
BOT
404
NODE
SERVICE
406
NODE
SERVICE
408

FIG. 4A

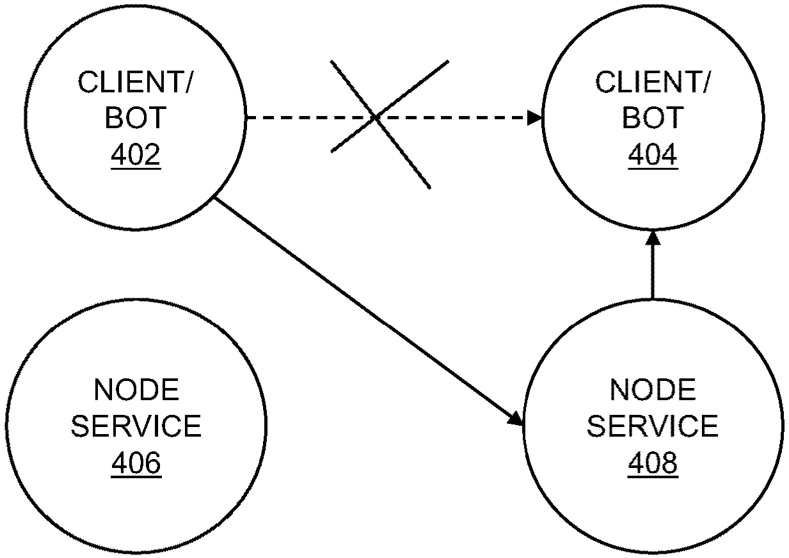
CLIENT/
BOT
402
CLIENT/
BOT
404
NODE
SERVICE
406
NODE
SERVICE
408

FIG. 4B

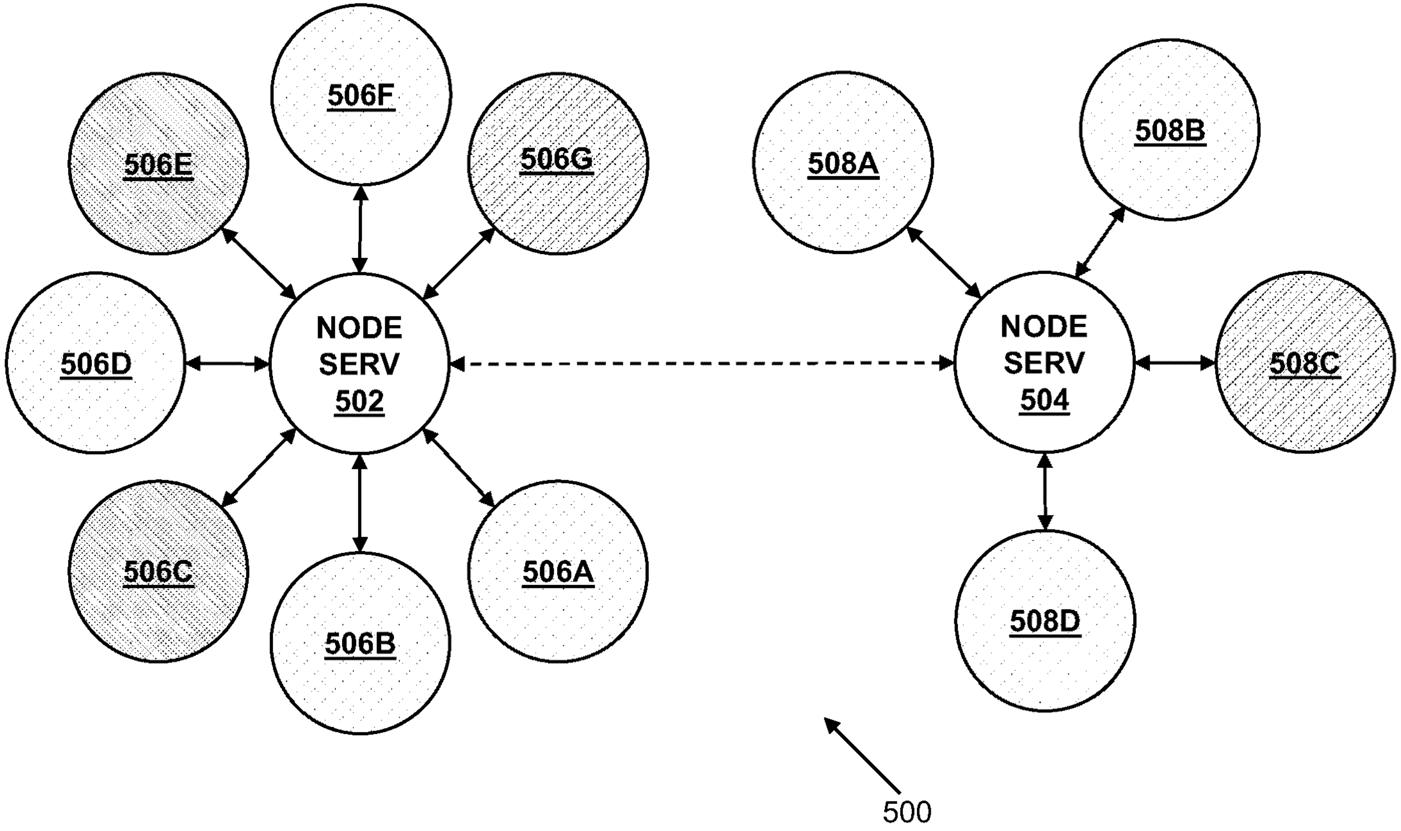
506E
506F
506G
508A
508B
506D
NODE SERV 502
NODE SERV 504
508C
506C
506B
506A
508D
500

FIG. 5

Application No. GB1711016.4 RTM Date :13 December 2017

The following terms are registered trade marks and should be read as such wherever they occur in this document:

Wi-Fi (page 19)

DATA COMMUNICATION SYSTEM AND METHOD

TECHNICAL FIELD

The present disclosure relates to data communication systems. Moreover, the present disclosure is concerned with methods of communicating data. Furthermore, the present disclosure is concerned with computer program products comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute aforesaid methods.

BACKGROUND

Contemporary home and office data communication networks are based upon connected devices in a physically open local network, wherein a given device can communicate with other devices and service providers outside its open local network. This exposes data services provided via the open local network to on-going attacks, eavesdropping, and other unwanted activities of abuse. A typical contemporary approach is to protect the devices using firewall and antivirus scanners. However, such an approach is not capable of protecting the devices against attacks made from inside the open local network.

Another contemporary approach is to provide an encrypted connection for data transmission between a given user device and a given server. However, information to be transmitted is encrypted only during transmission, and is stored in unencrypted form at both the endpoints, namely the given user device and the given server. As a consequence, the information is not safeguarded from possible abuses.

Moreover, contemporary services are generated by a service provider’s data centres. Such contemporary practices suffer from several disadvantages. Firstly, it is a well-known fact that contemporary data centres consume more energy for cooling than all airlines in the world together, as they remain idle most of the time. Secondly, contemporary data centres make information produced and used by a given user available to service providers for various purposes, for example, such as for targeted advertising based upon user profiling, namely selling such information to third parties for commercial use.

Furthermore, contemporary search engine services base their existence upon open and accessible information present on the Internet®, and their services create a foundation of a contemporary information society. These search engine services wield great power, and it is possible that information accessible to the search engine services is misused for various purposes, which is not desirable for individual user protection, companies or even in respect of legislation from different countries.

In light of the foregoing, there arises a contemporary need for a data communication system that is more safe, ecological and affordable as compared to conventional data centres.

SUMMARY

The present disclosure seeks to provide an improved data communication system.

Moreover, the present disclosure seeks to provide an improved method of communicating data.

A further aim of the present disclosure is to at least partially overcome at least some of the problems of the prior art, as described in the foregoing.

In a first aspect, embodiments of the present disclosure provide a data communication system comprising at least one network node and a plurality of network devices associated with the at least one network node, characterized in that:

(i) the at least one network node is operable to provide a network node service to a plurality of clients or bots executing on the plurality of network devices, wherein individual clients or bots of the plurality of clients or bots are communicably coupled around the network node service in a programmatic star configuration to create a local network;

(ii) a source client or bot is operable to communicate data to one or more destination clients or bots within the local network, by relaying the data through the network node service; and

(iii) the source client or bot is operable to encrypt information content of the data prior to communicating the data to the one or more destination clients or bots, wherein the source client or bot is operable to employ a key store to encrypt the information content of the data, the key store being associated with an owner of the source client or bot.

Embodiments of the present disclosure are of advantage in that the data communication system enables owners to produce services, via clients or bots, for their own use by using efficiently integrated local network devices in local networks, whilst protecting data produced by the services in respect of their respective owners.

In a second aspect, embodiments of the present disclosure provide a method of communicating data, via a data communication system comprising at least one network node and a plurality of network devices associated with the at least one network node, characterized in that the method comprises:

(i) operating the at least one network node to provide a network node service to a plurality of clients or bots executing on the plurality of network devices, wherein individual clients or bots of the plurality of clients or bots are communicably coupled around the network node service in a programmatic star configuration to create a local network;

(ii) operating a source client or bot to communicate data to one or more destination clients or bots within the local network, by relaying the data through the network node service; and

(iii) operating the source client or bot to encrypt information content of the data prior to communicating the data to the one or more destination clients or bots, wherein a key store is employed to encrypt the information content of the data, the key store being associated with an owner of the source client or bot.

In a third aspect, embodiments of the present disclosure provide a computer program product comprising a non-transitory (namely, non-transient) computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute the aforementioned method pursuant to the aforementioned second aspect.

Additional aspects, advantages, features and objects of the present disclosure would be made apparent from the drawings and the detailed description of the illustrative embodiments construed in conjunction with the appended claims that follow.

It will be appreciated that features of the present disclosure are susceptible to being combined in various combinations without departing from the scope of the present disclosure as defined by the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The summary above, as well as the following detailed description of illustrative embodiments, is better understood when read in conjunction with the appended drawings. For the purpose of illustrating the present disclosure, exemplary constructions of the disclosure are shown in the drawings. However, the present disclosure is not limited to specific methods and apparatus disclosed herein. Moreover, those in the art will understand that the drawings are not to scale. Wherever possible, like elements have been indicated by identical numbers.

Embodiments of the present disclosure will now be described, by way of example only, with reference to the following diagrams wherein:

FIG. 1 is a schematic illustration of a data communication system, in accordance with an embodiment of the present disclosure;

FIG. 2 is a schematic illustration of an example local network, in accordance with an embodiment of the present disclosure;

FIG. 3 is a schematic illustration of another example local network, in accordance with an embodiment of the present disclosure;

FIGs. 4A and 4B are schematic illustrations of how a client or bot may communicate with another client or bot from a different local network, in accordance with an embodiment of the present disclosure; and

FIG. 5 is a schematic illustration of a plurality of groups defined in a data communication system, in accordance with an embodiment of the present disclosure.

In the accompanying diagrams, an underlined number is employed to represent an item over which the underlined number is positioned or an item to which the underlined number is adjacent. When a number is non-underlined and accompanied by an associated arrow, the non-underlined number is used to identify a general item at which the arrow is pointing.

DETAILED DESCRIPTION OF EMBODIMENTS

In the following detailed description, illustrative embodiments of the present disclosure and ways in which they can be implemented are elucidated. Although some modes of carrying out the present disclosure are described, those skilled in the art would recognize that other embodiments for carrying out or practising the present disclosure are also possible.

In a first aspect, embodiments of the present disclosure provide a data communication system comprising at least one network node and a plurality of network devices associated with the at least one network node, characterized in that:

(i) the at least one network node is operable to provide a network node service to a plurality of clients or bots executing on the plurality of network devices, wherein individual clients or bots of the plurality of clients or bots are communicably coupled around the network node service in a programmatic star configuration to create a local network;

(ii) a source client or bot is operable to communicate data to one or more destination clients or bots within the local network, by relaying the data through the network node service; and

(iii) the source client or bot is operable to encrypt information content of the data prior to communicating the data to the one or more destination clients or bots, wherein the source client or bot is operable to employ a key store to encrypt the information content of the data, the key store being associated with an owner of the source client or bot.

Optionally, the at least one network node comprises at least a first network node and a second network node, and the plurality of network devices comprise a first set of network devices associated with the first network node and a second set of network devices associated with the second network node. Optionally, in such a case, the first network node is operable to provide a first network node service to a first set of clients or bots executing on the first set of network devices, while the second network node is operable to provide a second network node service to a second set of clients or bots executing on the second set of network devices. Optionally, in this regard, individual clients or bots of the first set of clients or bots are communicably coupled around the first network node service in a programmatic star configuration to create a first local network, while individual clients or bots of the second set of clients or bots are communicably coupled around the second network node service in a programmatic star configuration to create a second local network.

Optionally, when a given source client or bot is operable to communicate data to a given destination client or bot within a same local network, the data to be communicated is relayed through their associated network node service within the same local network.

Optionally, when a given source client or bot is operable to communicate data to a given destination client or bot from a different local network, the data to be communicated is relayed through a network node service associated with the given source client or bot and through a network node service associated with the given destination client or bot. As an example, when a source client or bot from the first local network is operable to communicate data to a destination client or bot from the second local network, the data to be communicated is relayed through the first network node service and the second network node service.

It will be appreciated that the data is communicated within the data communication system in real time or near real time.

Optionally, the source client or bot is operable to employ at least one key material that is stored in the key store to encrypt the information content of the data.

Optionally, the source client or bot is operable to communicate metadata together with the data. Optionally, in this regard, the metadata comprises encryption information indicative of a unique identifier (ID) of the key store and a key index of a key material to be derived from the key store for subsequent decryption of the encrypted information content. It will be appreciated that there can be a plurality of key stores associated with the owner of the source client or bot, the plurality of the key stores being dedicated for different service providers; in such a case, the unique ID of the key store identifies which key store from amongst the plurality of key stores is to be used for encryption/decryption purposes.

Pursuant to embodiments of the present disclosure, the source client or bot and the one or more destination clients or bots are provided with identical or mutually compatible copies of the key store. Optionally, the key store is provided by any one of the source client or bot or the one or more destination clients or bots. Alternatively, optionally, the key store is provided by a trusted third party. It will be appreciated that no harm arises even if the encrypted information content is accessed by unauthorized parties, because the unauthorized parties do not have access to the relevant key store and its key materials.

Optionally, the key store is implemented by way of a key container or a key generator that is capable of storing key materials and/or generating key materials based upon their key indexes in a reproducible manner. By "*reproducible*", it means that a same key material is generated from a given key index. As an example, the key store can be implemented as described in a UK patent document GB2538052. As another example, the key store can be implemented as described in a UK patent document GB 1620553.6.

Moreover, optionally, the metadata further comprises group information indicative of the one or more destination clients or bots to which the data is to be communicated. Optionally, the source client or bot and the one or more destination clients or bots together form a group.

Optionally, a plurality of groups are defined within the data communication system in a dynamic manner, wherein a given group of the plurality of groups comprises:

(i) at least one client or bot from the first local network and at least one client or bot from the second local network, or

(ii) at least two clients or bots from a same local network.

Optionally, each group of the data communication system is assigned a unique group tag. Optionally, in such a case, the group information of the metadata includes a group tag of the group comprising the source client or bot and the one or more destination clients or bots.

It will be appreciated that defining the plurality of groups "*in a dynamic manner*" means that the groups can vary based upon individual circumstances and requirements, and group structuring can be different at different points of time.

It will also be appreciated that the aforesaid encryption information and the aforesaid group information of the metadata enable the data communication system to perform a fast and reliable data delivery to the destination clients or bots.

Optionally, the metadata is communicated by way of one or more data streams.

According to an embodiment, the metadata is communicated in an unencrypted form. In such a case, a given network node service delivers (namely, relays) the encrypted information content of the data to desired parties, namely the one or more destination clients or bots, based upon the metadata, without a need to process the encrypted information content. In other words, only the information content of the data, which may contain sensitive information, is encrypted; the given network node service does not need to decrypt the encrypted information content and re-encrypt it. As a result, the given network node service does not compromise any sensitive information in respect of the owner of the source client or bot. Notably, a given network node providing the given network node service can be implemented in any kind of environment using any kind of device that need not have any security enhancements for protecting the data.

According to another embodiment, the metadata is communicated in an encrypted form. In such a case, it is required that the network node services are implemented to have their own key stores and suitable security modules associated with the key stores for protecting the key stores from unauthorized access and use, wherein the security modules are configured to perform actual encryption and decryption operations. This requires hardware-isolated security features from the network nodes executing the network node services. It will be appreciated that communicating the metadata in the encrypted form is particularly beneficial when it is desired to hide tracking information, so that it would not be possible for an eavesdropping third party to realize what type of data streams are being communicated and with whom the communication is occurring. This potentially enhances cost-efficiency of the data communication system.

However, it will be appreciated that the metadata is not required to be encrypted if there is no reason to hide the tracking information.

Throughout the present disclosure, the term "*network node*" refers to a physical network node that is operable to provide a network node service, such that the network node service is programmatically centralized to serve clients or bots executing on network devices in its own local network. It will be appreciated that a physical implementation of a local network does not require its network node and network devices to be arranged in a star network topology. In other words, the clients or bots are only programmatically coupled around the network node service in the programmatic star configuration. Throughout the present disclosure, the term "*programmatic star configuration*" refers to a software topology formed by a network node service and its associated clients or bots.

Moreover, a network node could be implemented either by way of a data communication equipment (for example, such as a modem, hub and the like) or by way of a data terminal equipment (for example, such as a router, a host computer and the like). Optionally, a given network node is implemented by way of a programmatic hub or a programmatic router.

Additionally or alternatively, optionally, a given network node is dynamically implemented by way of a local network device, wherein the local network device is operable to connect and communicate with other local network devices using a programmatically-built star configuration.

Embodiments of the present disclosure are susceptible to being employed in a wide range of systems, for example, such as smart telephones, smart watches, Personal Computers (PC's), vehicles, audio-visual apparatus, cameras, data storage devices, surveillance systems, video conferencing systems, medical apparatus, seismic apparatus, surveying apparatus, "*black box*" flight recorders, digital musical instruments, but not limited thereto.

It will be appreciated that a given network node service can be installed at a fixed physical location or a physically moving object. Examples of such moving objects include, but are not limited to, vehicles, smart telephones carried by their users, smart watches carried by their users, and other wearable devices.

Optionally, local networks of the data communication system are mutually interconnected, via network node services executing on their network nodes, to form a mesh network (see *https://en.wikipedia.org/wiki/Mesh_networking*). One such mesh network has been shown in conjunction with FIG. 1. Optionally, the mesh network is formed for grid computing purposes (see *https://en.wikipedia.org/wiki/Grid_computing*). It will be appreciated that different clients or bots executing on the network devices of the data communication system are used only when required, and can be shared by interconnection, for example, by grid computing to combine huge amount of computational resources. Thus, the data communication system is capable of offering a much safer, ecological and more affordable alternative to conventional data centres. Moreover, a given local network of the data communication system can be implemented using mobile or wearable devices to provide desired services through various clients or bots based on a dynamically-moving grid network.

It will be appreciated that a given network device is operable to execute a given client or bot that, when executed, is configured to provide a desired service to one or more clients or bots executing on one or more other network devices. It will be appreciated that actual data communication between two given network devices is performed by clients (see *https://en.wikipedia.org/wiki/Client_(computing)*) or bots (see *https://en.wikipedia.org/wiki/Software_agent*) executing on the two given network devices. Optionally, the given client or bot is, by default, persistently connected to the network node service provided by its associated network node. There is thereby provided a solution enabling local services to be provided in a local network of network devices, thereby replacing services that are contemporarily provided by conventional data centres.

It will be appreciated that a given bot is capable of providing a protected service from a possibly non-protected network device and software executing thereon to its owner and to desired third parties.

Pursuant to embodiments of the present disclosure, services are programmatically provided by clients or bots, which are connected to network node services provided by their corresponding network nodes. This enables such services to be produced on hardware-independent cross-platform software solutions. In other words, a same functionality of a given service can be executed on network devices having different target platforms (for example, such as x86/x64/AArch64 and so forth).

In an embodiment of the present disclosure, a given network node service is operable to process only compatible connections between two given clients or bots. Optionally, in this regard, the given network node service is operable to support a wide range of mutually different applications and services locally and remotely, for example, such as:

(i) a FaaS-like cloud computing kind of execution model (see *https://en.wikipedia.org/wiki/Serverless_computing*):

(ii) a PaaS-like application platform to manage and run applications without a typical infrastructure associated for developing and executing them (see *https://en.wikipedia.org/wiki/Platform_as_a_service*); and

(iii) a SaaS-like software delivery model that is centrally hosted (see *https://en.wikipedia.org/wiki/Software_as_a_service*).

In order to support the wide range of mutually different applications and services, the clients or bots are configured to perform certain functionalities for users of the data communication system, whether or not the users have interfaces.

Optionally, in this regard, the bots are implemented as software agents that are configured to act for a user, a program or a service in relationship of an agency. Optionally, such software agents are defined as three types of bots: a protocol bot, a client bot and a server bot, which are defined for different kinds of purposes to offer effective Application Programming Interfaces (API's) for third party service providers to develop and monetize their services based upon the data communication system pursuant to embodiments of the present disclosure. It will be appreciated that these types of bots provide an interface that enables different devices and services from private or public networks to establish a protected connection with the network devices of the data communication system.

Optionally, a protocol bot is configured to translate different communication and command protocols to support services provided by the network devices of the data communication system. As an example, a given protocol bot can be configured to connect different types of media players on different target platforms to support services provided by network devices that produce audio visual content (for example, such as surveillance cameras, televisions, playback videos, and so forth). In other words, the given protocol bot can be configured to adapt information content of communicated data and its content format as per a target device. Services provided by such bots are employed to adapt the information content as per a given platform of a target device, regardless of built-in ecosystem software of the target device.

Optionally, a client bot is configured to act as an application for users to offer different types of features. As an example, a given client bot can be configured to offer a feature of video recording and playback, wherein a given user is provided a Graphical User Interface (GUI) to select videos. As another example, a given client bot can be configured to offer a feature of a nurse or a doctor, based upon Artificial Intelligence (AI) to potentially assist a user.

Optionally, a server bot is configured to act as a server to provide a desired service. As an example, a given server bot can be configured to provide an e-mail service as per personal requirements of a given user. As another example, a given server bot can be configured to host a user database for a company to support different kinds of login interfaces on existing information systems.

Moreover, it will be appreciated that a given network node service and a given client or bot can be implemented in a same physical device or separate physical devices. Examples of target software platforms that are technically suitable for implementing the given network node service and the given client or bot include, but are not limited to, Unix®, Linux®, Windows®, OS X®, Android® and iOS®. Notably, a selected ecosystem on a given target software platform defines requirements for effective implementation and requirements for programming languages and tools. Thus, the data communication system pursuant to embodiments of the present disclosure is beneficially designed to work in Gurulogic Microsystem's Starwindow® ecosystem, which provides a Starwindow® framework Application Programming Interface (API) to support a high-level development environment to allow third-party services to be used in the data communication system. Moreover, the Starwindow® ecosystem is built based upon a multi-layer architecture, wherein everything else, but services for a given target platform, are built based upon a hardware-independent software solution.

Optionally, a given network node is implemented by way of a low power Central Processing Unit (CPU), by employing IOLoop technology. This makes it possible to deliver a network node service programmatically even with the low power CPU. Using the IOLoop technology, the given network node is operable to handle all connections to the network node service in one thread. This enables significantly more cost-effective Input/Output (I/O) communications and a technically faster implementation compared to conventional known approaches that provide a dedicated thread for each connection, which are executed in one or more CPU cores. As an example, contemporary communication technology for mobile communication devices is designed to work with minimal energy consumption; therefore, using the IOLoop technology for a new purpose provides a highly cost-effective solution as described with reference to embodiments of the present disclosure.

Furthermore, optionally, a given network node service is operable to validate and authenticate local services provided by clients or bots within its own local network. Optionally, in this regard, the given network node service is operable to authenticate the local services provided by these clients or bots with accepted credentials, when the clients or bots join the local network.

Additionally or alternatively, optionally, authentication requests are validated and authenticated by a registration service. Optionally, in this regard, the data communication system is operable to register, with a registration service, services provided by clients or bots of the first and second local networks. More optionally, the registration service is used to register connection addresses for the services and their clients or bots.

Optionally, the data communication system is operable to register, with the registration service, a given service provided by a given client or bot as a private service or a public service in respect of an owner of the given client or bot. Optionally, a given local service is registered as a private service or a public service for the owner of the given client or bot, after the given local service is validated and authenticated.

It will be appreciated that such registration makes it easier for a given owner to maintain and configure all services registered for the given owner. As an example, a third party service provider may build its own services and register these services with the registration service; in such a case, the third party service provider is the owner of these services. Optionally, the registration service is operable to provide a given owner with a user interface that allows the given owner, upon successful sign-in, to view all services that are available in the given owner's local networks and to enable or disable certain services for use.

Optionally, the registration service is provided as a centralized back-end service by a "*super node*" defined in the data communication system. Optionally, the node providing the registration service is selected from amongst the first network node and the second network node. Alternatively, optionally, the super node is provided by a third party.

It should be noted that a super node works in a static manner, whereas the network nodes are dynamic.

Optionally, the data communication system is operable to function in a hardware-independent manner, wherein secure services are produced in network devices of a given owner. Optionally, in this regard, all data produced by these services is protected in respect of the given owner, namely using a key store associated with the given owner.

Optionally, in a given network device, a given service provided by a client or bot executing on the given network device is integrated with a key store associated with an owner of the client or bot, such that only services integrated with the key store are allowed to access the key store and use key materials stored or generated therein. Optionally, once integrated with the key store, the service is provided by the client or bot executing on the given network device with protection from a kernel of the given network device.

Optionally, the information content of the data is encrypted by using one or more content encryption methods. Optionally, the content encryption is achieved by using a form of symmetrical encryption block cipher algorithm (see *https://en.wikipedia.org/wiki/Block_cipher*), for example, such as Advanced Encryption Standard (AES). Alternatively, optionally, the content encryption is achieved by using a stream cipher algorithm (see *https://en.wikipedia.org/wiki/Stream_cipher*), for example, such as ChaCha algorithm. Such content encryption enables the data communication system to function reliably and handle data produced therein in a manner that it is content-protected in respect of its owner, namely an owner of the data.

It will be appreciated that, in some cases, the owner of the data can be a group of users or devices in respect of which the data shall be protected. In such a case, even if the group is typically managed by one member of the group, other group members are also able to access the data produced by the group and to produce data to the group, pursuant to predefined group rules.

Optionally, at least one of the services is shared, pursuant to authorization by the given owner, with one or more registered users remotely. It will be appreciated that the data communication system allows the given owner to produce own services using local resources (namely, network devices) and to share these services with remote users without compromising security.

Additionally, optionally, the given owner is provided with a user interface that allows the given owner to control an extent to which data produced by the at least one of the services is divulged to third parties and subsequently utilized for various purposes (for example, such as marketing, targeted advertising and so forth). As a result, for example, search engines cannot gain access to the given owner’s protected data and make use of it without permission from the given owner. This enables a safer information society to be achieved.

Furthermore, optionally, in the data communication system, a given local network is created in a dynamic manner. Optionally, in this regard, the given local network is created dynamically as a programmatic local network, wherein a network node service provided by a network node of the given local network registers all locally connected services provided by network devices (namely, clients or bots executing on the network devices) of the given local network.

Optionally, the clients or bots executing on the network devices exist in a dynamic network environment, wherein the clients or bots are operable to find a centralized network node service in a Local Area Network (LAN) without prior configuration using one or more discovery protocols. Examples of such discovery protocols include, but are not limited to, Service Location Protocol (SLP; see *https://en.wikipedia.org/wiki/Service_Location_Protocol*) and Bonjour by Apple Inc. (see *https://en.wikipedia.org/wiki/Bonjour_(software)*).

Alternatively, optionally, a given local network is created in a static manner. Optionally, in this regard, clients or bots are statically addressed to connect to a given network node service. This is particularly beneficial in situations where services are produced in a static network environment, for example, inside a same network device or in a controlled corporate network.

Moreover, pursuant to embodiments of the present disclosure, a communication protocol is defined for enabling data communication in the data communication system, and is mutually agreed between the clients or bots executing on the network devices of the data communication system. Optionally, in this regard, a given network node service is operable to create a local network having the programmatic star configuration, and is inter-connected with at least one other network node service of another local network having the programmatic star configuration. The clients or bots communicate with each other via relay through their associated network node services. As a result, the data communication system is implemented in a form of a programmatically-built star configuration. Notably, a suitable content-encryption method is beneficially integrated into the communication protocol, so as to handle the data produced within the data communication system in a secure manner.

Pursuant to embodiments of the present disclosure, a client or bot of the first local network does not connect directly with a client or bot of the second local network, but relays data through the first and second network node services. However, it will be appreciated that the client or bot of the first local network may connect directly to the second network node service to relay the data to the client or bot of the second local network, if the connection address of the second network node service is known and is available for connection. This has been illustrated in conjunction with FIGs. 4A and 4B later.

Optionally, the data communication system is operable to utilize one or more data communication networks existing in the first and second local networks for data communication. It will be appreciated that the communication protocol is defined in a manner that it is practical and efficient for all the clients or bots of the data communication system, because the communication protocol has to utilize a physical network (for example, such as a wired Ethernet, a wireless Wi-Fi network, a wireless Li-Fi, or a wireless Bluetooth® connection) to execute actual data transmission tasks based upon communication of packet data. As an example, for home, office and factory working purposes, it is efficient to use existing wired or wireless data communication networks. Such data communication networks usually employ the Internet® protocol (IP).

Additionally, optionally, in the data communication system, data communication is implemented using low-energy communication techniques, for example, such as Bluetooth Low Energy (BLE) or by utilizing certain dedicated frequency-based communication technology. This potentially enables network devices involved in such a low-energy data communication to have a long-lasting battery.

Optionally, the communication protocol is technically based, by default, on a suitable packet data communication protocol. As an example, the communication protocol can be based on the Internet protocol, for example, such as the Transmission Control Protocol/Internet Protocol (TCP/IP). It is advantageous to use a communication protocol that is widely used in private and public networks, so as to be able to handle known issues with firewalls and anti-virus services.

It will be appreciated that the data communication occurring within the data communication system is transparent to a physical network infrastructure. In other words, wired or wireless communication technologies can be used as long as they can adapt to the mutually-agreed communication protocol. As an example, TCP/IP can be used with Wi-Fi and Bluetooth®.

As mentioned above, a given network node service tries to connect directly to other network node services, using physically available communication protocols. Optionally, when using the Internet protocol (IP), direct connections are used based on IPv4 or IPv6 connection addresses.

Optionally, when a direct connection cannot be established, for example in a case where other network node services exist remotely in different Local Area Networks (LAN's), the given network node service is operable to employ hole punching technology based on Session Traversal Utilities for NAT (STUN; see *https://en.wikipedia.org/wiki/STUN*) to traverse through endpoints that are located in different network addresses. However, some corporate firewalls can prevent STUN based technologies, because User Datagram Protocol (UDP) is not allowed to be used. Optionally, in such a case, the given network node service is operable to employ a technology that is based on Traversal Using Relays around NAT (TURN; see *https://en.wikipedia.org/wiki/TURN*). This will provide connectivity between the network node services, but will route all communication through a centrally available service. As an example, the centrally available service could be implemented by way of the registration service provided by the super node of the data communication system.

Optionally, the given network node service is operable to employ Interactive Connectivity Establishment (ICE; see *https://en.wikipedia.org/wiki/Interactive_Connectivity_Establishment*) for connecting to the other network node services. It will be appreciated that the ICE technique combines both STUN and TURN techniques.

Additionally or alternatively, optionally, in order to support direct connection between the network node services, a Universal Plug and Play (UPnP; see *https://en.wikipedia.org/wiki/Universal_Plug_and_Play*) networking protocol is employed to allow automatically configuring local network devices, for example, such as routers and firewalls, to open direct communication access between the network node services. However, in such a case, it is important that authentication is properly implemented to avoid any security problems.

Pursuant to embodiments of the present disclosure, the data communication system provides a cost-efficient and fault-tolerant solution for providing services for a given owner in network devices of a local network, in comparison to conventional data communication systems where services are provided via remote data centres. In other words, computing tasks associated with the services is offloaded to the local network, thereby saving on energy utilization. Thus, the services are provided for the given owner in a comprehensive and more cost-effective manner, namely in a more local manner. As a result, the data communication system pursuant to embodiments of the present disclosure is not only capable of fulfilling today's needs, but also future's needs, where owners can produce services for their own use, using efficiently integrated local network devices in local networks. Moreover, data produced by the services is protected in respect of the given owner.

In contradistinction to conventional data communication networks that are based upon connected devices in a physically open local network, the data communication system pursuant to embodiments of the present disclosure is operable to provide services in a local network for a given owner with an added data protection functionality. Data produced by the services is protected for the given owner using a built-in security service module, and is delivered via relay through a network node service of the local network. As a result, the data is protected from traditional forms of attack arising from both inside and outside of the local network. Moreover, it is not possible for traditional forms of attack to eavesdrop on the encrypted information content of the data.

Moreover, the aforementioned data communication system enables the owner to register the services as public or private services, and to share the public services with remote users. In other words, the data communication system enables the owner to decide as to where data produced by a given service is permitted to be shared and for what purposes. As a result, search engines and other third parties cannot gain access to the owner's protected data and make use of it without permission from the owner. This enables a safer information society to be achieved.

In a second aspect, embodiments of the present disclosure provide a method of communicating data, via a data communication system comprising at least one network node and a plurality of network devices associated with the at least one network node, characterized in that the method comprises:

(i) operating the at least one network node to provide a network node service to a plurality of clients or bots executing on the plurality of network devices, wherein individual clients or bots of the plurality of clients or bots are communicably coupled around the network node service in a programmatic star configuration to create a local network;

(ii) operating a source client or bot to communicate data to one or more destination clients or bots within the local network, by relaying the data through the network node service; and

(iii) operating the source client or bot to encrypt information content of the data prior to communicating the data to the one or more destination clients or bots, wherein a key store is employed to encrypt the information content of the data, the key store being associated with an owner of the source client or bot.

Optionally, the at least one network node comprises at least a first network node and a second network node, and the plurality of network devices comprise a first set of network devices associated with the first network node and a second set of network devices associated with the second network node. Optionally, in such a case, the method comprises operating the first network node to provide a first network node service to a first set of clients or bots executing on the first set of network devices, and operating the second network node to provide a second network node service to a second set of clients or bots executing on the second set of network devices. Optionally, in this regard, individual clients or bots of the first set of clients or bots are communicably coupled around the first network node service in a programmatic star configuration to create a first local network, while individual clients or bots of the second set of clients or bots are communicably coupled around the second network node service in a programmatic star configuration to create a second local network.

Optionally, when a given source client or bot and a given destination client or bot are from within a same local network, the method comprises relaying data to be communicated through their associated network node service within the same local network.

Optionally, when a given source client or bot and a given destination client or bot are from a different local network, the method comprises relaying data to be communicated through a network node service associated with the given source client or bot and through a network node service associated with the given destination client or bot.

Optionally, the method further comprises operating the source client or bot to communicate metadata together with the data, wherein the metadata comprises encryption information indicative of a unique ID of the key store and a key index of a key material to be derived from the key store for subsequent decryption of the encrypted information content.

Optionally, the metadata further comprises group information indicative of the one or more destination clients or bots to which the data is to be communicated, wherein the source client or bot and the one or more destination clients or bots together form a group.

Optionally, the metadata is communicated in an unencrypted form. Alternatively, optionally, the metadata is communicated in an encrypted form.

Optionally, the method further comprises operating the data communication system to utilize one or more data communication networks existing in the first and second local networks for data communication.

Optionally, the method further comprises operating a given network node service to validate and authenticate local services provided by clients or bots within its own local network.

Optionally, the method further comprises operating the data communication system to register, with a registration service, services provided by clients or bots of the first and second local networks. Optionally, the method further comprises operating the data communication system to register, with the registration service, a given service provided by a given client or bot as a private service or a public service in respect of an owner of the given client or bot, as described earlier.

Optionally, the method further comprises creating a given local network in a dynamic manner, for example, as described earlier.

In a third aspect, embodiments of the present disclosure provide a computer program product comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute a method of the aforementioned second aspect.

Next, embodiments of the present disclosure will be described with reference to figures.

FIG. 1 is a schematic illustration of a data communication system **100**, in accordance with an embodiment of the present disclosure. The data communication system **100** includes a plurality of network nodes, a super node and a plurality of network devices. These network nodes are operable to provide network node services **102a**, **102b**, **102c**, while the super node is operable to provide a registration service **104**. Clients **106d** and **106h** and bots **106a**, **106b**, **106c**, **106e**, **106f**, **106g**, **106i**, **106j** and **106k** (hereinafter collectively referred to as the clients or bots **106** for the sake of convenience) are executing on the plurality of network devices.

With reference to FIG. 1, the bots **106a**, **106b** and **106c** and the client **106d** are communicably coupled around the network node service **102a** to create a local network **108a**. The bots **106e**, **106f** and **106g** are communicably coupled around the network node service **102b** to create a local network **108b**. The client **106h** and the bots **106i** and **106j** are communicably coupled around the network node service **102c** to create a local network **108c**. The bot **106k** is communicably coupled to the registration service **104** to create a local network **108d**.

With reference to FIG. 1, the network node service **102a** is connected to the network node service **102c** and the registration service **104**, while the network node service **102b** is connected to the registration service **104**, thereby forming a mesh network.

As a first example, the bot **106a** is a protocol bot that could be configured to connect a television (TV) set to services provided by network devices that provide audio visual content.

As a second example, the bot **106b** is a server bot that could be configured to store collected statistical data at a data storage associated therewith.

As a third example, the bot **106c** is a protocol bot that could be configured to connect different types of media players on different target platforms to support services provided by a surveillance camera.

As a fourth example, the bot **106e** is a server bot that could be configured to provide an e-mail service as per a user's personal requirements.

As a fifth example, the bot **106f** is a server bot that could be configured to manage a file system thereof.

As a sixth example, the bots **106g** and **106i** are protocol bots that could be configured to translate information as per a target platform of a remotely connected device.

As a seventh example, the bots **106j** and **106k** are protocol bots that could be configured to translate audio-visual information as per media players associated therewith. Such media players could be executing on a local device or a remotely connected device. With reference to FIG. 1, the bot **106k** is coupled to a media player of a remotely connected device.

FIG. 1 is merely an example, which should not unduly limit the scope of the claims herein. A person skilled in the art will recognize many variations, alternatives, and modifications of embodiments of the present disclosure.

Referring next to FIG. 2, there is depicted an example local network **200**, in accordance with an embodiment of the present disclosure.

With reference to FIG. 2, the local network **200** is physically implemented on a vehicle, namely a car. The local network **200** includes a network node service **202**, which is installed in the vehicle, and bots **204a** and **204b** associated therewith.

The bot **204a** is configured to employ cameras of the vehicle for providing various services to an owner of the vehicle. As an example, images captured from a surrounding environment can be collected and processed to provide a safer traffic control.

The bot **204b** is configured to employ an On-Board Diagnostics (OBD) system of the vehicle for providing various services to the owner of the vehicle. As an example, data collected from the OBD system can be processed for various purposes, for example, such as for providing emergency services, for theft prevention, for crash detection and/or prevention, and the like.

The network node service **202** is connected to at least one other network node service, via a wireless communication interface that is based on, for example, Wi-Fi, Bluetooth®, Li-Fi and the like. The at least one other network node service could be a part of a local network that is physically available at the owner’s home or office premises. This allows the owner of the vehicle to monitor the vehicle remotely, for example, in a case when the vehicle is an automatic driverless vehicle.

FIG. 2 is merely an example, which should not unduly limit the scope of the claims herein. A person skilled in the art will recognize many variations, alternatives, and modifications of embodiments of the present disclosure.

Referring next to FIG. 3, there is depicted another example local network **300**, in accordance with an embodiment of the present disclosure.

With reference to FIG. 3, the local network **300** is implemented by way of a network node service **302**, a client **304a** and a bot **304b** executing on network devices that are carried or worn by a human user. Notably, these network devices are not fixed or physically installed on the user, but are only carried or worn by the user. Optionally, the network node service **302** is provided by a mobile communication device of the user, for example, such as a smart telephone, a smart watch and the like.

The client **304a** is configured to provide various services to the user, for example, for playing music on an earphone of the user, displaying virtual images on a virtual reality headset of the user, and the like.

Optionally, the bot **304a** is configured to employ at least one sensor for various monitoring purposes, for example, for monitoring a heart rate of the user, a work-out performed by the user, and the like.

The network node service **302** is connected to at least one other network node service, via a wireless communication interface that is based on, for example, Wi-Fi, Bluetooth®, Li-Fi and the like. As an example, the at least one other network node service could be a part of a local network that is physically available at the user's home. As an example, this could allow a family member to monitor the health of the user remotely. As another example, this could allow remote monitoring of a nursing service provided to a senior elderly person living alone in his/her home.

FIG. 3 is merely an example, which should not unduly limit the scope of the claims herein. A person skilled in the art will recognize many variations, alternatives, and modifications of embodiments of the present disclosure. For example, the network devices could be carried or worn by a creature.

FIGs. 4A and 4B are schematic illustrations of how a client or bot **402** may communicate with a client or bot **404** from a different local network, in accordance with an embodiment of the present disclosure.

With reference to FIG. 4A, the client or bot **402** does not connect directly with the client or bot **404**, but relays data through a first network node service **406** and a second network node service **408**, which are associated with the client or bot **402** and the client or bot **404**, respectively.

With reference to FIG. 4B, the client or bot **402** connects directly to the second network node service **408** to relay the data to the client or bot **404**, if the connection address of the second network node service **408** is known and is available for connection.

FIG. 5 is a schematic illustration of a plurality of groups defined in a data communication system **500**, in accordance with an embodiment of the present disclosure.

The data communication system **500** comprises network nodes providing network node services **502** and **504**, a plurality of network devices on which clients or bots **506A**, **506B**, **506C**, **506D**, **506E**, **506F and 506G** are executing, and a plurality of network devices on which clients or bots **508A**, **508B**, **508C and 508D** are executing.

The clients or bots **506A**, **506B**, **506C**, **506D**, **506E**, **506F and 506G** are communicably coupled around the network node service **502** in a programmatic star configuration to create a first local network, while the clients or bots **508A**, **508B**, **508C and 508D** are communicably coupled around the network node service **504** in a programmatic star configuration to create a second local network.

With reference to FIG. 5, three different groups have been defined in the data communication system **500**, wherein the clients or bots **506A**, **506B**, **506D**, **506F**, **508A**, **508B** and **508D** form a first group, the clients or bots **506G** and **508C** form a second group, and the clients or bots **506C** and **506E** form a third group. Notably, a given group may include clients or bots from a same local network or from different local networks.

FIGs. 4A-B and 5 are merely examples, which should not unduly limit the scope of the claims herein.

Modifications to embodiments of the present disclosure described in the foregoing are possible without departing from the scope of the present disclosure as defined by the accompanying claims. Expressions such as "*including*", "*comprising*", "*incorporating*", "*consisting of*", "*have*", "*is*" used to describe and claim the present invention are intended to be construed in a non-exclusive manner, namely allowing for items, components or elements not explicitly described also to be present. Reference to the singular is also to be construed to relate to the plural; as an example, "*at least one of*" indicates "*one of*" in an example, and "*a plurality of*" in another example; moreover, "*one or more*" is to be construed in a likewise manner.

The phrases "*in an embodiment*", "*according to an embodiment*" and the like generally mean the particular feature, structure, or characteristic following the phrase is included in at least one embodiment of the present disclosure, and may be included in more than one embodiment of the present disclosure. Importantly, such phrases do not necessarily refer to the same embodiment.

CLAIMS

We claim:

1. A data communication system comprising at least one network node and a plurality of network devices associated with the at least one network node, characterized in that:

(i) the at least one network node is operable to provide a network node service to a plurality of clients or bots executing on the plurality of network devices, wherein individual clients or bots of the plurality of clients or bots are communicably coupled around the network node service in a programmatic star configuration to create a local network;

(ii) a source client or bot is operable to communicate data to one or more destination clients or bots within the local network, by relaying the data through the network node service; and

(iii) the source client or bot is operable to encrypt information content of the data prior to communicating the data to the one or more destination clients or bots, wherein the source client or bot is operable to employ a key store to encrypt the information content of the data, the key store being associated with an owner of the source client or bot.

2. A data communication system of claim 1, characterized in that the at least one network node comprises at least a first network node and a second network node, and wherein the plurality of network devices comprise a first set of network devices associated with the first network node, and a second set of network devices associated with the second network node, wherein:

(iv) the first network node is operable to provide a first network node service to a first set of clients or bots executing on the first set of network devices, and the second network node is operable to provide a second network node service to a second set of clients or bots executing on the second set of network devices, wherein individual clients or bots of the first set of clients or bots are communicably coupled around the first network node service in a programmatic star configuration to create a first local network, and individual clients or bots of the second set of clients or bots are communicably coupled around the second network node service in a programmatic star configuration to create a second local network;

(v) when a given source client or bot is operable to communicate data to a given destination client or bot within a same local network, the data to be communicated is relayed through their associated network node service within the same local network; and

(vi) when a given source client or bot is operable to communicate data to a given destination client or bot from a different local network, the data to be communicated is relayed through a network node service associated with the given source client or bot and through a network node service associated with the given destination client or bot.

3. A data communication system of claim 1 or 2, characterized in that the source client or bot is operable to communicate metadata together with the data, wherein the metadata comprises encryption information indicative of a unique identifier (ID) of the key store and a key index of a key material to be derived from the key store for subsequent decryption of the encrypted information content.

4. A data communication system of claim 3, characterized in that the metadata further comprises group information indicative of the one or more destination clients or bots to which the data is to be communicated, wherein the source client or bot and the one or more destination clients or bots together form a group.

5. A data communication system of claim 3 or 4, characterized in that the metadata is communicated in an unencrypted form.

6. A data communication system of claim 3 or 4, characterized in that the metadata is communicated in an encrypted form.

7. A data communication system of any one of claims 1 to 6, characterized in that the data communication system is operable to utilize one or more data communication networks existing in the first and second local networks for data communication.

8. A data communication system of any one of claims 1 to 7, characterized in that a given network node service is operable to validate and authenticate local services provided by clients or bots within its own local network.

9. A data communication system of any one of claims 1 to 8, characterized in that the data communication system is operable to register, with a registration service, services provided by the clients or bots of the first and second local networks.

10. A data communication system of claim 9, characterized in that the data communication system is operable to register, with the registration service, a given service provided by a given client or bot as a private service or a public service in respect of an owner of the given client or bot.

11. A data communication system of any one of claims 1 to 10, characterized in that a given local network is created in a dynamic manner.

12. A method of communicating data, via a data communication system comprising at least one network node and a plurality of network devices associated with the at least one network node, characterized in that the method comprises:

(i) operating the at least one network node to provide a network node service to a plurality of clients or bots executing on the plurality of network devices, wherein individual clients or bots of the plurality of clients or bots are communicably coupled around the network node service in a programmatic star configuration to create a local network;

(ii) operating a source client or bot to communicate data to one or more destination clients or bots within the local network, by relaying the data through the network node service; and

(iii) operating the source client or bot to encrypt information content of the data prior to communicating the data to the one or more destination clients or bots, wherein a key store is employed to encrypt the information content of the data, the key store being associated with an owner of the source client or bot.

13. A method of claim 12, characterized in that the at least one network node comprises at least a first network node and a second network node, and the plurality of network devices comprise a first set of network devices associated with the first network node, and a second set of network devices associated with the second network node, wherein the method comprises:

(iv) operating the first network node to provide a first network node service to a first set of clients or bots executing on the first set of network devices, and operating the second network node to provide a second network node service to a second set of clients or bots executing on the second set of network devices, wherein individual clients or bots of the first set of clients or bots are communicably coupled around the first network node service in a programmatic star configuration to create a first local network, and individual clients or bots of the second set of clients or bots are communicably coupled around the second network node service in a programmatic star configuration to create a second local network;

(v) when a given source client or bot and a given destination client or bot are from within a same local network, relaying data to be communicated through their associated network node service within the same local network; and

(vi) when a given source client or bot and a given destination client or bot are from a different local network, relaying data to be communicated through a network node service associated with the given source client or bot and through a network node service associated with the given destination client or bot.

14. A method of claim 12 or 13, characterized in that the method further comprises operating the source client or bot to communicate metadata together with the data, wherein the metadata comprises encryption information indicative of a unique identifier (ID) of the key store and a key index of a key material to be derived from the key store for subsequent decryption of the encrypted information content.

15. A method of claim 14, characterized in that the metadata further comprises group information indicative of the one or more destination clients or bots to which the data is to be communicated, wherein the source client or bot and the one or more destination clients or bots together form a group.

16. A method of claim 14 or 15, characterized in that the metadata is communicated in an unencrypted form.

17. A method of claim 14 or 15, characterized in that the metadata is communicated in an encrypted form.

18. A method of any one of claims 12 to 17, characterized in that the method further comprises operating the data communication system to utilize one or more data communication networks existing in the first and second local networks for data communication.

19. A method of any one of claims 12 to 18, characterized in that the method further comprises operating a given network node service to validate and authenticate local services provided by clients or bots within its own local network.

20. A method of any one of claims 12 to 19, characterized in that the method further comprises operating the data communication system to register, with a registration service, services provided by the clients or bots of the first and second local networks.

21. A method of claim 20, characterized in that the method further comprises operating the data communication system to register, with the registration service, a given service provided by a given client or bot as a private service or a public service in respect of an owner of the given client or bot.

22. A method of any one of claims 12 to 21, characterized in that the method further comprises creating a given local network in a dynamic manner.

23. A computer program product comprising a non-transitory computer-readable storage medium having computer-readable instructions stored thereon, the computer-readable instructions being executable by a computerized device comprising processing hardware to execute a method as claimed in any one of claims 12 to 22.

Intellectual
Property
Office

Application No:	GB1711016.4	**Examiner:**	Dr Laurence Drummond
Claims searched:	1-23	**Date of search:**	13 December 2017

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1, 12, 23	US 2016/0065548 A1 (BROUWER ET AL.) See Fig 3
X	1-23	US 2013/0195272 A1 (NAGAI ET AL.) Figs 1 and 4, and paragraphs 41 and 54
X	1-23	US 2010/0031063 A1 (FASCENDA ET AL.) See paragraph 124
X	1-23	US 2009/0122984 A1 (FASCENDA ET AL.) See Table, page 3, and paragraphs 23 and 24
X	1-23	US 7096355 B1 (MARVIT ET AL.) See column 13 lines 1-53, and Figs 1 and 2

Categories:

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.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC

H04L

The following online and other databases have been used in the preparation of this search report

EPODOC, WPI, Patent Fulltext

International Classification:

Subclass	Subgroup	Valid From
H04L	0009/08	01/01/2006
H04L	0012/44	01/01/2006